

eForensics

Magazine

COMPUTER

VOL.3NO.09

Effective PHISHING Attacks

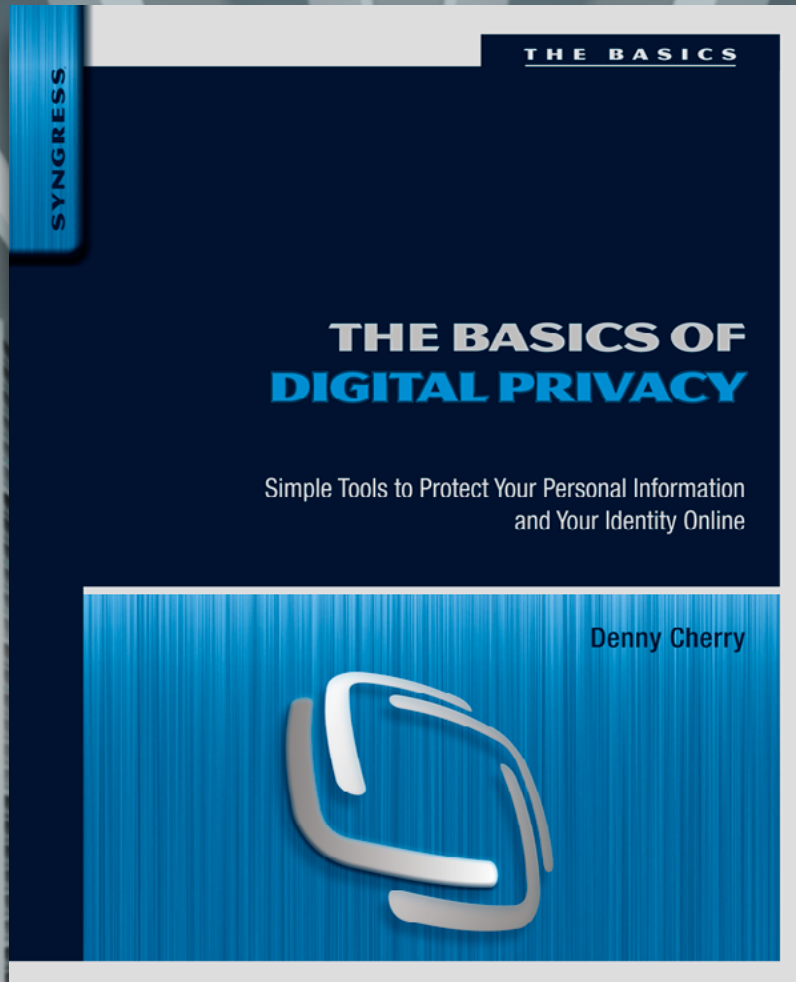
How To Steal User
Details

**SOCIAL MEDIA MINING
CAN YOU HACK A MODERN
AIRLINER?**

**BIOMETRIC FACIAL RECOGNITION
DATABASE SYSTEMS**

**DATA MASKING: A MUST KNOW FOR
COMPUTER FORENSICS**

**ANDROID APPS SANDBOX
CONTENT EXPLAINED**



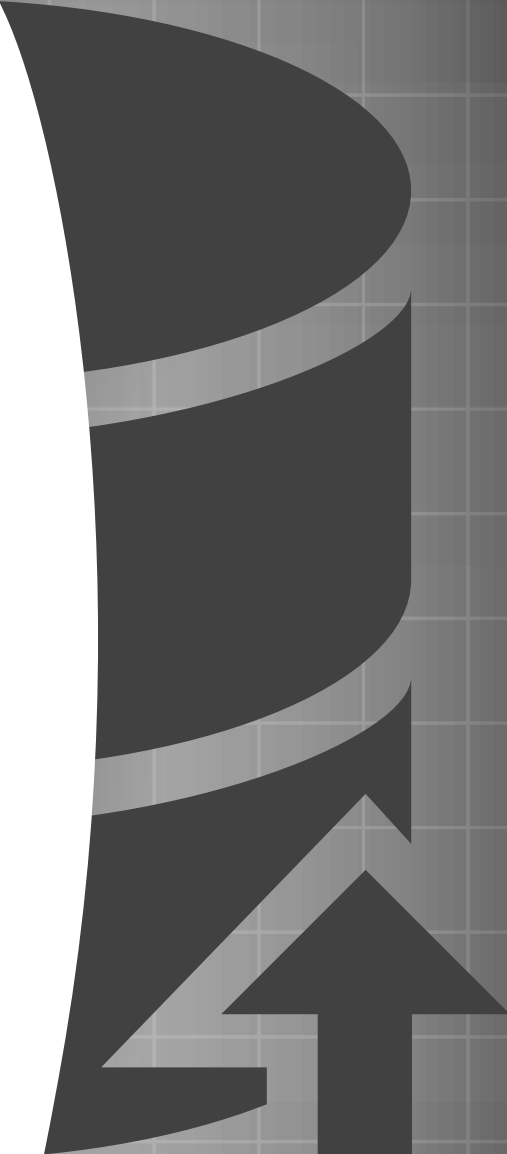
www.basicsofdigitalprivacy.com

The most straightforward and up-to-date guide to privacy for anyone who goes online for work, school, or personal use



DENNY CHERRY & ASSOCIATES CONSULTING

IS YOUR DATABASE... HEALTHY?



CRITICAL ALERT MONITORING
DISASTER RECOVERY PLANNING
SQL SERVER HEALTH CHECK
VSPHERE / HYPER-V HEALTH CHECK
STORAGE HEALTH CHECKS

AND MUCH MORE



WWW.DCAC.CO

Editor:

Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Betatesters/Proofreaders:

Olivier Caleff, Kishore P.V., JohanScholtz,
Mark Dearlove, Massa Danilo, Andrew
J. Levandoski, Robert E. Vanaman, Tom
Urquhart, M1ndl3ss, Henrik Becker,
JAMES FLEIT, Richard C Leitz Jr

Senior Consultant/Publisher:

Paweł Marciniak

CEO: Ewa Dudzic

ewa.dudzic@software.com.pl

Marketing Director: Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Art Director: Ireneusz Pogroszewski

ireneusz.pogroszewski@software.com.pl

DTP: Ireneusz Pogroszewski

Publisher: Hakin9 Media Sp. z o.o. SK

02-676 Warszawa, ul. Postępu 17D

Phone: 1 917 338 3631

www.eforensicsmag.com

DISCLAIMER!

*The techniques described in our articles
may only be used in private, local net-
works. The editors hold no responsibility
for misuse of the presented techniques or
consequent data loss.*

Dear Readers,

Proudly we would like to present you the newest issue of eForensics Magazine "Effective Phishing Attacks – How to steal user details".

This issue is not fully dedicated to one topic like we used to do in the past few months as we're during the process of changing our profile. Don't worry. Have you already heard about our online workshops? We started publishing the workshops on eForensics website for you. For everyone who missed the new please go to <https://eforensicsmag.com/workshops/> as you'll find there our first workshop dedicated to CSA START certification.

The idea is to create the monthly (or longer) workshop which will be divided into 4 stages. Each one would be dedicated to selected part of the entire task. We would like to make it as much practical as it is needed to achieve useful practical skills.

So starting from this month we will be publishing two issues + 2 online workshops per month. Workshops will be marked on our website as premium content but ALL our subscribers have automatic access to them. If you have any questions please contact me at joanna.kretowicz@eforensicsmag.com – I'm here for you.

We would like to thank you for all your feedback and support and invite you to follow us on Twitter and Facebook, where you can find the latest news about our magazine and great contests. Do you like our magazine? Like it, share it! We appreciate your every comment as for us eForensics means you and your needs, and we are here for our readers. We would be more than pleased if you could let us know what your expectations towards the magazine are? Which topics are you most interested in? I repeat it every time but it is You who shape eForensics!

Best Regards,
Joanna Kretowicz
eForensics Magazine Product Manager

SOCIAL MEDIA MINING

by Kevin Smith and Krystina Horvath

Social media allows users to share troves of data with their peers. From demographics to pictures and videos to status updates, this overabundance of social data allows users to clearly illustrate their personal lives. What is the catch? Privacy. This article will showcase the ease of social media mining and being able to hijack a social media profile along with the user's other online accounts. In addition, this article will highlight mitigation techniques that can be taken by social media websites to lessen the frequency of hijacked profiles and nefarious social media data mining.

08

CAN YOU HACK A MODERN AIRLINER? WHAT MAY HAVE HAPPENED TO MH370?

by Colin Renouf

With all of the media interest in the mystery of the behavior of Malaysia Airlines file MH370, a Boeing 777-200ER that took off from Kuala Lumpur, turned away from its original heading and headed off into the Indian Ocean for several hours before crashing, the world at large is interested to know if they are at risk from the same fate when flying on a Boeing 777, which is one of the mainstays of the modern airline fleet. One of the questions that has been asked is of interest to the security expert: Is it possible to hijack and aircraft from the ground using the techniques of the modern black hat hacker?

14

21ST. CENTURY IT SYSTEM MANAGERS – THE AVIATORS

by Robert Vanaman

This paper's scope will be limited to three specific areas of concentration relating to the plane, pilot, and a company. First the airframe, only systems found in light single and twin engine aircraft, both propeller and turbine (Read: jet) powered will be examined. Second, these aircraft and systems are flown by civilian pilots in a general aviation (GA) environment. Third, the avionic systems examined will be those manufactured by Garmin Ltd. This realm was chosen due to the author's personal experience in these areas.

22

EFFECTIVE W PHISHING ATTACKS STEALING USER DETAILS

by Colin Renouf

Phishing is a growing means of attack to which so many people succumb. This article explains the most effective methods of convincing an unsuspecting user that an email has come from someone who can be trusted; and the methods of capturing information from them – some of which don't necessarily involve the use of computers. Phishing is essentially a social attack. By learning the techniques used for surreptitiously stealing information from an unsuspecting user a security professional can use the techniques in penetration tests, but can also prepare users to defend against them.

34

COULD REAL-TIME EFORENSICS BE THE ANSWER TO CYBERSECURITY AND ANALYTICS?

by Larry Karisny

Most of us are familiar with forensics in the evaluation of a crime scene. There was a criminal incident that occurred and a team of forensic analysts come in to gather information that might lead to solving the crime. eForensics today is no different. A hack has occurred and a team of specialist sift through mounds of data, software, hardware, processes and people to determine how the systems processes have been breached. The commonality of both these forensic approaches is that they are both reviewing historical information and using tools and techniques that can analyze these historical incidents. These historical forensic approaches can in time possibly solve the crime or cyber breach but neither of these approaches can stop the crime or the hacker in advance.

40

CLOUD COMPUTING RISK ASSESSMENT

by Bryan Soliman

Cloud Computing is a phrase used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, Cloud Computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time.

44

58

DATA MASKING: A MUST KNOW FOR COMPUTER FORENSICS*by Cordny Nederkoorn*

Data masking is a process that is used to protect the information that is stored in data management systems. It is used to prevent data corruption and to give only users with the right authorization access to the data.

For computer forensics this is interesting, because it shows how a company can protect itself against external (and internal) data breaches. This article shows what data masking is by showing an example using software from Camouflage, a leading provider of enterprise-class data masking solutions for securing sensitive data.

64

BIOMETRIC FACIAL RECOGNITION DATABASE SYSTEMS*by Robert E. Vanaman*

A biometric system is effectively a pattern recognition system that operates by acquiring biometric data from an individual, and extracts a feature set from the acquired data for comparison purposes. The information needed for recognition is acquired by a sensor, and is converted into a digital format. This digitized representation of a feature, in this case a face, is then compared to a "biometric template" or a "gallery" stored in a database. This paper will delve into the Facial Recognition Database Systems (FRDBS) currently in place and cover predictions for future use, exploring the processes and methodology employed therein, specifically addressing FRDBS methodologies and techniques employed in capturing, storing, and comparing scanned images.

78


LESSON 02 – ANDROID APPS SANDBOX CONTENT EXPLAINED*by Lorenzo Nicolodi*

When a forensics expert needs to analyse an Android device, both commercial and free tools are available to recover data and to dump the content and some of them are also able to analyse the extracted files, generating report and letting the forensics examiner to find what he or she is looking for. Problem arises when a non-standard apps have to be analysed. Understanding how an Android application lives inside the operating system and what its home contains would probably help.

84

SSH COMMUNICATIONS SECURITY "PRIVILEGED ACCESS MANAGEMENT" IT SECURITY'S DIRTY LITTLE SECRET: ENCRYPTION MANAGEMENT FLAWS PUTTING ORGANIZATIONS AT RISK*by Jason Thompson, Director of Global Marketing, SSH Communications Security*

Even though the average person uses encryption every day to keep personal data safe and secure, they likely don't know much about how it works. As with all technologies, as they "age," their cost decreases. Often so much so that today encryption technology is perceived as a commodity and widely deployed as open source software. For example, the Heartbleed vulnerability was discovered in OpenSSL, an open source encryption software. There is a large debate as to whether commercial or open source security software is better for enterprises. Regardless of whether an organization is running commercial or open source, the main priority should be proper management.



Bridging the gap between business & technology

Ranked among the largest
minority-owned IT services firms
in the U.S. having Global Delivery
capabilities

Operations in the U.S., U.K., India,
Singapore and Philippines with
over 9000 professionals

Leading mid-tier IT vendor with
end-to-end IT capabilities
spanning Technology Consulting,
Application Outsourcing and
Infrastructure Services

Recognized on numerous
occasions by GS 100, The
International Association for
Outsourcing Professionals,
FinTech 100 & InformationWeek

Collabera
www.collabera.com

SOCIAL MEDIA MINING

by Kevin Smith and Krystina Horvath

Social media allows users to share troves of data with their peers. From demographics to pictures and videos to status updates, this overabundance of social data allows users to clearly illustrate their personal lives. What is the catch? Privacy.

What you will learn:

- Social media mining techniques
- Preventative measures that can be taken by social media websites to protect their clientele

What you should know:

- General understanding of the Internet
- General understanding of social media platforms such as Facebook and LinkedIn

These social media websites provide a vast array of data useful to businesses and consumers that help projected and current revenues and profits. At the same token, this data can be pilfered by hackers and used in nefarious ways. Social media mining can be beneficial but it can also reap harrowing effects upon individuals.

This article will showcase the ease of social media mining and being able to hijack a social media profile along with the user's other online accounts. In addition, this article will highlight mitigation techniques that can be taken by social media websites to lessen the frequency of hijacked profiles and nefarious social media data mining.

SOCIAL MEDIA AS DATA SOURCES

As examiners and investigators it is very difficult to excuse open source research options as viable sources of intelligence and evidence gathering when conducting our examinations. Particularly when we begin talking about social media, it would be very difficult to pin point all the useful resources and information that can be obtained by simply exploiting the data individuals willingly deposit into online social arenas such as *Facebook.com*, *Twitter.com*, *LinkedIn.com* and more.

During the course of our examinations we might rely heavily on commercial tools to parse out social media artifacts of evidentiary value, or to conduct Facebook visualization in order to identify criminal networks. Inevitably, with the ease of sharing massive amounts of data in today's digital device dependant society, the information shared can be used to establish timelines, locations, identify witnesses, and in many cases provide photo evidence of a crime taking place.

With that stated, it would be naïve for us as professionals to discard the fact that while we are making the most of the considerable amounts of personal information individuals are so eager to expose to the world through frivolous social media postings to solve crimes, criminals are using that same information to commit them. From the comfort and security from their own home, criminals are scouring personal online profiles and utilizing the information

contained within, to access the answers to your most personal questions in order to reset account passwords and not only gain access to your personal accounts, but to block you from accessing them as well.

SOCIAL MEDIA PROFILE INFORMATION

Naturally, a good portion of personal information is going to exist in a user's own profile. Questions such as where you were born, your favorite artist, favorite movie, and important dates such as anniversaries are all questions we are willing to answer when we are exposing ourselves to the digital world. Unfortunately, these are all very common security questions as well. We might share our achievements from our favorite high school sports, talk about the vacation we took last year, or share where we were the moment we met and fell in love with our spouse. Again, all of which provide useful information for resetting an account password.

How exactly can a malicious hacker obtain this information? This "hacking" technique is not technically driven. Instead, it uses investigative techniques along with psychology. We refer to this as social engineering. Social engineering uses persuasive methods to exploit vulnerabilities. These vulnerabilities and weaknesses are usually users. For this example, we will assume that the hacker wants to gain access into a user's LinkedIn account. How would he go about this without a technical technique? If the user has a Facebook and Instagram account, it can be easy. If the hacker is confirmed as a friend to the potential victim, he/she gains access to a treasure trove of personal information. Facebook allows users to post statuses about anything of importance or interest to them. This could include a life event that indicates an anniversary date or a post suggesting that the potential victim just bought a car in their favorite shade of blue. The same information can be shared through the user's Instagram account through pictures and their captions. Both of these pieces of information could be used as password reset question answers (when is your anniversary and what is your favorite color?). A hacker can then use this information to reset a password on the user's LinkedIn account and gain access into it.

MINING PHOTO ALBUMS

So, who was the maid of honor at your wedding? Aside from the veritable cornucopia of information one could learn from perusing through the history of an online profile, images and videos pose a great risk, even to individuals who might be more security conscious. An individual can take steps



cutting through complexity

Are you prepared?

kpmg.ca/forensic

INTRUSION

ATTACK • THREAT • CYBER SECURITY

TECHNOLOGY • CORPORATE

ELECTRONIC • INFORMATION • COMPLEXITY

DATA ANALYTICS

RISK • INFORMATION • TECHNOLOGY

DATA RECOVERY

COMPLEXITY • ELECTRONIC • INFORMATION

FORENSICS

DATABASE • ELECTRONIC • CONTROL

INTELLIGENCE

INFORMATION • RISK • TECHNOLOGY

eDISCOVERY

COMPLEXITY • THREAT • INTELLIGENCE

INVESTIGATIONS

TECHNOLOGY

COMPLEXITY • THREAT • DATABASE

INTELLIGENCE • PROTECTION

CORPORATE

to ensure they are censoring the information they post about themselves and can implement security measures to regulate how much of that data is typically shared with the public. The danger may not stem from a users own profile, instead information shared from another users postings might provide information that can be used to answer security questions.

For example, how many times have we seen large group photos taken at gatherings such as weddings, where the user who initially posted the image has “tagged” everyone in the photo? Using Facebook, Instagram or another social media website specializing in photo sharing, photo albums can be mined for personal information. Now if we imagine for a second that our picture on Facebook shows our victim standing in the middle of the photo, to one side would be her groom, and there is a good chance that standing at her other shoulder is not only her maid of honor, but the answer to one of the most common security questions we see during the account verification when resetting our online passwords.

What are some other questions one might be able to answer after briefly looking through your online photos, or photos others have tagged you in? Pictures posted of family functions and holidays with grandparents, aunts, and uncles can provide your mother’s maiden name, the caption under the video you posted of your favorite pet catching a Frisbee, or the “Throwback Thursday” photo you just posted of you with your first car, all provide answers to some of the most common security questions needed to reset a password and gain access to an online account.

PROFESSIONAL NETWORKING WEBSITES

Professional networking websites such as LinkedIn are not impervious to the scouring eyes of a criminal and can also provide critical information that can be used to reset passwords. In this case, we can use social engineering again to gather information about our victim. How hard would it be to find the High School Mascot of an unsuspecting user? We can look at just about any LinkinLn.com profile and see where each user attended High School, and a simple Google search later obtain the information needed for yet another common security question.

In addition, each account that is accessed by criminals using personal information to gain access and control of an account exposes further information that can be more private and nature, never intended for public viewing and increases the risk of losing access to other accounts. For example, if a criminal gains control of a Facebook.com account, they can easily view the account settings and identify a user’s email address, which can subsequently lead to gaining control of the email address through social engineering techniques, as well. After the hacker gains access to a user’s email account, any other linked accounts such as bank accounts, Paypal.com accounts, or other financially sensitive areas of our digital footprints can be detected and hacked.

ADDITIONAL CONSIDERATIONS

While the focus of this article is to highlight the ease of utilizing your profile information to reset your account passwords and gain access to your accounts, it would be remiss to not mention additional dangers posed by casual posting to social media websites that can easily be exploited by criminals. For example, utilizing GPS enabled applications to “check in” to a location such as a restaurant or posting pictures while on vacation could subject a victim’s home to burglary. EXIF data extracted from photos posted online can provide important location information pertaining to valuables, property and even other individuals, compromising their security. Most importantly, all the information posted in your online profiles provides insight and information that can be used to tailor phishing attempts, or worse, steal your identity.

SOCIAL MEDIA MINING MITIGATION AND PREVENTION

As previously discussed, data mining and scraping uses several techniques to pilfer personal information and use it to gain access to social media accounts. Who does social media mining and scraping affect? Who can mitigate and prevent it? What are the mitigation and prevention tactics that those effected can implement?

SOCIAL MEDIA COMPANIES

Vulnerabilities within these social media websites should be corrected by the company’s information technology and security staff. What techniques should these social media companies use to avoid social media scraping and mining of their clients? Prevention methods, as well as incident response measures should be implemented to protect their clientele.

Prevention tactics by these social media companies like Facebook and LinkedIn should be administered as part of the IT department's mission and responsibilities. Security practices that will help clientele avoid identity and data theft and possibly fraud should be the company's utmost concern.

In order to protect the client, who may be unaware of the data mining and identity theft issues associated with social media, the company should be enforcing the creation of strong passwords. By requiring complicated passwords that do not correlate to any of the user's personal information (the social media website should stress this recommendation), it would be more difficult for a hacker to figure out the password to the user's account.

The company should also offer two factor authentication sign in options. A two factor authentication provides a double layer of protection for the client when signing into the social media website. Facebook has allowed this option to its clients already. Two factor authentications require a user to input information in the form of two factors, normally a knowledge factor and a possession factor. A user will sign into the website with a registered username and password. This is their knowledge factor, or a piece of information that only the user should know. In addition, the social media website will verify the username and password with a possession factor using a mobile device that belongs to the user (the user possesses the mobile device). An SMS text message will be sent to the user's mobile device and the user will type the code in order to complete the log in process.

How does this two factor authentication secure a user's profile? Rather than simply requiring a user to set up a complex password with their account, this two step authentication process forces the user to have a possession (in this case, a mobile phone) in their hand and ready to supply information to the social media site for login. By requiring both a knowledge and possession factor, it makes hacking or simply figuring out a password to hack an account much more difficult. Two factors, rather than just one, provide a double layer of security for both the user and the social media company.

The previous recommendations discussed are specifically preventative measures to protect the user from a hacked profile and possible identity or financial theft. But what should a social media company do if a breach has already occurred? The best course of action would be to have an incident response procedure in place before the breach and alter it as needed to the specific type of incident.

As a general incident response plan, a social media company should keep the best security interest of their clientele as top priority. As a precautionary measure, the IT security departments of these companies should constantly be spot checking their clients' profiles and for any intrusions within their own networks. A network intrusion detection system (NIDS) along with an incident response consultant or full time employee with a vast background in network intrusion would be a wise investment for a social media company. In addition, these social media companies should always have legal counsel, external security and forensic consultants ready for any type of incident response case.

A social media company's incident response plan should include the following outline of time-sensitive measures. In each specific case, the company needs to evaluate the size and scale of the intrusion or breach of data and apply different means, accordingly.

- Response teams should be engaged first
 - Response teams need to identify the size and scale of the intrusion or breach
- The response teams and IT department should contain and eliminate the intrusion or breach as quickly as possible
- Senior management should be made aware and engaged within the incident response process
- Legal counsel teams/corporate communications should provide notification to regulators and/or mass notification, if needed

During each of these steps within the incident response plan, the company should be documenting every piece of information pertaining to the case. This will indicate that the social media company exercises preparedness and care for the stakeholders and clientele within the organization.

SOCIAL MEDIA CLIENTELE

Who is the other victim within an incident response case or data breach? The company's clientele is greatly affected by data breaches. Consider a mass hacking of profiles within a social media site. The users of that website will be most vulnerable to having their information pilfered and used nefariously.

What can users do to protect themselves from identity and possible financial theft? As mentioned as a recommendation for social media companies to require complex passwords that are unrelated to any of the user's personal information, it would be in the user's best interest to create a password that has no meaning. Instead, the password is a random selection of alphanumeric characters and symbols. This will deter any hackers from guessing a password related to the user's information quickly. What else can be done? The user can change their password routinely. This will help keep account access limited to just the user.

In addition, two factor authentication should definitely be utilized to add another layer of security to the user's profile. Both a knowledge factor and a possession factor will help secure the user's data.

Once the user's profile is created, the user should also be very stringent about information they provide. Birth date along with a full name and location can make it very easy for a hacker to guess any other passwords that might be related to the user's personal information. In addition to this, a user should be aware of privacy settings within the social media site. It is advised that a user shares information only with people that they know and trust on these social media platforms.

By following these recommendations, users can dramatically decrease their risk of becoming an identity or financial theft victim.

SUMMARY

Through demonstration, we have discussed just how easy it is to skim personal information from various social media sites and hack into other social media accounts for that individual.

Although identity and financial theft through social media websites cannot be prevented, there are several measures that both social media companies and users of these platforms can take that will reduce the frequency of social media mining.

ABOUT THE AUTHORS

Kevin Smith



Kevin Smith is a Senior Consultant for Booz Allen Hamilton and an expert witness. Previously, a digital forensic examiner with the United States Army Criminal Investigation Command he has conducted hundreds of forensic examinations of various media formats in support of felony investigations and supported agencies such as the Federal Bureau of Investigation and the United States Secret Service. His education includes multiple courses from the Defense Cyber Investigations Training Academy, the Federal Law Enforcement Training Center, and he is currently pursuing a Master's Degree in Digital Forensics and Cyber Investigations from the University of Maryland University College.

Krystina Horvath, MS, MBA



Krystina Horvath, MS, MBA is currently in the midst of a career change from finance to computer forensics. Krystina has completed Utica College's Master of Science in Cybersecurity program with a 3.97 GPA. Krystina recently became CompTIA Security+ certified. She is seeking full time employment in the digital forensics field, particularly a telecommute position. Please see her LinkedIn profile – www.linkedin.com/pub/krystina-horvath-ms-mba/14/809/309/.



The **only** existing System of its kind,
IncMan Suite has already been adopted
by a host of corporate clients worldwide

The Ultimate Forensic Case Management Software

Fully automated Encase Integration

Evidence tracking and Chain of Custody

Supports over 50 Forensic Software and third parties

Training and Certification available

Special discount for LEO, GOV and EDU customers



SPECIAL PROMO 15% OFF
single user perpetual license

<http://www.dimmodule.com>

promo code **E-FORNCS13**

DF Labs DIM is a forensic case management software that coherently manages cases, data input and modifications carried out by the different operators during Digital Evidence Tracking and Forensics Investigations.

It is part of the IncMan Suite, thus it is able to support the entire Computer Forensics and Incident Response workflow and compliant with the ISO 27037 Standard.

www.digitalinvestigationmanager.com

CAN YOU HACK A MODERN AIRLINER?

WHAT MAY HAVE HAPPENED TO MH370?

by Colin Renouf

With all of the media interest in the mystery of the behavior of Malaysia Airlines file MH370, a Boeing 777-200ER that took off from Kuala Lumpur, turned away from its original heading and headed off into the Indian Ocean for several hours before crashing, the world at large is interested to know if they are at risk from the same fate when flying on a Boeing 777, which is one of the mainstays of the modern airline fleet. One of the questions that has been asked is of interest to the security expert: Is it possible to hijack and aircraft from the ground using the techniques of the modern black hat hacker?

In this article we are going to look at answering the question that has been at the forefront of the news since the middle of March 2004: Is it possible to hack a modern airliner such as Boeing 777 to make it behave like the ill-fated Malaysian Airways MH370? If so, what would I need to do it, why would I do it, and can be done to mitigate against it. However, before we can answer these questions we have to understand how the systems on a modern aircraft work, and the similarities and differences from the other systems we are used to.

The simple answer as to whether a modern aircraft can be hacked is not only a simple “yes, it can be done with some physical access to the aircraft on the ground”, and there are possibly other techniques; but also it is something that is of concern to aircraft systems manufacturers that the step-by-step guides in the text books tell you to guard against it!

We will finish by asking what needs to change on the modern aircraft to add protection, and what can the aircraft industry learn from the wider IT industry.

SCENARIO – THE POLITICAL BACKDROP

First, a little explanation as to how this article came about. My first time at university was to get an Aeronautical engineering degree, but with the state of the industry and the more ready availability of opportunities in IT, I moved on

to a degree in IT and Social Sciences, and then on to greater things. For the last few years I have been writing on the subjects of IT architecture, infrastructure and security.

When the news as to the lack of information as to what happened to the missing Malaysian Boeing 777 airliner broke I kept being asked “If it wasn’t the pilots who took the aircraft off course, is there some way somebody could have hacked the aircraft to make it do what it did? With your background surely you must have some idea?” With all of the mystery I went back to my old text books and purchased the latest editions. This story is something the whole modern world is worried about and wants answers.

I’m not saying that what I am about to describe is what happened, but that it is a scenario that COULD happen.

Lets think of a typical James Bond movie for a moment. The bad guys are always effectively terrorists, but they always target the world as a whole rather than individual governments because they want power or money rather than to fight for a political cause, and in these films there is no reason to publicly clam responsibility for their acts of terror as the people they are scaring is the establishment as a whole. Even when the governments know who is responsible they work together to fight the evil doer and don’t make announcements to the general public as to perpetrator and his or her demands. So, assuming the author of the James Bond stories, Ian Fleming, understood global politics; and I think he did; then if an evil doer wanted to hold the world to ransom for power or money irrespective of political leanings it is unlikely we would hear about it.

MALAYSIAN AIRLINES MH370 – THE EVENTS

This aircraft, a Boeing 777 200 series model 200ER aircraft is a fairly modern twin jet widebody airliner and the backbone of the medium to long haul airline fleet; seating between 314 to 451 passengers over trip distances of a maximum range between around 9700km to 17300km (5200 to 9400 nautical miles). It was the first Boeing fly-by-wire airliner and as such all control requests from the pilot are mediated by the computer systems and turned into commands of the hydraulics. The key piece of information here is that normal operation requires direct intervention of computer systems to translate flight control requests and the pilot does not access the individual aileron and other control surfaces directly.

On the day of its disappearance, Saturday March 8th 2014, Malaysian Airlines MH370 set off from Kuala Lumpur International airport in Malaysia at 12:40AM local time, bound for Beijing in China with 239 people on board consisting of 227 passengers and 12 crew. Its initial hour of flight time was uneventful, but at the handover between Malaysian air traffic control and Ho Chi Minh air traffic control in Vietnam contact was lost. The low level sequence of events is not entirely clear, but voice contact with Vietnamese air traffic controllers was not made, the normal secondary surveillance radar transponder that identifies the aircraft appears to have been switched off, followed by the ACARS systems health information communications with the manufacturers.

The aircraft made a rapid ascent to 45,000 feet or 13,700 metres where it spent 23 minutes – above its normal operational ceiling – followed by a rapid descent to 5,000 feet or 1500 metres followed by a return to its cruising altitude of 30,000 feet or 9,100 metres; with a southwest bound turn back towards the commercial waypoint “Vampi” a along the N571 air corridor, followed by waypoint “Igrex” and the P628 air corridor from there it headed out over the southern Indian Ocean where it flew as a “ghost” plane for several hours, pinging the Inmarsat satellites every hour, before eventually crashing into the ocean.

With all this change of direction, surely the aircraft was under human control, but if an emergency caused a turn back why was there no communication and if the plane was hijacked why was there no claim of responsibility or demand?

THE MODERN AIRLINER

In the modern world, networking and interoperability are key to progress; with the Lego-like components that abstract their complexity and hide it behind well defined interfaces allowing ever more powerful and complex machines to be built based on the principles of previous generations. Individual components can be exchanged and upgraded without having to change every other system. Whilst this is true of the home, computers systems, cars and society as a whole; it is visibly the case with the external structure of an aircraft. Aircraft have improved in streamlining, performance, economics, range and the number of passengers that can be carried in comfort over great distances. The same is true of the aircraft systems.

Whilst financial and other systems are dependent on networks, with standards like TCP/IP, 1000Base-TX Ethernet, etc; from the ISO, W3, etc the same is true on an aircraft, but with different standards allowing the independence and interoperability between systems. The body behind those standards is Aeronautical Radio, Incorporated; a corporation owned by a number of airlines, aircraft manufacturers, and avionics suppliers with the simple goal of maintaining interoperability. The key core standard for aircraft avionic systems from which others were derived or developed from is ARINC-429; with new standards proposed and a number of peripheral standards. In this standard the cabling specification for a serial, shielded twisted pair interface with the electrical signals fully defined using bipolar return to zero (BRTZ) electrical signaling evolved from the earlier ARINC-575 Digital Air Data Systems (DADS) specification; which with ARINC-429 allows configuration of a transmitter and up to twenty receivers in a star topology, bus-drop topology or with multiple buses. Transmission speeds range from a lowly 12.5kbps to 100kbps.

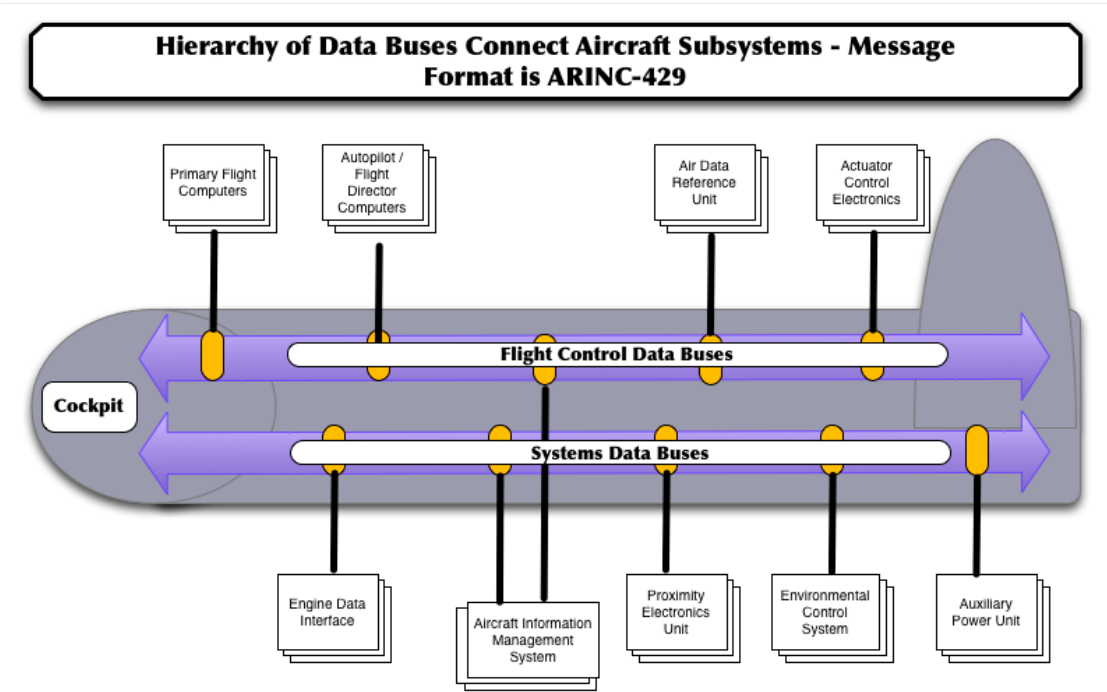


Figure 1. A Hierarchy of Data Buses connect Subsystems on a Modern Airliner – ARINC429 messages use this transport

The simplex communications in ARINC-429 consist of packets of 32-bit words with 8-bit data labels describing the 24-bit data (See Figure 1). For bi-directional communications two channels or buses are used. Data can be transmitted in binary, binary coded decimal (BCD), discrete data, two-way maintenance data, or a specialist bit-orientated file transfer protocol. Individual subsystems have no address but are identified by an Equipment ID.

32	31	30	29					11	10	9	8		1
P	SSM		MSB	DATA				LSB	SDI			LABEL	

Figure 2. ARINC-429 Standard Data Format

In an ARINC packet the label 8-bit field identifies the type of information being transmitted, e.g. an air-speed, altitude, etc. The P field is a parity field, with ODD parity used to inform the systems of a single bit error possibly occurring. The DATA field contains the numeric value being sent in either Binary Coded Decimal (BCD) format or twos compliment (BNR) format, and the SSM field assists in its interpretation by containing values for North, East, South, West, Plus, Minus, Above, Below, To, From, etc. The SDI field is the Source/Destination Identifier and allows members on the bus to be targeted, but is an optional field.

So, if the SSM bit fields are set to 0 with BCD data, or just bit 31 is set to 0 with BNR data in normal operation the value means Plus, North, East, Right, Above or To; and if set to 1s with BCD data or just bit 31 with BNR data in normal operation it means Minus, South, West, Left, Below or From. The value 01 means no computed data and 10 means a functional test value, and some operations use these fields to

indicate a failure warning. This representation system gives immense flexibility and is the foundation that allows interoperation of aircraft systems and the ability for a subsystem to be upgraded independently of others; and as we know such information hiding also reduces attack surfaces and protects against software debt – unless we use the representation as a weapon itself.

Equipment IDs, the first three bits of the DATA field (11-13), identify what is sending the information, e.g. Hex 001 for the Flight Control Computer (FCC)/Flight Director (FD) [autopilot], Hex 002 for the Flight Management Computer (FMC), Hex 007 for the radio altimeter, Hex A1 for the Flight Control Computer Controller, etc. These are always documented in Hex values.

Labels effectively identify the data type, not in IT terms but in aeronautical terms (e.g. barometric altitude, airspeed, etc), and are standardized amongst manufacturers and models so all air data computers will, for example, use label 203 to send barometric altitude information from that type of system; although there may be some minor variations in the data provided. Different types of system may reuse Labels for other things, but the combination of subsystem usage pattern, label, and equipment ID make clear what the data is, where it is from, and its expected use. So, the Flight Management Computer has an Equipment ID of Hex 002, and if it sends a value of 102 with BNR data the value represents a selected altitude, and other systems such as FCC Controller would be expected to use the label in the same way. Similarly, A Flight Controller (Hex 001) Roll request uses label 140 and a Pitch request uses Label 141; but these Labels mean Actual Fuel Quantity Display and Select Fuel Quantity Display respectively when the Equipment ID is Hex 05A for one of the pilot display units.

This is best explained with an example. Consider a packet with the LABEL of 103 telling us the value is a selected airspeed, and the DATA value of 268 knots; and the Equipment ID set to 001 in the DATA field to say the value came from the Flight Control Computer (FCC).

32	31	30	29			11	10	9	8		1
P	SSM		MSB	DATA		LSB	SDI			LABEL	
	11		268 (bits for 256, 8, and 4 set) – Equipment ID set to Hex 001 towards the LSB							103	

Figure 3. An ARINC-429 Packet informing Receivers of an airspeed of 268 knots from the FCC

Similarly, the Flight Management Computer (FMC) can instruct other systems that need to act on the information (such as the Autopilot or Flight Control Computer (FCC)/Auto Flight Control System (AFCS) to ascend to 13,106 meters or 43,000feet with the SSM field identifying the Data Value as Positive or Above and the Label field identifying it as a Selected Altitude. The commands sent to the autopilot by Malaysia Airlines MH-370 would include such an ARINC-429 command (the 777-200ER uses the uprated ARINC-629 standard) or some slight variation.

32	31	30	29			11	10	9	8		1
P	SSM		MSB	DATA		LSB	SDI			LABEL	
	00		13106 metres (43,000 feet) (bits 13, 12, 10, 9, 6, 5, and 2 set) – Equipment ID set to Hex 002							102	

Figure 4. An ARINC-429 Packet from the Flight Management Computer informing other systems to ascend to 13106m (43,000ft)

In the modern aircraft fibre optics are becoming prevalent; offering the benefits of improved performance and protection against Electromagnetic Interference (EMI). Even in this world, at the core are standard CPUs, operating system derivatives, etc. However, the standards on which these new systems are built are generally developed from the core of the ARINC-429 system.

Modern airliners have increased in the amount of automation to reduce the workloads on the crew, so Flight Management Systems (FMS) include software to interface to other systems on an aircraft and can automate an entire journey; with a database of waypoints and settings to use to provide instructions to the autopilot to make turns at appropriate points, update the engine controls to change speed and altitude, etc.

With the addition of Electronic Flight Bags (EFBs), the maps and planning for a flight that a pilot and co-pilot make that takes account of weather, time zones, air traffic control, etc allow the setting and control of the Flight Management Systems to also be automated. Integration of these uses the facilities provided by ARINC-429 and its successors.

With these types of systems regular updates are necessary with Field Loadable Software (FLS) and Database Field Loadable Data (DFLD) updates via CD-ROM or even with patches downloadable over the Internet. Software has to be heavily tested as it now forms part of a critical system for which failure may result in the loss of life. So processes for making updates include multiple copies (old and new) of software and data, and checks for consistency when downloaded. Processes for updating the software may include specific interfaces to specialist components, including special cables, power settings, etc (See Section 13.3.3 of Reference 1). It is in this area that the risk of hacking comes into play.

WHAT IS AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM (ACARS)?

This has been mentioned a lot with the monitoring of flight MH370.

THE BOEING 777-200ER AND MALAYSIA AIRLINES MH370

The Boeing 777 is a fly-by-wire system, meaning that data and communications between the pilot controls and the aircraft surfaces such as ailerons, flaps, etc has replaced hydraulics; which has greatly reduced the weight of a modern aircraft and allowed it to grow in size.

Originally, fibre optic FDDI (Fibre Distributed Data Interface) cabling as part of ARINC-636 was used in the Boeing 777 to reduce weight, with speeds of up to 100Mbps; with data in frames along with the Copper Distributed Data Interface (CDDI) and Shielded Twisted Pair Data Interface (STPDI) related standards; but this has increased cost and complexity so more modern derivatives are moving to plain copper Ethernet cabling and related standards.

The Boeing 777 introduced the ARINC-629 development of the ARINC-429 standard, with speeds of 2Mbps between components, up to 120 devices on a single bus, and bidirectional communications. The 777 has a modern data network for its avionics to connect the complex subsystems using a combination of fiber optic standards (1000BaseSX) and copper (1000BaseTX), but this is just a shadow of the Avionics Full Duplex (AFDX) data network on the Airbus A380 and Boeing 787 Dreamliner; but even on the 777 these days standard Ethernet is being seen more and more as new subsystems and digital computers are added (e.g. the Electronic Flight Bag for the 777-200ER variant that provides the pilot information and allows the complete flight to be preprogrammed with waypoints for routes that take account of weather, etc).

The modern computers and digital systems in the Boeing 777 are based on the AMD29050 32-bit RISC processor and its later Honeywell HI-29KII Application Specific Integrated Circuit (ASIC) derivative found in the Versatile Integrated Avionics (VIA) package. The CPUs are set up in a system called Voting where instructions are run in "lockstep" on two CPUs and compared, and if they don't match an error has occurred and is flagged. These VIA packages form modules that plug into a backplane on which other aircraft avionics systems are built.

Programming an AMD29050 system is like any other, with facilities to program in an assembler language, although complex compilers are usually used to make use of intelligent scheduling algorithms to keep each processor pipeline fed with instructions.

Thus, like all modern aircraft the heavily computerized Boeing 777 and its modern network of complex subsystems that cooperate using a derivative of the ARINC-429 standard does have the computing systems that represent a ripe target for attack.

ASSUMPTIONS

To attack aircraft system components using the protocols and standards outlined above:

Physical access is required to the aircraft to apply hardware to change the outputs and inputs to systems such as the Flight Guidance Computer

OR

Access is required to the servers hosting field loadable software updates for the same core system components in order to change the software download offered to airline maintenance workers

OR

A man in the middle attack between the avionic system or component vendor and the airline maintenance worker is required to tamper with the download

WHERE DO WE GET OUR INFORMATION TO BEGIN OUR ATTACK?

These days a large part of the flight is controlled by the “autopilot”; particularly on long haul flights with such long periods of little change and the resulting boredom for the pilot. On a fly by wire aircraft there are no points in the flight where some computer system is not partially or fully in control of the flight.

So, to take the plane off course we need to have overwritten the database used by the field loadable software in the flight management system (FMS) with new waypoints that the crew can’t override, so when each waypoint is transmitted to the autopilot to adjust the controls those the black hat hacker has provided are used. This could be performed from a secondary system such as the Electronic Flight Bag (EFB) systems that many pilots use with the inbuilt maps to load the waypoints in the first place.

Another alternative is to intercept the ARINC-429 messages and their derivatives, such as the ARINC-629 variant in the 777; blocking the originals and providing new commands. Since the formats are well documented a box such as Raspberry Pi could do the job, especially since many aircraft have started to adopt plain Ethernet as the communications mechanism, although placement for effectiveness would require some knowledge of the aircraft systems and access, requiring the black hat hacker to be an aircraft maintenance worker.

This all obviously only works if we have used the same techniques to alter the conditions on the aircraft such as to incapacitate the cockpit crew to stop them switching the autopilot off and flying the plane manually, which is more difficult on a fly-by-wire aircraft such as the 777, but is something pilots practice in simulators continually.

WHAT DO WE NEED TO TAKE CONTROL FROM OUTSIDE THE AIRCRAFT?

As mentioned earlier, the first thing we need is access to the software used to control the flight management computer or some physical access in which we can insert something to interrupt the signals using the ARINC-429 protocols. This access is controlled and in both cases is probably best given to a member of the maintenance crew to avoid suspicion; but a hacked server hosting maintenance software from the likes of Boeing would also give that access, and this latter approach is more likely available to a typical Black Hat hacker.

Given the architecture of the avionics systems and broadcast connectivity between them an event driven trigger could be placed in the software to initiate taking control, or possibly a particular ACARS message from the ground.

All we need to direct the course of the aircraft is to provide the messages in the appropriate format to the autopilot system, and the ARINC-429 standard and its derivatives give us the instruction set for doing this.

This is best seen with an example.

To send an instruction to change altitude as seen in flight MH-370 I would have to use the Equipment ID bits in an ARINC-429 message to say I am the Flight Management Computer (FMC), i.e. Hex 002; the Label field to 102 to say I am sending a Selected Altitude, the SSM field to say it is positive or above, and the Data to say the target altitude value (e.g. 13106 metres encoded in Binary Coded Decimal is 43,000feet). Other systems on the bus, such as the Automatic Flight Control System or autopilot would then take that instruction on the bus and perform the necessary operations to make the ascension happen until the aircraft was stable at that selected altitude. We have seen just such an instruction in Figure 3.

To then cause the aircraft to turn to a new heading another FMC issued message would be sent, and to change airspeed yet another FMC message with label 103.

Whilst field loadable software updates downloaded from the Internet or provided on a CD-ROM usually has an associated recommendation that it is virus checked and the checksum verified, this always assumes that the person performing maintenance using the software isn't malicious and that the providing source hasn't been compromised; and the updates for the Flight Management Systems (FMS) and Electronic Flight Bag (EFB) are just the targets that would allow an attack to bring about the behavior seen with Malaysian airways MH-370. However, if the perpetrator is an aircraft maintenance worker why not add a new subsystem to run interference and provide its own control commands using Ethernet and a small unit such as Raspberry Pi.

You might ask why a maintenance worker wouldn't just plant a bomb on board. In many ways, the mystery associated with unpredictable behavior of an aircraft gives more of a source of terror than a bomb. So, if someone has caused the MH-370 disappearance with a hack; only telling governments and not claiming responsibility can cause more fear.

HOW DO WE MITIGATE AGAINST THIS?

How about an Intrusion Detection System (IDS) for aircraft and a virus checker?

To build such systems we would need to have some means of interrogating each subsystem for its integrity and some way of identifying abnormal behavior.

The IDS would need to download signatures of known equipment every time a change occurred and have some way to perform a checksum to verify the equipment has not been tampered with; and it should know the expected flow of commands from a subsystem and the different possibilities of waypoints for given routes. Finally, the IDS should use ACARS to maintain communications with the ground at all times.

CONCLUSION

Modern aircraft have their own complex networks of subsystems, and like the Internet protocols are what allows these disparate systems to interoperate and the complexities within a system to remain hidden. This also allows systems to be upgraded independently. The very knowledge of this interoperation and the flexibility it brings gives a black hat hacker a blue print for an attack. Knowledge for how to pass information between subsystems allows an intruder to misinform systems and gain control of one subsystems from another.

The use of subsystems that rely on computing and software at the core with the need for "field upgradability" gives an avenue by which to initiate an attack. When updates are downloaded from the Internet or copied onto a CD-ROM for distribution they can be attacked at source, and the provided software can be tampered with. Such tampering could alter the waypoints in the database of the flight management system (FMS) in such a way as to completely alter the behavior of a flight, but other operations would need to incapacitate the crew to avoid them switching off the computers – something which is hard to do on a modern fly-by-wire aircraft such as the 777.

Whilst it is unlikely that this is the circumstance that led to the demise of Malaysian Airlines flight MH-370 the fact that it looks to be possible, and the lack of intrusion detection systems at the core of modern aircraft suggests that it is a possibility. Given the publicity surrounding the mystery of flight MH-370 it is likely that such a terrorist attack may not have been thought of in the past; but it is likely to be from now on. So, thought as to intrusion detection to protect against such attack is now needed.

REFERENCES

- 1) Aircraft Digital Electronic and Computer Systems, 2nd Edition, by Mike Tooley
- 2) Boeing Jeppesen 777 Electronic Flight Bag PDF

ABOUT THE AUTHOR

Colin Renouf is long standing IT worker, currently an Enterprise Architect in the finance industry, but having worked in multiple roles and industries over the period of decades. An eternal student, Colin has other degrees in varied subjects in addition to that for IT. Having written several books and articles ranging from architecture, Java, and security; and contributed to well known products from the likes of IBM or Oracle, he is even referenced on one of the most fundamental patents in technology. Colin has had several jobs in the past, but his first role after getting his earliest degree in Aeronautical Engineering was in the aerospace trade. Colin has two incredibly smart and intelligent children, and spends most of his time in his favourite country – Australia (the land of the free thinker and good food) – wondering how he manages to upset people so easily and trying to have a social life when he or close friends aren't working themselves into the ground. Thank you Red Bull.

THE ONE!



The Most Powerful Forensic Imager in the World



Provides the broadest drive interface support

Built-in support for SAS, SATA, USB 3.0 and Firewire. Supports IDE and other interfaces with adapters included with Falcon

Processes evidence faster than any other forensic imager

Image from 4 source drives up to 5 destinations

Perform up to 5 imaging tasks concurrently

Image to/from a network location

Imaging speeds of up to 20GB/min

NEW FEATURES AVAILABLE NOV 2013

- NTFS Support
- TrueCrypt Support
- Drive Spanning
- The fastest E01 imaging speed available



Visit our website today to see why Falcon is The One!
www.logicube.com

21ST. CENTURY IT SYSTEM MANAGERS – THE AVIATORS

by Robert Vanaman

The evolution of avionics [1] over the past decade has revolutionized the way pilots plan, navigate, communicate, and aviate their aircraft. Aviators in the 21st century have become trained, practiced, system managers; having all but replaced the flyboys of yesteryear. The era of seat of the pants flying has been superseded by integrated systems providing the pilot and crew with digital services that deliver real-time XM satellite weather, synthetic vision, approach plates and airport diagrams, all presented on multiple, customizable display screens. We have all experienced the electronic office; now we are living in the age of the electronic cockpit.

Far from elevating the burdens of pilots from their constant cross-checking (Read: monitoring) a conventional instrument panel, glass cockpits (GC) have created an airborne information technology (IT) system manager charged with all of the input, interpretation, evaluation, decision making and system analysis responsibilities of ground based IT executives. This paper's position is that modern technically advanced aircraft (TAA) have transformed pilots into IT system managers – *at altitude*.

This paper will briefly chronicle the early events – a few decades ago – which spawned the computerization within aviation. Then trace its progress, focusing on of the innovative equipment that changed the role, duties, and responsibilities of the pilot in command (PIC) at major milestones within this electronic revolution. Next, there will be an examination of today's state-of-the-art GC, and their implications on the current role of these now, *flying* IT managers. The paper will conclude by assessing what exciting future developments lie ahead, both in the near and long term.

This paper's scope will be limited to three specific areas of concentration relating to the plane, pilot, and a company. First the airframe, only systems found in light single and twin engine aircraft, both propeller and turbine (Read: jet) powered will be examined. Second, these aircraft and systems are flown by civilian pilots in a general aviation (GA) environment. Third, the avionic systems examined will be those manufactured by Garmin Ltd [2]. This realm was chosen due to the author's personal experience in these areas.

THE EARLY YEARS

To begin our study of avionics and their future, we should first briefly visit the past. Modern aircraft (post WWII) have traditionally relied on aircraft instruments that were analog in design, mechanical in nature, and (relatively) easy to comprehend. Instruments of eras past were referred to as steam gauges – a specious analogy to their superficial resemblance to steam locomotive gauges – they were either vacuum driven, electrically powered or used air pressure differentials to govern the gauges; and were notoriously difficult to keep calibrated. Many navigational and attitude gauges were gyroscopic mechanisms (employing the rigidity in space concept) and prone to precession [3].

Six main gauges became standard for light aircraft, referred to by pilots as the *Six Pack*. They, and their functions, are: Directional Gyro (DG) – where is my nose pointing, Airspeed Indicator (AI) – how fast am I, Altimeter – how high am I, Vertical Speed Indicator (VSI) – how fast am I ascending or descending, Heading Indicator (HI) – what is my direction, and the Turn Coordinator -how *precisely* am I turning. With the coordinated use of these flight instruments, the engine instruments, and communication gear, an aviator could aviate, navigate and communicate his way within his three dimensional domain.

That state of affairs existed for some years. Along the way more reliable, sensitive, even intuitive navigational equipment such as: Automatic Direction Finders (ADF), Distant Measuring Equipment (DME), Very High Frequency Omnidirectional Range (VOR), and Horizontal Situation Indicators (HSI), began a slow *evolutionary* pace towards increasingly sophisticated, workload intensive cockpits. Just as additional functions, features, and capabilities in hardware and software have led to increased complexities in computer operations. So too by adding additional equipment and/or more sophisticated equipment to an aircraft, leads to greater demands on the pilots attention, on pilot training, their Situational Awareness [4] (SA) – a new term, but *very* important – and their overall ability to *stay ahead of the aircraft*.

What occurred during the years after WWII, up to about a decade ago, was a slow, steady progress in aircraft analog instrumentation systems. Resulting in an increasingly complicated cockpit ambience of burdensome pieces of equipment configured with: dials, knobs, gauges and read outs of various sorts. All of which, to be of any use to the pilot and crew, must, by definition, distract them (one only has so much metal capacity after all) from their primary duties of flying the airplane.

AUTOPILOTS

Autopilots were one of the first electro-mechanical devices to provide assistance that allowed hands-off stick and rudder flying. Autopilots helped pilots SA with routine and often long-duration flights.

SINGLE-AXIS

In the late 1950s, GA was introduced to the single-axis auto pilot (single-axis is an important consideration; remember aircraft fly in a three-axis environment). The early models were simple to set by pressing a button or two when at the desired altitude. They attempted to maintain that altitude coupled with a wings level orientation. I say attempt because early auto pilots were not slaved to the navigation equipment in the aircraft. Therefore deviations due to crosswinds, and HI precession, etc., had to be periodically corrected for manually. However, this innovation did give the pilot time off from *hand flying* the aircraft, and it did increase the pilot's time for scanning the other instruments and the sky.

TWO-AXIS

The next real innovation came with the introduction of the two-axis auto pilot. This autopilot had all of the features of a single-axis autopilot with the ability to hold a precise altitude. Additionally, later two-axis models were slaved to the HI navigation instrument. Now, by merely twisting the Heading Bug (a small knob used to mark a desired course on the HI), the pilot could change course, and maintain altitude.

Today's autopilots have functions that while maintaining altitude while cruising, they can change altitudes at a specific rate of climb or decent and control pitch or roll angles. The sophisticated (at the time)

functionality that early autopilots provided, including assisting the crew to deal with windshear and turbulence, further illustrates the advantages of quasi-modern analog technology. They represent a real step in transitioning the pilot to a modern aircraft system management (The glass cockpit, p. 92).

There is still a good while before the hand-held GPS was introduced, so monitoring the course and altitude was still a priority for pilots. However, the era of “*buttonology*” had taken a foothold in the cockpits of GA aircraft.

THE GLOBAL POSITIONING SYSTEM

The Global Positioning System (GPS) is a network of 24 navigational satellites placed in orbit by the U.S. Department of Defense. Although originally intended solely for military use, they were freed for public participation in the 1980s (Garmin, 1999). This system of satellites is stable, robust and user friendly. They operate in all weather conditions, day and night, and maintain an orbit altitude of 20,200 km (UNSW School of Surveying & Spatial Information Systems, 1999). The GPS satellite system charges no subscriber fees and needs no setup. They are the quintessential high-ground *plug and play* device.

Although an exacting explanation of how the system functions is not necessary for this paper’s breadth, a basic understanding will enlighten the reader as to the requirements for the system to work as advertised. All the satellites orbit the earth twice a day at 7,000 mph. At any one time, four or more must be available for *polling* to establish a useful position in aviation (at some locations and periods around the globe there are many more than four available). An aircraft’s *fix* is found by “triangulation to calculate the user’s exact location” (Garmin, 1999). Once the aircraft’s 3D position has been determined, other specifics about the flight can be ascertained “such as speed, bearing, track, trip distance, (and) distance to destination” (Garmin, 1999).

In aviation, these satellites communicate with two *flavors* of GPS receivers: handheld portable units, and permanently installed panel mounted displays [5].

HAND HELD GPS

GPSMAP 196

The modern revolution in the way aviators flew (Read: managed) their aircraft started in a small Wisconsin town by the name of Oshkosh in the summer of 2002. Garmin Ltd. unveiling its hand held GPSMAP 196 (Figure 1) (Garmin media gallery, 2002).



Figure 1. GPSMAP 196

This GPS remains to this day an aviation milestone. Garmin had introduced other hand held GPS's earlier in their GPS product line, but the 196 was the one that acquired aviation's attention. It was small and portable, with a 3.8" diagonal black and white screen, weighting in at 24 oz. and had a standby battery mode of 16 hours (Garmin, 2010d). But that was not what set this unit apart from all the others. It incorporated: a GPS based moving map, a graphical representation of the aircrafts six pack, and a HSI, all functioning through the GPS satellite system (Garmin, 2010d).

Pilots the world over were stunned! Not only did the 196 provide the pilot with the much sought after *highway in the sky* (more on that concept later) based on the 24 satellite GPS navigation system, it also added a backup set of flight instruments to the cockpit in case of electrical power or engine failure! Never before had pilots of light aircraft had this much computing power in their cockpits, or this much computing distraction vying for their time and attention.

GPSMAP 296

Garmin's next iteration of this design was the GPSMAP 296. It was introduced in July 2004 and added a color screen, and Terrain Awareness and Warning System (TAWS) to the already rich list of features in the 196. With TAWS, pilots could observe their proximity to the ground (Read: mountains) or ground based objects long before they would be in actual visual range (Garmin, 2010d).

GPSMAP 396

Milestone number two for Garmin's hand held lineup came in the summer of 2005 with the advent of XM Satellite Weather (XMWX), Traffic Information Services alerts (TIS) and now audible TAWS alerts (The system talks to the crew through their headsets – "Terrain 500 feet, *Pull-up!*") in their GPSMAP 396. While including all the features of the 296, now came a portable device that gave the pilot *over the horizon* weather detection and avoidance, audio terrain alerts, and the ability to inform the PIC of traffic behind, above, below, and in front of the aircraft; again, long before the pilot or crew would be able to spot the weather, obstacle, or other aircraft (Garmin, 2010d).

GPSMAP 496

Garmin next introduced the GPSMAP496 in 2006 (Figure 2) (Garmin media gallery, 2006).



Figure 2. GPSMAP 496

Here altitude-sensitive alerts were displayed, and automatic logbook entries were included for the first time. Serial and USB interfaces were provided for external data up and down loading. Additionally, the 496 included many of the features found on Garmin's famous Nuvi automobile GPS's, making it as at home on the road as in the cockpit (Garmin, 2010d).

Pilots – with all their new toys – are now becoming *very* busy. They are interacting with the traditional controls to aviate and navigate the plane, plus communicating with Air Traffic Control (ATC) and now having to supplement those chores with manipulating the (anything but intuitive) controls on the GPS. Pilots heads (read: attention) are increasingly inside the cockpit managing their new computer systems, not focused outside *flying* the plane.

PANEL MOUNTED GPS

To the astute reader, a missing piece to the avionics equation is observable. The PIC is interacting with the flight controls and other aircraft systems, and interfacing (Read: fussing) with the hand held GPS as well. Astonishingly enough, the portable GPS is *not* interacting with the flight controls, instruments or communications gear in the craft. There is a void, a *great divide*, between this innovative apparatus, and a realized synergy between plane, pilot, and avionics.

The introduction of an integrated GPS, navigation (Nav), and communication (Comm) avionics device was a landmark event in GA. For the first time, all the advanced capabilities found in handheld GPSs were installed, and augmented with the aircraft's other systems.

Here again, although Garmin had introduced previous panel mounts, the two which are to this day the standard by which others are judged, are their GNS 430 and GNS 530 models.

GNS 430

Garmin's GNS 430 was first introduced in May 1998 (Figure 3) (Garmin media gallery, 2008a).



Figure 3. GNS 430

The astounding resources it introduced to GA were immediately embraced. This small 3.3 x 1.8 inch display changed the way pilots managed their aircraft in flight – *forever*. For the first time, the Nav, Comm, autopilot, and GPS were incorporated into a single unit, and functioned in concert with one another (Garmin, 2010a).

A small sampling of these unit's abilities included (when coupled with an autopilot) upon departure, allowing the PIC to input heading, altitude, and rate of climb instructions to intercept a specific course. In cruise, it maintains an exact heading and altitude without drift or need for periodic corrections from the pilot. When in the arrival phase of the flight – flying Instrument flight reference (IFR) -, landing approaches, holding patterns, procedure turns, and other position-critical maneuvers can be executed hands-off the controls, utilizing ground based instrument landing systems (ILS). Additionally, in case of an inflight emergency, the system aids the pilot in locating, and navigating to the nearest airport; while automatically handling supplemental chores such as tuning in the appropriate Comm and Nav frequencies (Garmin, 2010a).

GNS 530W

The next iteration in panel mounted systems from Garmin was introduced in October 1999, the GNS 530W (Figure 4) (Garmin media gallery, 2008b).



Figure 4. GNS 530

With its much larger 4 x 3 inch display and a higher 320 x 234 resolution, this unit was a welcome step forward. However, with all of the functions, integration, and innovations found in the GNC 430, the GNC 530 introduced one of the most monumental changes in the history of GA, the Wide Area Augmentation System (WAAS) (Garmin, 2010a, 2010f).

Before WAAS, IFR precision approach systems for aircraft were ground based radio navigation equipment, which were very large, and very expensive. This equipment, located at an airport, allows for confident and accurate landings in less than ideal weather conditions. The expense of installation and maintenance of these systems made them prohibitive for all but the larger airports. They essentially give slope (what angle am I descending at) and course (what heading am I flying at) guidance to the pilot, well before he or she can see the ground or runway in Instrument Meteorological Conditions (IMC). This system made modern airline travel (Read: on schedule, and without diverting) possible.

The WAAS is a GPS *satellite base* (not ground based) IFR precision approach system. WAAS utilizes the same GPS satellite system used in normal navigation, but it is augmented by 25 based ground stations positioned across the United States. These ground stations correct and enhance the GPS signal. This refinement in signal allows for WAAS equipped aircraft to fly IFR precision approaches to hundreds of smaller airports in IMC (Garmin, 2010f). Now guidance for approaches, holding patterns, procedure turns, and other position-critical maneuvers are available to pilots in remote locations. WAAS significantly increased the pilot's level of confidence and security on approaches.

GLASS COCKPITS

FLIGHT DECKS – G1000

Up until this point, all the innovations have related to the GPS/Nav/Comm portion of the avionics spectrum. Now the next grand transformation takes place with the introduction of the Garmin G1000 Flight Deck in August of 2007 (Figure 5) (Garmin media gallery, 2007).



Figure 5. G1000

This radical departure from traditional aircraft instrumentation dictated a new classification of aircraft: Technically Advanced Aircraft (TAA). This venture from the standard “six pack” of steam gauges to a *graphical representation* of the plane’s position and attitude was landmark. The speed, heading, altitude, and attitude, are displayed on a single Primary Flight Display (PFD). This display is juxtaposed with a second screen, the Multifunction Flight Display (MFD), both with 1280 x 1024 resolution screens. They together ushered in the age of the glass cockpit. This sophisticated configuration of instrumentation and avionics mandated a notable departure in the way pilots flew, managed, and viewed their aircraft cockpit responsibilities (Garmin, 2010b).

For the first time [6] a seamless, all-glass, integrated avionics suite is available to the GA community. Garmin’s G1000 presents its information on dual color 12 inch display screens with an 800 x 640 resolution. The G1000 displays “a wealth of flight critical data” its “glass flight deck presents flight instrumentation, navigation, XM satellite weather, terrain and traffic avoidance, and engine data on large-format, high-resolution displays” (Garmin, 2010b). For safer and enhanced arrivals and departures, Jeppesen’s digital charts (JeppView) are available to view on the MFD. The presentation allows the ship’s position to be *overlaid* on the electronic chart, offering unparalleled SA. The aircraft’s position on taxiways can be seen from a bird’s eye view, greatly reducing the possibility of runway incursion (Garmin, 2010b).

THE PFD

Garmin’s G1000 PFD exudes information. All six traditional instruments used to fly aircraft are now graphically represented in a stunning new format. Additionally, vital data that was once prohibited from display – due to unavailability or space constraints – is now readily available for pilot consumption. An overview of this fascinating display seems in order.

The six pack of instruments have undergone a facelift. No longer confined to a circular configuration, the flight instruments have been reinvented. The airspeed and altitude indicators are now exhibited on a graphical tape layout, with current speed and altitude magnified and highlighted on the tapes center. The VSI lies to the right of the altimeter on its own tape display. They border left and right of a centered AH *en suite* Flight Director [7] (FD). The turn coordinator has been entirely replaced by a split triangle icon at the top of the AH, and renamed a Skid/Slip indicator. The DG is now an integrated DG and Digital Horizontal Situation Indicator (DHSI) located just below the AH. The DHSI exhibits its data in the traditional compass card configuration as well as presenting the heading and course in digital fashion (Garmin, 2010b).

Various other pieces of data are visible on the display. They include, but are not limited (remember this is a user *customizable* display) to, Nav and Comm frequencies both active and stand-by, the next way-point (WPT) selected on the GPS with its distance (DIS), desired track (DTK) and current track (TRK),

transponder frequency [8] (XPDR) and setting, along with various selectable time zones for clock settings and outside air temperature (OAT) (Garmin, 2010b).

THE MFD

ENGINE INDICATION SYSTEM

Although aircraft have been equipped with engine instrumentation since early bi-planes, the gauges often acted as more of a confirmation that a problem has occurred rather than as a warning alert that a problem was developing. Garmin's Engine Indication System (EIS) leaps beyond conventional aircraft's temperature and pressure gauges and establishes a new standard. As for fuel monitoring, the EIS calculates gallons used, endurance, and range. The EIS presents a graphical bar displaying each cylinder head temperature (CHT) to assist in leaking the engine at altitude. This extends range and increases the life of the engine. The standard analog fuel and engine gauges – manifold pressure, RPM, oil pressure, fuel pressure, Amps, Volts, and left and right fuel tanks – are digitally represented with numeric read-outs. This configuration greatly enhances the readability of the cluster (Garmin technical publications, 2008).

SYNTHETIC VISION TECHNOLOGY

An astonishing option for the G1000 was unveiled in August of 2008, Garmin's synthetic vision technology (SVT). Synthetic vision augments the pilots view by mitigating the interference of "meteorological conditions like darkness, dust, fog, rain etc." (Moller & Sachs, 1994, p. 27-33). The implication for added crew and passenger safety is undeniable. This revolutionary "Synthetic Vision System (SVS) provides pilots with an always-available computer generated perspective view of the outside world ahead of their aircraft" (Garmin, 2010e). Utilizing GPS satellites, this is a computer generated 3-D graphic image of real-world, real-time aircraft positioning in relation to the external situation, minus the distracting environmental conditions that "affords enhanced spatial and terrain awareness during both darkness and poor visibility. This would especially benefit safety during approach and landing operations when knowing one's position relative to nearby terrain, obstacles, and the runway is of critical importance" (Goodman, Hooley, Foyle, Wilson, 2003).

Garmin's SVT is a significant enhancement for their Flight Deck. SVS's offer unprecedented SA for the pilot and crew. With 3-D depiction of land and water features, airport runways portrayed relative to the aircraft's position, terrain and traffic shown in their relative proximity to the plane, all create a situational depiction that is intuitive, and pictorial in nature. The PIC no longer needs to formulate a mental picture (an SA) from raw data displayed on glass panels or worse, interpreting steam gauge readings for their SA image (Garmin, 2010e).

A few of the Garmin SVT's attributes of particular interest are the color coded terrain, traffic avoidance, and Pathway in the Sky features. The color coded terrain aspect of the system colors the terrain in a realistic topographical pattern. For added clarity and safety, obstacles and terrain are portrayed in yellow and red when proximities to the aircraft are becoming an apparent risk. Garmin's traffic avoidance system (TCAS) shows traffic in 3-D perspective and enlarges the symbol depicting the traffic as the traffic nears the aircraft. Of all the facets of SVT, the Pathway in the Sky feature is one of the most remarkable. The Pathway in the Sky uses a straightforward approach to enroute navigation by creating a 3-D graphical gateway, projected on the PFD that the pilot simply *flies through*. These pathways are magenta colored rectangular gates and are suspended in a perspective view, growing larger as they approach, and appear to *fly* towards the pilot. By their orientation (left, right, up or down), they visually guide the pilot's hand for the appropriate control inputs. This 3-D pathway is not merely for cruising at altitude, it can be employed for procedure turns, and ILS or GPS/WAAS approaches as well (Garmin, 2010e).

INFORMATION OVERLOAD

Suddenly the amount of information available to the flight crew is staggering in its quantity, its quality, its complexity, and its interpretability. Pilots are becoming saturated with data, literally becoming as burdened with IT system overload as their ground based counterparts. It is no longer a question of how much control pressure to input on the stick or rudder, or how much or little to advance or retard the throttle to control the aircraft, the question now for the PIC of a TAA is what kind of system input is necessary to manage the aircraft's digitally based, computer controlled, avionics suite.

As stated earlier, as with all IT systems, the addition of new features, enhancements to existing features, complexities of customizable displays, an overall expansion of a system's capabilities, all require

the acquisition of new skills on the part of the pilot. Now, couple a fresh new user interface employing soft keys, now rigorous new educational and training requirements are mandated.

With all of the GPSs or flight decks that were presented, whether portable or panel mounted, and especially with the G1000, there is a commonality between them; their utter lack of user friendliness. The scholarly nature of this paper prohibits me from expressing in exact terms the language aviators use to describe these devices' *unintuitive* nature.

The dexterity (planes tend to bounce) and sheer memory requirements to input commands in these systems is daunting. There is, after all, no mouse for point and click commands. There is no keyboard [9] in the Garmin G1000 flight deck for alpha-numeric input. There are no touch screens or voice to text capabilities available at this time. The state-of-the-art flight deck for GA aircraft leaves much to be desired in interfacing with the pilot and crew. They abound with knobs within knobs to tune in Comm and Nav frequencies and to input airport identifiers on the flight plan page [10]. Pages within pages within pages for GPS, engine, flight plans, etc., with no pull down menus or Windows like GUI interface. The soft keys seemingly change their function in a random pattern when different page screens are selected and displayed.

This new breed of airmen who have been morphed from flyboys to IT system managers, have all the cores of any data entry personnel while burdened with a computer input scenario that would not be tolerated in a ground based IT setting. All of the above contribute to an extremely high workload – and at times – frustration level for pilot and crew.

THE NEAR FUTURE

GARMIN G3000

The future of aviation and avionics is appearing brighter with regards to the ease of interaction between man, computer, and machine. Within the next two years, Garmin will have Federal Aviation Administration (FAA) approval for their G3000 Flight Deck (Figure 6) (Garmin media gallery, 2010).

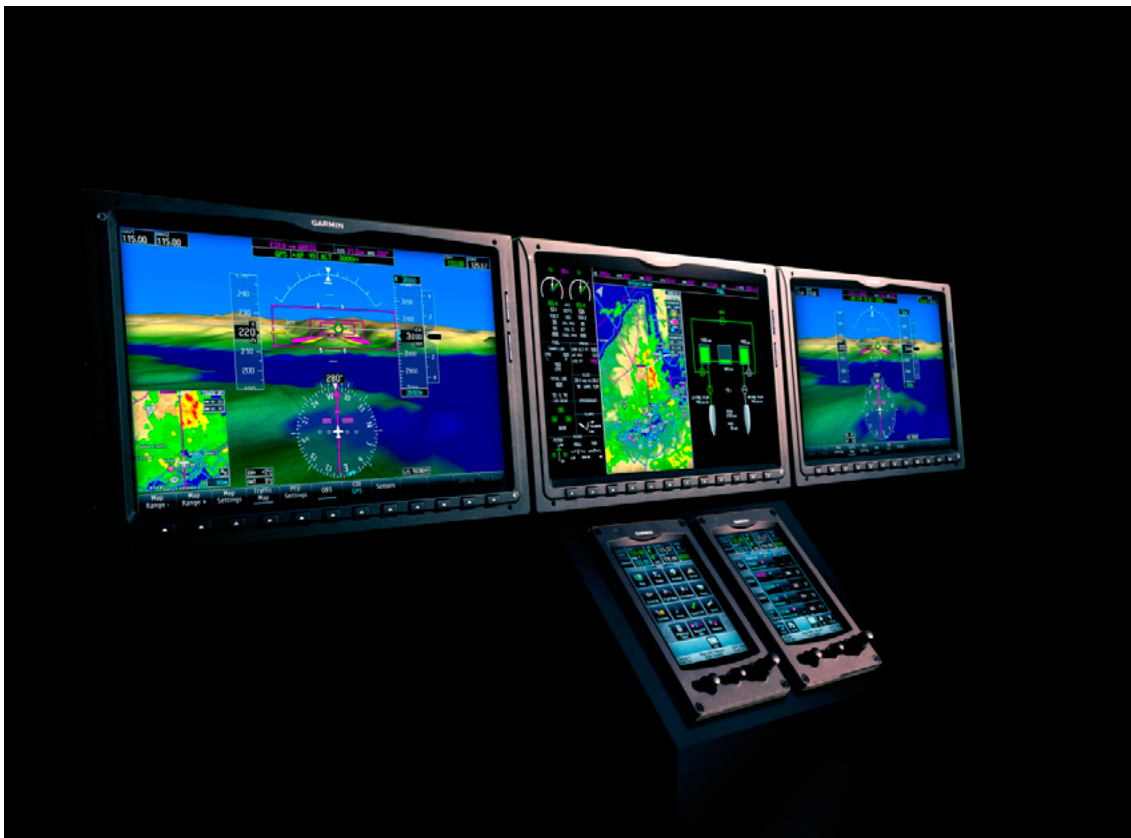


Figure 6. G3000

This evolutionary system will usher in a new level of synergy and safety within the cockpit setting.

The G3000 largest contribution will be the introduction of touch screen technology for the flight deck. This will simplify and streamline data entry. The G3000 will eliminate the crowded cluster of knobs, buttons, and switches with user friendly touch screen accessibility. The system will feature a “desktop-style, icon-driven interface built on a new “shallow” menu structure” (Garmin, 2010c). Additionally, new (to the cockpit, standard for decades on PC’s) *Back* and *Home* keys will allow for fast retracing of inputs, and straightforward desktop navigation. This eliminates the need for memorizing lengthy input sequences. Further enhancing the PC’s desktop look and feel, a dedicated GPS map *joystick* has been included as well (Garmin, 2010c).

The dual G3000 displays are large 14 inch screens with a familiar 16:9 ratio. The PFD and MFD are completely interchangeable adding robustness to the system. These larger displays allow for an increased SA for pilot and crew. This further enhances Garmin’s SVT by offering a wider “more visual area for the simulated 3-D perspective topography” and providing additional “peripheral cues from an extended horizon line” (Garmin, 2010c). The G3000’s presents “a detailed graphical landscape, a virtual reality perspective view of ground and water features, obstacles and traffic – all shown in relative proximity to your aircraft” (Garmin, 2010c).

The PFD’s other half the MFD, will be no less astonishing. The G3000’s MFD acts as a display *suite*, allowing for two independent pages to be viewed side by side in conjunction with the EIS strip for engine and fuel monitoring. This innovation takes the customizable, user configurable GC to a new level. With its split-screen capabilities the MFD can combine: a “satellite weather and flight planning pages” (Garmin, 2010c) when preparing for departure. Configure a “GPS map, or traffic, or radar, or TAWS” (Garmin, 2010c) when in flight. Then can present an “airway chart and your approach plate” (Garmin, 2010c) when on the arrival leg of a flight.

The Garmin G3000 will finally bring to GA what has been promised for decades: an IT system that integrates man, machine, and computer.

DISTANT FUTURE

FLIGHT MANAGEMENT

On the forefront of all aviation design, training, and pilotage, is aircraft, passenger, and crew safety. Safety concerns dominate aviation like few other arenas. To that end, GA is anxiously awaiting the day when flight management systems (FMS) “comprising the autopilot and auto-throttle system” (Suzuki, & Yanagida, 2008) will effectively render in flight emergencies a nuisance, instead of a life threatening scenario.

Cirrus Aircraft has, for over a decade, incorporated a ballistic parachute system in their planes. However, this system, when deployed, does effectively deliver the occupants safely to earth, it just as effectively, destroys the aircraft [11]. Not the most ideal solution.

What is needed, and is on drawing boards around the globe, is a computer driven “fault tolerant flight control system (FTFCS)” (Suzuki, & Yanagida, 2008). The system would be comprised of two components. A “fault tolerant control system (FTCS) and a fault tolerant guidance system (FTGS)” (Suzuki, & Yanagida, 2008).

The FTCS would initially stabilize the plane with an *adaptive* flight control system. This is in case the flight control surface is damaged or is malfunctioning. Then it would configure/reconfigure the control inputs for stable flight. The FTGS would then navigate and aviate the aircraft to the nearest safe landing zone (Suzuki, & Yanagida, 2008).

This would all be accomplished without the need for the pilot or crew to initiate either avionic or manual control inputs. In emergency situations, utilizing a FTFCS, the pilot and crew have accentually become *passengers*.

FLY BY WIRE

In a further departure from autonomously pilot controlled aircraft, and again for safety concerns for passengers and crew, is the Fly by Wire [12] (FBW) flight control system. FBW has been in military aircraft for some time; however the cost of such systems makes them prohibitive for civilian aircraft at this time.

Civilian FBW application is directed at a breach from accepted controlled inputs. A significant innovation in FBW flight control is *envelope protection*, which allows the flight-control system to limit the pilot's inputs to those that will not stress the aircraft beyond its design limits. Thus, for example, while turning, banking, or climbing, if necessary, pilot inputs are reduced to levels that are safe for the aircraft (The glass cockpit, p. 92). In effect the pilot becomes a mere *voting member* of their avionics suite.

VOICE RECOGNITION

A final instance of a GC pursuing IT ground based systems is in the astonishing proposal for "voice guided general aviation aircraft" (Rogalski, & Wielgat, 2010). This concept would utilize a limited vocabulary. A discrete system would certainly precede a continuous speech recognition system. The software would undoubtedly require training the system on the user's behalf. Voice commands that could be accepted would include: course direction – "heading 090", changes in altitude – "descend to five thousand five hundred feet @ five hundred feet per minute", voice tuning of Comm/Nav frequencies – "Comm 1 Tune 127.05".

The implications for a "control system which can be the base for developing a voice controlled general aviation aircraft" (Rogalski, & Wielgat, 2010) are far reaching. Applications for this remarkable system might permit (nay, *encourage*) the disabled to take to the skies in comfort and safety. Allow ATC, or other ground personnel, or perhaps a pilot in another aircraft, to control a second aircraft – by way of a voice activated radio interface – in the event of a pilot's incapacity, or other such emergency.

CONCLUSION

Within the last decade, the advancements in GA avionics have stunned even the most imaginative pilots. Aviators of the 21st century are experiencing greater challenges, and have witnessed greater changes, than any other generation of GA pilots.

Pilotage and dead reckoning have been replaced with GPS guidance. The era of stick and rudder airmanship has been swapped for a "buttonology" mentality. The mental acuity – always problematic – necessary to form an accurate SA picture within a three dimensional environment has been replaced by a virtual world display, courtesy of SVT. Yet, all of the skills and daring of aviators from a bygone age need to be retained by today's flyers, while juxtaposed with IT management capabilities.

Just as earth bound IT system managers have experienced information overload, so too have their aviation brethren. Multi-display, multifunctional, customizable flight management systems have recreated all the duties and tasks that traditional IT managers contend with; however, aviators contend with them, – *at altitude*.

REFERENCES

- Abbott, M., Kailey, L., Mowery, J., Willits, P. (Eds.). (2003) Guided flight discovery: Instrument commercial. Englewood, CO: Jeppesen Sanderson, Inc.
- Abbott, M., Kailey, L., Willits, P. (Eds.). (2002) Private pilot manual. Englewood, CO: Jeppesen Sanderson, Inc.
- Garmin. (1999). Garmin: What is GPS? Retrieved from <http://www8.garmin.com/aboutGPS/>
- Garmin. (2010a). Garmin: Avionics: GPS/Nav/Comm Retrieved from <https://buy.garmin.com/shop/shop.do?cld=156>
- Garmin. (2010b). Garmin: G1000. Retrieved from <https://buy.garmin.com/shop/shop.do?cld=153&pID=6420#featureTab>
- Garmin. (2010c). Garmin: G3000. Retrieved from <https://buy.garmin.com/shop/shop.do?cld=153&pID=66916>
- Garmin. (2010d). Garmin: Portable GPS. Retrieved from <https://buy.garmin.com/shop/shop.do?cld=156>
- Garmin. (2010e). Garmin: SVT for G1000. Retrieved from <https://buy.garmin.com/shop/shop.do?plD=37630#>
- Garmin. (2010f). Garmin: What is WAAS. Retrieved from <http://www8.garmin.com/aboutGPS/waas.html>
- Garmin media gallery (2002). GPSMAP 196. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-00301-00&agree=on&getImages=Get+Images>
- Garmin media gallery (2006). GPSMAP 496. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-00578-00&agree=on&getImages=Get+Images>
- Garmin media gallery (2007). G1000: Non-airframe specific. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-00578-00&agree=on&getImages=Get+Images>
- Garmin media gallery (2008a). GNS430. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-00139-11&agree=on&getImages=Get+Images>
- Garmin media gallery (2008b). GNS 530 with TAWS. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-00182-01&agree=on&getImages=Get+Images>
- Garmin media gallery (2010). G3000: Center facing. Olathe. KA: Garmin Ltd. Retrieved from <http://www8.garmin.com/company/newsroom/mediagallery/items.jsp?product=010-G3000-00&agree=on&getImages=Get+Images>
- Garmin technical publications (2008). G1000 integrated flight deck cockpit reference guide for the DA40/40F. Olathe. KA: Garmin Ltd.
- Global Positioning System. (2010). Aviation. Retrieved from <http://www.gps.gov/applications/aviation/index.html>
- Goodman, A., Hooey, B., Foyle, D., Wilson, J., (2003) Characterizing visual performance during approach and landing with and without a synthetic vision display: A part task study. NASA aviations safety program conference on human performance modeling of approach and landing with augmented displays. Retrieved from http://aeronautics.arc.nasa.gov/assets/pdf/AvSP-HPM_CP2003.pdf#page=77

- Knight, J. (2007, October). The glass cockpit. Computer, 40(10), 92-95. Retrieved from <http://www.computer.org/>
- Moller, H., & Sachs, G. (1994, January) Synthetic vision for enhancing poor visibility flight operations. Aerospace and Electronic Systems Magazine, 9(3), 27-33. Retrieved from <http://md1.csa.com/partners/viewrecord.php?requester=gs&collection=TRD&recid=A0699120130AH&q=&uid=789661533&setcookie=yes>
- Rogalski, T., & Wielgat, R. (2010) A concept of voice guided general aviation aircraft. Aerospace science and technology, 14(5), 321-328. doi:10.1016/j.ast.2010.02.006
- Suzuki, S., & Yanagida, A. (2008). Research and development for fault tolerant flight control system – part 1. Intelligent flight control system. 26th international congress of the aeronautical sciences. Retrieved from <http://icas-proceedings.net/ICAS2008/PAPERS/426.PDF>
- UNSW School of Surveying & Spatial Information Systems. (1999). The GPS satellite constellation. Retrieved from http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap2/222sats.htm

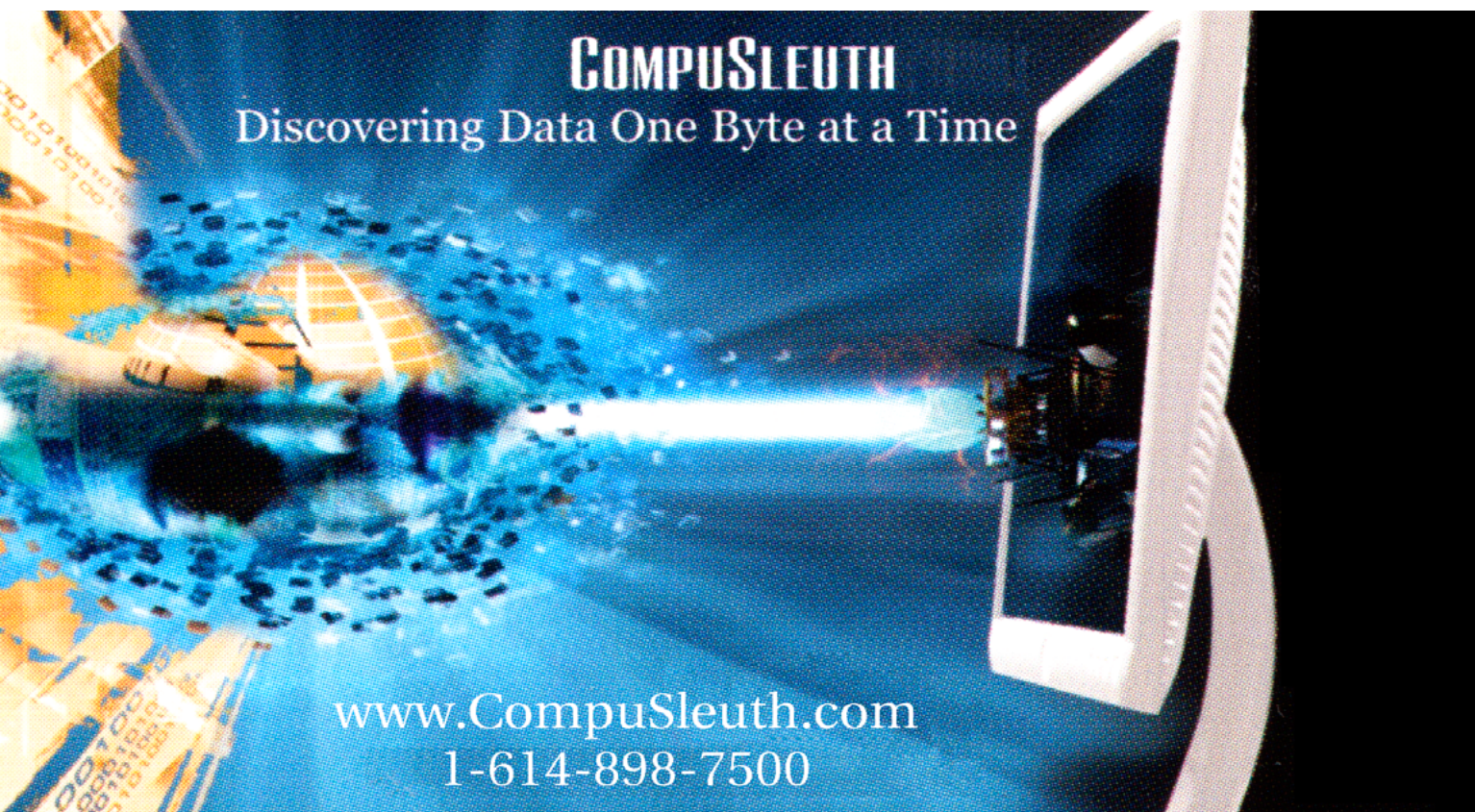
SOURCE

- [1] Avionics is a contraction of aviation and electronics.
- [2] Garmin is a worldwide leader and innovator in avionics and GPS technology.
- [3] This is the “slow drifting and minor erroneous indications in the gyroscopic instruments” (Jeppeson, p. 2-64).
- [4] SA is the complete comprehension of all aspects of the planes position relative to other aircraft, airports, terrain, and climatic conditions.
- [5] There is actually a third kind, a rarely encountered hybrid consisting of a panel mounted portable unit, that for are proposes will be ignore.
- [6] We are ignoring Avidyne’s PFD and MFD due to their reliance on the Garmin GNS430 for their functionality.
- [7] A flight director presents a visual presentation of the aircraft and its desired position and directs pilots control inputs.
- [8] The transponder squawks a discrete frequency allowing air traffic control (ATC) to locate the aircraft’s position and altitude on radar.
- [9] Cirrus aircraft equipped with their Perspective, Avidyne based PFD and MFD displays do offer a rudimentary keyboard. However it is not a QWERTY keyboard, which poses its own set of problems for inputting data and/or instructions.
- [10] A “page” is a specialized screen within a specific function, such as navigating, flight planning, etc.
- [11] The term “ballistic” is apt; the parachute blows a hole through the top of the aircraft.
- [12] FBW replaces traditional hydraulics, or push rods and cables, with electrically driven, computer managed, flight control surfaces.

ABOUT THE AUTHOR

I have been a microcomputer consulting professional since 1983. I formed my consulting firm MicroTraining in 1985. Here, I designed RDBMSs and their associated programs. I have instructed at the collegiate level for over a decade, and within the business community spanning over a quarter of a century. I provide both strategic counsel and technical support in microcomputer software, hardware configurations and their installations and maintenance. I have a Master of Business Administration and a Master of Science in Database Systems degrees from University of Maryland University College (UMUC). Currently, I am the Team Lead, Database Modeler (DBM), Developer (DBD), and Administrator (DBA) for the Amazon Model initiative for the Maryland-National Capital Park and Planning Commission (M-NCPPC), USA. I originated this Innovative Proposal Initiative (IPI) with the Commission – which has been fully funded for seven figures. The initiative was conceived during my MBA program at the University of Maryland, and is designed to increase class, event, and activity enrollment at the Commission’s applicable facilities; this by utilizing Amazon.com’s suggested products marketing methodology through automated e-mail merges and social media notifications.

a d v e r t i s e m e n t



COMPU SLEUTH
Discovering Data One Byte at a Time

www.CompuSleuth.com
1-614-898-7500

EFFECTIVE PHISHING ATTACKS

STEALING USER DETAILS

by Colin Renouf

Phishing is a growing means of attack to which so many people succumb. This article explains the most effective methods of convincing an unsuspecting user that an email has come from someone who can be trusted; and the methods of capturing information from them – some of which don't necessarily involve the use of computers. Phishing is essentially a social attack. By learning the techniques used for surreptitiously stealing information from an unsuspecting user a security professional can use the techniques in penetration tests, but can also prepare users to defend against them.

In this article we will explain the techniques of convincing users with nothing more than an email that we are someone we are not and that what we put in the email can be inherently trusted to such an extent that they will part with key information. We will look at the techniques of masquerading and how to have both the users and security systems trust our content. Next we look at how to capture information from the user; and remember that sometimes it is easier to do this using non-computer oriented techniques to avoid detection from intrusion prevention systems.

The main aim of phishing is to capture user information – so the aim of this article is to provide information to the user and the IT professional on how to identify a phishing attack and avoid it.

In this article we will describe two actual successful phishing attacks used by the author to demonstrate the approach, and will provide an examples of one approach adapted to be humorous using a government web site as the base.

BACKGROUND – WHAT IS PHISHING AND WHAT ARE WE AIMING TO ACHIEVE?

The definition of phishing is informative.

“Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online”.

Whilst this definition is informative, the last part doesn't necessarily give the full picture as the disclosure of information doesn't have to be entirely online. However, let's start with looking at what makes an effective phishing attack.

The most important thing in a phishing attack is to give the recipient of the email the impression that they are dealing with someone important that they should trust. To do this, the trick is to do everything possible to “be” the original trustworthy someone wherever possible. So, how do we pretend to be someone we aren't?

IMPERSONATING SOMEONE IMPORTANT – SOCIAL INVESTIGATION

There are many aspects to this. Remember that the aim of a phishing attack is to send an email that tricks someone into parting with key information. So, when doing this in films a mask is worn that looks like the actual individual being impersonated; and in the case of a phishing attack the same approach is used.

Now the foundation of every successful security attack is the social and psychological investigation of the target ahead of time. It's important to represent somebody that people implicitly trust; like a government body or large “trusted brand” corporation; and it must be one they would expect to hear from. There also has to be some believable incentive to get them to follow the link.

Let's look at an example. To pull off a successful phishing attack in the past, but for demonstration purposes to a targeted security audience and their families; a popular advertising campaign for a broadband company was used. The target audience was middle-aged families, with older parents still alive. So, the broadband advert was customized and an additional special offer was added to the existing offers with a believable, but very cheap offer for broadband. Since the target company was known for its humour, each recipient had to call a number and say “Eyesight fading, hearing failing, hard of thinking – I'm a silver surfer and want your broadband deal”. Then each had to leave their full name and address, birthday, and phone number. The deal being targeted for a particular age range made it legitimate to ask for a date of birth. Note that this targeting used a phone number to minimize outgoing web requests to non-legitimate web sites that can flag warnings to an intrusion detection system.

To best impersonate someone we have to put on their “mask”, which in the case of the Internet is to mimic their web site. Then we take the contents of this web site and embed it in an email. So, start by mirroring it to your own disk using the “wget” mirroring functionality, e.g.

```
wget -m http://www.mytargetsite.com
```

This will create a local copy of the *www.mytargetsite.com* that you can experiment with. This is used to explore the layout and feel of the site, and get an understanding of its structure.

FOOLING THE RECIPIENT – HOW DO WE PRESENT OURSELVES?

From this downloaded web site we want to create our email file. Whilst emails are sent using the SMTP protocol to port 25 for in the clear communications and port 465 for secured SSL/TLS communications, they can also be dropped into a directory for sending in .eml format.

To create a mass email a script is needed to substitute the names of the targets in the .eml file – remember that the email should be uniquely directed as mass CC lists or TO lists are often flagged as spam – and this needs to be in two places for both the SMTP protocol and the more complex email clients to read and use. So, create a semi-colon separated list of target first names and email addresses in a file or database and read one by one, e.g.

Listing 1. Code Example

```

NAME="Colin"
EMAIL="colin.renouf@someemail.net"
DATE=$(date)
FILENAME=""
TMPCONTACTFILE="/tmp/contact$RANDOM.txt"
FILE="contacts.txt"

#####
# For each row in the contacts list read the name and email into a      #
# variable.                                                              #
#####
while read -e line
do
    echo $line > $TMPCONTACTFILE
    NAME=$(cut -d";" -f1 < $TMPCONTACTFILE)
    EMAIL=$(cut -d";" -f2 < $TMPCONTACTFILE)

    #####
    # Create a random filename as an empty file to pipe the statement    #
    # email contents into.                                              #
    #####
    FILENAME="/tmp/${basename $0}.$RANDOM.eml"
    printf "X-Sender: pm@pm.gov.au \r\n" > $FILENAME
    printf "X-Receiver: %s\r\n" $EMAIL >> $FILENAME
    printf "MIME-Version: 1.0\r\n" >> $FILENAME
    printf "From: pm@pm.gov.au \r\n" >> $FILENAME
    printf "To: %s\r\n" $EMAIL >> $FILENAME
    printf "Date: $DATE\r\n" $(date) >> $FILENAME
    printf "Subject: Tony Talks - A Message from the Prime Minister \r\n" >> $FILENAME
    printf "Content-Type: text/html; charset=us-ascii\r\n" >> $FILENAME
    printf "Content-Transfer-Encoding: quoted-printable\r\n" >> $FILENAME
    cat message_header.txt >> $FILENAME
    printf "Dear %s,<br>\r\n" $NAME >> $FILENAME
    cat message_body.txt >> $FILENAME
done < "$FILE"
rm $TMPCONTACTFILE

```

The X-Sender and From names should match, and if talking to SMTP directly would match the MAIL FROM: part of the message, and the X-Receiver and To should match the RCPT TO: SMTP field if used.

In the above, we are (forgive me Aussie government) creating a message from the Australian Prime Minister. The target audience in this case was middle-class professional Australians in a particular company, but with an interest in politics. The trick in this case was to introduce something humorous, but believably offensive enough that the recipients would test the links and then click on one to give unfavourable feedback on the message content. If any link is followed or checked, it refers to the real site – except for the one we are using as our lure to the phishing attack.

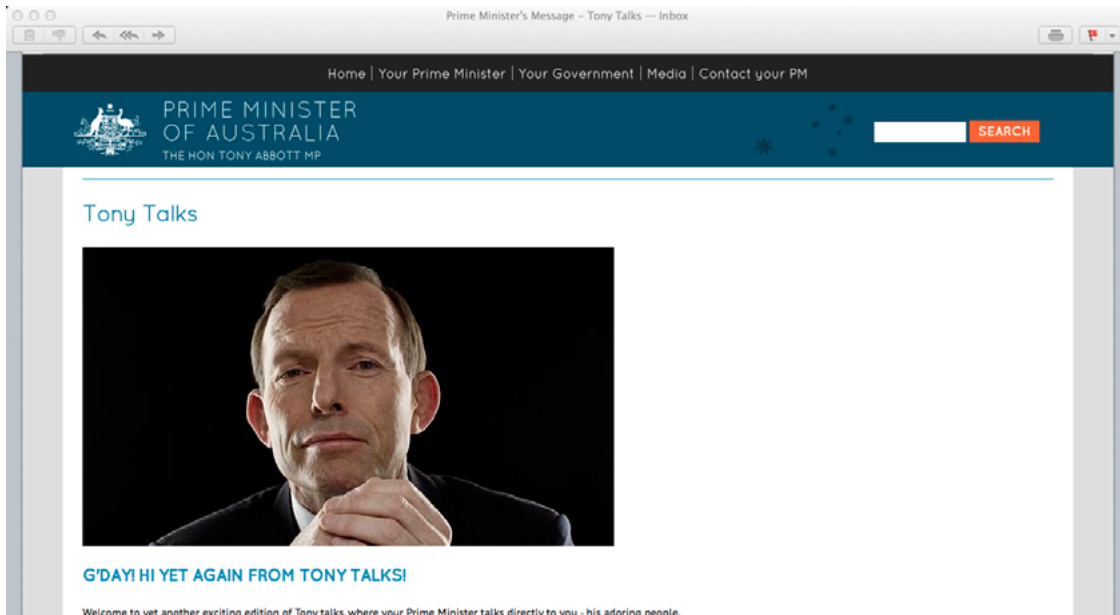


Figure 1. Spear Fishing Spoof Email - Looks like the real thing

WHY IMITATE WHEN YOU CAN BE REAL?

To pretend to be the real thing in both examples above the trick is to use the real site links throughout, and same formatting, style sheets, etc. In the above we have a text file called “message_header.txt”, and this is piped into the .eml file, so to emulate the official Australian Prime Ministerial communications a header like the following – copied from the actual site – is used.

Listing 2. Code Example

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML+RDFa 1.1//EN">
<html lang="en" dir="ltr" version="HTML+RDFa 1.1"
xmlns:content="http://purl.org/rss/1.0/modules/content/"
xmlns:dc="http://purl.org/dc/terms/"
xmlns:foaf="http://xmlns.com/foaf/0.1/"
xmlns:og="http://ogp.me/ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:sioc="http://rdfs.org/sioc/ns#"
xmlns:siocct="http://rdfs.org/sioc/types#"
xmlns:skos="http://www.w3.org/2004/02/skos/core#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
<head profile="http://www.w3.org/1999/xhtml/vocab">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="dcterms.type" content="Text" />
<meta name="dcterms.format" content="text/html" />
<link rel="shortcut icon" href="http://www.pm.gov.au/sites/all/themes/gamburra/favicon.ico"
type="image/vnd.microsoft.icon" />
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, minimum-scale=1,
user-scalable=no" />
<link rel="schema.AGLSTERMS" href="http://www.agls.gov.au/agls/terms/" />
<meta name="dcterms.creator" content="Department of the Prime Minister and Cabinet" />
<meta name="generator" content="Drupal 7 (http://drupal.org)" />
<meta name="description" content="On 18 September 2013, the Hon Tony Abbott MP was sworn in as
Australia's 28th Prime Minister." />
<link rel="canonical" href="http://www.pm.gov.au/" />
...
<title>Prime Minister of Australia | The Hon Tony Abbott MP</title>
<style type="text/css" media="all">@import url("http://www.pm.gov.au/modules/system/system.base.
css?muh4hk");
```

```
@import url("http://www.pm.gov.au/modules/system/system.menus.css?muh4hk");
@import url("http://www.pm.gov.au/modules/system/system.messages.css?muh4hk");
...
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/modules/contrib/jquery_update/
replace/jquery/1.7/jquery.min.js?v=1.7.1"></script>
<script type="text/javascript" src="http://www.pm.gov.au/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://www.pm.gov.au/misc/drupal.js?muh4hk"></script>
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/modules/contrib/admin_menu/admin_
devel/admin_devel.js?muh4hk"></script>
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/modules/contrib/panels/js/panels.
js?muh4hk"></script>
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/modules/contrib/views_slideshow/js/
views_slideshow.js?muh4hk"></script>
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/libraries/flexslider/jquery.
flexslider-min.js?muh4hk"></script>
<script type="text/javascript" src="http://www.pm.gov.au/sites/all/modules/contrib/google_analytics/
googleanalytics.js?muh4hk"></script>
<script type="text/javascript">
...
<link href='http://fonts.googleapis.com/css?family=Quicksand:400,300,700|PT+Sans:400,700,400italic,700i
talic' rel='stylesheet' type='text/css'>
</head>
<body class="html front not-logged-in page-homepage homepage">
<div id="skip-link">
<a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
</div>
<div class="page clearfix" id="page">
<header id="section-header" class="section section-header">
<div id="zone-menu-wrapper" class="zone-wrapper zone-menu-wrapper clearfix">
```

...Note that all of the links in the above are the original links. Clicking on those links connects to the real web site. Hovering over an image brings up the name of the original site in the URL.

In the case above, the entries are all real, but in the email I am aiming to trick someone into clicking on a link or calling a phone number, so I add a "<div>" between the real ones where I can add my spoof section. Only in here are the links not referring to the real web site for the Australian Prime Minister. In the case above a particular picture and message are embedded.

Listing 3. Code Example

```
<div class="TonyTalks">
<hr/>
<h2>Tony Talks</h2>

<p><h3><strong>G'day! Hi again from Tony Talks!</strong></h3></p>
<p></p>
<p>Welcome to another edition of Tony talks, where your Prime Minister talks directly to you - the
people.</p>
<p></p>
```

...At the end of the section I add a phone number to call and a link, but what the link says is a real link is in fact the real one, but it is best to make it look like one similar to the real one.

```
<strong>Do you have a comment on this message?</strong>
<a href="http://pm.au.gov.net/feedback">Feedback</a>
```

This does have the problem of being picked up by intrusion detection and can be blacklisted. Sometimes it is better to include a phone number, which does not suffer from this potential issue, as in the silver

surfer broadband phishing attempt. Tell the caller the message will be recorded and identity will be requested so they know what to expect, again lulling the entrapped individual into a false sense of security.

```
<strong>Call our helpline to give feedback: 0410 999999</strong>
```

```
<strong>Note details of all voters must be recorded for quality purposes. Your will be asked to confirm your identity</strong>
```

SENDING THE MESSAGE

To send the message it is important to send the message through a legitimate server. Normally, this entails using a server that has an SSL certificate assigned to it, and having the appropriate setup in the sendmail/postfix “main.cf” (assuming a Linux/Unix base) e.g.

```
relay_domains = pm.gov.au
```

and if possible it should be passed through another legitimate server. This all adds up to being trusted by the receiving SMTP server.

WHAT HAVE WE LEARNED?

The key to phishing attacks is simple. It comes down to sociology – research your victims to find out what puts them at ease; and psychology – what will make them want to make contact. It is important that the chosen message appears to be from someone they trust and would expect to contact them, and that the message is of high quality throughout. Referring as much of the message as possible back to the original web site helps bring about the trust and makes the site appear to be legitimate.

ABOUT THE AUTHOR

Colin Renouf is long standing IT worker, inventor, and author; currently an Enterprise Solution Architect in the finance industry, but having worked in multiple roles and industries over the period of decades. An eternal student, Colin has studied varied subjects in addition to IT. Having written and contributed to several books and articles on subjects ranging from architecture, Java, and security; he is even referenced on one of the most fundamental patents in technology. Colin has two incredibly smart and intelligent children, and spends most of his time in his favourite country – Australia (the land of the free thinker and good food) – trying to contribute to the well being of society. He looks to his awesome and perfect best friend Sally for inspiration, without whom he would probably be unable to survive; and can only thank wonderful ladies like Lana, Taina, Hellena and Sandra for the immense beauty they bring to world. Lana, I said I'd dedicate the article to you for being so special and kind, and I do – thank you for your perfect smile that brightens my day. Ladies – I wish you could all see how special you are through my eyes. To the haters I simply ask – why? What more is there to say, but thank you Red Bull.

a d v e r t i s e m e n t

IT-Securityguard

Lets secure IT



Android Vulnerability Scan



Web Penetration testing



Secure hosting

contact: contact@it-securityguard.com

www.it-securityguard.com

COULD REAL-TIME EFORENSICS BE

THE ANSWER TO CYBERSECURITY AND ANALYTICS?

by Larry Karisny

eForensics may be more than a good name for a magazine. Understanding what digital forensics does in real time may be the holy grail of cybersecurity. The information technology security industry explains cybersecurity in terms of complex algorithms or virus detection systems that only a scientist or software developer can understand. In reality what cybersecurity really is just the authenticated use of validated causal actions taking place in a predetermined process that is used to accomplish specific results.

Cybersecurity is achieved when these action and processes are authenticated, viewed, analyzed, audited, activated or blocked in real time during data in motion. If we can do this we will be secure. We are not doing this today. With the ever increasing demand of security in ever increasing digitally intelligent world it may be time for paradigm shift if we are to reach true cybersecurity. It maybe time for real-time eForensics.

THE SEEN OF THE CRIME

Most of us are familiar with forensics in the evaluation of a crime scene. There was a criminal incident that occurred and a team of forensic analysts come in to gather information that might lead to solving the crime. eForensics today is no different. A hack has occurred and a team of specialist sift through mounds of data, software, hardware, processes and people to determine how the systems processes have been breached.

The commonality of both these forensic approaches is that they are both reviewing historical information and using tools and techniques that can analyze these historical incidents. These historical forensic approaches can in time possibly solve the crime or cyber breach but neither of these approaches can stop the crime or the hacker in advance.

The current cybersecurity methodologies using passive process monitoring are proving to be the wrong place and the wrong time in attempts to

achieve system cybersecurity and intelligence analysis. To accomplish information technology security and intelligence we need to focus on technologies that stop and analyze information technology processes real-time during data in motion. This is where a technology paradigm shift needs to occur in the cybersecurity industry and real-time eForensics can accomplish this.

CAN OUR CURRENT CYBER SECURITY AND ANALYTIC TECHNOLOGIES KEEP UP?

Increased varieties of connected devices are being added daily to our already complex intelligent world. Unfortunately these intelligent technologies are being released by the millions at the cost of increasing cybersecurity threats while using complicated digital intelligence analysis techniques that are neither effective nor can keep up with the amount of data input these system devices and software produce. Cybersecurity experts are beginning to realize that current passive process monitoring using historical data aggregation and database analytics techniques are no longer efficient or effective methodologies for cybersecurity and system intelligence.

Current approaches fail due to the inability to secure or properly analyze the many real-time messaging application actuaries that occur in our increasingly complex digital intelligent system processes. The current historical passive security and analytical technologies only tell what might have happened after the causal action has occurred not what did happen. Monitoring active process causal actions in the process tell what actually is happening in real-time during networked data in motion which is where the point of new security and process analytics need to occur.

As we are increasingly connecting and interconnecting our digital intelligence in the forms of software, hardware, apps and now Internet of Things (IoT), These casual actions multiply making the process more complex and difficult to track. While these interconnected technologies continue to be leveraged in digital intelligence we are losing control of the where and when point of causal actions that are actually occurring in the system processes. This is point where securing and analyzing causal actions and processes need to be secured and analyzed. We are not doing this today.

LOSING CONTROL OF DIGITAL INTELLIGENCE AND CYBERSECURITY

We have reached a point in intelligent operation complexity that even trained operators are not sure what the digital control systems actuators are actually initiating what actions in the process. We are losing control between human to machine and machine to machine system processes while we increasingly inter-connected software, cloud and IoT application messages that in many cases are not secured, audited or even seen in the system process.

Causal messages are constantly being sent in real-time during data in motion in these complex system processes and can be exploited to manipulate the process results. Hackers know this and are successfully targeting and exploiting these weaknesses affecting every individual and every industry that uses digital intelligence in their information technology processes. Hackers have already attacked cars, homes, business process systems, factory control system and critical infrastructure control systems by manipulating the causal messaging action within these system processes.

THE DANGER OF ALGORITHMS AND ANALYTICS IN CYBERSECURITY

For years we have had a false sense of security that was built around mathematical algorithms. This is what the encryption Intrusion Detection System (IDS) security has been based on for years. Recent disclosure of the NSA's involvement of the control and release of these encryption algorithms and their direct relation with RSA has caused the loss of considerable trust in cybersecurity industry. This combined with weaknesses found that were not able to be disclosed caused a boycott of major encryption scientists in the last RSA conference. The encryption games are over and for many the use of encryption in security is no longer technically effective and certainly not trusted.

Intrusion Detection Systems (IDS) security technologies are no better off now admitting they can't stop denial of service attacks (DDoS) while sophisticated and aggressive cyber weapons like Snake and Stuxnet are now part of the arsenal of cyber war weapons with critical infrastructure as its main target. Analytic approaches are also showing their weakness in being used in process action discovery. They are having difficulty even understanding what all the big data means and could fall victims to subjective analyst methodologies to explain what the historical data means. Clearly if we are to secure and understand all these new intelligent actions in our control processes we need

new methods and even a new place confirming that these complex and layered control system actions are actually correct.

ADDING SECURITY WHILE ADDING INTELLIGENCE

Intelligent control systems are faced with a two edge sword of needing digital intelligence and securing this intelligence. They need the digital intelligence to assist in physical security and the monitoring complex process systems processes while also faced with making sure this digital intelligence can't be access or exploited by hackers. In critical infrastructure applications, such as the process control of a power grid, there is no room for error or good enough security. When you have machine to machine (M2M) IoT or cloud services sending actuary messages without human intervention, these system processes must be digital authenticated, viewed, audited and blocked in real-time data in motion in order to be effectively secured and analyzed.

Having focused in critical infrastructure cybersecurity for years, my many industry colleges and I have come to a similar conclusion. The cybersecurity and analytical methodologies used today are flawed and cannot achieve the stringent security requirements or the volume of analytical data needed to protected and understand our increasing complex and interconnected control system operations. In fact both Intrusion Prevention System (IPS) security and Intrusion Detection System (IDS) security methodologies are increasing showing security prevention and detection failures.

Current analytical approaches cannot even scale to address the billions of applications and terabytes of big data need to be evaluated in the increasing complex processes. We must deploy security technologies that can secure and understand the millions of causal events and interconnected causal events that take place in the control system process on the network. This can be done by using an active business process monitoring process firewall during on the network the data input data in motion point of digital intelligence transfer. This is where the beginning of a new paradigm shift is occurring and where real-time eForensics can be achieved.

THE PARADIGM SHIFT OF INTELLIGENT CYBERSECURITY

A recent MIT paper addressing both physical and digital security found that the current cybersecurity solutions focusing on securing data and networks are 50 year old technologies were really made for the electrical-mechanical processes and not the digital processes. Rather than focus on securing networks and data the study suggested that security must target at the causal action which is the true point of system security. The new approaches detect anomalies not meant in the causal action and system process. The difference in these approaches is determining at what point in the data in motion is the causal identified, secured and how it is analyzed.

Layer 7 Firewall is an active monitoring system on the network that secures the device against rogue applications (example: smartphone private information accesses by unauthorized apps.) OSI layer numbers are commonly used to discuss networking topics. A troubleshooter may describe an issue caused by a user to be a layer 8 issue. As the industry jokingly refers this as layer 8, in reality this human to system causal action event is where true authenticated application security must be achieved.

The layer 7 OS firewall can secure the application but there needs to be an additional message intelligence layer if we are to secure active live message applications that are continually active in the transfer of system intelligence. There are constant data in motion message actuaries that are constantly creating real-time causal action in a typical control system process. This is where things really get switch on or off and desired or undesired actions need to be authenticated viewed, audited, activated and blocked. This message application intelligence firewall needs to be placed at the data in motion flow of desired process not the end to end points of data transfer on the network. Securing data end points has been a main stay in cybersecurity for years but can no longer secure the billions of actuaries predicted in cloud and IoT systems.

THE INTELLIGENT CAUSAL ACTION FIX

Security companies are beginning to understand the importance of anomaly detection and its relationship to the system process. They all though have the same problem of using historical security and analyzing methodologies in detecting of the anomaly at the data output level. They use algorithms in the protection of the input to output data and then use analytics to determine the anomaly. The end

point of these methodologies are at the historical data output level and does not offer the security of digital intelligence or the analysis of the anomaly to take place during the real-time data in motion data input level.

After many years of work and research a patented anomaly detection approach from a company called Decision Zone has uniquely accomplished the ability to authenticate, view, audit, activate and block tera-bytes of real time digital intelligence in milliseconds at the input data in motion level. Today's security systems use a passive monitoring collection and aggregation data methodologies on the network and analyzes this information at the historical data output level. Decision Zone offers active application message monitoring on the network using graphical process rules and utilizing its patented causal inference engine. This new intelligent process layer firewall can protect the application infrastructure against any unauthorized causal action or system process.

This significant achievement by Decision-Zone offers a paradigm shift in cybersecurity methodologies by uniquely addressing security and system intelligence at real-time data in motion data input level. It doesn't not use historical data output or analytics to evaluate the anomaly which is currently allowing hacker a window of system exploit. It uses process logic mapping to validate the interactions of the multiple layers of causal action processes which allows it the ability to even detect human to machine and machine to machine causal action process errors.

If we are going to continue remove to human intervention from our control system processes while allowing layers of human to machine and machine to machine actions to occur in these systems, we must use a method to real time secure and analysis the casual events and the intelligence processes in the system. Decision Zone offers a unique data in motion application message firewall that can authenticate, view, evaluate, audit, activate and block any causal actions across any software, hardware, cloud or IoT platform. For a more thorough explanation of this capability see the presentation Layer 8 Process Firewall (L8PF) or go the decisionzone.com.

CONCLUSION

Spending years in the networking world I like many of my colleagues considered cybersecurity the protection of the end to end network and its data flow. This information transport has served us for many years but is now showing its weaknesses as does the IPS and IDS security technologies that are currently protected it. With everything today being about the cloud, the app and the IoT, we must apply new security methodologies to secure these growing and ever increasingly interconnected intelligent system technologies.

Hackers are exploiting the causal actions of the process and are manipulating message application system actions to their benefit. We must move the firewall from protection of the output data transport systems to the real-time data in motion data input level if we are to stop these cyber breach actions and achieve true cybersecurity and analytical system intelligence. The use of real-time eForensics in evaluating and security causal events and system processes are critical to the understand and security of digital intelligence today and in the future.

ABOUT THE AUTHOR

Larry Karisny is the director of ProjectSafety.org, a cybersecurity expert, advisor, consultant, writer and industry speaker focusing on security solutions for mobility, the smart grid and critical infrastructure.

CLOUD COMPUTING RISK ASSESSMENT

by Bryan Soliman

Cloud Computing is the use of multiple server computers via a digital network acting as one unit of storage. The 'Cloud' itself is a virtualisation of resources (network, servers, applications, data storage, and services) allowing on-demand access for the end user. These resources can be provided with minimal management or service provider interaction.

By 2014, Cloud Computing is expected to become a \$150 billion industry, and for good reason – whether users are on a desktop computer or mobile device, the cloud provides instant access to data anytime, anywhere there is an Internet connection. For businesses, Cloud Computing also offers myriad benefits, such as scalable storage for file, applications and other types of data; improved collaboration regardless of team members' locations; and saved time and money by eliminating the need to build a costly data center and hire an IT team to manage it.

Most businesses, however, have one major concern when it comes to Cloud Computing: Exactly how safe is the Cloud? Although most reputable Cloud providers have to-of-the-line security to protect users' data, experts say there is no such thing as a completely safe Cloud system.

This article discusses the risk assessment of the Cloud Computing technology and the impact of such technology on businesses, privacy and private and public IT Jobs. The article also exposes the benefits and challenges of Cloud Computing.

INTRODUCTION

Cloud Computing is a phrase used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, Cloud Computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time.

The term "Cloud" is essentially a metaphor for the Internet. Marketers have further popularized the phrase "in the Cloud" to refer to software, platforms and infrastructure that are sold "as a service" (i.e. remotely through the Internet). Cloud Computing relies on sharing of resources to achieve coherence and economies of scale, similar to electricity grid over a network. At the foundation

of Cloud Computing is the broader concept of converged infrastructure and shared services, and as such; the technology focuses on maximizing the effectiveness of the shared resource. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. For example, a Cloud Computer facility that serves European users during European business hours with a specific application may reallocate the same resources to serve North American users during North America's business hours with a different application. Such approach allows maximizing the use of computing powers and also reducing environmental damage.

The term "Cloud Computing" is mostly used to sell hosted services in the sense of application service provisioning that run client server software at a remote location. Such services are given popular acronyms such as 'SaaS' (Software as a service), 'PaaS' (Platform as a service), 'IaaS' (Infrastructure as a service), 'HaaS' (hardware as a service) and finally 'EaaS' (everything as a service). End users access Cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. One key question to consider when chooses the Cloud Computing solution is: Which of the three cloud models will you use?

- **Public Clouds** – are multitenant architectures that provide pay-per-use, scale-on-demand benefits, along with standardized configurations, security protections, and services levels- but little customization. They are most suitable for temporary or unpredictable demand, rapid development projects, and situations in which multiple environments are needed.
- **Private Clouds** – are built exclusively for multiple business units or functions within single organization, which controls and configures the cloud's infrastructure, security and capacity. They are a good choice when sufficient demand exists to set up an internal infrastructure that offers the same benefits as a public cloud.
- **Hybrid Clouds** – features the functionality of a public Cloud, while offering the security and control of internally hosted environments. They are most suitable for highly integrated applications that have a shared production environment, applications, that need temporary capacity, or applications that required multiple configuration or massive computing power.
- **Community Clouds** – The Cloud infrastructure is shared by several organizations and supports a specific community that has common interests (e.g. mission, industry collaboration, or compliance requirements). It might be managed by the community organizations or a third party and could exist on or off the premises.

While the benefits of the Cloud Computing is quite obvious, there are legal and reputational risks that any business needs to understand, and as such; organizations need to ask the following questions before implementing such solution:

- Does the service provider meet your required standard of privacy?
- Are there procedures in place to keep your data secure?
- What is the risk your data could be lost or not given back?

Is your data made available to others for tracking or advertising purposes? Privacy Responsibilities and Considerations is a series of tip sheets prepared by the Office of the Privacy Commissioner of Canada and Offices of the Information and Privacy Commissioners of Alberta and British Columbia and it can be found via following link: http://www.priv.gc.ca/information/pub/gd_cc_201206_e.asp – These documents provide insightful information on the advantages, risks, and legal obligations that come with Cloud services.

THE CHALLENGES OF CLOUD COMPUTING

DATA LOCATION

Cloud Computing technology allows Cloud servers to reside anywhere, thus the enterprise may not know the physical location of the server used to store and process their data and applications. Although from the technology point of view, location is least relevant, this has become a critical issue for data governance requirements.

DATA SECURITY AND PRIVACY

Application sharing and multi-tenancy of data is one of the characteristics associated with cloud computing. Although many Cloud Service Providers (CSPs) have multi-tenant applications that are secure, scalable and customizable, security and privacy issues are still often concerns among enterprises.

The most pervasive fear about cloud computing is the risk of compromising data security and privacy. The reality is that vendor responsibility for security and privacy is limited to the infrastructure provided; at the application-level, you are responsible for security and privacy. Unlike a data center, which is run by an in-house IT department, the Cloud is an off-premise system in which organizations outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture however, is that organizations are trusting their data for someone else to look after, and the downside is that organizations are abrogating responsibility for data, and accordingly, someone else has access to it, and someone else is responsible for keeping it safe.

Although Cloud providers may ensure your data is safe, some are not always looking after your best interests. No business is ever going to be as extreme about looking after your data as you would or should be. Cloud providers are in the business of making money from you, after all, and securing your data sometimes becomes a marketing mantra more than a way of life.

CLOUD SECURITY POLICY/PROCEDURES TRANSPARENCY

Some CSPs may have less transparency than others about their information security policy. The rationalization for such difference is the policies may be proprietary. As a result, it may create conflict with the enterprise's information compliance requirements. The enterprise needs to have detailed understanding of the service level agreements (SLAs) that stipulate the desired level of security provided by the CSPs.

CLOUD DATA OWNERSHIP

In the contract agreements it may state that the CP owns the data stored in the Cloud Computing environment. The CSP may demand for significant service fees for data to be returned to the enterprise when the Cloud Computing SLAs terminates.

LOCK-IN WITH CSP'S PROPRIETARY APPLICATION PROGRAMMING INTERFACES

Currently many CSPs implements their application by adopting the proprietary APIs. As a result, Cloud services transition from one CSP to another CSP, has become extremely complicated, time-consuming and labor-intensive.

COMPLIANCE REQUIREMENTS

Today's cloud computing services; can challenge various compliance audit requirements currently in place. Data location and, Cloud Computing security policy transparency are all challenging issues in compliance auditing efforts. A good example of the compliance requirements including privacy, *Payment Card Industry* (PCI) requirements, and financial reporting laws.

DISASTER RECOVERY

It is a concern of enterprises about the resiliency of Cloud Computing, since data may be scattered around multiple servers and geographical areas, it may be possible that the data for a specific point of time cannot be identified. Unlike traditional hosting, the enterprise knows exactly where the location is of their data, to be rapidly retrieved in the event of disaster recovery. In the Cloud Computing model, the primary CSP may outsource capabilities to third parties, who may also outsource the recovery process. This will become more complex when the primary CSP does not ultimately hold the data.

COMPATIBILITY AND STANDARDIZATION

Many Cloud infrastructure runs on common standardized platforms, but server management is often performed using the vendor platform's application programming interfaces (APIs). The more complex the application, the more complex the APIs can become, and the more difficult it can be to move to a new provider or bring the application back in-house, thereby creating lock-in situations for many organizations.

What makes a Cloud "safe"? A provider could have the latest security features, but due to the general lack of Cloud standardization, there are no clear-cut guidelines unifying Cloud providers. Further, given the flooded implementation of Cloud services in different sectors, it becomes problematic for users when determining exactly how "safe" their Cloud really is.

The question of how safe the Cloud is has many sides, and the answer depends on the Cloud services provider, the type of industry an organization is in, and the accompanying regulations concerning the data it is considering storing in the Cloud. Since not all Cloud providers are build the same, one provider's definition of "safe" may not be the same as another's.

COMMERCIAL VIABILITY

The ROI of the Cloud Computing may look attractive, but if not managed carefully, it can turn negative. At first, transition costs and run rates can seem low, but depending on how applications consume memory, storage, processing power, support, and bandwidth, their costs can quickly escalate.

Many Cloud service providers are relatively young companies; hence the projected longevity and profitability of the Cloud services are unknown. Cloud Computing service providers might eventually go through a consolidation period, and as a result, CSP customers might face operational disruption or suffer the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions.

AVAILABILITY AND RELIABILITY

It is important to recognize that Cloud providers guarantee infrastructure and access, but not the reliability of the underlying architecture of customers' applications. Also, data stored in the Cloud is not necessarily available everywhere.

NETWORK DEPENDENCY

Cloud Computing is dependent on the Internet. The most basic drawback of Cloud Computing is fact that users to such technology need connection to access the cloud and this direct tie to the Internet means that this system is prone to outages and service interruptions at any time. This could occur in the middle of a task or transaction, meaning the action could be delayed or lost entirely if time sensitive.

CENTRALIZATION

In Cloud Computing, network dependency is a drawback due to outages. Centralized data can certainly add another risk to Cloud Computing, if the provider's services go down, all clients are affected.

DATA INTEGRITY/SECURITY

There is already a huge risk with data hosted in-house, thus no secret that data offsite sits at even high risk. With data offsite, more avenues for attack and the fact that it will be travelling more makes it easier to be intercepted. With technology always improving, there are ways to make sure of better encryption. However, with technology always improving, there are always people out there improving their hacking skills.

CYBERATTACKS

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the Cloud, where volumes of data are stored by all types of users on the same Cloud system. The scary part of the Cloud is the vulnerability to Distributed Denial of Services (DDoS) attacks and the concentration of so much data represents a great problem since the Cloud represents a single point of failure (i.e. if something goes bad it impacts a very wide group of people, and for hackers, it's always better to steal and disrupt in bulk).

INSIDER THREATS

Just as cyberattacks are on the rise, so are security breaches from the inside. The Edward Snowden breach at the NSA is a wake-up call that the most serious breaches are due to insider threats and privileged user access. Once an employee gains or gives others access to your Cloud, everything from customer data to confidential information and intellectual property are up for grabs. The Cloud makes this problem 10 times worse since administrative access to the Cloud management platform, either by an employee or an attacker posing as an employee, enables access to copy and steal any virtual machine, undetected as well as potentially destroy the entire Cloud environment in a matter of minutes.

GOVERNMENT INTRUSION

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data, government entities and technology companies anywhere in the world may be inspecting your data as it is transmitted or where it resides in the Internet, including within Clouds.

LEGAL LIABILITY

Risks associated with the Cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against any organization. The latest risks of using Cloud for businesses are compliance, legal liability and business continuity. Data breach incidences are on the rise, and so are

lawsuits. While the Cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures. Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security, and the more you have of one, the less you have of the other.

LACK OF SUPPORT

Imagine being unable to access your Cloud before a big meeting, or, worse, being in the middle of a cyberattack that has taken down your entire bread and butter – your website. Now, imagine trying to contact your provider, only to find that their “Customer Services” is nonexistent. While some Cloud providers have excellent customer support, others could leave you in the cold.

The most frustrating thing when something goes wrong is not being able to speak directly with an engineer; and most Cloud providers specializing on compliant Cloud hosting. If the organization supports mission-critical systems, or having online presence is critical for business to operate smoothly, organizations have to be prepared to invest in a Cloud and Cloud provider that is capable of providing a level of protection commensurate with organizations’ needs.

THERE’S ALWAYS A RISK

The biggest risk when it comes to Cloud Computing is that organizations never know what is up ahead. Hackers have been around from the start, and they are not going anywhere any time soon, and as technology advances, so do the risks that come with adopting them.

Given these current and future dangers, do the benefits of Cloud Computing outweigh its risks? It depends on the business, the Cloud is not for everyone, and like with all solutions, organizations have to weigh what level of risk such organizations are comfortable dealing with. Even the biggest and best Cloud services can be dismantled due to service interruptions, attacks or some miscellaneous issue with the vendor. Cloud services haven’t been around long enough for analysts to have come up with a predictable, clear model of all the possible risks, the likelihood of those risks being realized, the probability of security failures and how much, if at all, these might negatively affect customers.

CLOUD SOLUTION PRICING PREDICTABILITY

Many CSPs offer a pay-as-you-go pricing model, which makes calculation the cost of the Cloud services appear simple. However, the ability to determine the return on investment a few years down the road is encumbered or hindered by Cloud Computing’s limited existing price trending history on which to base calculations. For example, can organizations’ management predict whether the prices of Cloud solutions will rise or fall in the future? How long will the current pricing of Cloud services remain in effect? Are caps on pricing increases stipulated in contracts?

LEGAL AMBIGUITY ABOUT DATA JURISDICTION

An organization may be subject to multiple legal jurisdictions, depending on where the organization resides, the location of the Cloud infrastructure, and where data is stored. Organizations’ management should consult with legal counsel to determine the related risks and challenges of complying with applicable laws if Cloud Computing solutions where to support some or all of the organization’s processes. Some of the legal aspects of Cloud Computing that should be considered include:

- In what country is the data stored when the CSP’s solution is in use?
- To what legal jurisdiction are the data and systems subject? Are there multiple jurisdictions?
- If the CSP stores data in a country different from the country of the organization and the organization’s customers, what are the legal implications, and what are the organization’s legal rights if a foreign court subpoenas the organization’s or its customers’ data?
- If a legal authority subpoenas the data of the organization’s CSP or the data of a fellow Cloud tenant can the organization’s data be separated or isolated from the data that’s being confiscated?
- What tax jurisdictions govern any transaction processing that is taking place?
- If a law enforcement agency sees the CSP’s server in its legal jurisdiction and it contains data about the organization’s customers in a different legal jurisdiction, would the organization be violating the legal rights of its customers (and related data protection laws) for storing customers’ records in a public or hybrid Cloud solution in the first place?

I would like to point out that many of the risks highlighted in the above points are not likely to be mitigated by contractual clauses with a CSP (assuming the contract is even negotiable – most commodity Cloud contracts are not). As Such; all of the Cloud Computing risks discussed above should be given careful consideration as the materialization of any of these risks will present very undesirable consequences.

An organization should recognize the risks and other effects Cloud Computing can have on its operating environment, and the need to expend a great amount of effort to analyze Cloud Computing risks and perform the related due diligence may be counterintuitive. Consequently, management could neglect to perform time-consuming steps such as confirming compliance with legal or regulatory requirements or evaluating the potential impact of the CSP on the organization's operations and risk profile.

It is paramount that management also understands that with most Cloud solutions (with the possible exception of an internal private Cloud) the organization has less direct control of the solution and consequently a higher level of inherent risk. For example, an organization using Cloud Computing has shifted responsibility for some or all of its IT functions, including controls to a third-party provider. As such; organizations' management should evaluate the Cloud deployment and delivery models in the context of acceptable risk levels as this will determine the preferred type of Cloud Computing environment and related requisite controls.

In many Cloud scenarios, the organization no longer has complete or direct control over technology and technology-related management processes. Management must determine if it has the risk appetite for potential events associated with a given Cloud solution as some of these events extend beyond the organization's traditional borders and include some events that have an impact on the CSP supporting the organization.

As organizations' management contemplates its Cloud Computing position and strategies, it should address some of the following key questions:

- Does the organization anticipate rapid growth that might require using Cloud solutions?
- Is the organization is a mature market that might require using Cloud Computing to save costs to remain competitive?
- Are the organization's operational functions and processes mature and formalized enough to allow for a change in the underlying technology platform?
- What is the capability and maturity of the organization's current IT function?
- Should Cloud Computing be embraced to capitalize on its benefits, or rejected to avoid risks such as data breaches or noncompliance with complex requirements?
- How can the organization manage its risks adequately while operating in a business environment with Cloud Computing?

IS THE CLOUD SECURE?

The potential of the Cloud is clear: transforming IT from cost center to business engine. It promises the agility and scalability that tech dreams are made of. By leveraging the Cloud, you can complete typical IT tasks in hours rather than weeks or months, allowing you to dedicate staff to innovation, not just maintaining systems and infrastructure.

However, reduced costs and increased flexibility don't come without costs. Security is always a concern when sensitive data is involved, and that concern is heightened when it comes to Cloud services that sit outside the corporate firewall.

Security in the Cloud is of paramount importance where massive databases are attractive to cybercriminals, and Internet services have proven to be difficult to protect. Organizations must protect personal information with safeguards appropriate to the sensitivity of the information they handle. Tools such as Privacy Impact Assessments (PIA) or Threat Risk Assessments (TRA) could be valuable to help make assessments of safeguards. In order to ensure that personal information is protected, organizations using Cloud Computing services should:

- Limit access to the information and restrict further uses by the provider. Do not assume that the provider's general terms of services or policies will be adequate to establish such restrictions.
- Ensure that the provider has in place appropriate authentication/access controls. The level of authentication should commensurate with the risk to the personal information being protected.

- Manage encryption. Determine if the encryption method is adequate and the access to encryption keys is properly managed.
- Ensure that there are procedures in place in the event of an outage to ensure business continuity and prevent data loss.
- Ensure periodic audit are performed. It is important for an organization to have some measure of oversight over a Cloud provider's policies and practices.
- Have an exit strategy. Ensure the termination procedures permit the transfer of personal information back to the organization and require that the Cloud provider securely delete all personal information within reasonable and specified timeframes.

While online data storage services claim your data is encrypted, there are no guarantees. With the recent revelations that the federal government taps into the files of internet search engines, email and Cloud services providers, any myth about data "privacy" on the Internet is definitely illusion. Experts say there's simply no way to ever be completely sure your data will remain secure once you've moved it to the Cloud.

While providers of email, chat, social network and Cloud services often claim (as stated in their services agreements) that the day they store is encrypted and private, most often they're the ones who hold the encryption keys. That means a rogue employee or any government "legally" requesting encryption keys can decrypt and see your data.

Even when service providers say only customers can generate and maintain their own encryption keys, there's no way to be sure that others won't be able to gain access or decrypt these keys.

Freedom of Information Act requests by the American Civil Liberties Union (ACLU) revealed that the U.S. government claims the right to read personal online data without warrants. Governments seem to believe that if data is recorded and available, they should be able to access it. In addition it is also true that Internet giants such as Google, Microsoft, and Yahoo have for years been handing over data in response to government requests. Think about possible points of entry for an attacker in a Cloud environment through the following scenarios:

- A customer uses an insecure mobile phone to access your network... you can be attacked.
- A contractor on your network uses a web application that has an embedded vulnerability, a back door that is not protected... you can be attacked.
- A database administrator at the cloud provider shares a password with someone... your data can be breached.

The above represent just some of the scenarios that keep the chief information security officer awake at night.

Securing the security perimeter of the traditional data center was made relatively straightforward with the help of firewalls and intrusion detection systems. When we traded terminals for PCs, anti-virus software helped keep those devices safe. With employees, customers, business partners, suppliers and contractors increasingly accessing corporate applications and data with mobile devices from the Cloud, protecting the edge of the network is no longer enough. As the traditional perimeter disappears, securing such technology becomes very difficult goal to reach in various cases.

The CSA (Cloud Security Alliance) has identified "The Notorious Nine", the top nine Cloud Computing threats for 2013. The report reflects the current consensus among industry experts surveyed by CSA focusing on threats specifically related to the Shared, on-demand nature of Cloud Computing:

DATA BREACHES

CSA pointed to a research paper describing how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of information, if a Cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other client's data as well. The challenge in addressing these threats of data loss and data leakage is that "the measures you put in place to mitigate one can aggravate the other" according to the report. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data and if you opt to keep offline backup of your data to reduce data loss, you increase your exposure to data breaches.

CLOUD COMPUTING ENVIRONMENT

A malicious hacker might delete a target's data out of hostility or you could lose your data to a careless Cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting your data to ward off theft can backfire if you lose your encryption key. You could also get into hot water with the feds if you're legally required to store particular data to remain in compliance with certain laws, such as HIPAA.

ACCOUNT OR SERVICE TRAFFIC HIJACKING

Cloud Computing adds a new threat to this landscape, according to CSA. If an attacker gains access to your credentials, he/she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. According to CSA, organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible.

INSECURE INTERFACES AND APIS

IT admin rely on interfaces for Cloud provisioning, management, and monitoring. APIs are integral to security and availability of general Cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services, and as such; introduces the complexity of the new layered API, it also increases risk, as organizations may be required to relinquish or hand over their credentials to third parties in order to enable their agency. Weak interfaces and APIs can expose an organization to such security issues pertaining to confidentiality, integrity, availability and accountability.

DENIAL OF SERVICE ATTACK (DOS)

DoS has been an Internet threat for years, but it becomes more problematic in the age of Cloud Computing when organizations are dependent on the 24/7 availability of one or more services. DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, such attack may still cause so much processing time that it becomes too expensive for any organization to run, and will be forced to take the service down.

MALICIOUS INSIDERS

Such threat can be initiated by a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. In an improperly designed Cloud scenario, a malicious insider can create even greater devastation. In situations where a Cloud services provider is solely responsible for security, the risk is great. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

CLOUD ABUSE

Malicious attackers use Cloud servers to launch a DDoS attack, propagate malware, or share pirate software. The challenge here is for Cloud providers to define what constitutes abuse and to determine the best processes for identify it.

INSUFFICIENT DUE DILIGENCE

That is, organizations embrace the Cloud without fully understanding the Cloud environment and associated risks. For example, entering the Cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if an organization's development team isn't sufficiently familiar with Cloud technologies as it pushes an app to the Cloud.

SHARED TECHNOLOGY VULNERABILITIES

Cloud service providers share infrastructure, platforms, and application to deliver their services in a scalable way. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. If an integral components gets compromised that represents a shared platform component, or an application, it exposes the entire environment to a potential of compromise and breach.

The effect of the growing dependence on Cloud Computing is similar to dependence on air transportation, which forces us to trust organizations over which we have no control, limits what we can

transport, and subjects us to rules and schedules that wouldn't apply if we were flying our own planes. Trusting Cloud Computing security is very much like trusting the telephone company or Gmail, or even the post office to keep your communications private. Some of the questions that should be raised when Cloud services are in the process to be implemented with any organization are:

- How is data encrypted, both in use and at rest, when stored in the Cloud infrastructure?
- Are fine-grained access controls in place?
- How well are web applications protected?
- How much of the Cloud infrastructure is redundant?

There's increasing pressure on organizations to have services in the Cloud, and the only way really to manager some of the risk in the Cloud is with Cloud security services. As organizations move services from their data centers into the Cloud, not only do they want their security services there, but they want those security services to emulate other Cloud offerings which definitely has an impact of the cost and the hidden costs of such services.

THE IMPACT OF CLOUD COMPUTING ON IT JOBS

Many jobs will change because of Cloud Computing. Some job roles will likely be reduced demand, some will have more demand, and even some new jobs will be created – both within and outside of IT. The following are some prediction to these job roles:

JOBS WITH REDUCED DEMAND

There are unfortunately, some jobs in the IT industry that are predicted to have less demand in the future, now that organization are moving their systems to Cloud services. The main advantage of Cloud Computing is the ability to scale hardware and software as required by organizations, by an external Cloud provider – resulting in quicker implementation times and less cost. This means there will be less demand or jobs such as “System Administrators” and “Database Administrator”. Professionals with these skills would likely be in demand from Cloud providers, rather than the organizations using the system. The pre-Cloud Computing method was to have locally or internal systems and servers, which were managed by internal staff or contractors. With Cloud Computing; the internal servers are no longer needed, since they can be supplied by Cloud providers. Also, much of the help desk support functionality will be moved over to Cloud providers and in lower numbers since they would be responsible for a wider range of organizations on centralized infrastructure.

JOBS WITH CONTINUED DEMAND

There will be still demand for IT Project managers. Their knowledge will need to include concepts of Cloud Computing and how it can impact the projects they work on. Business analysts will also be in demand. Organizations will need software and systems that reflect their requirements and business processes. The business analysts will also need to expand their knowledge so they know how to include Cloud-related services and software in their roles. Software developers should also continue to be in demand. Software will still need to be created. Data Integration jobs will increase in demand because the use of multiple Cloud-based vendors that must be integrated into a cohesive data model. Technologies with a deep understanding and working knowledge of private and hybrid clouds will be in high demand as large organizations try to implement Cloud-based technologies inside their data centers. Infrastructure specialists will also be in high demand because of the increased need to move data in and out of the data center and the high availability and throughput that are required to reduce the latency inherent in Cloud-based applications. There will also be an increased need for highly skilled security specialists because increased Cloud vendors means more openings through organizations' firewalls and potentially the need for manual procedures to manage user access to Cloud-based applications.

NEW JOBS CREATED

Several studies, including one article published by Forbes, stated that many new jobs will be created as a result of the Cloud. People working at Cloud providers will need to skills to be able to communicate with organizations that provide services for and provide information to – this will require the rare blend of relationship management and technical knowledge. One of the more common roles that have appeared is that of a Cloud architect. Similar to an enterprise architect, a Cloud architect is someone who has knowledge of Service-Oriented Architecture (SOA) and Cloud concepts, as well as enterprise architect skills.

Finally, the bad news is that ready-to-use Cloud-based applications will reduce the number of programmers needed within IT. The good news is that someone is needed to build all of these ready-to-use

Cloud-based applications and this is where the programmers come in. As a result, there will be a shift in demand for programming professionals from IT organizations to Cloud-based software vendors. With demand for programmers with the Cloud software vendors, will also required the need for additional business analysts, infrastructure specialists, projects managers, testers, and other related technical professionals. Besides the traditional IT job roles that Cloud will affect, it will also create some new opportunities, even for non-IT professionals. A marketing professional who knows how Cloud can help in a new product development or campaign will be able to take advantage of that and leverage business opportunities.

HIDDEN COSTS OF CLOUD COMPUTING

The business case for Cloud is compelling. Even after all the numbers for the obvious things get crunched, one has to ponder what “gotchas” could result in higher costs than originally planned. Business interruptions, outages, poor performance, or issues with service availability are obvious risks that can increase costs, but there’s an even more insidious set of issues that Cloud drive up costs.

Some of these hidden costs were explored in a survey of 486 CIOs, conducted by Research In Action and underwritten by Compuware Corporation. The study found that the majority of CIOs (79%) actually think a lot about potential hidden costs, and what they may mean to the business. From a management perspective, the top Cloud Computing concerns are:

- Poor end user experience due to performance bottlenecks (64%). This goes right to the customer end-user experience.
- The impact of poor performance on brand perception and customer loyalty (51%).
- Loss of revenue due to poor availability, performance, or troubleshooting Cloud services (44%).
- Increased costs of resolving problems in a more complex environment (35%).
- Increased effort required to manage vendors and services level agreements (32%).

The above is a cost driven factors and these costs are difficult to quantify and measure. An outright outage or system failure is easy to quantify, and can be relatively simple to address. However, a slowdown or partial glitch somewhere in the process is more challenging and can eventually add up to real money lost.

The survey also finds that 73% of organizations are still using outdated, or even manual, methods to track and manage Cloud application performance. The most common metric used to track application performance in the Cloud is simple availability or uptime, rather than more granular end-user metrics such as response time, page rendering time and user interactivity time. The key point of measuring these factors; is the ability for organization to monitor applications and run analytics to measure their performance, as well as provide visibility to what end users are seeing and experiencing. It should come as no surprise as this point that organizations of all sizes are flocking to the Cloud with high hopes of reducing cost, enhancing scalability, making management easier and improving disaster preparedness. A new study by Symantec (2013) found that 94% of enterprises are at least discussing Cloud or Cloud services, but the report shows that companies that rush into cloud deployment inevitably encounter a host of hidden costs. Some of the factors of Cloud hidden cost are:

CLOUD IMPLEMENTATION

The survey found that 40% of organizations who reported the implementation of the Cloud experienced the exposure of confidential information as a result. More than 25% said they faced account takeover issues, defacement or removal of Web properties or stolen goods or services as a result. However, for organization to take control of cloud deployments, such organization can seize advantage of the flexibility and cost savings associated with the Cloud, while minimizing the data control and security risks linked with the Cloud deployment.

CLOUD BACKUP AND RECOVERY ISSUES

The survey also found that Cloud complicates backup and recovery processes. Organizations are rushing to move to the Cloud, but they don’t think through how important backup and recovery is! Over 61% of such organizations use three or more solutions to backup physical, virtual and Cloud data which is really inefficient solutions. Such solutions lead to increased risk and training costs, and in addition, 43% of such organizations say they have lost Cloud data and had to recover from backups. Lost of data could mean data have been deleted or even lost or damaged by the Cloud service provider. To make matters worse, 68% of organizations reported recovery failures when attempting recovery of data in the Cloud. Such recovery never happened in a timely fashion, and 22% of organizations reported that the recovery

process can take three or more days to recover from a catastrophic loss of data in the Cloud which is not in time to meet a particular need.

INEFFICIENT CLOUD STORAGE

The simplicity of provisioning storage in the Cloud leads to another hidden cost. In theory, organizations pay only for what they use, but in reality; that can be cost effective if organizations work to maintain efficiency in their data storage. The problem is compounded by the fact that about half of these organizations admit that little if any of their Cloud data is duplicated.

COMPLIANCE CONCERNS

Organization are concerned about meeting their compliance obligations when it comes to data in the Cloud. The survey found that over 23% of such organizations have been fined for privacy violations in the Cloud, and that indicates a bigger problem than most people have recognized. As more and more data moves to the Cloud globally, there's more and more regulation about how that data needs to be managed. Organization needs to think about compliance in the context of the overall organization. The survey found that 49% of these organizations were concerned about meeting compliance requirements and 53% were concerned about being able to prove they have met Cloud compliance requirements.

DATA IN TRANSIT ISSUES

According to the study, managing the exploding number of SSL certificates held by organizations is already a struggle today, and the Cloud is compounding the problem. Assets in the Cloud require SSL certificates to protect the data – personal information, financial information, business transactions and other online interactions -in transit. Many organizations think the issue of managing SSL certificates is highly complex, and over 40% of organizations admit that they're not sure that their Cloud-partner's SSL certificates meet or comply with their own internal corporate standards.

Poor Cloud performance relays on the organization's full understanding of what pieces of infrastructure are in play, what's under-performing, and how improvements can be made. However, Cloud performance also has a lot to do with application optimization, since moving applications to the Cloud can also result in performance bottlenecks for reasons as simple as organization's hardware is running an older OS that's no long supported, or even simple points of failure on the client side if infrastructure being used to support the application's developments. Breaches on the Cloud can cost serious dollars to many organizations, especially where fines can be levied for lapses in compliance protocol. However, monitoring is the key to understand where efficiencies are lacking: whether resources are ongoing but unused, or if there are available resources that should be brought to bear for a project. Another hidden cost associated with monitoring is that lack of focus can result in errors going unreported and unaddressed, leading to greater inefficiency or even failure. Poorly defined SLAs between an organization and an outsourced Cloud provider can lead to an increase of the hidden costs. Business continuity is a major issue when considering how Cloud will impact an IT strategy, and can become a real cost center if not properly geared towards the needs of both the application, and the business. Downtime, after all, is the largest potential loss of revenue for a business.

In a public-cloud world, organizations tend to have more capacity because of noisy neighbors consuming more resources than organizations can expect on that shared host. While over-provisioning can sometimes be necessary, it's also easy to go overboard in the opposite direction, and as such the Cloud solution will be very expensive if such organizations are not continuously studying and right-sizing instances, storage pools, memory footprint, etc. Cloud Computing costs can soar when new customers assume that an initial deployment needs to be as large as the internal infrastructure being converted to Cloud. Also, storage performance and contention have long been problems in the Cloud, and while there are ways to improve, they're not free. These costs look small at the time, but as organizations start to multiply out hours and days and bytes, all of a sudden such organizations talking significant money.

Most organizations make blindly focused on raw face value costs, and they lose focus on the bigger picture, namely their Total Cost of Ownership (TCO). Too many organizations focus on comparing Cloud vs. On Premise costs in a purely single dimension, and they mistakenly believe that costs stop and start with how much new hardware/software is needed to put a solution into place. Such organizations when they think about Cloud, all they see is that recurring monthly service cost. However, the real picture of what's cheaper goes much deeper than the cost of a new server or a year's worth of office 365 subscription fees. Some of other hidden factors related to the Cloud solutions are:

CLOUD BANDWIDTH

When your servers are in-house, your only limits are your internal network's infrastructure. Switches; and cabling that is usually more than sufficient to serve bandwidth hungry applications inside office walls. Cloud scenarios are getting smarter with how they leverage bandwidth these days, and there is no getting away from the fact that offloading hefty workloads to the Cloud will call for a bigger pipe and extra hidden fees. As such any increased needs in Internet connection costs should be accounted for in an objective comparison of going Cloud or staying in-house.

OUT BOUND BANDWIDTH FROM CLOUD

Most Cloud providers they let organizations to move as much data as they need into their Cloud servers, but when it comes to pulling data out, it's on such organizations' dime after certain threshold. There is no such thing as a free lunch, and Cloud server bandwidth is no different.

THE FORGOTTEN "5 YEAR RULE"

The Cloud approach always entails a subscription cost which brings higher recurring monthly fees than hosting in-house. Organizations aren't getting knocked with any year 5 Rule spikes in capital expenditures because Cloud providers are constantly moving their services to better servers behind the scenes, Giving organizations the benefits of stable hardware replacements without organizations' knowledge, however such procedures can eventually increase the risk of paying for more costly hardware/software Cloud's migration fees.

WHAT DOES EACH HOUR OF DOWNTIME COST YOUR BUSINESS?

The real question here which applies to both on-premise and in Cloud environment is: What does each hour of downtime cost your business? InformationWeek shed light on a nice 2011 study done by CA Technologies which tried to give us an idea of what downtime costs businesses on a broad scale. Of 200 surveyed businesses across the USA and Europe, they found that a total of \$26.5 Billion USD is lost each year due to IT downtime. That's an average of about \$55, 000 in lost revenue for smaller enterprises, \$91,000 for midsize organizations, and a whopping \$1 million+ for large organizations.

Finally, "Research in Action from Compuware" survey revealed that failure to properly manage the performance of Cloud-based applications results in increased costs and prevents organizations from realizing the full potential benefits of Cloud Computing. Loopholes that may have been missed by Cloud fanatics are the concerns of power shortages and security issues. These potential glitches can actually bring up the costs for any organizations. Other cost factors in the Cloud implementation is the subscription fees, system and staff setup and training, applications' performance bottlenecks, poor end-user experience, loss of revenue, and high maintenance.

CONCLUSION

Businesses are under increasing pressure to sharpen their business practices. Too few people are aware of the security threats that are emerging. Nevertheless, they are responsible for ensuring that sensitive data will remain authentic, accurate, available, and will stratify specific compliance requirements. Thus, it is essential for an organization to understand their current IT risks profile in order for them to determine the organization's level of IT risk tolerance and IT risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal controls systems.

Organizations cannot afford to ignore the promise of Cloud Computing, however, they should not rush into it. Rather, business managers and IT executives should carefully evaluate whether they will use the cloud as a source of infrastructure, a development platform, or a software delivery mechanism, and determine the right Cloud architecture for their needs. To achieve this, they must fully understand the key opportunities, and risks inherent in data security, privacy, reliability, and commercial viability among others.

Using Cloud solutions is like kissing someone you don't know – you don't know what types of germs they have, and whether you'll catch something from them. For business using or considering migrating to Cloud, all you can do is to be as prepared as you can possible. The key is getting to know providers as much as you can, both as an organization, and from an end-user perspective.

Some of the unique aspects of Cloud Computing can pose new challenges to many organizations. The apparent simplicity of adapting Cloud Computing contradicts how complex its management can become when risks materialized. It would be naïve to think that Cloud Computing will allow an organization

to avoid adverse or unfavorable events – criminal activity, human error, and unforeseen accident and disruptions – that can befall or overtake any type of organization. An effective Cloud governance program is highly dependent on an accurate understanding of the risks combined with well-contemplated risk mitigation or acceptance strategies. A serious potential security risk with Cloud Computing will be any laws intended to guarantee the ability of law enforcement to monitor computations that they suspect of supporting criminal activity. Back doors of this sort complicate security arrangements.

Don't let salespeople guide your decisions based on their pitches alone. If you can objectively compare your own standing from Total Cost of Ownership (TCO) to downtime cost per hour, among other factors mentioned within this research, you're in a position of power to make the best choice slated in solid fact and such position will invariably leads to the best results. Finally, despite the fact that those new categories of jobs arising from Cloud Computing; surveys show various organizations adopting Cloud solutions for the purpose of reducing their headcount, will increase the chances for more workers to lose their jobs where systems and database administrators are no longer required.

REFERENCES

- Stephens, M. (2010) The benefits and challenges of cloud computing [Online]. Available from: <http://www.moorestephens.com/cloud-computing-benefits-challenges.aspx> (Accessed: 4 February 2014).
- Alvares, E. & Gupta, P. (2010) Eyes Wide Open Mitigating Risk in Cloud Computing [Online]. Available from: http://www.strategyand.pwc.com/media/file/Eyes_Wide_Open.pdf (Accessed: 4 February 2014).
- Shagin, A. (2012) The Risks and Benefits of Cloud Computing [Online]. Available from: <http://blogs.sap.com/innovation/cloud-computing/risks-and-benefits-of-cloud-computing-020025> (Accessed: 4 February 2014).
- Angeles, S. (2013) 8 Reasons to Fear Cloud Computing [Online]. Available from: <http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html> (Accessed: 4 February 2014).
- Siciliano, R. (2014) Risks and Solutions in Cloud Computing [Online]. Available from: <http://www.atmmarketplace.com/blog/12131/Risks-and-solutions-in-cloud-computing> (Accessed: 4 February 2014).
- Office of the Privacy Commissioner (2012) Cloud Computing for small and Medium-sized Enterprises: Privacy Responsibilities and Considerations [Online]. Available from: http://www.priv.gc.ca/information/pub/gd_cc_201206_e.asp (Accessed: 4 February 2014).
- Mearian, L. (2013) No, Your data Isn't Secure in the Cloud [Online]. Available from: http://www.computerworld.com/s/article/9241553/No_your_data_isn_t_secure_in_the_cloud (Accessed: 4 February 2014).
- Olavsrud, T. (2013) How Secure is the Cloud? It Pros Speak Up [Online]. Available from: http://www.cio.com/article/703064/How_Secure_Is_the_Cloud_IT_Pros_Speak_Up (Accessed: 4 February 2014).
- Samson, T. (2013) 9 Top Threats to Cloud Computing Security [Online]. Available form: <http://www.infoworld.com/t/cloudsecurity/9-top-threats-cloud-computing-security-213428> (Accessed: 4 February 2014).
- Talbot, D. (2009) How Secure is cloud Computing [Online]. Available from: <http://www.technologyreview.com/news/416293/how-secure-is-cloud-computing/> (Accessed: 4 February 2014).
- Strom, D. (2010) How Secure Is the Cloud [Online]. Available from: <http://www.tomshardware.com/reviews/cloud-computing-security,2829.html> (Accessed: 4 February 2014).
- Mello, J. (2013) Cloud-based Security Services Poised for Rapid Growth [Online]. Available from: <http://www.csoonline.com/article/745018/cloud-based-security-services-poised-for-rapid-growth> (Accessed: 4 February 2014).
- McKendrick, J. (2013) Hidden Costs of Cloud Computing, Revealed [Online]. Available from: <http://www.forbes.com/sites/joemckendrick/2013/07/17/hidden-costs-of-cloud-computing-revealed/> (Accessed: 4 February 2014).
- Olavsrud, T. (2013) 6 Hidden Costs of Cloud and How to Avoid Them [Online]. Available from: http://www.cio.com/article/726995/6_Hidden_Costs_of_Cloud_and_How_to_Avoid_Them (Accessed: 4 February 2014).
- McKendrick, J. (2012) Hidden Costs of Cloud Computing, Revealed [Online]. Available from: <http://www.forbes.com/sites/joemckendrick/2013/07/17/hidden-costs-of-cloud-computing-revealed/> (Accessed: 4 February 2014).
- Venkatraman, A. (2013) Hidden Cost of Cloud Computing is CIO's biggest Concern [Online]. Available from: <http://www.computer-weekly.com/news/2240188240/Hidden-cost-of-cloud-computing-is-CIOs-biggest-concern> (Accessed: 4 February 2014).
- Gardner, J. (2013) Are Hidden Costs Dampening Cloud Computing Benefits? [Online]. Available from: <http://www.logicworks.net/blog/2013/09/hidden-costs-dampening-cloud-computing-benefits/> (Accessed: 4 February, 2014).
- Pariseau, B. (2013) Unexpected Cloud Computing Costs Cause Sticker Shock [Online]. Available from: <http://searchcloudcomputing.techtarget.com/news/2240203550/Unexpected-cloud-computing-costs-cause-sticker-shock> (Accessed: 4 February, 2014).
- McCoy, C. (2013) Businesses Showing Concern Over Hidden Costs of the Cloud [Online]. Available from: <http://www.pcworld.com/article/2044654/businesses-showing-concern-over-hidden-costs-of-the-cloud.html> (Accessed: 4 February, 2014).
- Layo, I. (2013) 79% of CIOs Are Concerned About Hidden Costs of Cloud Computing [Online]. Available from: <http://cloudtimes.org/2013/07/27/cio-hidden-costs-cloud-computing/> (Accessed: 4 February, 2014).
- Wlodarz, D. (2013) Comparing Cloud vs. On-Premise? Size Hidden Costs People Always Forget About [Online]. Available from: <http://betanews.com/2013/11/04/comparing-cloud-vs-on-premise-six-hidden-costs-people-always-forget-about/> (Accessed: 4 February, 2014).
- Brumm, B. (2012) The Impact of Cloud Computing on IT Jobs [Online]. Available from: <http://www.computer.org/portal/web/computingnow/careers/content?g=53319&type=article&urlTitle=the-impact-of-cloudcomputing-on-it-jobs> (Accessed: 4 February, 2014).
- Bloom, E. (2012) Effect of Cloud Computing on Future IT Jobs [Online]. Available from: <http://www.itworld.com/career/322016/effect-cloud-computing-future-it-jobs> (Accessed: 4 February, 2014).
- Machado, H. (2013) How Cloud Computing Will Impact Your IT Job [Online]. Available from: <http://thoughtsoncloud.com/2013/05/how-cloud-computing-will-impact-your-job/> (Accessed: 4 February, 2014).
- Mckendrick, J. (2012) 9 Ways Cloud will Impact IT Employment [Online]. Available from: <http://www.zdnet.com/9-ways-cloud-will-impact-it-employment-7000002940/> (Accessed: 4 February, 2014).

ABOUT THE AUTHOR

Bryan Soliman is a Senior Solution Designer currently working with Ontario Provincial Government of Canada. He has over twenty four years of Information Technology experience with Bachelor degree in Engineering, bachelor degree in Computer Science, and Master degree in Computer Science.

FREE eBook DOWNLOAD

ENCRYPTION KEY MANAGEMENT SIMPLIFIED

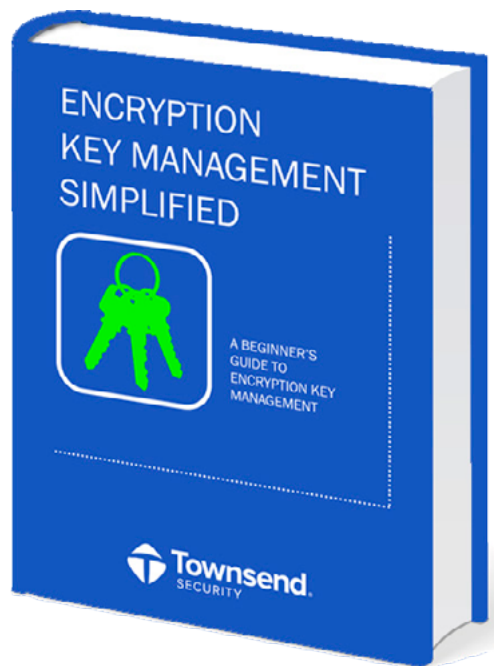
Learn the Fundamentals

What is encryption key management and do I need it?

Key management best practices

How to meet compliance regulations (PCI-DSS, HIPAA/HITECH, GLBA/FFIEC, etc.) with encryption key management

How encryption key management works on every platform including Microsoft SQL Server '08/'12, Oracle, and IBM i



DOWNLOAD THE eBook
townsendsecurity.com/eforensics

HACKERS DON'T BREAK ENCRYPTION.
THEY FIND YOUR KEYS.

DATA MASKING: A MUST KNOW FOR COMPUTER FORENSICS

by **Cordny Nederkoorn**

Data masking is a process that is used to protect the information that is stored in data management systems. It is used to prevent data corruption and to give only users with the right authorization access to the data. For computer forensics this is interesting, because it shows how a company can protect itself against external (and internal) data breaches. This article shows what data masking is by showing an example using software from Camouflage, a leading provider of enterprise-class data masking solutions for securing sensitive data.

What you will learn:

- Basics of data masking
- Basics of data masking software Camouflage

What you should know:

- Basic understanding computer forensics

Bob, a forensics investigator, is called in by a known grocery store after a security breach is noticed. It seems files with personal data from clients are breached.

One of these files, called the 'Black list', contains the addresses of top clients.

When Bob sees the file he is surprised. The file shows data which is not logically related to each other. It seems the data is shuffled all over the table.

When notifying the grocery's CEO about this, the CEO calls for his IT-specialist George.

Bob shows his findings and George starts to smile.

Why? Well, it seems the file here is used for testing purposes. The data is masked. Production data is used, and by data masking the customer's privacy is ensured and its data is useless for hackers.

However, software testing is still possible, because the original file is not tampered with, and the data is still usable as proper testing material because it still feels like real data.

Now Bob is intrigued. How does this data masking work and what tools are used?

DATA MASKING

Data masking, also known as anonymization or data obfuscation, is the process of de-identifying (masking) specific data elements in data stores (like a database).

It is a known technique in software testing for de-identifying production data for testing purposes. Production data contains personal or commercial sensitive data, which can be masked for privacy or commercial protection reasons and still be usable for software testing.

George, the IT-guy, uses the software from Camouflage to mask the data for use during software testing.

CAMOUFLAGE

The company Camouflage is a leading provider of enterprise-class data masking solutions for securing sensitive data. Other companies delivering data masking solutions are Informatica, Oracle and IBM.

Initially released in 2004, Camouflage delivers unified Discovery, Data Masking and Subsetting solutions engineered for today's organizations and the complex systems that drive them.

Camouflage offers a cross-platform advantage by automating time consuming manual scripting efforts to identify and secure sensitive information.

USING CAMOUFLAGE

Camouflage can be used to mask data in a database or flat files.

Because the 'Black List' is a flat file in csv-format, we will use the Flat file 'procedure'.

Let's say we have a flat file with company addresses named 'Black List'.

MASKING THE 'BLACK LIST'

First, we have the original 'Black List'

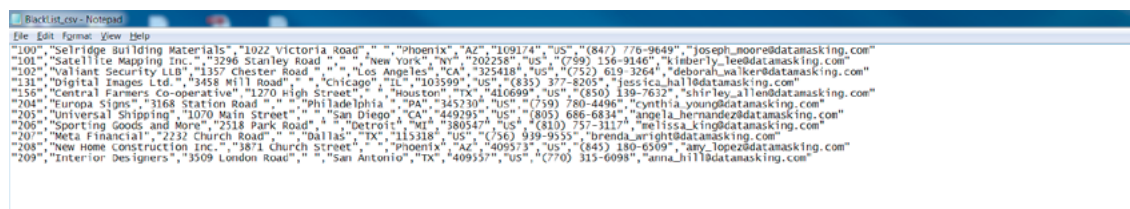


Figure 1. the original 'Black List'

For this exercise I downloaded a free trial of Camouflage.

The basic steps for masking the data in the 'Black list' are:

STEP 1.

Set up a Flat File Connection.

STEP 2.

Create a Flat File Configuration.

STEP 3.

Configure each file to be masked under Flat File Configurations.

STEP 4.

Create and configure Record Groupings for each Flat File Configuration.

STEP 5.

Set up masking targets against the Record Groupings configured in the Flat File Configurations.

STEP 6.

Run the masking targets.

Let's follow these steps:

After opening Camouflage create a new Project. For this I made a copy of the flat file demo Camouflage offers with the trial.

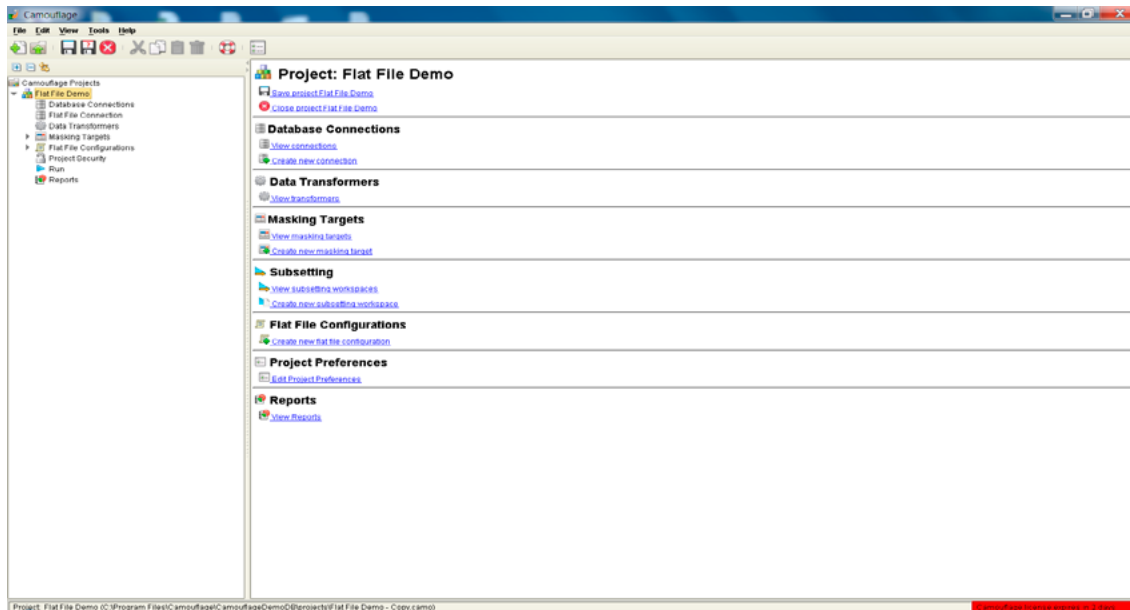


Figure 2. Camouflage Project view

First we have to make a connection to our flat file, as shown in Figure 3:

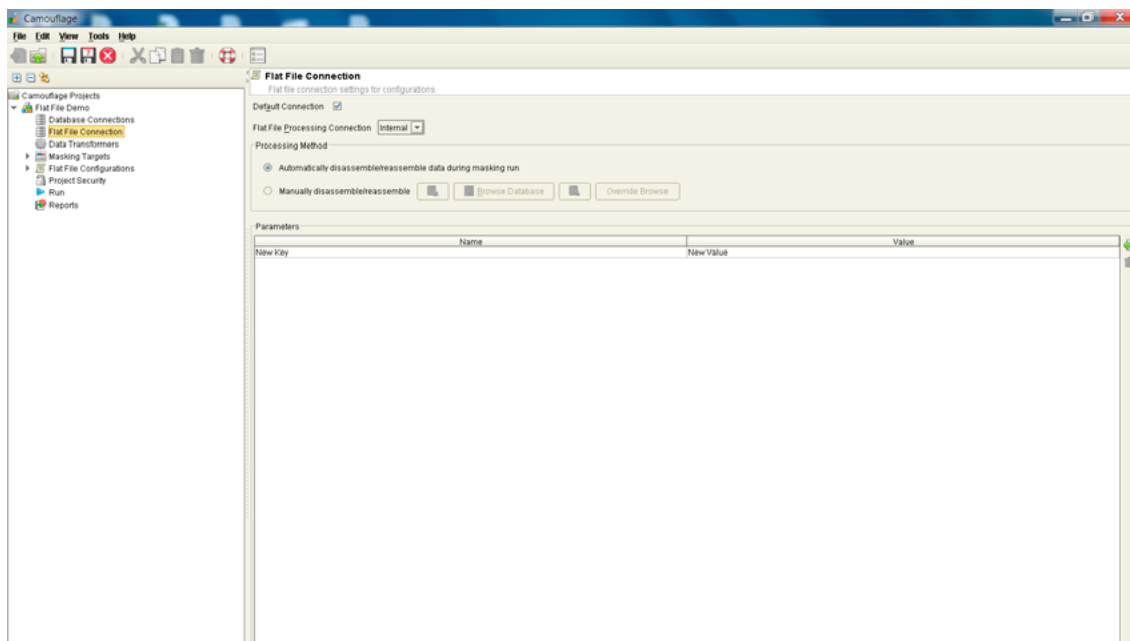


Figure 3. Making the Flat File Connection in Camouflage

Default connection should be marked and the internal Flat file processing connection should be used.

STEP 2 AND 3. CREATE AND CONFIGURE A FLAT FILE FOR DATA MASKING

Next, the flat file configuration should be made. Select the corresponding menu in the navigation panel. Select 'Create new flat file configuration' as seen in Figure 4.

The location of the source file (the original 'Black List') and the destination of the masked file should be entered as above for the file format Delimited.

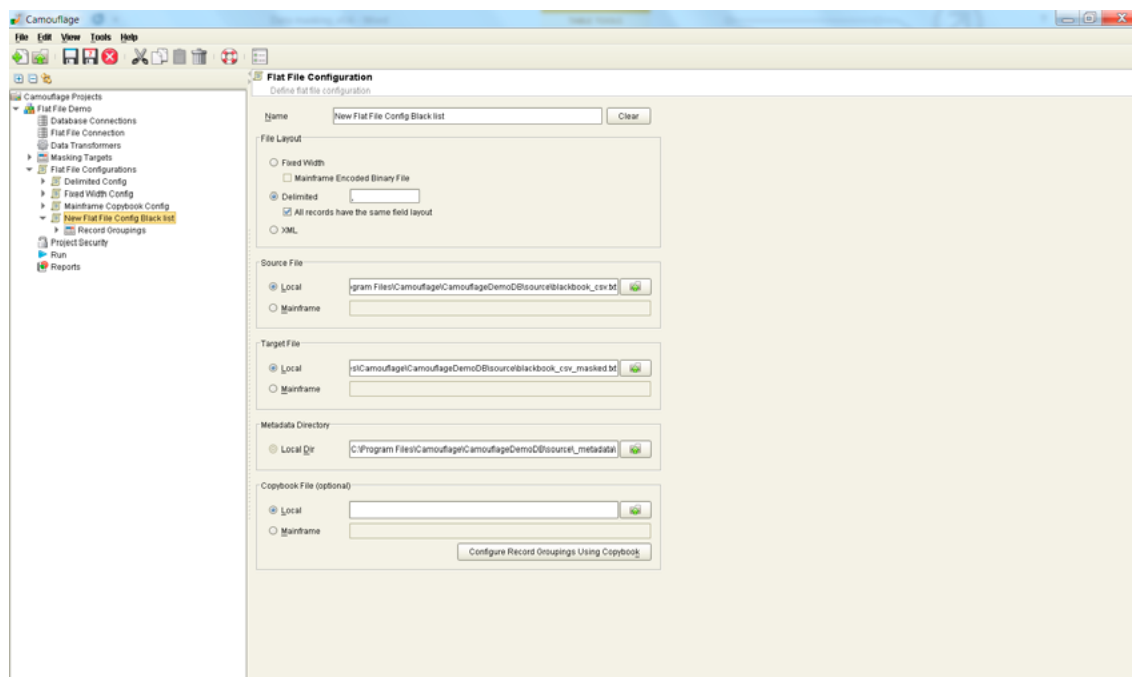


Figure 4. Making the Flat File Configuration in Camouflage

STEP 4. RECORD GROUPING

Via the flat file config-menu record grouping can be made, also known as defining the metadata. Fill in the fields and verify if the lowest pane is filled with the data as seen in the "Black list".

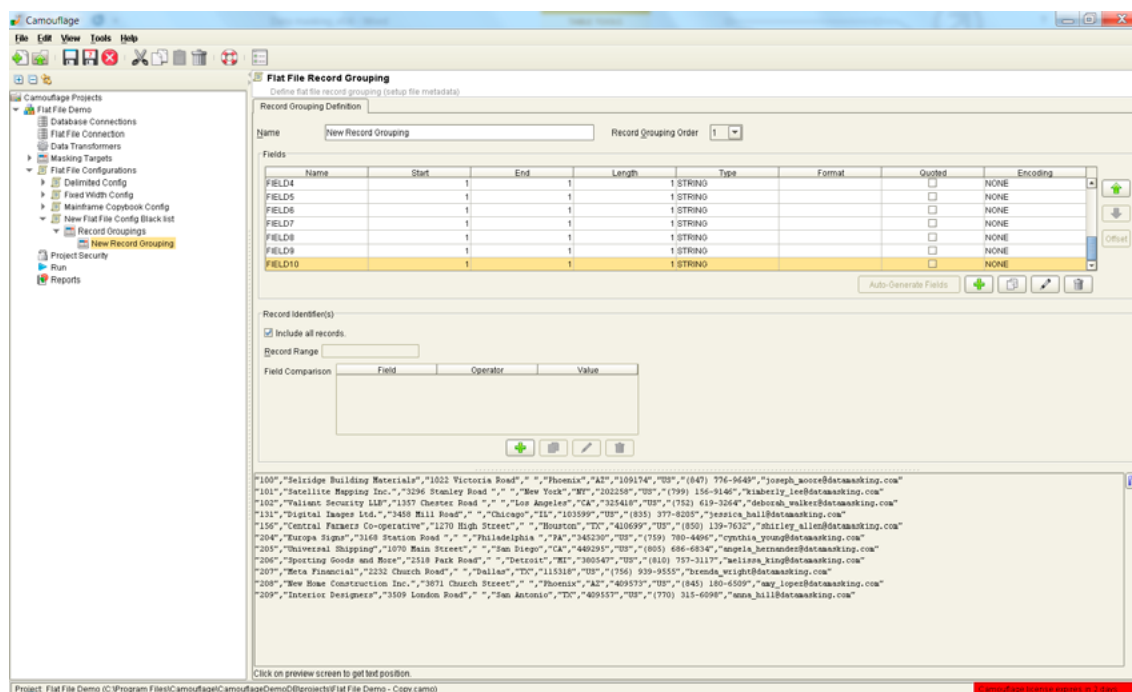


Figure 5. Making the Flat File Record Grouping in Camouflage

STEP 5. SETUP MASKING TARGETS

A masking target defines the data transformer that will be used to mask selected fields on a table. Select Masking Targets in the navigation panel to display a list in the content panel.

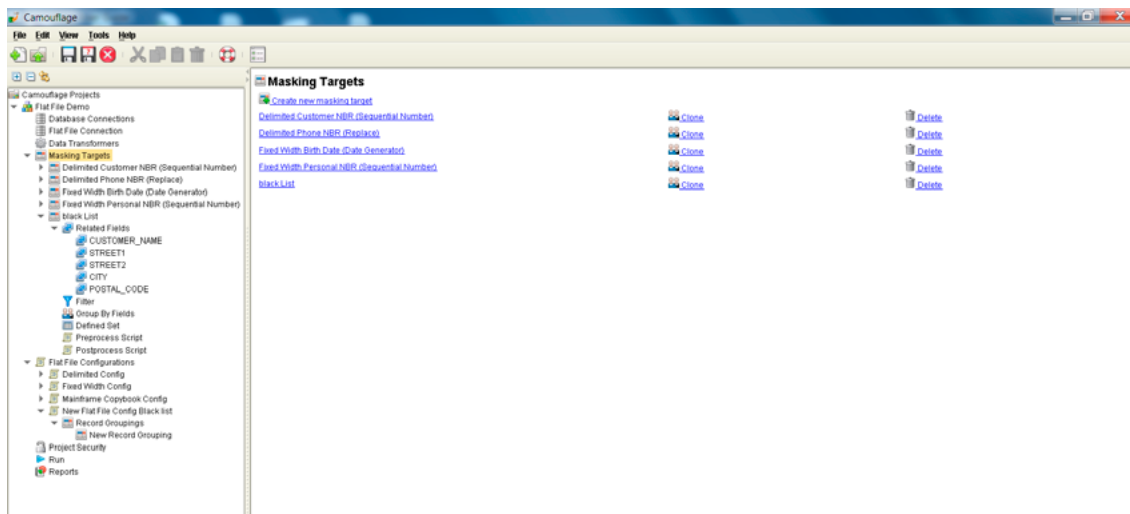


Figure 6. The Masking Targets menu in Camouflage

Here the 'Black List' Masking target is already made. Selecting it gives Figure 7.

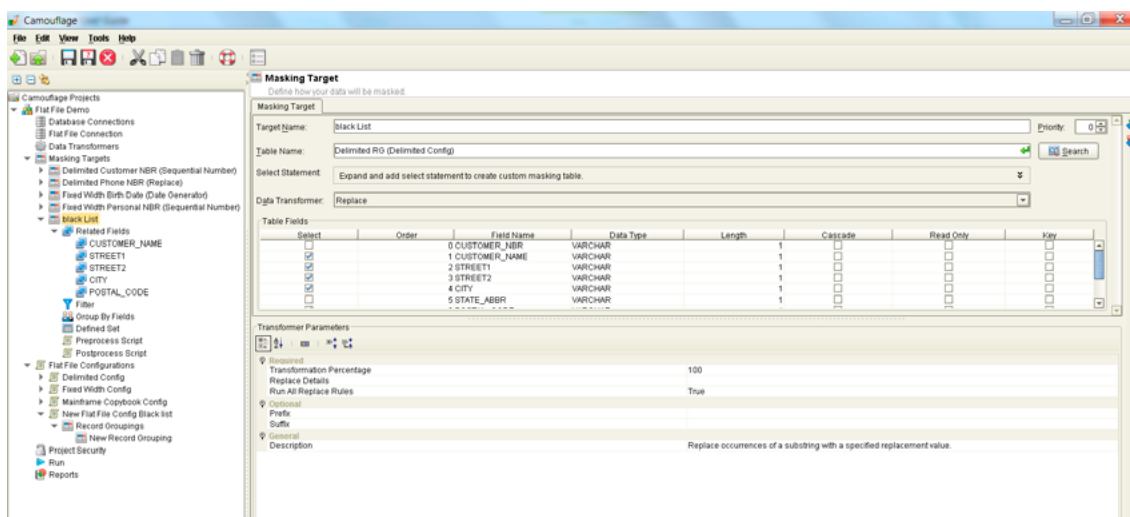


Figure 7. Details of the Masking Target 'Black List'

Important here is the selection of the correct Data transformer. Here, 'Replace' is used, because this is the way the data is masked: by replacing the original data.

The data to be masked can be selected in the Table field's pane, as seen in Figure 7.

One of the Transformer Parameters is 'Replace Details' where you can fill in what the rules are to replace which kind of data.

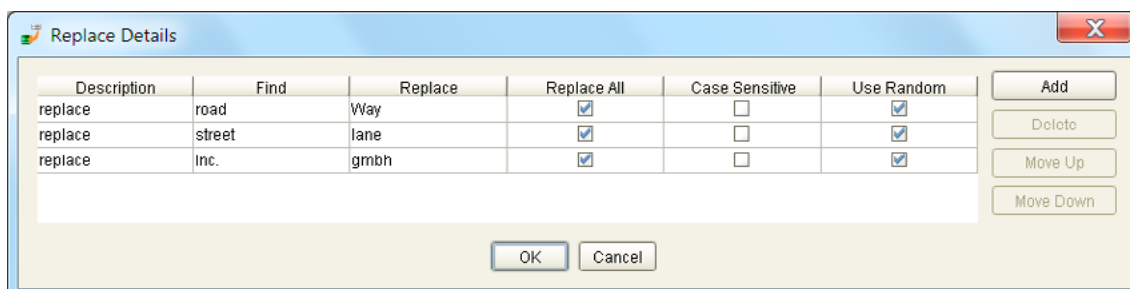


Figure 8. The transformer Parameter 'Replace details' for the 'Black List'

This way we can mask the address details and company names.

As seen in the navigation panel, these Table fields are also mentioned in the Related Fields menu.

STEP 6. RUN DATA MASKING

Highlight Run button in the navigation panel, select the Masking targets to be run for the Flat file engine and click the Start-button. This results in the following screen:

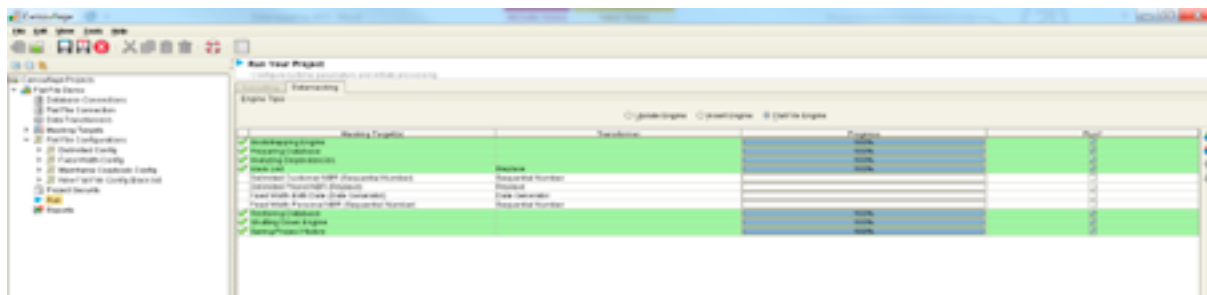


Figure 9. The Run menu in Camouflage

If the run is a success, all lines will be green, otherwise red.

If the run succeeds the file 'Black List' is masked and will look like Figure 10:

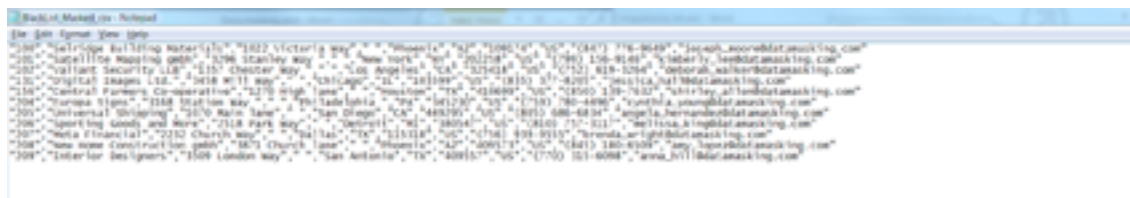


Figure 10. the masked 'Black List'

Comparing Figure 1 and 10 will show the replacements as seen in Figure 7 has been made, enabling a software tester to work with the 'masked' data.

For reporting a special module is available in the navigation panel.

This reporting can be done historical over previous runs or per run.

This ends the demonstration of data masking of a flat file via Camouflage.

CONCLUSION

This article showed a demo of the data masking possibilities of Camouflage. It just gave a small subset of all of its features. Not only flat files can be masked, data from databases from different vendors can also be masked. It shows data masking can be done through the software from Camouflage.

Interesting for computer forensics, because data masking protects against non-authorized personnel viewing personal client-information in production data. Next to this, it also protects the personal client-data against hackers viewing this data through security breaches.

ABOUT THE AUTHOR



Cordny Nederkoorn is a Dutch software testengineer, employed by Onegini, which delivers an easy to use solution including all the security standards and monitoring tools so your mobile Apps can access your enterprise data. Mobile App developers can focus on the functionality and do not have to trouble themselves about security. On a personal level Cordny helps Kantara Initiative improving the quality of the specification and implementation of UMA (User-Managed Access), a web authorization protocol building on OAuth 2.0. He discusses his work on different social media. Blog: <http://testingsaas.blogspot.com> | Twitter: <http://www.twitter.com/testingsaas> | Facebook: <http://www.facebook.com/TestingSaaS>

BIOMETRIC FACIAL RECOGNITION DATABASE SYSTEMS

by Robert E. Vanaman

For millennia, humans have availed themselves of the body characteristics of one another such as face, speech, gait, size, etc. to recognize each other. This instinctual differentiation has evolved into the science of Biometrics. Biometrics is nothing more than a form of bioinformatics [1] that applies biological properties in the identification of individuals (Animetrice, 2008a).

Facial recognition (FR) is a subset of the broader science of Biometrics. A biometric system is effectively a pattern recognition system that operates by acquiring biometric data from an individual, and extracts a feature set from the acquired data for comparison purposes (Jain, Prabhakar, & Ross, 2004). The information needed for recognition is acquired by a sensor, and is converted into a digital format (Biometrics.gov, 2011a). This digitized representation of a feature, in this case a face, is then compared to a “biometric template” (Biometrics.gov, 2011b) or a “gallery” (Bronstein, Bronstein, & Kimmel, 2004) stored in a database. This paper will delve into the Facial Recognition Database Systems (FRDBS) currently in place and cover predictions for future use, exploring the processes and methodology employed therein, specifically addressing FRDBS methodologies and techniques employed in capturing, storing, and comparing scanned images.

HISTORICAL BACKGROUND

The term biometrics is derived from the Greek words “bio” meaning life and “metrics” implying to measure (Biometrics.gov, 2011c). Although the advent of modern (Read: computerized) biometric systems have been possible only in the most recent times, the concept of using body characteristic to distinguish one another was conceived hundreds, perhaps thousands of years ago. As evidence of this assertion, handprints found in caves estimated to be over 31,000 years old, are believed to represent “un-forgeable signatures” (Renaghan, 1997) of their authors. Evidence that fingerprints were used in Babylonia in 500 B.C. can be found in the clay tablets of the day used to record business transactions (International Institute of Hand Analysis, 2005).

In Europe, with the emergence of a more mobile population in the mid-18th century, justice systems were tasked with tracking and cataloging first-time, versus repeat, offenders across a larger sampling of populous as well as in a growing geographic area. A formal system was needed, and devised to accomplish this. First there was the Bertillon system in France, which measured various body dimensions. This approach was called anthropometrics. The second method, which is still in use today, was a card file of indexed fingerprints, which was discovered to be exclusive on individuals, based on the patterns and ridges found on fingers (Biometrics.gov, 2011c). Today, biometric identification and verification systems have proliferated beyond 19th century fingerprinting and palm printing indexed card files (one of the first scientific application of biometrics) to include 21st century computerized DNA, ear, gait, hand geometry, hand vein, iris, keystroke, odor, retina, signature, and speech recognition processes, as well as FRDBS (Jain, Prabhakar, & Ross, 2004).

It should be noted early in our discussion that FR systems are broadly divided into two distinct classifications: authentication and recognition (Bronstein et al., 2004). Authentication is the process of comparing a claimed identity with a designated template in the gallery. Here, the FR algorithm is tasked with only a one to one (1:1) relationship comparison. Furthermore, in an authentication scenario, the enrolled individual is “assumed to be collaborative” (Bronstein et al., 2004). In stark contrast, the processes involved in recognitions are far more rigorous. Here, the FR algorithm must compare the subject with all the templates in the database. This entails a one too many (1:M) relationship matching, a far more arduous undertaking. Compounding this undertaking is that a collaborative demeanor on the part of the subject is highly unlikely.

QUALIFIABLE CONSTRAINTS

Before the techniques and methods of the comparisons of images to templates can be examined, an understanding of what qualifies as a measureable biological biometric needs defining. Any number of “human physiological and/or behavioral characteristics” (Jain, Prabhakar, & Ross, 2004) can be engaged as long as they comply with the following four constraints:

- *Universality*: everyone has this characteristic or trait.
- *Distinctiveness*: One individual's characteristic or trait must be sufficiently dissimilar from other individuals.
- *Permanence*: the characteristic or trait should be persistent over time with respect to its measurable biometric criterion.
- *Collectability*: characteristic or trait can be analyzed – measured – quantitatively (Jain, Prabhakar, & Ross, 2004).

As with most theoretical scenarios, if a practical field based operation is to be deployed, several other constraints which could place limitations regarding the system's practicality must be addressed. These would include, though not limited to:

- *Performance*: this criterion is composed of two elements. First, the ability of the system to make accurate comparisons; that is to minimize false matches and false non-matches. Second, the speed at which the operation renders an acceptable and reliable result.
- *Acceptability*: this is a measurable indicator of the extent that a particular biometric system is embraced – or at minimum – tolerated in the public's daily life.
- *Circumvention*: a reflection of the robustness of the system's ability to resist unlawful criminal acts of evasion (Jain, Prabhakar, & Ross, 2004).

To summarize, a feasible biometric scheme should meet or exceed the specified recognition precision and speed parameters, be innocuous to the scanners and ones being scanned, be sufficiently benign to be adopted by the selected group of the populous intended for its use, and be sufficiently vigorous in thwarting various devious methods of attack on the reliability of the system (Jain, Prabhakar, & Ross, 2004). Table 1 is a synopsis for a comparison of the aforementioned Biometric recognition processes and their corresponding effectiveness in respect to the constraints.

Comparison of Various Biometric Technologies							
Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palm print	M	H	H	M	H	M	M
Retina	H	M	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H = High, M = Medium, and L = Low

Probability of Accuracy

Advantages and Disadvantages

Why favor FR as the viable approach for identification over other biometric methods? First, FR is stealthy; it does not require the active participation of the participant, and may be acquired from a distance. Concisely, FR is “unobtrusive and discrete” (Animetric, 2008a) and recognized as a natural, non-intimidating and universally accepted biometric identification method (Bronstein et al., 2004). Second, the infrastructure necessary for the system to operate is already widely in place, and relatively inexpensive. Security cameras are a common fixture from airports and retail establishments to ATMs and private residences. Lastly, a multitude of private companies have stored “photo ID records” (Animetric, 2008a) and virtually every governmental and intelligence agency has vast quantities of surveillance photos and videos in legacy database repositories.

Historically the fundamental drawback to FRDBS has been the 2D personality of the stored image. These two dimensional (2D) representations of a three dimensional (3D) face introduce unacceptable failure rates. A 2D view measures only the height and width, with a corresponding measurement between facial features. Additionally, faces reflect light casting shadows, faces change with expressions or head pose, “facial hair, the use of cosmetics, jewelry and piercings” (Bronstein et al., 2004) all have their influence, thereby creating a different visual persona under different circumstances (Animetric, 2008a).

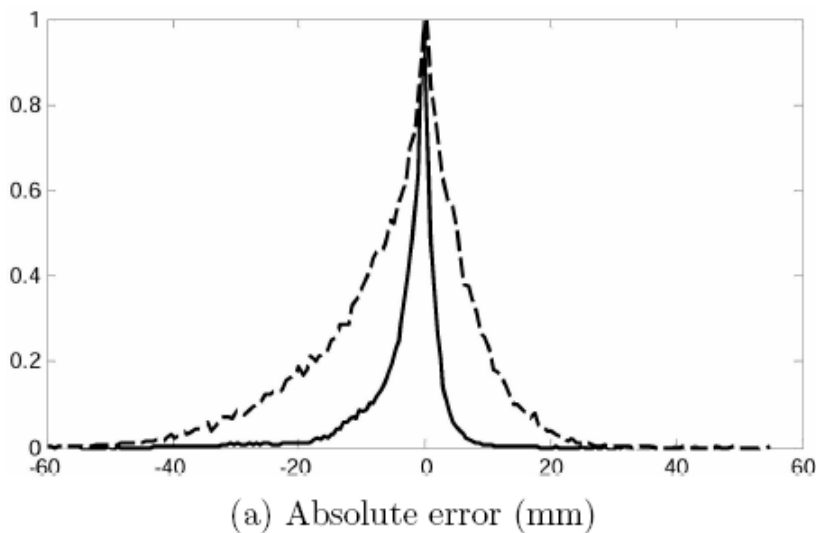
A partial solution to this quandary came after the 2002 Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) initiative that concluded that a 3D FR system was the solution. 3D FR systems address the issues of variable circumstances and can be implemented without the use of specialized cameras, thereby utilizing existing infrastructure equipment (Animetric, 2008a).

3D FRDBS DESIGN

3D FR Systems is a comparatively fresh approach in the science of Biometrics. It, in many ways, breaks with the long-term approach of attempting to interpret human facial features by employing the traditional human visual recognition methodology – which is utilized in 2D models – that have yielded such limited success. These results impart, to the attributed graphic flat representation of the compound curved, 3D facial surface (Bronstein et al., 2004). 3D facial geometry systems accomplishes its mission by representing the internal anatomical structure of the face as an alternative to the external representation utilized by 2D models that are susceptible to various environmental considerations (Bronstein et al., 2004). Consequently, 3D FR systems are insensitive to diverse illumination backgrounds and the interfering effects of cosmetics and head pose.

A fundamental postulate of 3D FR systems is that once facial features are modeled as isometrics [2] in the context of Riemannian geometry [3] facial surfaces are regarded as deformable objects. The advantage of this approach results in the inherent geometric characteristics of the facial surface becoming “expression-invariant” (Bronstein et al., 2004). This hypothesis of facial expressions being invariant once modeled as isometrics, juxtaposed upon the framework of Riemannian geometry, can be proven quantitatively by locating a set of attribute points on the facial contour, and calculating how the expanse between them is altered due to facial expressions. In 2004, Alexander and Michael Bronstein, in concert with Ron Kimmel, conducted an experiment that placed “133 markers on a face and tracked how the distances between these points change due to facial expressions” (Bronstein et al., 2004). They concluded that the divergence from of the geodesic [4] distances due to facial expressions is insignificant (which justifies our model), and that the discrepancy is less half than the applicable change of the Euclidean model. This signifies that the isometric model portrays the character of facial expressions over as twice accurately, when compared to the inflexible 2D systems (see graphic 1) (Bronstein et al., 2004).

Michael M. Bronstein, Alexander M. Bronstein, Ron Kimmel



Normalized histogram of the absolute error of the geodesic (solid) and the Euclidean (dashed) distances

A 3D PROTOTYPE

At the Geometric Image Processing laboratory a prototype 3D FR system, based on the expression-invariant representation of facial surfaces was developed and tested. This prototype is capable of operating in the 1:1 authentication mode, and in the more demanding 1:M recognition methodology. An AMD Opteron64 workstation, utilizing a Microsoft Windows XP operating system, was employed in the data processing and data analysis, as well as managing the graphical user interface for commands and visualization (Bronstein et al., 2004).

The data processing and analysis was disseminated into several discrete phases. First, the face is scanned in three dimensions, producing a shroud of data points corresponding to the facial surface. This pseudo-image is then “cropped, smoothed and subsampled” (Bronstein et al., 2004). The next steps involve a feature detector that isolates a few critical standard points for comparison. These points then

result in a computed geodesic mask. Finally, the facial surface undergoes a canonization [5] utilizing a multidimensional scaling [6] (MDS).

The conclusions presented in this study confirmed that this 3D FR system, relying on models as isometrics in the configuration of Riemannian geometry, and then processed – *massaged* – in a perspective of canonization incorporating MDS, comprehensively out performed traditional 2D and 3D systems. This system's expression-invariant nature asserts its relevance in commercial applications, which pre-conceives a less than collaborative subject, in various environments and situational circumstances. Additionally, a high level of public acceptability would exist due to the clandestine nature of the scanning process. A further benefit of utilizing a canonical forms methodology is their irreversibility. Canonical forms cannot be reversed -engineered back – to a facial surface features that would be recognizable in traditional human identification images. It essentially hides the actual identification of the subject in the database gallery. This feature has a prominent benefit in commercial systems, where the security of biometrics data is of paramount importance.

STORAGE AND RETRIEVAL

AN ELEMENTARY SYSTEM

One form of FRDBS is utilized primarily in criminal and forensic identification, but has intelligence and broader-security applications in which subjects need to be authenticated against passport or other recognition, documentation, or credential photographs (Forensic Science Communications, 2008). Here the FBI, in conjunction with the Magna Science Adventure Centre in Rotherham England, by means of digital stereo photography (Geometrix FaceVision FV802 Series Biometric Camera) and 3-D laser scanning (Cyberware 3030PS Head and Neck Scanner) equipment captured 30 craniofacial anthropometric landmark sites (see appendix A. Table 2) (Forensic Science Communications, 2008) on the 3D images of 3115 volunteers. These images were captured with the “Geometrix FaceVision system which (is) based on eight digital cameras” (Forensic Science Communications, 2008). The 30 landmark sites are mapped on one of the photographs in Image 1.



The Geometrix database contained 3115 folders and was a combination of a Microsoft Excel 2003 spreadsheet where each row (tuple) contained attributes (columns) including the age, gender, and ancestry of the subject and including the 3D Cartesian coordinates [7] of each of the landmarks. There was untouched stereophotographic image data, including eight JFIF images that corresponded to each of the eight cameras. The 3D facial wireframe models (see appendix A. Figure 1) (Forensic Science Communications, 2008) and the textured-mapped surface data images (see appendix A. Figure 2)

(Forensic Science Communications, 2008) were stored in three formats, DXF, AutoCad and Virtual Reality Modeling Language (VRML) (Forensic Science Communications, 2008). As of the publication date of this article, the Geometrix database was considered the largest such collection in existence (Forensic Science Communications, 2008).

AN ADVANCED SYSTEM

A more advance in FRDBS has recently emerged in Japan. This hybrid-system utilizes both 2D and 3D facial images superimposed (Clement & Marks, 2005). Although this application is primarily a 1:1 authentication system, it promises future refinements to allow for 1:M recognition. The key refinement in this approach is that the two facial images can be oriented by the rotation of the 3D model. Furthermore the system draws upon morphometric [8] matching using facial outlines and anatomical landmarks. This methodology as before, provides results based on empirical, numerical data. Commercially available software packages thus far are limited to frontal image comparisons under current two dimensional technology. In contrast, this robust system for FR comparison allows for “severely disadvantageous angles” (Clement & Marks, 2005) of comparisons thereby rendering it effective in a structured database and real-world environment.

In the storage phase of the FRDBS, a software package called “3D-Rugle3 for Face-To-Face” (Medic Engineering, Kyoto, Japan) was used for “automatically adjusting the facial orientation of all the 3D images in the database” (Clement & Marks, 2005). Once this procedure was accomplished, all the 3D images were stored within the system and normalized in the orientation to the “Frankford horizontal [9] plane”. Next, fourteen orienting landmarks were mapped on the 3D facial image, and their discrete distances and coordinates were calculated and stored (see appendix A. Figure 3) (Clement & Marks, 2005). Correspondingly, the 2D facial images were subjected to identical treatment (see appendix A. Figure 4) (Clement & Marks, 2005). Again, discrete distances and coordinates were calculated and stored. Once specific parameters for rotation angle and facial dimensions were plotted from the anatomical landmarks, comparisons from the two images could be accomplished by superimposing a single 2D image upon multiple 3D images (Clement & Marks, 2005).

In the retrieval phase of the process, a “Commercial off-the-shelf software (COTS)” (Kendall, & Kendall, 2011) call “FaceList” developed by OMRON Co. of Japan, was substantially modified in its robustness when tasked in appraising variations in facial ordination. This package was then employed to identify the target subject’s 2D image against the stored 3D images in the FRDBS. This customized software is largely founded on the graph-matching methodology. Here, images are first overlaid with a course matching algorithmic graph of fixed parameters, followed by progressively finer matching functions of dynamic design. Once an acceptable graph is defined and selected, it contains fifty nodes with the distances between each and their illuminated grid properties calculated and accounted for (see appendix A. Figure 5) (Clement & Marks, 2005).

FRDBS FUTURE

A stunning example of FRDBS practical application at work now, and destined to affect the future, is the development and deployment of a new biometric security system, Broadway 3D, that recently concluded tests at Moscow’s Sheremetyevo International Airport. The system, designed and build by Artec Ventures [10], represents a *multi*-magnitude jump in 3D surface imagery. Broadway 3D boasts numerous advancements that until now were merely items on biometric scientists’ wish lists. First, the system “is highly automated and minimizes the need for human supervision” (HSNW, 2010). Second, during a single one month testing period, over 3,500 individuals were scanned and processed with their 3D images stored in a database gallery. These scans resulted in 100% accuracy rates when templates were compared to database images; no false/positives, no false/negatives. Third, the quality of recognition is unaffected by glasses, hairstyles, facial hair, cosmetics, or head pose. Additionally, due to the controlled environment in which the imagery is captured (the subject passes through a turnstile where the 3D camera emits a light pattern at parallel angles to the face), the illumination considerations are mitigated. The monumental advancement in Broadway 3D’s success rate can be attributed to several factors. First, the 3D image, is composed of 40,000 data points (Image 2) (Artec ID, 2011), compared to a few dozen in previous FR systems. This allows for a vastly more accurate mapping, and thus, a far more precise comparison algorithm of a subject’s template to the stored gallery image in the database (see appendix A. Figures 6-10) (Artec 3D, 2011). Second, the recognition time is a phenomenal one second, with enrollment time in the database of less than three seconds, and the exposure time for the subject of a mere 0.2ms. These unheard of time frames resulted in a throughput capacity, utilizing a turnstile, of up to 30

people per minute. Lastly, the diminutive size of the equipment cannot be over emphasized. The scanning unit measures a five feet four inches, by nine inches square, and weighing a little over thirty-five pounds. This enables the system to be portable, thus flexible, making it deployable and practical in the extreme (Artec ID, 2011).

Having overcome numerous shortcomings of previous FRDBS earns Broadway 3D compliances with all of the qualifications necessary for a measurable biological biometric. The human face has universality, distinctiveness, permanence, and collectability. Additionally, it meets the requirements for a field practical system by exhibiting outstanding performance, with its contactless identification and diminutive size it merits public acceptability, and the systems robustness prevents circumvention measures.

CONCLUSION

From prehistoric handprints discovered upon cave walls, which bare mute witness to their creator's existence and demise, too millisecond facial recognition systems at 21st century airports, the science of biometrics has changed the path of human history, and is destined to change the direction of humanity's future. From politicians, to security specialists, to administrators, all struggle with the real-world consequences and ramifications of biometrics in seeking a balance between an individual's right to privacy, against that same individual's right to safety. These juxtaposed apprehensional quandaries will be abolished as the science of biometric facial recognition systems become more reliable and less detectable. As with all modern day sciences, FRDBS are waiting on advancements in computer technology for advancement in their given field. The latter must precede the former. Additionally, as the boundaries of what constitutes an acceptable, viable, measureable, biological biometric shrink, due to the speed, accuracy, and the progression of the system's miniaturization – all of which continue to astonish – the public's acceptance will to continue to escalate at an *accelerated* rate.

Final perceptions: as biometric identification processes become a larger part of everyday life, clearly social concerns, legal issues, and ethical considerations will rise to the forefront of contemporary debates. As the miniaturization and stealth of biometric identifications systems continues to make their omnipresence diminish, their proliferation will only intensify. What is clear is that their governance must be a global endeavor. Any attempt to govern identification technologies will be an international effort, or will be ineffective (Challenge Liberty & Security, 2005). Lastly a word of caution, biometric identification system's influence on individual freedoms and individual safety can be benevolent or nefarious. It is mankind's responsibility to remain a faithful Argus of this proto-science. Unleashing its promise for humanities betterment, rather than succumbing to its potential for the demise of *both* mankind's liberties and mankind's protection.

EPILOGUE

Completed in June of 2013, and deployed at Sochi's International Airport, Elektronika, LLC – a Russian security system integrator – has developed and implemented an integrated security system for the 2014 Winter Olympics. The system "provides a wide range of functional capabilities including security monitoring and alarm situation detection, as well as its rapid response" (Artic ID, 2013). Over 550 high-definition surveillance cameras, along with checkpoints and automatic alert detection cover Sochi's entire premises. This unified monitoring system is feed into single dispatch center collecting data from the entire airport tract. Although utilizing the cerebral capabilities of various technologies, the system is built on a singular software platform – Elektronika's ESM. One of these technologies is a biometric access control system based on 3D facial geometry recognition.

The Artec Group's (formerly Artec Ventures) Broadway 3D facial recognition system was selected by Elektronika, and is currently operational at Sochi International. As expounded earlier, geometry of a human face is one of the most precise biometrics that is available, it possesses a universality, distinctiveness, permanence, and is unobtrusively collectible; moreover, it is near impossible to fool or fake (Jain, Prabhakar, & Ross, 2004, Artic ID, 2013). Additionally, Broadway 3D was selected for its safety and *fast* performance. The system is designed to prohibit both the access of any unregistered individual or unauthorized employee. The latest version of Broadway 3-D, "is capable of identifying a person while walking, wearing hats or sunglasses and can also decipher between identical twins" (designboom, 2013). Furthermore the system's high throughput with registration taking no longer than two seconds and with a 60 person per minute rate of scan is quite capable of handling critical rush-hour volume. Below, is a YouTube link to a short video depicting how Artec Group's Broadway 3D facial recognition operates at Sochi: http://www.youtube.com/watch?feature=player_embedded&v=mFmUqDnsitc

Since August, 2011 when this paper was first penned, biometrics and specifically facial recognition database systems have moved out of the secretive world of governmental security, and into the mainstream realm of retail technology and consumer sciences. This migration includes inroads into such realms as shoplifter identification and various types of market basket analysis; the latter, a mainstream of data mining prospecting techniques (Greg, 2014). Biometric gurus FaceFirst of Camarillo, California are already providing security protection to retailers by identifying known shoplifters when they enter the facilities facial recognition surveillance security zone. This system sends text messages and emails notifications to select individuals within the organization sounding an alert that an identified shoplifter has entered the premises. This software is envisioned to recognize the “bad guy” unaided, and promptly send the appropriate message to the appropriate authorities. However, other biometric facial recognition systems are used for more lucrative purposes by lodgers and retailers.

A touted capability of the NEC Corporation is their “V.I.P. identification software”. This innovative facial recognition system is designed for hotels, casinos, and other facilities “where there is a need to identify the presence of important visitors” (Singer, 2014). FaceFirst intends on adding this capability to the existing capability of their current system. Joseph Rosenkrantz, the CEO of FaceFirst explains “Just load existing photos of your known shoplifters, members of organized retail crime syndicates, persons of interest and your best customers into FaceFirst”. Then “Instantly, when a person in your FaceFirst database steps into one of your stores, you are sent an email, text or SMS alert that includes their picture and all biographical information of the known individual so you can take immediate and appropriate action.” (FaceFirst, 2014). Additionally, for the V.I.P. shopper and high rollers, the software autonomously notifies these individual sending personalized offers to their smart phones, tablets, and other Web enabled electronic devices (Singer, 2014).

There is a caveat to employing commercial facial recognition technology, although it “has the potential to provide important benefits and to support a new wave of technological innovation, [it] also poses consumer privacy challenges” (Singer, 2014). Legislation is currently pending, having been introduced by the White House and in conjunction with the National Telecommunications and Information Administration, to draft and enact baseline federal consumer privacy legislation. This legislation would require opt-in consent for consumers.

Essentially, the same privacy concerns, concerning DNA sequencing – that of measuring biological patterns unique to individuals – are at the heart of whether a person has a right to control who has access to his or her biometric data; and how, when, and where it can be used (Singer, 2014).

REFERENCES

- Animetric. (2008a). Biometrics and facial recognition. Retrieved from <http://www.animetrics.com/technology/frapplications.html>
- Animetric. (2008b). Bioinformatics. Retrieved from <http://www.animetrics.com/library/definitions.php>
- Answers.com. (2011). Geodesic distances. Retrieved from <http://www.answers.com/topic/geodesic-distance>
- Artec 3D. (2011). Interactive 3D. Retrieved from <http://www.artec3d.com/gallery/interactive-3d/>
- Artec ID. (2011). Broadway 3D. Retrieved from <http://www.artecid.com/download-f/a4-en-edited%20copy.pdf>
- Artec ID. (2013). Broadway 3D Face Recognition System is installed at International Sochi Airport. Retrieved from <http://www.artecid.com/news/1-news/88-broadway-3d-face-recognition-system-is-installed-at-international-sochi-airport.html>
- Biometrics.gov. (2011a). Introduction to biometrics. Retrieved from <http://www.biometrics.gov/ReferenceRoom/Introduction.aspx>
- Biometrics.gov. (2011b). Biometrics frequently asked questions. Retrieved from <http://www.biometrics.gov/Documents/FAQ.pdf>
- Biometrics.gov. (2011c). Biometrics history. Retrieved from <http://www.biometrics.gov/Documents/BioHistory.pdf>
- Bronstein, A., Bronstein, M. & Kimmel R. (2004). Three-dimensional face recognition. Department of Computer Science, Technion – Israel Institute of Technology, Haifa 32000, Israel. Retrieved from <http://www.cs.technion.ac.il/~ron/PAPERS/BroBroKimIJCV05.pdf>
- Challenge Liberty & Security. (2005). Ethical and social implications of biometric identification technology: Towards an international approach. Retrieved from <http://www.libertysecurity.org/article695.html>
- Clement, J. G., & Marks, M. K. (2005). Computer-graphic facial reconstruction. Burlington, MA: Elsevier Academic Press.
- DeLeon, V. B., Lele, S. R., & Richtsmeier, J.T. (2002). The promise of geometric morphometrics. Yearbook of Physical Anthropology, 45, 63-91. doi:10.1.1.117.443
- Designboom. (2013, September 7). 3D facial recognition airport security at Sochi 2014 Olympics. Retrieved from <http://www.designboom.com/technology/3d-facial-recognition-airport-security-at-sochi-2014-olympics/>
- Encyclopedia Britannica. (2011). Riemannian geometry. Retrieved from <http://www.britannica.com/bps/dictionary?query=Riemannian+geometry>
- FaceFirst. (2014). Retail. Retrieved from <http://www.facefirst.com/services/retail>
- Forensic Science Communications. (2008, April). The Magna database: A database of three-dimensional facial images for research in human identification and recognition. Retrieved from http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/archive/april2008/research/2008_04_research01.htm
- Greg, A. (2014, February 2). Facial recognition software to be used to track spending habits and send offers to customers' cell phones when they enter stores. Mail Online. Retrieved from <http://www.dailymail.co.uk/news/article-2550593/Facial-recognition-software-used-track-spending-habits-send-offers-customers-cell-phones-enter-stores.html>
- HSNW. (2010). Largest Moscow airport testing of facial biometric system. Retrieved from <http://www.homelandsecuritynewswire.com/largest-moscow-airport-testing-facial-biometric-system>
- International Institute of Hand Analysis (2005). Dermatoglyphis. Retrieved from <http://www.handanalysis.net/>

- Jain, A. K., Prabhakar, S. & Ross, A. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for video Technology, Special Issue on Image – and Video-Based Biometrics, 14(1). doi: 10.1109/TCSVT.2003.818349
- Kendall, K. E., & Kendall, J. E. (2011). Systems analysis and design (8th ed). Upper Saddle River, NJ: Prentice Hall.
- Merriam-Webster. (2011). Cartesian coordinate. Retrieved from <http://www.merriam-webster.com/dictionary/cartesian%20coordinate>
- Renaghan, J. (1997). Etched in Stone. Zoogoer 26(4). Retrieved from <http://nationalzoo.si.edu/Publications/ZooGoer/1997/4/etchedin-stone.cfm>
- Singer, N. (2014, February 1). When no one is just a face in the crowd. New York Times. Retrieved from <http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html>
- Stackoverflow. (2011). What does the term "canonical form" or "canonical representation" in Java mean? Retrieved from <http://stackoverflow.com/questions/280107/what-does-the-term-canonical-form-or-canonical-representation-in-java-mean>
- TheFreeDictionary. (2011). Isometry. Retrieved from <http://www.thefreedictionary.com/isometry>
- Top Rhinoplasty. (2011). Frankford horizontal. Retrieved from <http://toprhinoplasty.com/researching-rhinoplasty/rhinoplasty-glossary/#f>

SOURCE

- [1] The application of computer technology to the management of biological information. Specifically, it is the science of developing computer databases and algorithms to facilitate and expedite biological research (Animetrice, 2008b).
- [2] "A function between two metric spaces (such as two coordinate systems) which preserves distances. A rotation or translation in a plane is an isometry, since the distances between two points on the plane remain the same after the rotation or translation" (The-FreeDictionary, 2011).
- [3] "A non-Euclidean geometry in which straight lines are geodesics and in which the parallel postulate is replaced by the postulate that every pair of straight lines intersects" (Encyclopedia Britannica, 2011).
- [4] In mathematics, it refers to the shortest line – distance – between two points on a curved or flat surface. For our purposes, the two points rest on a Riemannian manifold and it is the geodesic that connects them (Answers.com, 2011).
- [5] "A process for converting data that has more than one possible representation into a "standard" canonical representation. This can be done to compare different representations for equivalence" Stackoverflow. (2011).
- [6] "A generic name for algorithms that compute the canonical form by minimization of the stress with respect to" (Bronstein et al., 2004) examining likenesses or divergence in data.
- [7] "Any of three coordinates that locate a point in space and measure its distance from any of three intersecting coordinate planes" (Merriam-Webster. 2011).
- [8] Morphometrics "by definition, involves the quantitative study of form. However, the measures we collect to study form contain information pertaining to a combination of size and shape" (Deleon, Lele, & Richtsmeier, 2002).
- [9] "A plane used in craniometry that is determined by the highest point on the upper margin of the opening of the ear canal and the low point on the lower margin of the left orbit and that is used to orient a human skull or head" (Top Rhinoplasty, 2011).
- [10] "Artec Ventures founder Art Yukhin, was a member of the team of researchers that first invented facial recognition technology in 1999" (HSNW, 2010).

APPENDIX A

Table 2.

Label	Name	Description
g	Glabella	The most prominent midline point between the eyebrows
sl	Sublabiale	Determines the lower border of the lower lip and upper border of the chin
pg	Pogonion	The most anterior midpoint of the chin
en	Endocanthion (l, r)	The point at the inner commissure of the eye fissure
ex	Exocanthion (l, r)	The point at the outer commissure of the eye fissure
p	Pupil (l, r)	Determined when the head is in the rest position and the eye is looking straight forward
pi	Palpebrale inferius (l, r)	The lowest point in the mid-portion of the free margin of each lower eyelid
se	Sellion	The deepest landmark located in the bottom of the nasofrontal angle
prn	Pronasale	The most protruded point of the apex nasi
al	Alar (l, r)	The most lateral point on each alar contour
c'	Highest point of columella (l, r)	The point on each columella crest, level with the tip of the corresponding nostril
ls	Labiale superius	The midpoint of the upper vermillion line
li	Labiale inferius	The midpoint of the lower vermillion line
sto	Stomion	The imaginary point at the crossing of the vertical facial midline and the horizontal labial fissure between gently closed lips, with the teeth shut in the natural position
ch	Cheilion (l, r)	The point located at each labial commissure
sa	Superaurale (l, r)	The highest point on the free margin of the auricle
sba	Subaurale (l, r)	The lowest point on the free margin of the ear lobe
pa	Postaurale (l, r)	The most posterior point on the free margin of the ear
obi	Otobasion inferius (l, r)	The point of attachment of the ear lobe to the cheek

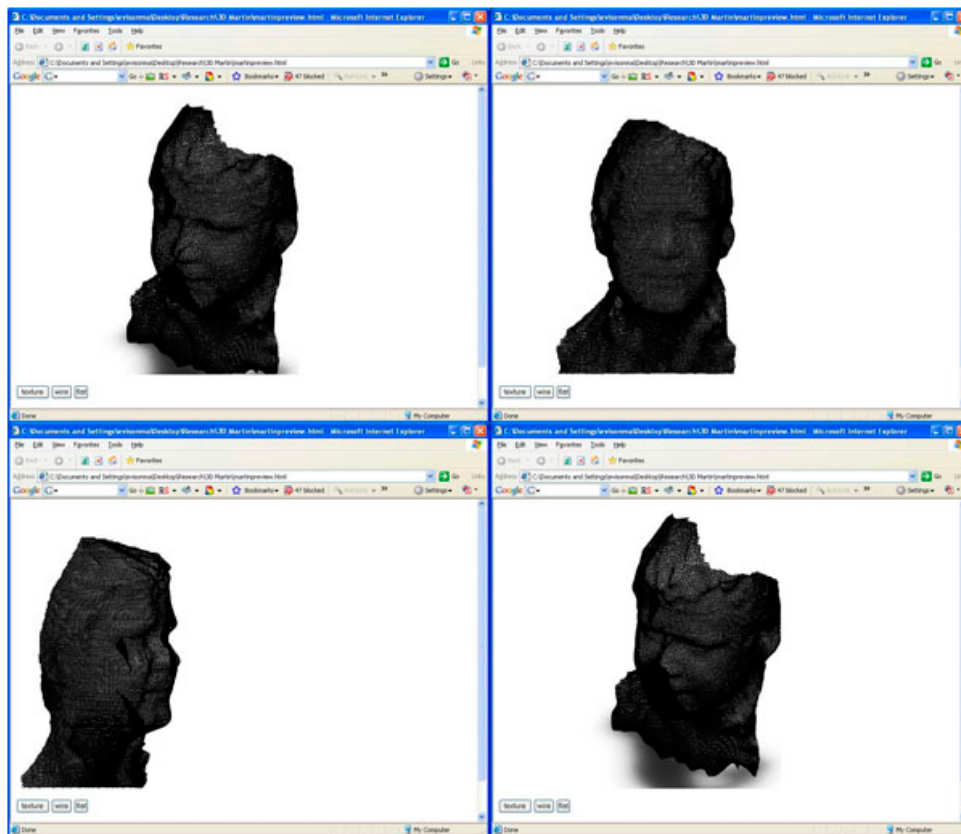


Figure 1.

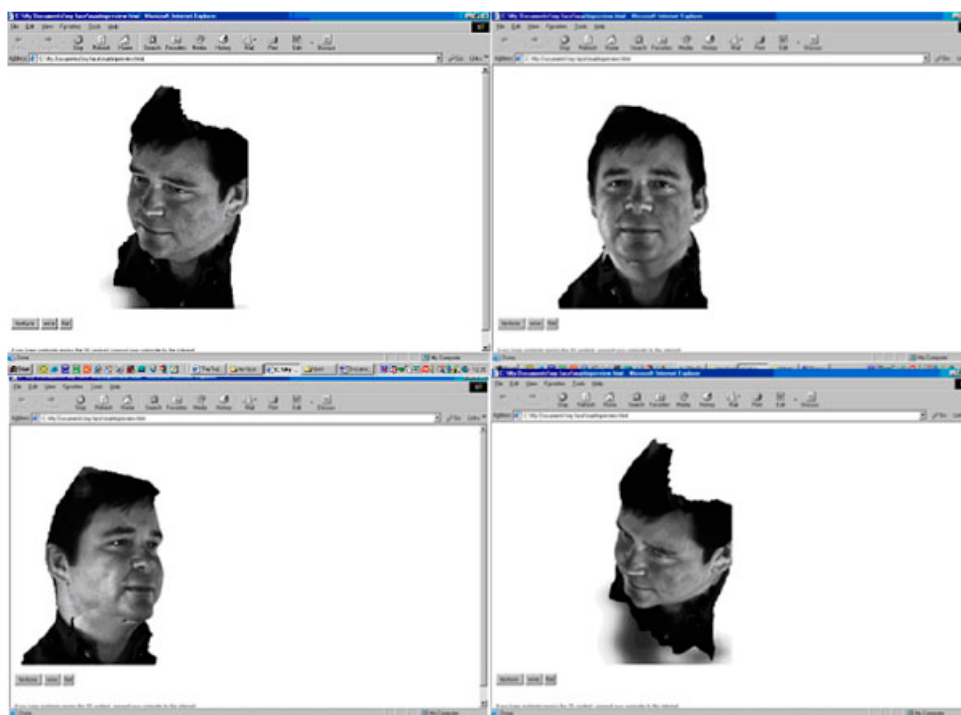
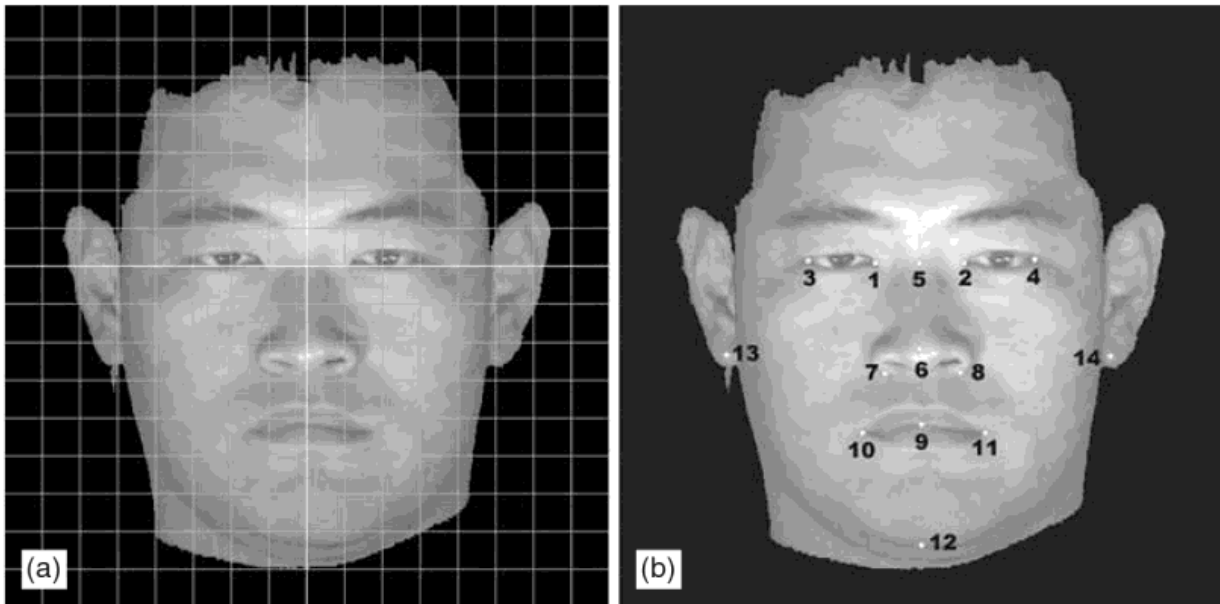


Figure 2.



The normalized 3D **facial** image of (a) a model suspect and (b) 14 anatomical landmarks.
(1) right entocanthion, (2) left entocanthion, (3) right ectocanthion, (4) left ectocanthion, (5) mid-point of both entocanthion, (6) pronasale, (7) lower point of right alare, (8) lower point of left alare, (9) stomion, (10) right cheilion, (11) left cheilion, (12) gnathion, (13) right ear lobe, (14) left ear lobe.

Figure 3.

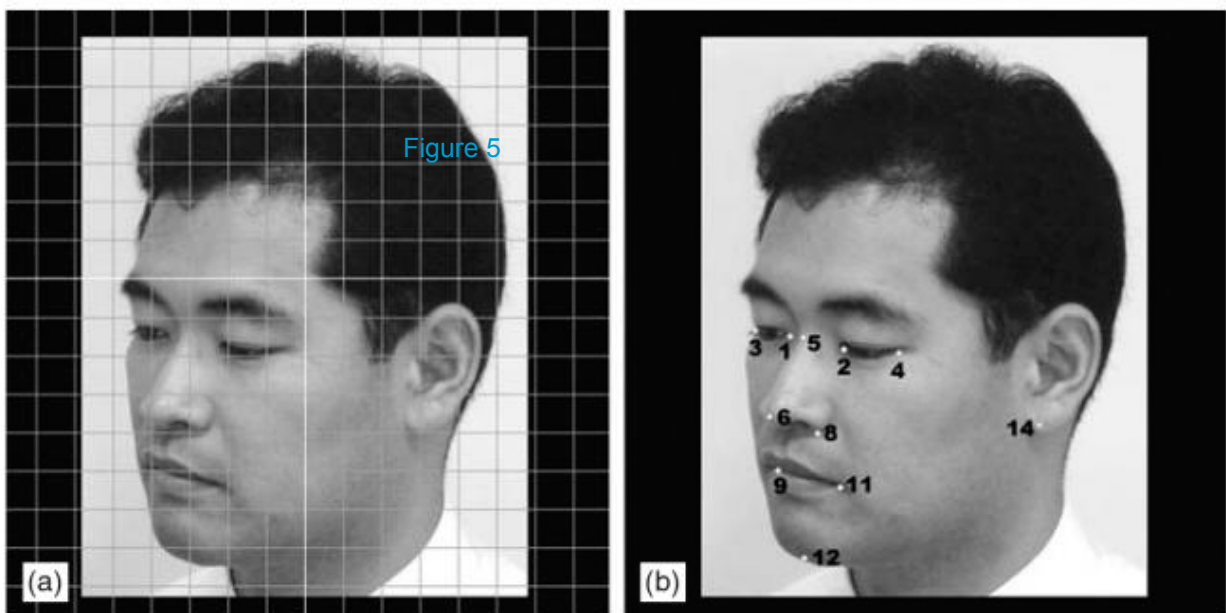


Figure 4.

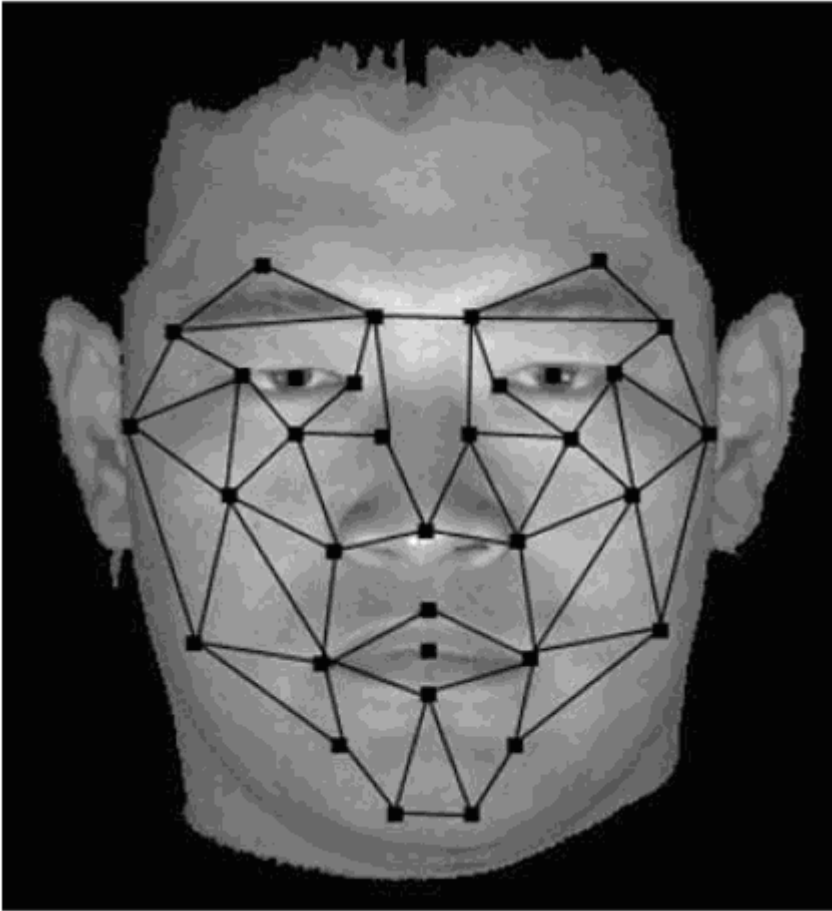


Figure 5.



Figure 6.



Figure 7.



Figure 8.

ABOUT THE AUTHOR

I have been a microcomputer consulting professional since 1983. I formed my consulting firm MicroTraining in 1985. Here, I designed RDBMSs and their associated programs. I have instructed at the collegiate level for over a decade, and within the business community spanning over a quarter of a century. I provide both strategic counsel and technical support in microcomputer software, hardware configurations and their installations and maintenance. I have a Master of Business Administration and a Master of Science in Database Systems degrees from University of Maryland University College (UMUC).

Currently, I am the Team Lead, Database Modeler (DBM), Developer (DBD), and Administrator (DBA) for the Amazon Model initiative for the Maryland-National Capital Park and Planning Commission (M-NCPPC), USA. I originated this Innovative Proposal Initiative (IPI) with the Commission – which has been fully funded for seven figures. The initiative was conceived during my MBA program at the University of Maryland, and is designed to increase class, event, and activity enrollment at the Commission's applicable facilities; this by utilizing Amazon.com's suggested products marketing methodology through automated e-mail merges and social media notifications.



NIGHT LION[®]
S E C U R I T Y

Information Security Risk Management
24/7 Emergency Incident Response

1.844.HACK.911

www.NightLionSecurity.com

LESSON 02 – ANDROID APPS SANDBOX CONTENT EXPLAINED

by **Lorenzo Nicolodi**

When a forensics expert needs to analyse an Android device, both commercial and free tools are available to recover data and to dump the content. Investigators are often able to analyse the extracted files, generating reports and allow the forensics examiner to find what he or she is looking for. Problems arises when a non-standard applications need to be analysed. Understanding how an Android application lives inside the operating system and what its home contains would probably help.

What you will learn:

- What is inside an Android .apk file
- The meaning and the content of the files composing an .apk
- How an application interacts with the system and with the other applications

What you should know:

- Some previous knowledge about Linux would help
- Some concepts explained in lesson 1, will not be explained again; reading lesson 1, would help the reader to better understand this article.

What you need:

- A Linux or Windows operating system, with a ZIP unpacker (7-zip would suffice)
- A text editor
- Desire to experiment

Android is basically Linux and as every Linux distribution, also Android has a specific format for its applications: the .apk archive. It contains all the files needed for the application to run: compiled code (in dex format), libraries, XML files describing the application properties, other files specific for each application, images, and so on. All these files, when the application is installed, are distributed in some specific file system paths and can be recovered and analyzed, with some tricks, even on non-rooted devices without the need of any specific tool. An important note before starting: in this article I am going to use the word “hacker” meaning a highly skilled technology and security enthusiast with the ability to think differently and outside any ready-made mental schema. For a formal definition of a hacker, the reader should get a look at the “how to become a hacker” guide written by Eric S. Raymond [1].

APPS, SANDBOX AND ROOTING

On mobile devices, inside browsers, on every operating system, an important concept is sandboxing; when an application, a user, a system is *sandboxed*, it is confined in a container where it has free reign, as if it was alone. Normally, in Android, every application is confined in a sandbox and it has the ability to access only the data contained inside its sandbox and it cannot, in any way, access the data contained in the other’s applications sandbox; as you can image, this has a great impact while trying to keep the system and, even more important, user data, safe.

In Android, this isolation is enforced creating, during the installation process of every application, a new user account without administrative rights, granting only to that user access to the application sandbox which is, practically speaking, the home folder of the application.

This is great, but this is not always the case. Normally, in Android, the user and the installed applications do not have administrative access to the device; when a device is *rooted*, it means that the root access to the system has been unlocked, either using an operating system feature or using an exploit. On one hand, this allows the user to unlock a series of features, capabilities and resources that are normally not accessible but, on the other hand, can compromise the isolation enforced by the apps sandbox; in fact, an administrative account can access nearly every place in the system and, hence, can access every application folder, walking around the isolation, enforced using restricted account.

Sometimes, application developers care about the fact the device can be compromised and enforce data security adding extra layers (for example, encrypting the data saved inside the sandbox). The majority of the time, they don't. From a forensics examiner's point of view, this could help; moreover, the fact a device is rooted, could also greatly help in the acquisition phase (rooting the device sometimes is required even by commercial tools).

EXTRACTING THE EVIDENCE

There are multiple ways to get evidence from an Android device: some are forensically sound while the other modifies the acquired system, potentially leading to problems when presenting the evidences in court.

Any forensics expert will use a technique or a tool, for the first time, investigating a real case device. A simple way getting the application sandbox content is, when returning the content of the private folder of every application, even if the device is not rooted. The trick is simple and has been already used in other contexts: if you cannot directly access the evidence, backup it up and work on the backup. This technique is not perfect, but it is simple and it works and can be useful in situations where other tools are not provided.

a d v e r t i s e m e n t



better safe than sorry
www.demyo.com

If the device is unlocked, the forensics expert can enable the development tools (if not already enabled) and then, after connecting the device to his or her Linux analysis workstation, it can create a backup using adb, with the following command:

```
adb backup -all -shared name-of-the-backup.ab
```

The “-all” option allows the backup all the installed applications, while the “-shared” option enables the backup of the shared memory (the external memory, stored in the SDCard, where available).

After confirming the creation of an unencrypted backup, as requested by the Android device, this command will create an .ab archive, which is not ready to be directly extracted; to do that, it has to be converted to a .tar archive, using Android Backup Extractor, which is available as an open source project on SourceForge. The syntax to convert the .ab archive to a .tar archive is the following:

```
java -jar abe.jar unpack backup.ab backup.tar
```

Now, the .tar archive can be extracted with

```
tar -xvf backup.tar
```

Resulting in an “apps” folder containing the sandbox of the installed application. Now, it is time to examine what is inside this set of folders.

Note: This procedure works if the device memory is not encrypted; in this case, only an encrypted backup can be created (the user has to submit the unlocked password in that case, to allow the backup).

INSIDE THE SANDBOX

After getting access to the sandbox of an Android application, listing the files and folders returns a set of XML files, .db files, text files, no-extension files, etc...

Are they interesting?

What information do they contain?

How can the content be examined?

On one hand, every application has its own set of files but, on the other hand, some are standard and needed by the application to work and some others are “standard solutions to store data”.

In any case, inside a sandbox, the examiner can find:

- **AndroidManifest.xml:** This file is vital for any Android application and contains the version of the application, its name, the permissions granted to it, and so on. The structure of the file is quite complex and its precise description can be found in the Android Developer Guide [2]
- **.db files:** the 99% of the times, these are SQLite files, which are files containing a whole database, with tables, indexes and so on. Android heavily uses SQLite db around the system and even famous application (for example, WhatsApp), use SQLite to store logs, caches, etc...
- **Text files:** sometime, the KISS principle is used when an application is created and packaged so sometimes a text file is the best solution to store non-critical data, properties, etc...
- **Library files:** if the application developers used Android NDK (Native Development Kit), they created some library using C/C++ and they imported and used them in the Java code using JNI (Java Native Interface).
- **Highly critical files:** some security concepts are complex and sometimes developers do not understand them, as they should. One example is symmetric / asymmetric cryptography: as demonstrated in 2013 by GitHub, where hundreds of users uploaded their private keys on public repositories [3], misunderstanding some concepts can lead to disasters, so the examiner should not be surprised when she or he finds, inside the sandbox, private asymmetric keys, keys used for encrypting with symmetric cryptography, account credentials left there “to debug purpose only”, and so on. [[make 3 or more sentences...]]
- **Binary files / strange files / no-extension files:** even if “security by obscurity”, as said multiple times, simply does not work, there are still people out there who think that putting information inside a binary file is a really smart way to protect them, because

“nobody will suppose I am going to store critical information inside a binary file / strange file / no-extension file and if they try to open it, they will be not able to get anything”. Yes, you are right, but be careful about the unicorn on your left.

GETTING EVIDENCES AND INFORMATION FROM ACQUIRED FILES

As explained in the previous paragraph, the types of files available in a sandbox are quite large so knowing their purpose and how to deal with them is critical to avoid time waste and to be effective during the analysis.

ANDROIDMANIFEST.XML

Sometimes, AndroidManifest.xml file does not exist, being replaced by its binary counterpart, named `_manifest`.

The XML file can be reconstructed using, for example, `aapt` (a tool contained in the Android SDK), with the following command:

```
aapt d xmltree ApplicationUnderExam.apk _manifest
```

Note that it could even happen that the file is named `AndroidManifest.xml` but it is, in fact, a binary XML.

.DB FILES

SQLite files can be browsed in different ways.

From the shell of a unix / linux machine, running the command

```
sqlite3 name-of-the-file.db
```

Will fire up the SQLite command line; from there, the examiner can execute SQL queries to get the content of the tables, even for discovering the list of tables inside the database, with the following statement:

```
.tables
```

In the same way, the examiner can display the tables columns with the command:

```
.schema <name-of-the-table>
```

In these db, the forensics examiner should expect to find a lot of evidences, even quite critical and non-standard format.

It happens sometimes that the db is used to store binary files, images, pdf, etc... encoded in base64, to allow their storage inside the database TEXT fields. Decoding these entries can result in interesting evidences.

TEXT FILES

Examining them should be quite straightforward, using either a text editor or some filtering tools and languages available on the examiner's unix / linux analysis machine (`cat`, `grep`, `awk`, `sed`, etc...). In this category fall the configuration files, wrongly used sometimes to store credentials.

LIBRARY FILES

If the application uses any non-standard encryption mechanism, it could be the case that it has been developed utilizing NDK, because it is harder to reverse. If the evidence to be recovered are important enough, reversing the library files and attacking the encryption algorithm could be the only way to achieve the result, keeping in mind that developing strong self-made encryption algorithm is harder than reversing a library and attacking the weak encrypting code.

If it is not feasible, putting the application in debug mode and tracing its memory at runtime could be another solution, but I will cover this approach in the next articles.

HIGHLY CRITICAL FILES

As said, the forensics examiner should expect to find also critical files inside the application sandbox, which could be useless on their own, but are imperative solving the case.

Imagine an application which encrypts all the evidences and the traffic it creates, and also capable to detect debuggers; if this application uses, a private key which is common to all the installed instances and which is stored in the application sandbox, getting it and using it could be quite useful.

If the reader has doubts about this could ever happen, the suggestion is to read the Symantec article reporting it [4], explaining how criminals let the decryption keys on the machine infected by their own ransomware.

BINARY FILES / STRANGE FILES / NO-EXTENSION FILES

Apart from all the standard file presented up to now, sometimes happen that the file to deal with are binary files, files with proprietary format and extension, serialized object saved as files or file without any extension. In this case, looking at the code as presented in lesson 1, could clarify how the file is created and its internal structure, allowing the examiner to write its own code to extract evidence from those files.

Last but not least, three important notes:

- As the reader probably knows, linux does not care about the filename extension as Microsoft operating systems, preferring the use of headers and footers bytes to identify the type of file it is dealing with, and the same does Android (with some exception, for example where the operating system expects a precise file name).
- If the examiner looks at the application sandbox, she or he will not find the classes.dex file; this is because it is not stored there. The apk, after the installation, is saved in /data/apps/, while the dex file can be found in /data/dalvik-cache/ (if the old Android virtual machine is used, instead of ART, the new virtual machine, packaged since Android KitKat).
- Extracting the .apk content and evaluating the content of the application's strings (contained in the res/values/ folder) could result in discovering important evidences, such as credentials.

CONCLUSIONS

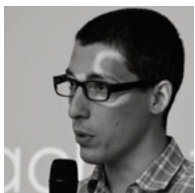
Most of the time, the forensics expert will encounter and analyze standard application with open source, free and commercial tools but when these are not available due to the particularity of the app under examination, knowing how to deal with these files could save his or her day (and night).

In this brief article, the examiner has been presented with the content of the Android application sandboxes and a simple way to get them from the device, explaining what a sandbox is and what kind of evidence can be retrieved from it, showing their meaning and content and suggesting what can be extracted from each of them, and how.

REFERENCES

- How to become a hacker
 - <http://www.catb.org/esr/faqs/hacker-howto.html>
 - <http://developer.android.com/guide/topics/manifest/manifest-intro.html>
- Github Kills Search After Hundreds of Private Keys Exposed <http://slashdot.org/story/13/01/25/132203/github-kills-search-after-hundreds-of-private-keys-exposed>
- CryptoDefense, the CryptoLocker Imitator, Makes Over \$34,000 in One Month <http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month>

ABOUT THE AUTHOR



I started working full-time in the IT field in 2006, when I joined the Bachelor course in Applied Computer Science at the Free University of Bolzano. Working for three different companies in 5 years, I earned experience in IT, networking and security while improving my development and analysis skills until I graduated in 2011. Now I am working as Android Mobile Analyst in Padua (Italy). You can contact me at lo@hidden-bits.com and check my LinkedIn profile (<http://www.linkedin.com/profile/view?id=71754670>).

UPDATE
NOW WITH
STIG
AUDITING

“IN SOME CASES
nipper studio
HAS VIRTUALLY
REMOVED
the **NEED FOR** a
MANUAL AUDIT”
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com



www.titania.com

SSH COMMUNICATIONS SECURITY

“PRIVILEGED ACCESS MANAGEMENT”

IT SECURITY’S DIRTY LITTLE SECRET: ENCRYPTION MANAGEMENT FLAWS PUTTING ORGANIZATIONS AT RISK

by Jason Thompson

Over the past year alone several advanced threats and security breaches made headlines including Careto (also known as The Mask), Heartbleed and the infamous Edward Snowde; all of which spotlighted how critical IT processes – like encryption – are often overlooked. In each of these cases, a lack of management control and visibility rendered it possible for malicious parties to access sensitive information illicitly.

What you will learn:

- How encrypted channel monitoring provides a holistic approach to privileged access management that prevents attackers from using back doors or workarounds to exfiltrate data
- Why organizations must assess their network environments and put into place next generation security solutions
- IT teams can uncover and address the PAM issues that have been hidden far too long beneath the surface by examining and reevaluating the organization’s Secure Shell environment

What you should know:

- A lack of encryption management leaves organizations vulnerable to security breaches
- Security breaches are typically a result of ineffective privileged access management (PAM) and not because of flaws in the encryption protocols themselves
- Conventional PAM practices are not enough to keep data safe and secure

Even though the average person uses encryption every day to keep personal data safe and secure, they likely don’t know much about how it works. As with all technologies, as they “age,” their cost decreases. Often so much so that today encryption technology is perceived as a commodity and widely deployed as open source software. For example, the Heartbleed vulnerability was discovered in OpenSSL, an open source encryption software. There is a large debate as to whether commercial or open source security software is better for enterprises. Regardless of whether an organization is running commercial or open source, the main priority should be proper management.

The unfortunate reality is that encryption technology isn’t typically top of mind for IT managers and executives, which as time has shown can be a serious problem. Software will always have vulnerabilities and breaches will occur, but it’s important to remember that it’s typically not the software itself or the encryption protocol that is the issue. In most cases, a lack of encryption management leads to unmonitored and ineffective access controls that create back doors and workarounds into secure systems.

LEAVING NETWORK DOORS WIDE OPEN

While recent breaches have helped raise awareness around the importance of encrypted network management, there is still a lot more going on behind closed doors that deserves attention.

In the case of Secure Shell-protected networks, key-based authentication is a common way users gain access to sensitive information. At their most basic level, keys are simple text files. They are easy to create and upload to the appropriate system making them widely implemented. With each specific key is an assigned identity, either a machine or a person that grants access and performs specific tasks. These tasks – such as the ability to transfer a file – may seem simple, but oftentimes Secure Shell keys provide access to some of the most critical information on the network.

If one were to do that math based on every employee, contractor and application that has been granted key-based access within an organization over the past decade or longer, there's potentially over a million keys circulating in any given enterprise. In one example, a large financial institution had over 1.5 million keys in its network environment. Approximately 150,000 of these keys granted high-level administrator access. This number represents a huge vulnerability in the form of open doors that no one was monitoring for unprivileged access. This might seem like an extreme case, but in reality this is a fairly common situation wherein keys are created but never monitored.

In other instances "convenience" factors can leave systems vulnerable to attack. Application developers and system administrators commonly create and deploy keys in order to easily gain access to systems they are currently working on. These keys usually grant a fairly high level of privileged access and simultaneously used across multiple systems for ease-of-use. The downside is that these keys often have a one-to-many relationship that puts the system at risk. In the event that an employee is terminated or reassigned within the company, that employee will continue to carry the same level of access via their assigned Secure Shell keys. It's a common misconception that terminating the account is enough to remove access; in fact, the individual keys must also be removed or the access will remain in place.

a d v e r t i s e m e n t



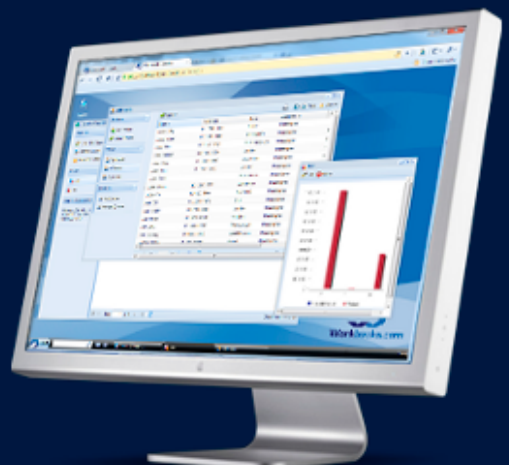
Web Based CRM & Business Applications for small and medium sized businesses

Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

Contact Us to Find Out More

+44(0) 118 3030 100
info@workbooks.com



PRIVILEGED ACCESS MANAGEMENT WORKAROUNDS

Another commonplace danger of unmonitored Secure Shell keys is the use of the keys to subvert privileged access management systems (PAMs). Many PAM systems utilize a gateway or jump host that administrators log into to gain access to the network. PAM solutions connect directly with user directories to assign privilege, monitor user activity and record any actions taking place. While this may sound like an airtight way to monitor administrators, it's actually quite easy for an admin to log into the gateway, create and deploy a key and then use key authentication to gain access; a clever work around any PAM safeguards.

In encrypted environments, lack of access control is only part of the story. Conventional PAM solutions that utilize gateways and focus solely on interactive users are designed to monitor administrator activities. However, as mentioned above, these solutions end up being fairly easy to bypass. In addition, data-in-transit encryption blinds hacker activities the same way it blinds security operations and forensic teams. Because of this, encrypted traffic is rarely monitored and is usually allowed to flow freely in and out of the network environment. This creates obvious risks and negates security intelligence capabilities to a large degree. In order to eliminate this risk, an organization must decrypt and inspect all traffic moving in and out of the network.

ENCRYPTED CHANNEL MONITORING

To decrypt Secure Shell traffic, an organization needs to utilize an inline proxy with access to the private keys – essentially a friendly man-in-the-middle – that won't cause network interference. If this process is done successfully, all encrypted traffic for both interactive users and M2M identities can be monitored. Additionally, because this monitoring is done at a network level, malicious parties can't execute workarounds. By using this method, enterprises can proactively detect suspicious or non-policy traffic. This approach is called "encrypted channel monitoring" and is the next generation of PAM solutions.

Encrypted channel monitoring helps an organization deploy a more holistic approach to PAM and prevents attackers from using an organization's own encryption technology against itself. Keeping track of encryption data also permits organizations to utilize inline access controls and user profiling to control which activities a user is permitted. For instance, policy controls can be enforced to prohibit file transfers from specific systems. With even more advanced solutions, organizations can even block subchannels from running inside the encrypted tunnel; the preferred method for quickly exfiltrating data.

MOVING FORWARD

The IT industry has embraced encryption technology for many years, using it ubiquitously in computer networks, data centers, applications and other foundation infrastructure. Recent security breaches have shown the technology community that widely used, critical technologies like encryption have lived below the surface for too long, operating without proper monitoring and management.

The majority of enterprises do not employ best practices for managing encrypted networks, like centralized provisioning, even given the obvious risks of ignoring proper monitoring and management. Rarely do organizations implement encrypted channel monitoring and many assume that conventional PAM are solving the problem when in fact, easy workarounds can render these methods ineffective.

IT security managers should feel compelled to invest in solutions that ensure these technologies are as secure as possible. The first step for any organization is to take a serious look at its encrypted networks to ensure layered defenses are in place and that proactive monitoring is ongoing. Encrypted channel monitoring can have a profound impact on preventing critical, widespread security disasters and keep an organization's critical assets safe and secure.

ABOUT THE AUTHOR



Jason Thompson is director of global marketing for SSH Communications Security. Mr. Thompson brings more than 12 years of experience launching new, innovative solutions across a number of industry verticals. Prior to joining SSH, Mr. Thompson worked at Q1 Labs where he helped build awareness around security intelligence and holistic approaches dealing with advanced threat vectors. Mr. Thompson holds a BA from Colorado State University and an MA for the University of North Carolina at Wilmington.



Penetration Testing



HP ArcSight Consultancy



SIEM Deployments



CYBER SECURITY EXPERTS

From security assessment services to complex SIEM deployments, we have the experience to deliver an unrivaled service.

Visit our website to discover how we can help you develop advanced threat detection capabilities within your enterprise



The Best SharePoint Training in the World returns to Boston!

Choose from more than 80 classes and tutorials!



"I really enjoyed it. I can hardly wait to get back to work and start using what I learned. I will encourage employees and co-workers to attend future SPTechCons. The conference had great speakers with relevant subjects, and the whole thing was well organized."

—Greg Long, Infrastructure Development Manager, ITG, Inc.

"I prefer SPTechCon over Microsoft's SharePoint Conference in Vegas. I'm definitely going to tell others to go."

—Ray Ranson, Senior Architect, RSUI



September 16-19, 2014

The Boston Park Plaza Hotel & Towers

Bolster your career by becoming a SharePoint Master!

- Learn from SharePoint experts, including dozens of SharePoint MVPs and Certified SharePoint Professionals
- Master document management
- Study SharePoint governance
- Find out about SharePoint 2013
- Learn how to create applications for SharePoint that solve real business problems
- Exchange SharePoint tips and tricks with colleagues
- Test-drive SharePoint solutions in the Exhibit Hall

If you or your team needs Microsoft SharePoint training, come to SPTechCon Boston!

Register Early and SAVE!



www.sptechcon.com





Dr.WEB®

since 1992



Dr.Web 9.0

for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search



© Doctor Web
2003 — 2013

www.drweb.com

Free 30-day trial: <https://download.drweb.com>

New features in Dr.Web 9.0 for Windows: <http://products.drweb.com/9>

FREE bonus — Dr.Web Mobile Security:
<https://download.drweb.com/android>

