eForensics Magazine

NETWORK

VOL. 1 NO. 4

David Sun

CEO of SunBlock Systems

Pragmatic Solutions: Adapt, Learn, and Overcome

Real-Time Intrusion Detection for Critical Infrastructure Protection: CockpitCI Approach

Ways to Detect BIOS Clock Anti-Forensics

How KPMG Uses EnCase® tools to Solve Clients' E-Discovery Challenges in Canada

DIY Remote Networked OS X Monitoring

Security in Wireless Sensor Networks Major Attacks, Encryption Algorithms and Security Protocols

Network Intrusion – Understanding the Threat Environment

Are all Secure FTP Servers Secure

Issue 4/2012 (4) December

ISSE

INTEGRATED SAFETY & SECURITY EXHIBITION

LEADING NATIONAL SAFETY & SECURITY EXHIBITION IN RUSSIA

INTEGRATED SAFETY AND SECURITY EXHIBITION

2013

May 21-24

Moscow,
All-Russia Exhibition Center, Hall 75

- Protection & Defence
- Technical Facilities for Border and Customs Control
- Security Technical Systems and Equipment
- Fire Protection
- Rescue Equipment
- Disaster Medicine
- Environmental Safety
- Industrial Safety
- Equipment for Nuclear, Chemical and Biological Safety
- Information and Communication Security
- Transport Safety

www.isse-russia.ru

Organizers:

Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequencies of Natural Disasters (Emercom of Russia)

Ministry of the Interior of Russia

Federal Service of Military-Technical Cooperation

XRY COMPLETE

IT'S NOT ABOUT DATA. IT'S ABOUT MEANING.

If you think mobile forensics is just about extracting data – think again. Its not only what you get, but what you do with it that really makes the difference.

XRY has an intuitive GUI that's easier to use, has better display capabilities and superior analysis functionality.

MICRO SYSTEMATION

msab.com

eForensics Magazine
TEAM

Editors: Stanisław Podhalicz
stanislaw.podhalicz@eforensicsmag.com

Betatesters/Proofreaders: Antonio Merola, Olivier Caleff, Danilo Massa, Gabriele Biondo, Simohammed Serrhini, Stephen Patton, Andrew J Levandoski, Dan Dieterle, Nicolas Villatte, Jan-Tilo Kirchhoff, Henrik Becker, Cindy Brodie, Alex Rams, Jeff Weaver, Vaman Amarjeet, Salvatore Fiorillo, Liora Farkovitz, Danny Lavardera, Larry Smith, Vernon Jones, Johan Snyman

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director: Ewa Dudzic
ewa.dudzic@software.com.pl

Publisher: Software Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.eforensicsmag.com

DISCLAIMER!

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

Dear Readers!

I would like present eForensics Network, a publication with an expanded focus. While supplying our readers with IT Security updates and new product concepts, we are also reaching a larger audience. Digital forensics is increasingly important to the law enforcement professionals who are pursuing criminals on a daily basis. It's not necessary, or easy, to become a computer forensics expert, but it's very important to know how to recognize the digital evidence which will reinforce cases and to know who to turn to for help.

The opening interview by Liora Farkovitz with David Sun sheds some light on how important it is to include IT specialists in either a company or Police investigation. He provides several true stories, sharing his experience as a hands on investigator that are interesting, but he takes it a step further demonstrating the importance.of working together with academia, the legal system and product development to provide meaningful tools..

Next, IT veterans – Yasakethu and Jiangreat (both PhDs) give us a magnificent insight into CockpitCI – a program which can take actions during real-time cyber attacks.

The article written by David Sun (our interviewee), points out a couple of basic but often easily forgotten operations while examining the suspects' computer. For example, a check on the BIOS Clock was manipulated can save a lot of time and work when you know how to do it – this is really well explained in the article.

Dominic Jaar shares his views about big companies which use forensics programs to work remotely, safely and fast across huge distances.

Lost in an earlier transition, but found and published at last, the article by Israel Torres who addresses the topic of Apples OS X. He explains how to control it remotely. We would like to assure you that there will be more issues concerned with the topic in the future.

Deivison Franco spreads his in depth knowledge about the main vulnerabilities, attack encryption algorithms and security protocols for Wireless Sensor Networks.

You can seize the opportunity to learn about environmental threats from Damon Petraglia, the subject of our interview in the October edition, who presents his thoughts about the issue. The article may be treated as your first step toward creating unsurpassed security.

Last but not least, the article from Neil Maher. It is definitely Secure FTP Servers in a
nutshell. The knowledge gained from reading the article can be used instantly.

In Poland we have a tradition of not only capitalizing "I" but the words that reflect the humanity of all of us, and in this tradition, I hope You enjoy the publication as much as I have enjoyed editing it for You. I will be more than pleased to hear your opinions about this edition of the magazine. I would like to thank to all the people who helped me with the issue. There would not be an issue without you.

Thank you,
Stanisław Podhalicz
& eForensics Team

PRAGMATIC SOLUTIONS: ADAPT, LEARN, AND OVERCOME

06

by Liora Farkovitz

In the field of Digital Forensics there are three interactive elements; academia, governments, and businesses. In an ideal world these three elements create a synergy between one another that ultimately fuels the growing and diverse needs of forensic investigators.

18 REAL-TIME INTRUSION DETECTION FOR CRITICAL INFRASTRUCTURE PROTECTION: COCKPITCI APPROACH

by Lasith Yasakethu and Jianmin Jiang

Cyber-attacks against control systems are considered extremely dangerous for critical infrastructure operation. Today, the protection of critical infrastructures from cyber-attacks is one of the crucial issues for national and international security. Over the past ten years, intrusion detection and other security technologies for critical infrastructure protection have increasingly gained in importance.

WAYS TO DETECT BIOS CLOCK ANTI-FORENSICS

26

by David Sun

The ultimate purpose of any forensic computer investigation is to correlate activities on a computer with real world actions by an individual. Accomplishing this can help a trier of fact decide what actually happened in a given situation.

30 HOW KPMG USES ENCASE® TOOLS TO SOLVE CLIENTS' E-DISCOVERY CHALLENGES IN CANADA

by Dominic Jaar

Clients of KPMG in Canada turn to us when e-discovery challenges loom and they're not sure they have the internal capability to meet their legal obligations in a cost-effective fashion. What we bring to those clients is our experience providing tested and reliable processes and solutions customized to their particular situations.

DIY REMOTE NETWORKED OS X MONITORING

36

by Israel Torres

Remote access to a machine (or more so machines) is status quo these days; we are creatures of convenience and if we can operate as easily from a remote location as we can at the office we'll take it.

44 SECURITY IN WIRELESS SENSOR NETWORKS MAJOR ATTACKS, ENCRYPTION ALGORITHMS AND SECURITY PROTOCOLS

by Deivison Pinheiro Franco

Article is an approach regarding safety analysis in Wireless Sensor Networks (WSNs), which displays components, concepts and operational aspects of security for WSNs. It demonstrates how to operate sensors, process and transmit information based on the processes of decision making, according to processing regions.

NETWORK INTRUSION – UNDERSTANDING THE THREAT ENVIRONMENT

54

by Damon Petralgia

The following article discusses the cyber threat landscape through a non-technical broad approach. It is not meant to be all encompassing and should be an introduction to network intrusion threats for some, whereas for others it should serve as a review. Understanding the current threat landscape and the methods used for network intrusion are crucial to investigators who work to solve criminal acts.

56 ARE ALL SECURE FTP SERVERS SECURE

by Neil Maher

When discussing Secure FTP Servers, one must first define what is meant by the term. For the purposes of this article, we are defining Secure FTP to mean FTP over SSH, commonly known as SFTP. SSH is used worldwide as an encryption method not only for secure access into a remote Unix or Linux server, but also as a transport protocol for file transfer.

PRAGMATIC SOLUTIONS

ADAPT, LEARN, AND OVERCOME

AN INTERVIEW BETWEEN LIORA FARKOVITZ AND DAVID SUN, CEO OF SUNBLOCK SYSTEMS

by Liora Farkovitz

In the field of Digital Forensics there are three interactive elements; academia, governments, and businesses. In an ideal world these three elements create a synergy between one another that ultimately fuels the growing and diverse needs of forensic investigators.

The tools and procedures that each discipline develops are carefully crafted by professors, forensic technologists and business executives. The cycle then refines implemented tools by way of students, interns, legal professionals and the academic realm. Continuing education systems keep current professionals up to date, and also draw from their experience by sharing the pitfalls and advantages of various methodologies with professionals they interact with.

Personally, as a small business owner, providing consulting and product development services, I have always enjoyed the process and the journey more than "arriving" at a preconceived destination. An untold amount of research goes into identifying the needs of a consumer group, identifying the problems that exist, and the issues that must be overcome. What those challenges are and how they present themselves are as varied as both the number, and the types of, stars in the skies. Choosing which ways to respond to those demands is part of the love-hate relationship every business owner has with their own enterprise. As soon as you think you've finished your product, it's time to change it all over again to meet new demands.

While educational institutions provide an amusement park worth of thrilling rides and experiences and access to the world's brightest minds, and governments, through its investigations and enforcement and legal systems; and serve as the ultimate computer laboratories, small businesses bring certain pragmatism and a lightening fast application of our combined knowledge and experience. Businesses, whether for profit, or non-profit, are alternatively demonized and hopefully, more often praised.

For this issue, I interviewed David Sun, who is the CEO of SunBlock Systems, which is nestled near Washington, D.C., the capital of the United States. His own personal story is a mirror reflection of academia, government needs, and the agile response of a small business responding to the needs of the communities it serves. David is a consultant, technician, expert witness, and product innovator, as well as collaborator. In the flurry of peo-

ple I first interviewed, we juggled schedules and ended up getting to know one another “on the fly” without a lot of preparation. I hope you enjoy discovering David Sun, every bit as much as I have.

LF: My background is – I’ve worked in technology all of my adult life. About five or six years ago, I had a legal experience that did not go so well. One of the things I discovered was that a lot of people that work in the court systems don't really understand very much about technology. I mean things that I took for granted, they had no clue about, so I wrote a technology guide for legal professionals and published it and developed an online course with the hope of getting attorneys and judges to pay a little bit more attention to the basics so that they aren't dismissive of the kinds of things you do. I hear you laughing. This could be an exercise of futility on my part!
DS: Well, no. There's actually a lot of value in that, there's definitely some pertinence to this and what you can do. What I'm doing, as part of my business, is actually developing courses for all these attorneys who have CLE (*Continual Learning Education*) requirements.

LF: They're CLE courses. That's what mine is, eventually… I hope to have that label.
DS: That's exactly what we're doing. We're developing CLE courses related to computer forensics, e-discovery, and topics like that. Obviously, there's a CLE course for everything out there. They have classes for how to track your time better for building purposes, so you can do a CLE for anything that benefit the legal profession. It sounds like the kind of stuff you're talking about would be a great CLE class that gets them to understand some of my stuff.

LF: The challenge that I have is that I've always worked on my own. I'm an entrepreneur and have been for a long time, but I just don't have the resources that I did before the NASDAQ crashed. I had to shut down my company as a result the stock market problem. I've done consulting and that sort of thing and I have a really bizarre set of specialties. They don't necessarily merge that well because it's so heavy in publishing in that kind of thing, but you never know… I was looking at your BitFlare. I think that's a really interesting product. I like how you've designed it in a way that's idiot-proof, pretty much, and that puts the onus on your staff to be able to filter through everything and it protects the individual from hurting their evidence or their case and that's really something that I think is needed. I think it was a smart approach.
DS: Yes. Unfortunately for us, as well as others who subsequently copied our product, a lot of us have found that as wonderful of a technical development for the industry, as BitFlare and its approach is, we're finding that judges and lawyers are quick to dismiss what they don't understand from a technology standpoint. This means they often just go and say, "Well, this is new. I’m not comfortable using it."

LF: Well, they don't want to try it… because it's as though you were going to explain quantum physics… and have it not be called "magic." This is something that people just don't understand. They're very afraid of it. You have to give it to people in their own vernacular and in a context that makes sense to their everyday world, and a lot of people that are technical are not sensitive to the obvious. They think that people shouldn't be offended by the obvious, but sometimes they are. Anyway, I've always been good at explaining that and I think that's because, for whatever reason, my brain is pretty much equally artistic and humanistic and technical and mathematical, so I'm able to bridge both worlds and I enjoy doing that. I ended up being asked to write for e-Forensics as a result of what I had written. I was (also) writing about research that I was doing related to fed-

eral funding and how certain types of cases are falling through the cracks, particularly cases of child pornography or trafficking or pedophilia; these are getting kind of lost in the legal system between the civil and criminal sides of our legal system. So sometimes I speak and do those kinds of things too. This is the second interview that I've done for e-Forensics (the third published). My first article was about Shaun Winter of the Brooklyn D.A.'s office, he's their Supervising Investigator. So the first article I did was about him. He happened to plant a wire tap in a judges chambers and his evidence convicted him of taking bribes on custody cases.

DS: Wow.

LF: So it was pretty interesting. I didn't get to write about that in that article, but it was interesting to talk to him about this and it's the nature of these kinds of conversations. I don't really know when we're done talking exactly what angle I'll take, but you know probably something along the lines of what you're trying to accomplish with BitFlare, and bridging that gap that there is between the public and people like us who take technology for granted. So what's your background? Tell me. I didn't get a chance to read everything.

DS: Well, I'm a technical person. So I started off in technology. I went to school and got a Bachelor's in Electrical Engineering and then did a Masters in Electrical Engineering with a focus in electromagnetics. I actually even started working on a PhD for a while, and it was a lot of hours in the field that's heavy in physics. You use quantum physics as an example, but honestly what I did had something to do with quantum physics! To give you a better idea of what I was doing in graduate school, as well as working with the company while in grad school, I was dealing with fiber optics and light and electromagnetics. Basically the best example that I tell people is, you know in "A Beautiful Mind", that movie with Russell Crowe playing the main character? He's a physicist and he's writing all these crazy equations on the board.

LF: Right…

DS: I used to write those types of equations. I used to do a lot of technical, intellectually stimulating type of research and I did that for a while. I even started on a PhD thinking that would be fun, and, like I said, it was very intellectually stimulating. But then I kind looked around and looked at the guys that got their PhDs before me in the same program- a really well known program at the time in the country. I watched these guys sitting around looking for jobs after they got their PhD, and they can only go to one of about three or four places in the country. Unless they want to teach in academia, if they wanted to go in the industry they can only go to three or four places in the country and usually they're sort of waiting for somebody to retire or die so that they could take their position. I kind of realized the job mobility wasn't what I wanted it to be.

LF: We all have these bitter realizations when we get out of school that we're going to have to be a lot more patient than we had planned.

DS: Yeah, so at the end of the day I kind of though, "Well, that's interesting, maybe I should look for a career path with broader appeal". At that time the technology, the internet, AOL (*America Online*), and that industry was really starting to pick up and so I ended up being fortunate enough to find a job supporting research and development for a lot of the telephone companies. Ultimately what happened was, in 1994, when AOL was advertising their new high-speed 56k modems.

LF: I remember.

DS: Around the year 1994, I was actually doing work for what is now Verizon. I was actually working for NYNEX, PacBell, and Bell Atlantic and we were building back then what has now become FiOS.

So in 1994 we had 1.5 megabit DSL lines, which seems slow now, but back then 56k was the leading edge. We had 1.5 megabit DSL lines to people's homes delivering digital video and people could use video on demand. They could start a movie when they wanted to. They could stop it, pause it, and rewind it, all that type of stuff. And that was in 1994 when AOL was just advertising their 56k modems.

LF: Were you in New York when you were working for NYNEX?

DS: Actually what happened was NYNEX, Bell Atlantic at the time, and Pacific Telesis (PacBell), formed a joint venture. It was an R&D type of group. They had a New York office that was the marketing executives and all the Hollywood mogul types. Then they had a California, Los Angeles office where they would attract the Hollywood talent because they were trying to get the Hollywood studios to buy into the video-on-demand concept and make their movies and title available to telephone companies for video-on-demand. Lastly they had the systems and technology team that was actually centered in Virginia because, in Reston, Virginia, AOL was here; MCI was in the DC area, so all the high-tech stuff was in the northern Virginia area for Telecom. So they created their technology division here in Reston and that's where I worked.

LF: So you started a company in 2002. What did you do between that project and starting your company?

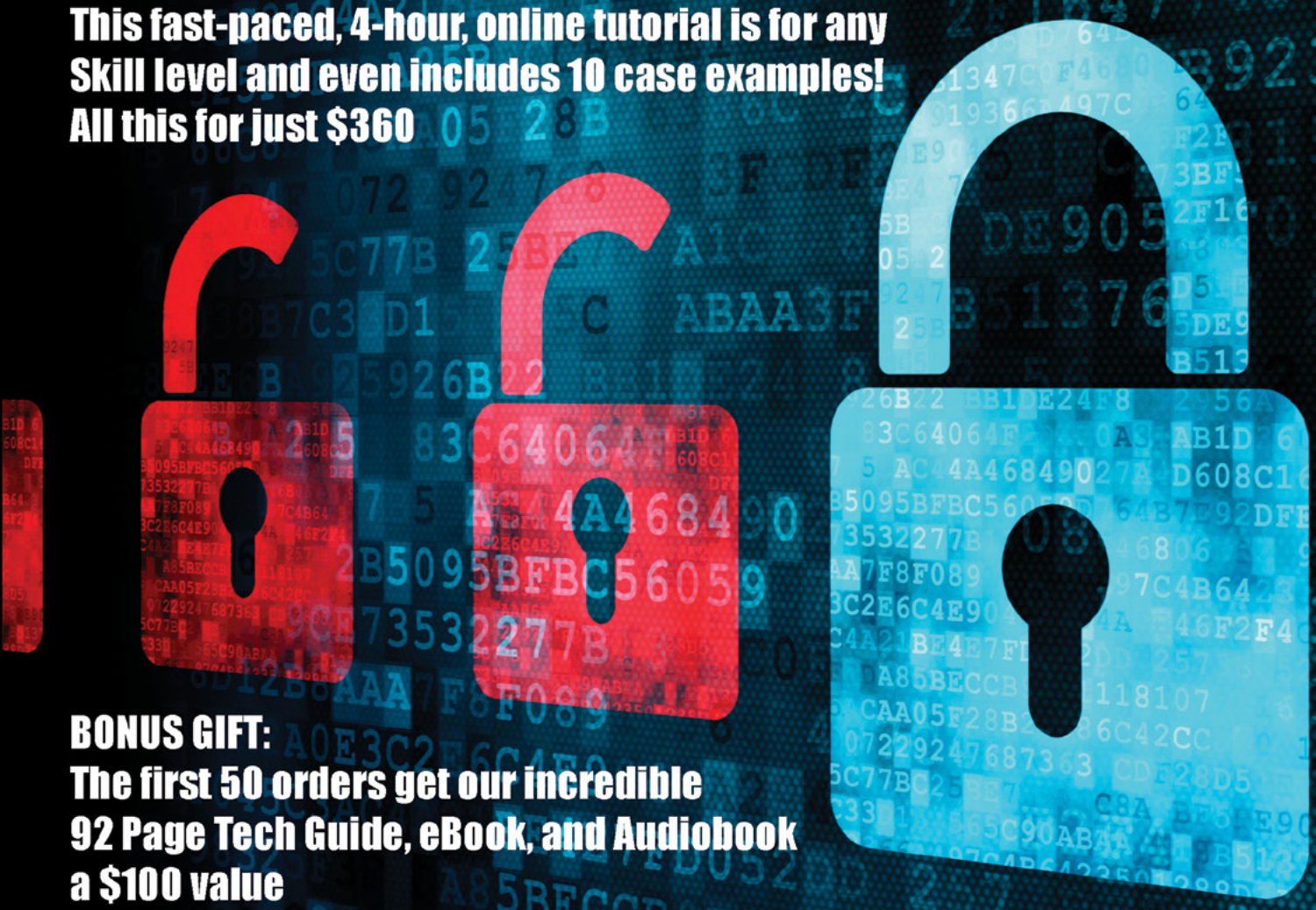
DS: I left that project and decided, again this is 1994-95, thought, "Well, this DSL stuff is great but

Make them hang on your every word...
Put them on the edge of their seats when you speak...

Leave them wanting more...
It can happen, but ONLY IF YOU GET THIS:

THE ELECTRONIC ADVANTAGE: 101 the Basics

This fast-paced, 4-hour, online tutorial is for any Skill level and even includes 10 case examples! All this for just $360



BONUS GIFT:
The first 50 orders get our incredible 92 Page Tech Guide, eBook, and Audiobook a $100 value

Go here now and order:
www.technologicalevidence.com

it's just not fast enough and it's not going to work the way it's supposed to for video." The way I saw it back then was, video-on-demand is going to happen but it's going to be delivered over the internet because this is when the internet started taking off. In 1994, 56k modems really weren't taking off quite yet. It was taking off, but it wasn't in everybody's home and you didn't have your e-commerce, you didn't have your streaming media. You didn't have any of that type of stuff.

LF: Nobody said, "World wide web," yet.
DS: Yeah, very few people did, but by 1995-96 I could see the internet really taking off and I could see how 1.5 megabit DSL was still difficult to get to people's houses. The technology wasn't there yet. So I figured, "You know, I need to spend time on this internet stuff because I think video and all this content that we're talking about doing is really going to come to people's houses eventually through the internet. And so I went over to UUNET and worked over there for a little. I don't know if you remember UUNET, but they were a big company playing a big part in building the internet. I worked over there for a little while and I was doing engineering for them. I did that for a couple of years, and then I ended going over to a telecom startup. It was back in '99 so it was during the dot.com boom.

I went to a well funded, VC (venture capital) startup company, and I went there to do video over internet to businesses and their high-rise corporate office buildings. I was there to do that, but again the technology still hadn't quite matured yet, so I ended up doing a lot of systems development and security related type of stuff. Long story short, the dot.com bubble burst, company went under, I got laid off.

LF: Yes, I remember… (Note: and I say this forlornly because my own company hit the skids at the same time!)
DS: Yup, and I ended up starting my own company. I took all the different pieces I had and what really happened was I met up with a corporate investigations group with a bunch of guys who were retired FBI, retired Air Force OSI, basically a lot of retired law enforcement types who were doing corporate investigations for companies. What they said was, "We're doing all these investigations and at the end of the day what we're finding is people aren't writing down the stuff they do anymore. They just do it all through email and the computer". This is around 2000-2001. They said "so our suspects these days are doing everything on the computer, and we don't know how to investigate this computer stuff". Again, these are retired government guys. "We don't understand how this computer stuff works so well, but we know the evidence is in that box on the desk. You seem to know a lot about computers. How about this: come team up with us. We'll work with you on the investigative aspect of things and you work with us on the computer related type of things". In short, these guys were saying, "It's a lot harder to teach a cop how to be an IT guru, and a lot easier to teach an IT guru how to shoot a gun". So we kind of went down that route together and shared a lot of industry experience together.

LF: I do. Well, I mean, for you to have the principles of surveillance or the chain of custody, you know, how to isolate evidence and maintain its integrity, I think there are some similarities because there is a certain science behind it and there are steps.
DS: So what I say is that for chain of custody, all that kind of stuff, they pretty much teach young guys how to do that in three months in police academy, so that's not that hard to learn. Whereas the technology, the fundamentals, from soup to nuts, everything from the internals of Windows to an Exchange server, not just how they work, but how people actually use it, the human aspects and the human interaction, that takes years to really understand and grasp. But that's the key for computer forensics. We not only have to understand how computers work, we have to have knowledge about how people use computers from a human perspective.

What do people normally do with computers? Where do they squirrel away the data? We know they're told to keep it on a network folder for the company because it's all backed up. *But what do they really do?* Well they usually keep it on their desktop. Sometimes they drop if off onto the root of the C: drive. Sometimes they save stuff in that temporary directory when you double-click the attachment in Outlook, and then they edit it and save it and next thing you know it's buried in some really, really deep, hidden directory somewhere that's meant only for temporary stuff but because the user doesn't know any better they keep it there. That's the kind of stuff that happens, and you don't really learn that reading a book. You have to live that technology for years.

LF: And so you've been in business for 10 years now. That's a good accomplishment.
DS: Yes, it's been about 11 or so years now. We incorporated probably in 2002 but I was doing this for a little before that.

LF: So one of the questions that came up for me when you were talking about working with law enforcement, are these same people still involved in your business today? Are they still working with you or did they refer other types of technology based business at this point? Are they investigating in conjunction with what you do?

DS: So I still work with some of these investigators, forming investigative teams. They do the traditional investigation work and I work with them on the technology components. It's like a cop or a detective when they come on a crime scene on TV. They look at everything. They send the blood to the forensics lab. They say, "Oh, take that computer. Send it to the forensics lab. I'll get them to analyze it". So we're that forensics lab for them. They come to us when they have an issue they're investigating and they find a computer involved. They call us up and we come and get the computer and do the analysis. Along the way I'll work with the investigator to tell them what we've found on the computers that might be pertinent to their investigation. So that's how I interact with those guys. Sometimes we get clients that call us directly that say, "Hey, I have a problem". We have companies that call us. We have HR (Human Resources) Executives or CEOs who call and say, "Hey, we have a problem," and we'll lead the investigation. So this really depends on how things come to us.

LF: I want to go over a couple of different types of investigations that you do. If you want to give me an example of a corporate investigation and a law enforcement one, and then I don't know if you've ever done anything on more of an individual sort of civil lawsuit level. Have you done any kinds of cases in that realm?
DS: Like domestic, in divorce cases and things like that, you mean?

LF: Yes.
DS: We've done a bit of that. It's a smaller percentage of what we do, but sometimes people, high net worth individuals, will call us up asking for help so we help them out.

Well we actually had BitFlare being used by a housewife in Louisiana. She suspected that her husband might be doing something strange. His computer activity was a little strange. She had a daughter from a previous marriage living in the house with them so she was concerned for the daughter's safety among other things. One of the issues was she wanted a forensics examination on the computer but she couldn't send the computer to us or she couldn't take the computer out of the house because her husband would notice that it was gone. She also couldn't afford to have us come down from DC to Louisiana to do an in-house or on-site copying and couldn't find local experts. She was very lucky she called us because most people would say, "Sorry, can't help you under those constraints". Because we had BitFlare, we actually provided her a copy by just sending it down to her on a CD. Then she went to Best Buy and bought an external USB drive and she used BitFlare. Following the instructions in BitFlare, she herself made a forensic copy of the hard drive. Afterwards she sent the hard drive to us and we did the analysis in the lab., By using BitFlare, she saved a significant amount of money in terms of getting the image done, and it allowed her to do that for free. For her to make the forensic image it didn't cost anything because that's the way BitFlare works. So she didn't have to pay anybody to come out to do the imaging and she didn't have the risk of the husband finding out. She just did it one day while he was at work. The result of that investigation is that we looked at the computer and we found all these pornographic images that the husband had been viewing. We found a chat log and evidence of him chatting with other men, sexual conversations with other men and some of these men provided photos where they were cross-dressed. It was very much sort of "out there" in terms of that type of stuff.

So we gave her the evidence and said, "This is the kind of stuff we're finding". She looked at it and obviously she was devastated by it. But at the same time she said, "Now I know. Now I know the problems I have to deal with".

And she confronted her husband with the information and they had a challenging experience but at the end of the day she was so grateful and so happy with the outcome of it. She loved it. She sends me emails and gives me updates.

LF: Well, you know, that's somebody that you've walked through a bath of fire with so of course she would feel connected to you. I mean compared to a traditional investigation, do you have a ballpark of how expensive it was for her to do that investigation as compared to if she had gone about surveillance and having somebody track him down and maybe not even have access to his information?
DS: I'd give you some ballparks but the thing to keep in mind is that doing this, she actually tapped into a completely different avenue of evidence that she could not have gotten through surveillance.

LF: She wouldn't have found the evidence of what he was saying or looking at.
DS: Exactly, and in this case I don't know, but it could've been a situation where he only conducted those activities online versus in person, in which case surveillance would've provided nothing.

LF: So then on the corporate cases you were mentioning Fortune 100 companies there, I mean, I don't know if they still are but they were at one time for sure. And so the kinds of investigations that you're doing on a corporate level are, what type of cases are they? Are they more embezzlement or fraud?
DS: Any of the above. All of the above. I'll give you an example. I've worked for large manufacturing companies where they've had employees on

strike, and during the strike period all of a sudden computers and manufacturing systems that are computer based start breaking. So we're investigating industrial sabotage there. These are the striking employees sabotaging the systems so that the scabs can't use them and they have to shut the plant down. We've investigated situations like that.

We've helped investigate companies like a large car manufacturer, where large parts were going out and being "lost" and they were ending up on the black market or aftermarket. When I say large parts I'm not talking like a steering wheel or a transmission. I'm talking frames. Frames for entire cars were walking out of the back of the plant, and it was a network of people and they were colluding to steal these and sell them. Another example of an investigation we did was a large pharmaceutical manufacturer who has a drug. It's a very popular painkiller, and when abused, it can be abused – and it is abused – and it's very addictive but it's a valid painkiller and doctors prescribe it all the time.

What happened was the company had a team of scientists who were involved in manufacturing and there were foreign nationals. They're in the US working legally, but they had their own immigrant clique and they would all get together at lunchtime in the cafeteria and hang out and speak their native language, so they were all very close personally. They were friends, having family dinners together and all that type of stuff. But this group of scientists was one of the core teams for manufacturing this drug. The company heard rumors that the set of scientists may have been setting up an offsite manufacturing lab to create these drugs and sell them on the black market. There was a lot of speculation that some organized crime may also have been involved in this enterprise.

So they're obviously very, very concerned.

LF: Which wouldn't have been very surprising at all, that's exactly the kind of thing organized crime likes to get involved with.

DS: That's the kind of stuff they do, so we were helping them investigate that.

What other corporate stuff? I had another that was a California based company. It was a financial institution and there was a lot of internal politics going on and at one point one of the technology departments lost a hard drive. I mean, the hard drive just got stolen off a guy's desk.

It was one of those external hard drives and it was developer who was doing system testing and the drive had a data set that he could test against. Well, it's a financial institution so you can imagine that the data set had client data such as customer names, addresses, phone numbers, bank accounts, statements, logins, all types of stuff. And the hard drive was missing which obviously was a major problem. They brought us in to investigate and try to figure out who stole the drive and what the exposure to the company would be. My partner, a traditional investigator, went down that path of: Who would have the motivation? Who would have the means? Who would have the opportunity? Who would've stolen it? I was brought in because it was technology systems type people involved so it was going to be involved with all IT talk. I helped do the interviews but also I was able to reconstruct what was on the missing hard drive. If you think about this, I'm identifying data that's on a hard drive that I've never seen or touched before.

That's a pretty hard thing to do, but we were able to do it because through interviews I was able to identify who put the data on the hard drive, what kind of data they put on the hard drive, and I was able to go to their computer and look at the data they had accessed from their computer to then get a good idea of what data was extracted to the missing hard drive. Knowing what kind of personal data was on the hard drive was critical because it's a California based company and in California anytime you lose personally identifiable information, you must report it. You're legally obligated to report to your clients that there's a potential loss or breach of your personally identifiable information. And so that was a major concern because it would have been quite an embarrassment. So I was able to at least help them clarify where they stood with their duty to report.

LF: So you were able to reconstruct the whole thing by going to all these different people. How many different sources were there that were going into the system?

DS: Well, we interviewed like 15 to 20 people, but at the end of the day we found a couple of guys who were responsible for extracting the information on the hard drive for the tester. So I was able to find the right people and go to their computers and help them reconstruct what they did as part of putting the data on that drive. I was able to locate old database queries, old database reports, and various files they had touched around that time frame. So we were able to reconstruct what we believe, with a reasonable level of certainty, was on the missing drive. We were able to get an idea of what data fields were actually pulled out of the database and put on that hard drive.

LF: So you knew their vulnerability through that.

DS: Exactly.

LF: When you first started talking about the story I was wondering, on a hardware basis, you know, if you were to attach a hard drive to a system through a USB port, can you tell what data has been directed to a particular piece of hardware?

MONITOR STRONY

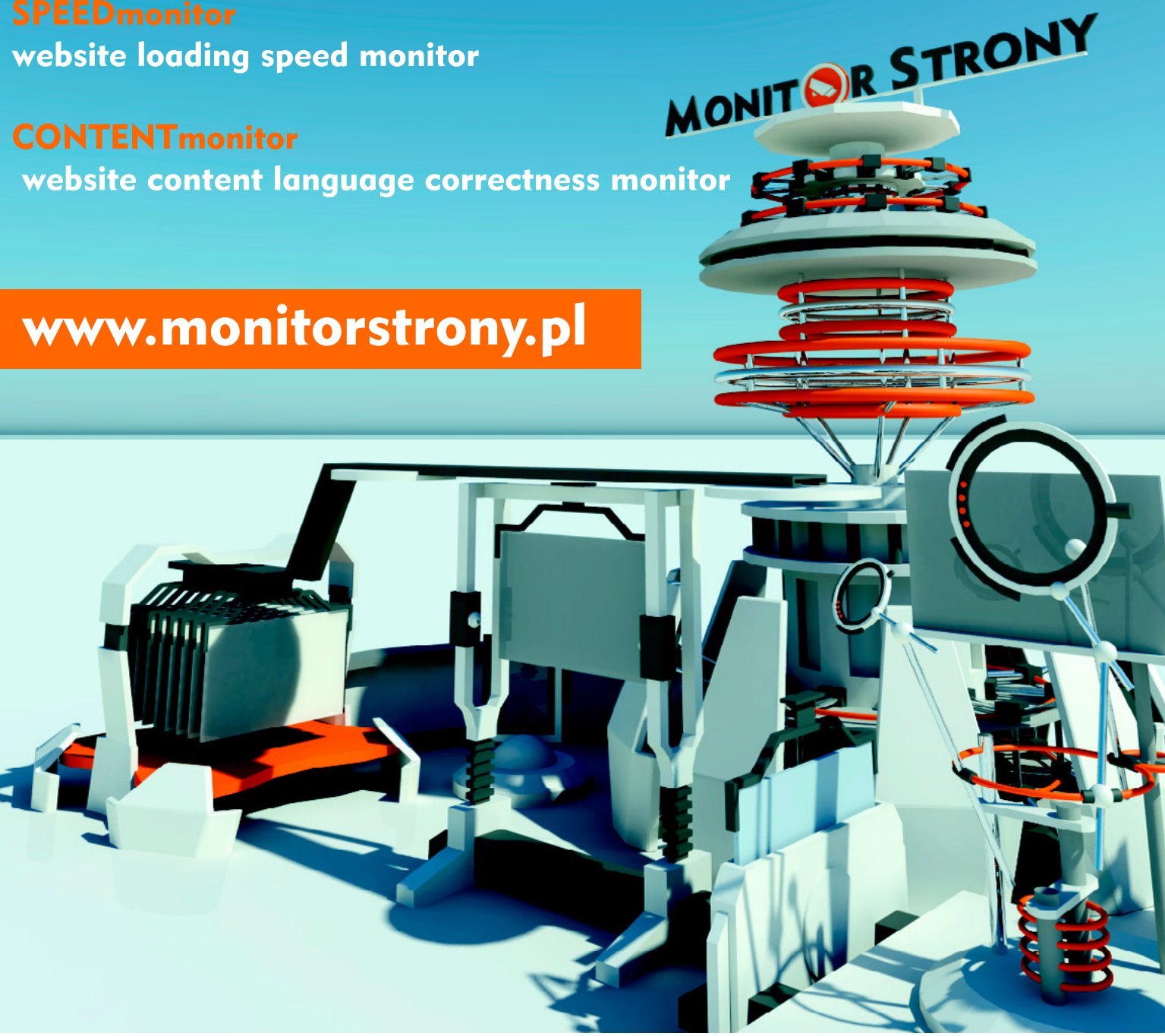
Innovative e-services for websites monitoring

SEOmonitor
SEO website monitor

SPEEDmonitor
website loading speed monitor

CONTENTmonitor
website content language correctness monitor

www.monitorstrony.pl



FUNDS FOR INNOVATIONS

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

PROJECT CO-FINANCED BY THE EUROPEAN REGIONAL DEVELOPMENT FUND UNDER THE OPERATIONAL PROGRAMME INNOVATIVE ECONOMY

DS: Yeah, there are some cases when you can. I actually had a case where I worked for a large insurance company, one that is too large to fail, and what happened was an executive, this is back in the boom days, an executive at the company went to start a competing financial institution. So they were going to start a financial firm, and I was investigating this executive because he basically copied all the data off his company computer before he left. In that investigation, by looking at the computer and various forensic artifacts, I was able to identify when the guy inserted the USB drive on his computer. I was then able to identify thousands of files that he "touched" in the span of two minutes. You can't really touch thousands of files in the span of two minutes, right? If the computer says you've "touched" 2,000 files or 1,000 files in two minutes it's reasonable to conclude that what you really did is you copied them.

So I reconstructed a timeline. USB insertion here. One minute later, thousands of files being touched, and then so on and so forth. Those files were all intellectual property for the company, and so we were able to identify that theft. Actually, I put a sworn affidavit together. They took it to a hearing for temporary restraining order, a TRO hearing. There was actually an article in the New York Law Journal that talks about the judge's reaction where it says "The moment I saw this affidavit by the forensic expert in front of me, I looked at the defense attorney and asked him if he had seen it, and when he said, 'No,' I suggested that he read the affidavit and discuss this with his client because if it's true it would be catastrophic for his case".

LF: That's amazing. That had to feel great!
DS: Oh, it was a grand slam. It doesn't happen often, but that was a total grand slam. Our client was very happy.

LF: I love puzzles and always have. I can remember being a little kid and taking music boxes apart to see how they worked and things like that. And when you get that kind of satisfaction, it's the same satisfaction you get as a kid when you crack open a plastic box and you finally see how that worked. I can really appreciate, that's just sort of a gut-level happy when that happens. I wanted to ask you some more about your international cases. You had mentioned in an email to me earlier that you had done a number of international cases.
DS: Well, one international case I worked on was fairly early on in the mid 2000s, and what it was a US subsidiary of a large, large multinational corporation. The US subsidiary was publicly traded and they announced, this is in the mid-2000s so there's a lot of earnings errors, problems with earning reports. So what happened was this company came out with a press release saying, 'We have to restate our last year's earnings. There are potential accounting errors and issues, and that we will indefinitely postpone our most recent quarterly earnings announcement.'

Basically all the financials were questionable, that is the best way to describe it, and I'm not using an official term but that's what happened. So when they announced this, they very quickly got a federal grand jury subpoena. The subpoena directed them to produce all the documents, electronic and otherwise, relating to their press release and earnings restatements. Again, this is mid 2000s so while computer forensics been around from an investigative standpoint, mostly for internal investigations, it was not quite widely used in the full-blown discovery productions for trials. E-discovery was just starting back then, getting footholds, and the processes were still very ambiguous as far as what to do, how to do it. So we got involved, and as it turns out the company was a multinational, and while the subpoena was for the US subsidiary, to be extra cautious, some of the investigating extended back to their international headquarters. As a result, I had a team in Europe at their headquarters and we also went to other countries which had large stores of data such as France, Spain, Bermuda, and others.

And so I had to send teams to all these other countries to do forensics and imaging, document preservation, and those types of things. I had a team in Switzerland for two months. We were imaging hard drives. We were doing analysis and the interesting part with Switzerland is, as you may or may not know, is that they have their Swiss banking laws. Their secrecy law basically makes any cooperation with a foreign investigation against the law, and if you release Swiss documents for a foreign investigation, you're breaking the law. Clearly, this is a US based investigation so cooperation and export of documents was a major concern. So we had to really weave our way around that and actually what we did was very interesting. We found a loophole in the Swiss law which says that if a document, as part of its natural course of business, left Switzerland then it is not bound by Swiss privacy law. So what we were able to do was we were able to do something where we actually invented a tool which could reasonably track the routes of old emails and where the emails had traveled. So if an email went out of Switzerland, whether because the recipient was out of Switzerland or even if the recipient was in Switzerland, but because of the internet routing, went out of Switzerland, we were able to identify that stuff.

LF: Even if it went through just a network – if it went into any other country at all?
DS: Within Switzerland, if you sent it from one Swiss person to another Swiss person, and the

sender and recipient were both in Switzerland, but because of internet traffic routing, it went out of Switzerland, we identified those messages.

LF: I wonder if that changed the way that they did their networking later on, so that there were certain documents that they could maintain the Swiss protection over?
DS: I don't know, but the Swiss counsel indicated to us that if something had left Switzerland, even the sender and recipient were Swiss, but because of network routing it left Switzerland, those documents would be subject to different regulations.

LF: Amazing. That's a really interesting story!
DS: Yeah, we invented a system that could identify those documents. So we were able to perform our duties despite the laws of the land that prevented.

LF: So what kind of educational background are you looking at? Are you looking for someone that is trained at say, John Jay or someone that's trained at MIT? What is your preference when you're recruiting for someone to come and work with you.
DS: There are a couple of components to it. I'm a pragmatist. All things being equal, one guy's got an MIT background, the other guy doesn't, well you take the guy with the MIT background. But never is anything completely equal. What's more important to me than somebody's educational background is their ability to learn, adapt, and overcome. To that end, I've hired guys who didn't have a technical degree. I've had one guy, one of my senior people who had an entomology degree. He studied bugs.

LF: Right, and they weren't viruses either.
DS: No, they're not talking about viruses. Straight up insects.

I had another person work for me who had a Rhetoric Major. Not English, but Rhetoric Major. And there's nothing wrong with these majors. My point is that they're not technical in nature, but all these guys learned technology and they actually learned it before they came to me. They had a technical foundation and then they were able to learn the rest of the stuff, and the reason that learning and the adaptability is so important is because with any type of investigation or litigation, nothing ever goes as planned.

LF: No…
DS: Nothing. So you got to be able to know how things are supposed to be done and then when you go out there and all your plans change, figure out how to make it all happen anyway, and people who can't adapt, learn, and overcome will have a very difficult time in this environment. When I say a difficult time, I don't just mean they'll have a hard time doing the imaging onsite. I just mean that it just takes more effort and energy and heartache for somebody to live in that type of work environment and so they're not going to be happy at a job like this.

LF: No, they'll be constantly stressed out and frustrated.
DS: Yeah. The kind of people who think, “OK, I come to work Monday through Friday. 9 to 5. I want to be able to count on the fact that every day at 5:00 I'm out of work and by 6:00 I could be at little league with my son or I can be on the golf course with my friends or I could be, whatever." If you want that type of consistency and reliability, litigation and investigations is not the right industry to be in.

LF: No, because you might be there for days on end. I mean, almost anything in technology can be really demanding in terms of what it expects of you in time or odd hours and numbers of hours worked in a week. That's always been my experience of it, is that you just have to expect the unexpected.
DS: In investigations they teach you at private investigators academy when you’re going to go do surveillance on someone, make sure you got an overnight bag in the backseat of your car because if you’re surveilling somebody and they get in the car and they get on the highway, who knows where they’re stopping? It may be five states over, eight hours later.

LF: Yeah, you have no idea.
DS: You have no idea where they're going, and if you're surveilling them, what are you going to do? Stop because you're at the town limits? No, you keep going and you follow them and you make sure you can continue tracking where they are. So, I mean, even as a regular investigator that's the kind of thing you have to deal with.

LF: It sounds like it wouldn't have hurt you to have, maybe a background in law, not even just as a law enforcement professional, but just in terms of what the law is and your ability to understand the law, like the situation that you described in Switzerland. That was very important to understand the detail of what you could and couldn't do and how to circumvent that issue. David, this has been so interesting. I really enjoyed learning from you. I hope that you teach somewhere. You're very articulate. Everything that you say has a picture attached to it and it's not difficult to follow what you say or overwhelming and it's a fascinating story. There are a lot of things about you that are interesting to me because you wear a lot of hats at one time. So I didn't have much of a chance to form very concrete ideas about what your life or job was going to be all about, you know, how versatile it is, how responsive you are to the circumstance, and how creative you are to resolving those problems. And I could see using a catchphrase that you use your-

self, "adapt, learn, and overcome", and how that applies in all these many different circumstances that you've learned and the ways in which you prepared for a really fascinating career in business.

DS: I don't see computer forensics as being a profession that you decide at a young age to pursue and go through formal training, education, or schooling so that when you're done and get your degree, boom you're ready to go.

That works as a traditional career path, in a more established industry such as lawyers, doctors, and architects. You can decide early on I want to go to Law School; I want to go to Medical School. You do your many years of schooling and apprenticeship, whatever the industry requires, and at the end, you're a doctor, you're a lawyer, you're an architect. The way I see computer forensics, the technology changes so fast that traditional educational career paths don't work because they take too long. For a young person growing up today saying "one day I want to be a computer forensics expert", by the time they go through college, there may not even be computers as we know them anymore.

So, this is one of the industries that I think a person needs to grow into and while you can take classes and get certifications, you really need to be able to do things that allow you to keep you up on your own. Every 2 years Microsoft releases a new version of Windows. Similarly, every so often iOS and Linux versions also change. Combined, there is a major change occurring on a yearly basis if not more often. Then you bring in other devices like Android and tablets which weren't on anyone's radar just a few years ago. Each one of these changes can significantly alter the forensic process of their respective devices and possibly the entire industry. By the time someone has a new device figured out from a forensics standpoint, created a course to teach forensics on them, and the student takes the course, it may already be outdated. Unless someone is able to sit down and dissect something on their own, if they have to wait to be taught it, they will always be behind the curve. Unlike the human body or legal system, technology changes to quickly for the formal education process to keep up. How useful is a Palm Pilot forensics expert today? 15 years ago they would have been considered innovative and in high demand.

LF: I think that going through these ideas of things that I would like to do in the future, with academia and business and government is it is incredibly fluid. It is probably one of the most fluid areas between these three different sectors; you have the very best of all worlds. You have academic people who are studying and exploring, really getting into the nooks and crannies of all the issues surrounding, law enforcement investigation. Then you have people that are already working in that field that are already using the tools that have been developed and who are identifying what the needs are, and you have to respond to this stuff very quickly because of the technology becomes obsolete so fast. If you were to go through the same kind of traditional way that we were talking about, a doctor or a lawyer or somebody would come of age in this. Then you would be so far behind the learning curve that the criminals would never be accountable, and in a way that's already an issue because it changes it so quickly. But to bring in the element of someone like yourself in small business, makes it a very agile, responsive community where there's an interplay that is constantly addressing the creativity of people who are committing crimes and the people who are trying to prevent them from committing them, and that is, I think, the magic, if you will, of the field that we work in because there's just room to respond to that in so many different ways.

DS: I agree. I think the agility and speed is important but you also need the self-motivation. If you try to go by a traditional career path where you start off with formal schooling and education, by the time you get out, you're already behind the curve.

LF: I think that you can take the big picture. You know, what is the philosophy, if you will, behind, investigating certain types of crimes. I had a conversation with a professor who said that what I wanted to do with BitFlare in terms of searching for predatory behavior. She's asking, "Isn't that a witch hunt?" And I was saying, "No, because you're not going to take this, into someone's home or scan their computer unless you have probable cause, and so then, you're looking at Fourth Amendment and seizure and, these kinds of issues that we're exploring anyway through, NDAA and other types of, investigatory systems that Homeland Security is doing. Where are the boundaries? And that is a philosophic question, and it's more a legal question in terms of law school than I think it is just technology, but we're in the world where we can take those ideas and apply them. If you and I have an idea now, it's November, very likely, we're well on our way to implementing it by June. And I love that about product development, what we're doing in this field, so towards that end.

David Sun

David Sun is the founder of SunBlock Systems, an international consulting firm specializing in Computer Forensics and Electronic Discovery. He leads teams of investigators assisting large multi-national corporations with litigation issues related to electronic evidence and discovery. Mr. Sun has taught computer forensics at the University level as well as offered training to various legal and business professionals.

Audiobook

PRODUCTION

WANTED: 100 Forensics Authors!

You're missing out on the exploding Audiobook industry and massive amounts of unclaimed revenue!

Get your book professionally narrated and produced into an Audiobook and sell on Audibles.com, iTunes and Amazon.

Watch your credibility, your fame and your profits skyrocket...

FACT:
More people are listening instead of reading because it's more convenient and easier than traditional books.

So get with the program!

Visit www.legacy-strategic-development.com

REAL-TIME INTRUSION DETECTION

FOR CRITICAL INFRASTRUCTURE PROTECTION: COCKPITCI APPROACH

by Lasith Yasakethu and Jianmin Jiang

Cyber-attacks against control systems are considered extremely dangerous for critical infrastructure operation. Today, the protection of critical infrastructures from cyber-attacks is one of the crucial issues for national and international security. Over the past ten years, intrusion detection and other security technologies for critical infrastructure protection have increasingly gained in importance.

What you will learn:

Critical Information Infrastructure Protection, Machine learning techniques applied to Intrusion detection and new European Framework-7 funded project related to Critical Infrastructure Protection.

What you should know:

Very basic understanding of information technology & machine learning (references are given to support this).

However, strictly speaking, they are not effective intrusion detection methods, as they require knowing what kind of attack is expecting, which deviates from the fundamental object of intrusion detection. In this article we describe an intelligent intrusion detection approach, which does not require any attack signatures, proposed for a new European Framework-7 (FP7) funded research project, CockpitCI.

INTRODUCTION

In today's growing cyber world, where a nation's vital communications and utilities infrastructure can be impacted depending upon the level and sophistication of hostile attacks, the need for *Critical Infrastructure Protection* (CIP) and advanced cyber security is at all-time high. In this article we describe an intelligent intrusion detection approach proposed for a new *European Framework-7* (FP7) funded research project, CockpitCI. The article provides the CockpitCI concept and roles of intelligent machine learning methods to prevent cyber-attacks. A discussion on this concept emphasizes the need of intelligent risk detection, analysis and protection techniques for *Critical Infrastructures* (CI). With the intelligence of machine learning solutions, CockpitCI will contribute to a safer living environment for people especially by providing smart detection tools, early alerting systems and strategic security system, which allows isolating default systems and ensuring the safeguarding of living environment. The distributed framework of the system will ensure an operational deployment of the security all over Europe and will improve

the European *Critical Information Infrastructure Protection* (CIIP) strategy.

CockpitCI will focus on cyber-attacks to control systems of energy grids that are typically interconnected with public Telco networks. Power grids and Telco networks have a large impact on daily life and are typically referred as CI since their correct operation is essential for the everyday life of our modern society. There are bi-directional dependent relationships and reciprocal influences among CIs, named interdependencies. That is especially true because CIs are more and more reliant on information and communication technology and mainly through this reliance they have become more and more interdependent. The successful delivery of any essential CI service depends upon the operating status not only of the CI which is intended to deliver such a service but also on the operating status of any interdependent CIs. Initial disturbances in (or even destruction of) parts of one CI, may result in cascading effects in the infrastructure itself or/and in the other interdependent CIs.

The paradox is that Power and Telco CIs massively rely on newest interconnected (and vulnerable) *Information and Communication Technologies* (ICT), while the control equipment is typically old, legacy software/hardware. Such a combination of factors may lead to very dangerous situations, exposing the systems to a wide variety of attacks. This article first discusses machine learning based intrusion detection strategies for CIP and then introduces an advance intrusion detection technique which will be developed as a part of the CockpitCI project to protect CI from such cyber-attacks.

MACHINE LEARNING BASED INTRUSION DETECTION

Intrusion detection is the process of observing and analysing the events taking place in an information system in order to discover signs of security problems. Traditionally, *Intrusion Detection Systems* (IDS) are analysed by human analysts (security analysts). They evaluate the alerts and take decisions accordingly. Nevertheless, this is an extremely difficult and time consuming task as the number of alerts generated could be quite large and the environment may also change rapidly. Machine learning has the capability to: 1) gather knowledge about the new data, 2) make predictions about the new data based on the knowledge gained from the previous data. This makes machine learning techniques more efficient for intrusion detection than human analysts.

IDS monitors the activities that occur in a computing resource to detect violations of a security policy of an organization. These violations may be caused by people external to the organization (i.e. attackers) or by employees/contractors of the organization (i.e. insiders). During the recent past, intrusion detection has received considerable motivation owing to the following reasons [1] [2]:

- If an intrusion is detected quickly enough, an intruder can be identified quickly and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to pre-empt the intruder, the sooner that the intrusion is detected, the less is the amount of potential damage done and the more quickly that recovery can be achieved.
- An effective intrusion detection system can serve as a deterrent, acting to prevent intrusion.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to analyses the new threats and to strengthen the intrusion prevention facility.

Along with the above motivations, the intention of intrusion detection can be summarized as follows:

- Detect as many types of attacks as possible (i.e. including internal malicious/non-malicious and external opportunistic/ deliberate attacks), thereby increase the detection rate.
- Detect as accurately as possible, thereby reducing the number of false alarms.
- Detect attacks in the shortest possible time, thereby reducing the damage of the attacks.

The above requirements have prompted researchers to develop various types of IDS that fulfil the above goals to prevent Supervisory Control And Data Acquisition (SCADA) systems from cyber-attacks. SCADA systems are vulnerable to cyber-attacks due to design and implementation flaws in the cyber-security system. Malicious users attack the cyber-

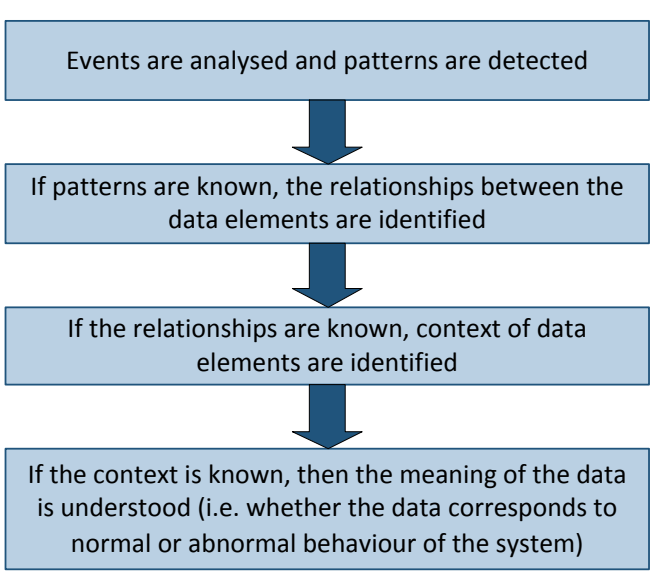


Figure 1. *Core process of threat identification by machine learning*

security system vulnerabilities by using a sequence of events to break in to the SCADA system [3, 4]. These events result in characteristics that are defined by patterns of attack. The goal of any machine learning techniques, in intrusion detection, is to analyse the input event data and to detect patterns that would reflect possible threats to the cyber-infrastructure. The core process of threat identification by machine learning is illustrated in Figure 1.

According to the detection principle used for the process shown in Figure 1, intrusion detection techniques can be classified into following main modules (but not limited to): Signature detection (misuse detection), Anomaly detection. Detection principles behind each module are discussed in the following subsections.

SIGNATURE DETECTION (MISUSE DETECTION)

Signature detection also known as misuse detection generates alarms when a known cyber-attack occurs. In this technique the behaviour of the system is compared with unique patterns and characteristics of known attacks, called signatures. This is typically done by measuring the similarity between the input events and signatures of known attacks. If a match is found, an alarm is triggered. As a result, known cyber-attacks can be detected immediately with a low false-positive rate. However, if there is no similarity match, the event is classified as normal behaviour and the detection approach will search for further patterns. Thus, signature detection can only detect known attacks. Figure 2 illustrates the approach of signature detection.

Signature detection heavily relies on the prior knowledge of attack signatures. Thus the effectiveness of the detection mechanism relies on a frequent updating of the signature database.

Due to the availability of prior knowledge on attack signatures, hence the availability of labelled data, supervised machine learning techniques are generally used for signature based intrusion detection.

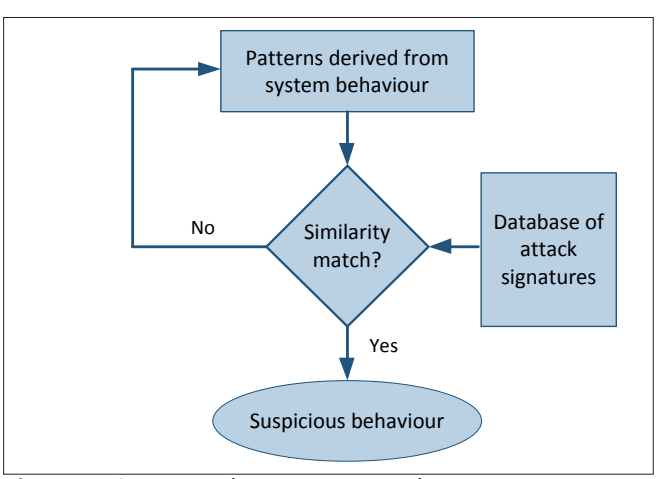


Figure 2. *Signature detection approach*

ANOMALY DETECTION

Anomaly detection is an IDS triggering method that generates alarms when an event behaves different from the normal behaviour patterns. Thus this can be defined as a problem of finding patterns in data that are different to the expected behaviour of a system. Figure 3 illustrates the anomalous data patterns in a simple 2-dimentional data set. In this example the data has two normal regions, N1 and N2. Data that sufficiently deviate from these regions, i.e. point A1, point A2 and region A3 are considered as anomalies.

The anomaly detection approach has two main steps: training and detection. In the training step, machine learning techniques are used to generate a profile of normal behaviours that define the healthy cyber-infrastructure. In the detection step, an event is classified as an attack if the event records deviates sufficiently from the normal profiles. Unlike signature detection, anomaly detection has the potential to detect novel attacks. However, anomaly detection typically has a high false-positive rate. This is because in anomaly detection any sufficient deviation from the base line is flagged as an intrusion. Thus it is likely that non-intrusive behaviour that falls outside the normal region generates an alarm, resulting in a false-positive.

The key challenge for anomaly detection in intrusion detection is the analysis of huge amounts of data with high dimensional feature space. It requires computationally efficient data mining techniques to handle large amounts of input data. Furthermore, the data typically comes in a streaming fashion, thus requiring online analysis. As the data amounts to millions, even a few false alarms can be overwhelming when it comes to decision making.

In anomaly detection, labelled data corresponding to normal system behaviour are usually available, while the labelled data for intrusions are not. As a result, unsupervised machine learning techniques are preferred for anomaly detection.

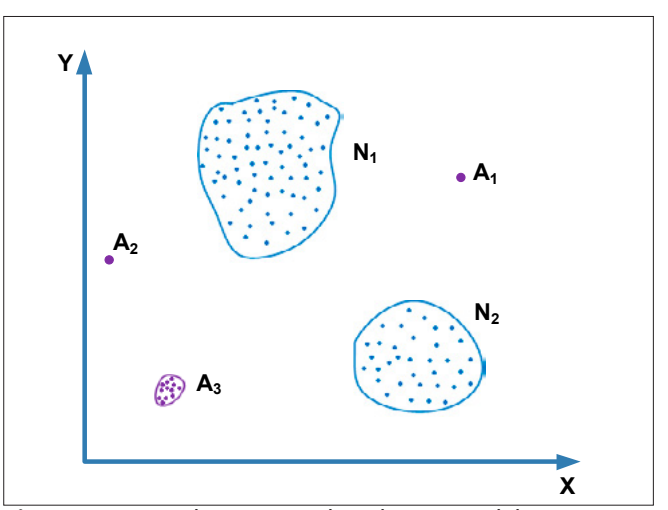


Figure 3. *Anomalies in a simple 2-dimentional data set*

The following paragraphs explain the supervised and unsupervised machine learning techniques mentioned in the above signature and anomaly detection.

SUPERVISED AND UNSUPERVISED MACHINE LEARNING

Machine learning algorithms are designated as either 'supervised' or 'unsupervised'. The distinction is drawn from how the learning model classifies data.

In supervised machine learning, the algorithm is fed with sampled data that are labelled. The data in supervised learning can be represented as pairs of (X, Y), where Y s are actual labels of different data elements in X. This labelled information is used for training and obtains a model to classify new data. Supervised machine learning techniques for intrusion detection are fed with 'normal' (which corresponds to the normal behaviour of the system) and 'attack' data along with their labelled information to train the detection model. In general the training data needs to be balanced (i.e. amount of normal and attack data are approximately equal) for an accurate classification. Most popular supervised machine learning methods include k-nearest neighbour (KNN) [5], artificial neural network (ANN) [6], support vector machine (SVM) [7] and hidden Markov model (HMM) [8].

Unsupervised machine learning algorithms are not provided with labelled data. The basic task of unsupervised learning is to develop classification labels automatically. Unsupervised algorithms seek out similarity between pieces of data in order to determine whether they can be characterized as forming a group. In the context of intrusion detection, unsupervised learning methods rely on the following assumptions: 1) normal data covers majority while intrusion data are minor; 2) normal and intrusion data are similar in their identity groups while statistically different in between groups. Unsupervised detection is an unbalanced learning problem and considers that normal and intrusion data can be clustered. Thus, most of the solutions to unsupervised intrusion detection are clustering based intrusion detection techniques such as k-means clustering.

COCKPITCI INTRUSION DETECTION APPROACH

As discussed earlier, the protection of the national infrastructures from cyber-attacks is one of the main issues for national and international security. To overcome such threats, the CockpitCI project develops machine learning based advance intrusion detection tools to provide intelligence to the field equipment. This will allow the field equipment to perform local decisions in order to self-identify and self-react to abnormal situations introduced by cyber-attacks.

Several techniques and algorithms have been reported by researchers for intrusion detection. One of them is to define the abnormal conditions, however due to the difficulty of defining unknown behaviours these rules based algorithms are always not applicable in the real applications. Generally, anomaly detection can be regarded as a binary classification problem and thus many classification algorithms are utilized for detecting the anomalies, such as artificial neural network, support vector machines, k-nearest neighbour and Hidden Markov model. However, strictly speaking, they are not effective intrusion detection methods, as they require knowing what kind of intrusion is expecting, which deviates from the fundamental object of intrusion detection. Moreover most of these methods are sensitive to noise in the training samples. Segmentation and clustering algorithms seem to be better choices because they do not need to know the signatures of the series. The shortages of such algorithms are that they always need parameters to specify a proper number of segmentation or clusters and the detection procedure has to shift from one state to another state. Negative

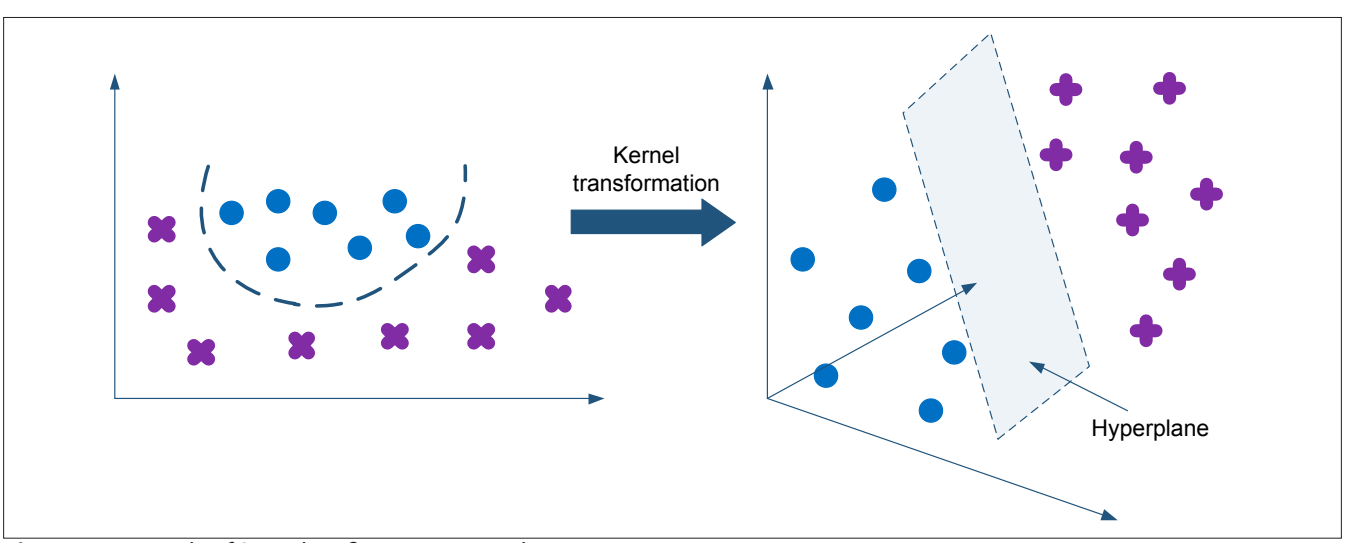


Figure 4. *Example of SVM classification approach*

selection algorithms [9] are designed for one-class classification; however, these algorithms can potentially fail with the increasing diversity of normal set and they are not meant to the problem with a small number of self-samples, or general classification problem where probability distribution plays a crucial role. Furthermore, negative selection only works for a standard sequence, which is not suitable for online detection. Other algorithms, such as time series analysis are also introduced to intrusion detections, and again, they may not be suitable for most of the real application cases. Table 1 presents and analysis of some of the intrusion detection strategies discussed above.

To minimize the above mention drawbacks, an intelligent approach based on OCSVM [One-Class Support Vector Machine] principles is proposed for intrusion detection in CockpitCI. OCSVM is a natural extension of the support vector machine (SVM) algorithm to the case of unlabelled data, especially for detection of outliers. Hence OCSVM is an unsupervised machine learning technique. Whereas SVM algorithm is a supervised machine learning method and it is essentially construed as a two-class classification algorithm (i.e. it requires class labels of both positive and negative samples). SVM uses a kernel function to map data into a space where it is linearly separable. The space where the data is mapped may be of higher dimension than the initial space. The SVM allows finding a hyper-plane which optimally separates the classes of data: the hyper-plane is such that its distance to the nearest training da-

Table 1. *Analysis of intrusion detection strategies*

Methodology	Working mechanism	Advantages	Disadvantages
Support vector machine (SVM) [7]	Separate data in to 2-classes (normal and potential attacks) using a hyper plane in the higher dimension	Produce very accurate classifiers Low computational time	Prior knowledge the anomaly type is required Sensitive to noise samples
Rule-based [10]	Events violating the established rules are identified as potential attacks	Strong association rules can effectively identify causality between event attributes and class labels	All the knowledge of the system need to be written in the form of rules Difficult to define unknown behaviours
Artificial neural network (ANN) [6]	Transform inputs into outputs that match targets through nonlinear processing in a connected group of neurons	Low computational time Nonlinear data analysis	Prior knowledge of the anomaly type is required Training data needs to be adequate and balanced. Thus a large number of attack training data is required
k-Nearest neighbour (KNN) [5]	Computes the approximate distances between different input vectors, and then assigns the unlabelled point to the class of its k-nearest neighbours	Simple to understand and easy to implement	Prior knowledge of the anomaly type is required Sensitive to noise samples Difficult to classify complex data
Hidden Markov model (HMM) [8]	Clusters of temporal data are specified by a mixture of dynamic models	Suitable for coping with data dependency among temporal data Solid statistical foundation	Prior knowledge of the anomaly type is required High computational complexity Large number of unstructured parameters Need large amounts of data
k-Means clustering [11]	Assigns objects into groups (clusters) by demining the distance between the objects over multiple dimensions of the data set	No signatures (class labels) required Simple to understand and easy to implement	Need parameters to specify number of segmentations and the detection procedure has to shift from one state to another state Different initial partitions can result in different final clusters Produce less accurate classifiers for complex data

ta points is maximal (maximum margin). An example is shown on the Figure 4. The SVM has shown superior performance in the classification problem and has been used successfully in many real-world problems. However, the weakness of SVM is that it needs the prior labelled data and is very sensitive to noise. A relatively small number of mislabelled samples (noise samples) can dramatically decrease its performance. In the case of CI monitoring, which patterns in the data are normal or abnormal may not be obvious to operators. Thus, although SVM proved to be a powerful classification tool its implementation in CI intrusion detection is difficult without the availability of adequate labelled data. To overcome this issue and other drawbacks mentioned in Table 1, an intelligent unsupervised machine learning approach based on OCSVM principles is proposed for intrusion detection in CockpitCI.

Unlike SVM or similar classification methods, OCSVM does not need any labelled data for training or any information about the kind of intrusion is expecting for the detection process. In summary, the OCSVM possesses several advantages for processing network performance data and automate the network performance monitoring, which can be highlighted as:

- no signatures of training data are required
- robustness to noise samples in the training process
- algorithm configuration can be controlled by the user to regulate the percentage of anomalies expected
- each anomaly detector can be trained to produce a small number of data samples to make decisions, which makes its implementation efficient and effective
- the detectors can operate fast enough for its online operations

Most of the current intrusion detection commercial software's are based on approaches with statistics embedded feature processing, time series analysis and pattern recognition techniques. Some software considered elements of machine learning such as clustering and neural networks. However, none of them has yet considered using OCSVM principles in commercial software's although research have shown great potential in the area of intrusion detection [12,13,14].

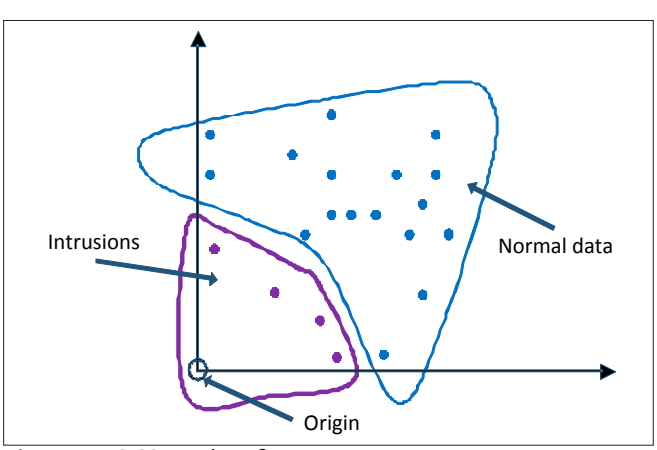


Figure 5. *OCSVM classification*

ONE CLASS SVM WORKING MECHANISM

The OCSVM separates outliers from the majority and the approach can be considered as a regular two-class SVM where all the data lies in the first class and the origin is the only member of the second class [4, 5] as shown in Figure 5. The basic idea of the OCSVM is to map the input data into a high dimensional feature space and construct an optimal separating hyper-plane, which is defined as the one with the maximum margin (or separation) between the two classes. This optimal hyper-plane can be solved easily using a dual formulation. The solution is sparse and only support vectors are used to specify the separating hyper-plane. The number of support vectors can be very small compared to the size of the training set and only support vectors are important for prediction of future points. By the use of kernel function, it is possible to compute the separating hyper-plane without explicitly carrying out the mapping operations into the feature space and all necessary computations are performed directly in the input space. A brief description of the intrusion detection algorithm is given is the in the following paragraphs.

Considering a data set with $N = \{x1, x2, \ldots, xl\}$, $x \in R^N$, the task is to find a function f that takes the value *"+1"* for most of the vtectors in the data set (i.e. for normal or attack free data), and *"-1"* for the other very small part (i.e. data corresponding to intrusions). As explained above, the strategies for the OCSVM are: first, map the input data into a feature space H (commonly known as Hilbert space) according to a mapping function $X = \phi(x)$, and separate the data from the origin to its maximum margin. A hyper-plane $f(x)$ is built up to mark the boundary of this separation. The key idea for the separation is that it doesn't really need all the data to be separated to the same side of the hyper-plane $f(x)$, on controversy, a small number of points can be lying on the other side of the hyper-plane. In order to allow this, slack variables are introduced to the objective function of support vector machine, and the OCSVM solves the following quadratic optimization problem:

$$\min_{w \in F} \frac{1}{2}\|w\|^2 + \frac{1}{vl}\sum_i \xi_i - \rho \quad (1)$$

$$s.t.\, f(x) = w.\varphi(x_i) - \rho \geq -\xi_i,$$
$$where\ i = 1,2,\ldots l\ and\ \xi_i \geq 0 \quad (2)$$

In equations (1) and (2), w is the norm that perpendicular to the hyper-plane and ρ is the bias of

the hyper-plane. ξ_i are slack variables acting as penalization in the objective function. $v \in (0,1)$ is the trade-off parameter to balance between the normal and data corresponding to intrusions in the data set and a maximum of $vx100\%$ data points are expected to return negative values according to $f(x)=w.\phi(x)-\rho$. Deriving its dual representations, the OCSVM is to solve the following problems:

Select the kernel function $K(x,x')$ in the Hilbert space H and the trade-off parameter v, construct and solve the following optimization problem to find the solution for the Largrangian multiplier α:

$$\min_{\alpha} \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}\alpha_i\alpha_j K(x_i,x_j) \quad (3)$$

$$s.t. 0 \le \alpha_i \le \frac{l}{vl}, i = 1, \dots, l \quad (4)$$

$$\sum_{i=1}^{l}\alpha_i = 1 \quad (5)$$

The parameter v directly determines the sensitivity of outlier detection (i.e. intrusions) in the algorithm. Is called as kernel function and can be with various format. In literature it is reported that the Radial Basic Function (RBF), as shown in equation (6) is the most widely used kernel in SVM [15], and RBF kernel is adopted in the proposed approach. is the standard deviation in equation (6).

$$K(x_i,x_j) = e^{(-\|x_i-x_j\|/2\sigma^2)} \quad (6)$$

For any x, if the $f(x)$ is negative, x is detected as a possible intrusion, otherwise x is normal. Figure 6 shows the structure of the proposed intrusion detection algorithm. In the algorithm, the OCSVM principles are used to train the offline data and generate the detection model, and then the model function is employed for intrusion detection. A negative value returned from the decision function will imply an abnormal event. Events with negative values are moved to the threat assessment module to quantify the risk(s) associated with the attack. This will allow the field equipment to perform local decisions in order to self-identify and self-react to abnormal situations introduced by cyber-attacks.

CONCLUSION

The researches performed during the CockpitCI project will allow improving the cyber-security industry. In the real world application, it is difficult to find sufficient attack data for training and testing intrusion detection techniques. Most attacks will remain unknown. Thus, the design and application of real-time intrusion de-

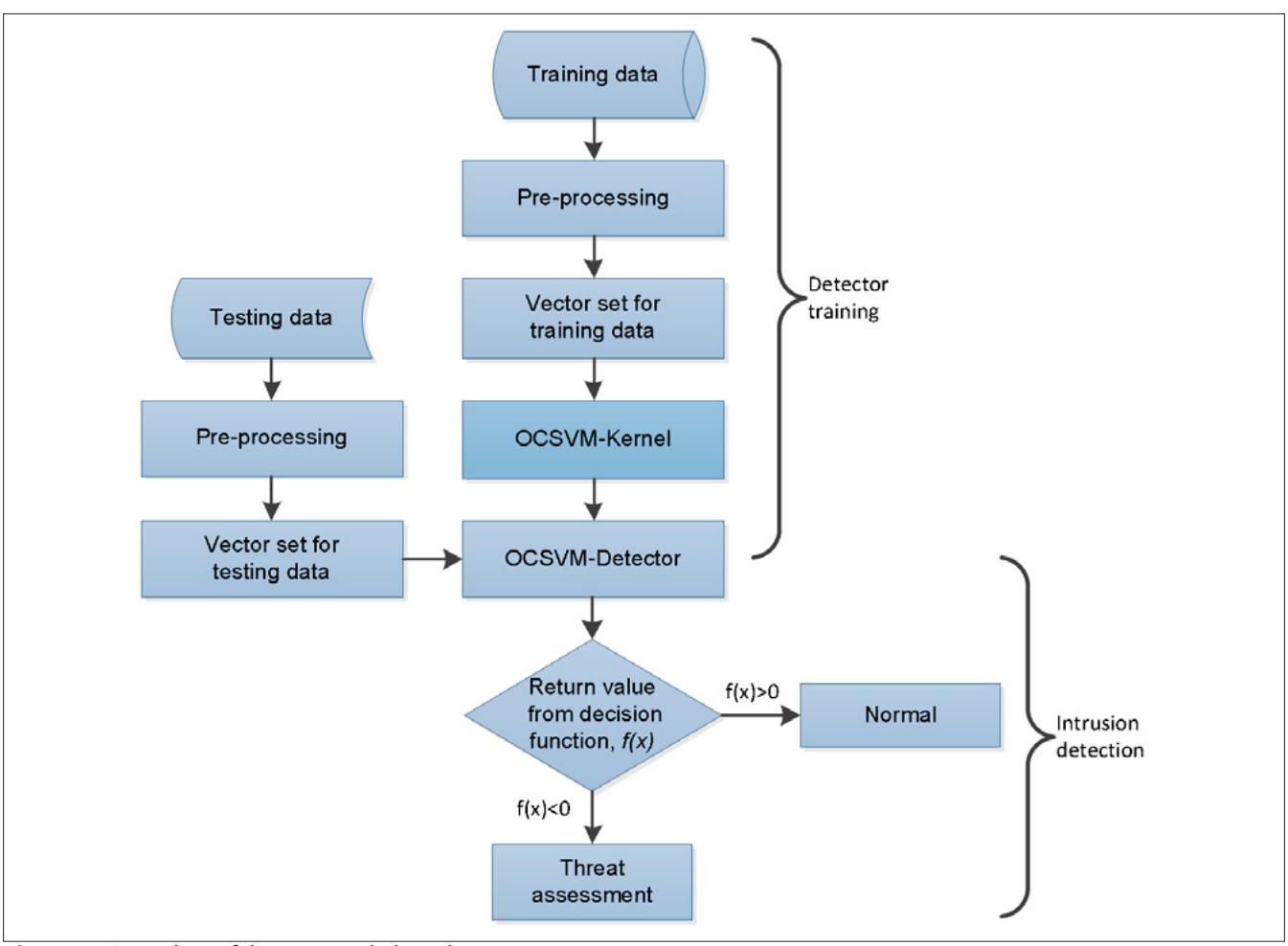


Figure 6. *Procedure of the proposed algorithm*

References

[1] S.V. Sabnani, Computer Security: A Machine Learning, Approach, Technical report, 2008
[2] William Stallings, Network Security Essentials: Applications and Standards (3rd Edition), Prentice Hall, 2006.
[3] L. O'Murchu N. Falliere. W32.Stuxnet dossier, Symantec White Paper, February 2011.
[4] S. Bologna, and R. Setola, "The Need to Improve Local Self-Awareness in CIP/CIIP", Proc. of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp. 84-89, Darmstadt, Germany, 3-4 November 2005.
[5] P. Cunningham and S.J. Delany, k-Nearest Neighbour Classifiers, Technical Report UCD-CSI-2007-4, March 27, 2007.
[6] Gershenson C. Artificial neural networks for beginners. In: Cognitive and computing sciences. University of Sussex.
[7] Christopher. J. C. Burges, A tutorial on support vector machines for pattern recognition, DataMining and Knowledge Discovery, 2(2):955-974, Kluwer Academic Publishers, Boston, 1998.
[8] Rabiner, L. R. (1989). "A tutorial on hidden Markov models and selected applications in speech recognition." Proceedings of the IEEE 77(2): 257-286.
[9] Zhou Ji, Dipankar Dasgupta, Revisiting Negative Selection Algorithms, Evolutionary Computation, Summer 2007, Vol. 15, No. 2.
[12] J. Ma and S. Perkins, Time-series novelty detection using one-class support vector machines, Proceedings of the International Joint Conference on Neural Networks, July, 2003, pp. 1741-1745
[13] K. Li, H. Huang, S. Tian and W. Xu, Improving one-class SVM for anomaly detection, Proceedings of the Second International Conference on Machine Learning and Cybernetics, Xi'an, 2003, pp. 3077-3081.
[14] B. Schölkopf, J. Platt, J. Shawe-Taylor, A.J. Smola, and R. Williamson, "Estimating the support of a high-dimensional distribution," Neural computation, Vol. 13, No. 7, pp. 1443-1472, 2001.
[15] S.S. Keerthi and C.J. Lin, Asymptotic behaviors of support vector machines with Gaussian Kernel, Neural Computation, vol. 15, no. 7, 2003, pp. 1667-1689.

tection methods, which does not require any attack signatures, will be important in developing future CIP and advanced cyber security solutions. CockpitCI will develop such smart detection tools for CI protection and likely to give a real advantage in the security market. With the developments of intelligent machine learning based solutions CockpitCI will be able to:

- Deploy smart detection agents to monitor the potential cyber threats and transmit alerts to the central control centre belonged to the CI owner.
- Analyse the threat, and perform simulation to predict cyber risk level and predicted quality of service (QoS) level for the whole CI.
- Design reaction strategy and assess the impact on QoS.
- Broadcast alerting message to other CIs to assess impact and enhance the cyber security of interconnected CIs.

ACKNOWLEDGMENT

The authors would like to thank the partners of the CockpitCI consortium and acknowledge the funding support from European Framework-7 Program for the project (Grant no. 285647).

Author bio

Lasith Yasakethu received his BSc. Engineering degree (First Class Hons.) in Electrical and Electronic Engineering from the University of Peradeniya, Sri Lanka, in 2007. He was awarded the prize for best performance in Electronic Communication Engineering by the University of Peradeniya for his achievements in undergraduate studies. In Oct. 2007 he was awarded the Overseas Research Scholarships Award by the Higher Education Funding Council of England to pursue PhD at the University of Surrey UK. After completing his PhD he worked as a Research Engineer for Technicolor Research & Innovations (formerly known as THOMSON R&D), in Rennes France, from Oct. 2010 to March 2012. Currently he is working as Research Fellow in Computing Department, University of Surrey UK. His research interests include Cyber-security, Machine Learning, Quality of Experience (QoE) in multimedia communications, 2D/3D video processing and transmission, Content creation for 3D cinema and 3DTV. He has worked for several EU FP6 and FP7 projects in the above fields. He is a member of IEEE.

Author bio

Jianmin Jiang received B.Sc degree from Shandong Mining Institute, China, in 1982, M.Sc degree from China University of Mining and Technology in 1984, and PhD from the University of Nottingham, UK, in 1994. From 1985 to 1989, he was a lecturer at Jiangxi University of Technology, China. In 1989, he joined Loughborough University, UK, as a visiting scholar and later moved to the University of Nottingham as a research assistant. In 1992, he was appointed a lecturer of electronics at Bolton University, UK, and moved back to Loughborough University in 1995 as a lecturer of computer science. From 1997 to 2001, he worked as a full professor of Computing at the University of Glamorgan, Wales, UK. In 2002, he joined the University of Bradford, as a Chair Professor of Digital Media, and Director of Digital Media & Systems Research Institute. He is now a Professor of Media Computing at University of Surrey, United Kingdom. He is also an adjunct professor at Tianjin University, China. He is a chartered engineer, fellow of IEE, fellow of RSA, member of EPSRC College, and EU FP-6/7 evaluator. His research interests include, image/video processing in compressed domain, digital video coding, stereo image coding, medical imaging, computer graphics, machine learning and AI applications in digital media processing, retrieval and analysis. He has published around 400 refereed research papers.

WAYS TO DETECT BIOS CLOCK ANTI-FORENSICS

by David Sun

The ultimate purpose of any forensic computer investigation is to correlate activities on a computer with real world actions by an individual. Accomplishing this can help a trier of fact decide what actually happened in a given situation.

What you will learn:

Ways to detect user manipulation of BIOS clock settings.

What you should know:

Relevance of file time stamps. Basics concepts of Windows Registry.

Correlating computer activities with real world actions is typically accomplished by creating a timeline of activities on the computer from available forensic evidence. Fortunately for investigators, computers tend to be very good at documenting their own activities and often incorporate timestamps indicating the date and time an action occurred. However, there are times when a savvy user may falsify the BIOS clock on the computer in an attempt to impede the ability of an examiner to create an accurate activity timeline. This anti-forensic tampering can be difficult to detect, so an examiner may not even realize it has occurred.

Computer examiners are fortunate in that computers automatically generate a significant amount of data allowing the construction of an activity timeline. Whenever files or directories are created, deleted, modified, or accessed on the hard drive, the *operating system* (OS) records the date and time of that action. This occurs for simple, user managed files such as documents, spreadsheets, and presentations as well as system managed files such as program files, web browser cache, and other OS internals. Timestamps are also found in log files generated by many computer processes that document their activities along with a timestamp for auditing and troubleshooting purposes. One thing that all of these timestamps have in common is that they come from a singular source – the computer BIOS clock.

The computer BIOS clock is maintained on the motherboard and used as a reference clock for the entire operating system. The OS and pro-

grams running on it accept the BIOS clock time without question and incorporate it in their operation. By manipulating the BIOS clock value, a user can induce various anti-forensic effects onto the computer and significantly complicate any examination. Events can be made to appear occurring out of order, such as making the editing of a file appear to have been done in the past, prior to a real world event. Alternatively, manipulating the clock into a future time can make the editing appear to happen after the actual event. These actions impede the ability for an investigator to assemble an accurate timeline of activity on the computer and findings may not make sense or correlate with real world activities. This is especially the case if the BIOS clock is changed multiple times.

In addition to obscuring the order of events on a computer, changing the system clock can also cause automated processes to begin such as the purging of log files and other data that is only intended to be kept for a limited amount of time. An example of such data purging would be the Microsoft Windows System Restore Points which are set by default for deletion after 90 days (*http://support.microsoft.com/kb/301224* , last viewed November 8, 2012). These effects could further complicate any forensic analysis by eliminating key data.

There are a few places in which an investigator can check for signs of BIOS clock manipulation. They are included below in no particular order.

CHECK BIOS CLOCK VALUES AT TIME OF DRIVE IMAGING

Recording the BIOS clock value is a critical part of any computer investigation, even without the concern of clock manipulation. Whenever a drive is imaged, it is wise to find and record the BIOS clock setting and compare it to a reliable clock source (mobile phone synchronized to a cell carrier's network time is a good example). It is not unusual to find a computer with a BIOS clock that is incorrect by some amount. The discrepancy may be explained by simple reasons such as a small variance of few minutes due to clock drift or whole hours due to differences in time zone settings. Documenting common discrepancies such as these is important so the examiner will know how much to offset any time values on the computer when comparing them to real world activity.

In some cases the BIOS clock may also be off by days or even years. Such larger or random clock discrepancies may be an indication of clock manipulation. This will allow the examiner to proceed with caution when constructing the activity timeline.

It is also important to note that an accurate BIOS clock at time of drive imaging does not preclude the possibility of prior clock manipulation. The user may have changed the clock back after completing their anti-forensic measures. Similarly, an incorrect BIOS clock does not demonstrate nefarious intentions on its own. Occasionally older computers with a depleted BIOS battery may fail to hold clock information properly causing the clock to reset to a default value when the computer is powered on.

WINDOWS SYSTEM EVENT LOG

The Windows System Event is an activity log for the operating system. It documents various operational activities on the computer and includes a timestamp for each of those activities. In Windows7, changing the BIOS clock within the OS generates an event in the System Log (see Figure 1). For older versions of Windows, system clock changes are not logged by default. However, the sequence of events for the Windows Event Log is maintained separately and those entries can be sorted by sequence instead of time. Therefore an examination of the event logs may indicate a jump forward or backward for the system time in which events occurred (see Figure 2). An aberrant jump in system time between sequential events may indicate a deliberate BIOS

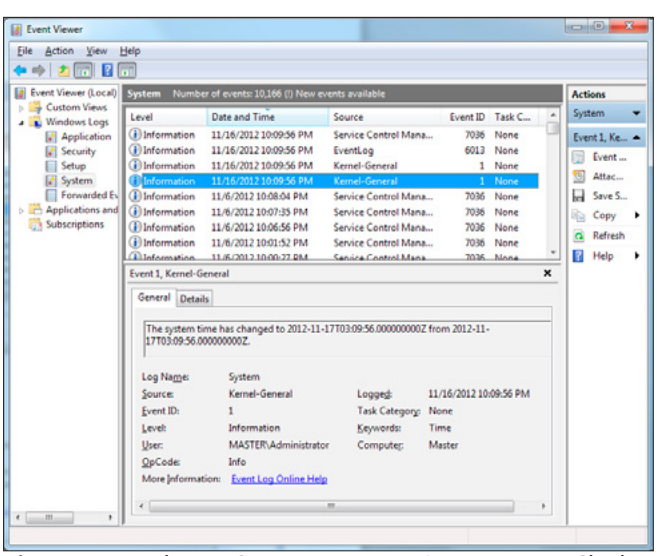


Figure 1. *Windows 7 System Event Log Documenting Clock Change*

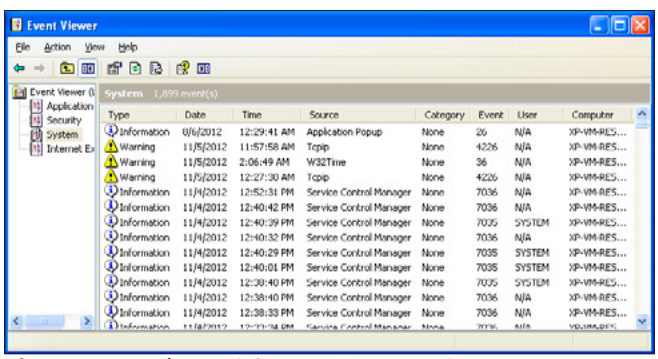


Figure 2. *Windows XP System Even t Log Demonstrating a Gap in Clock*

clock manipulation. Obviously for jumps forward in time, the examiner must take into consideration how long the computer was powered off before subsequent use. In other words, a gap in timestamps for entries in the Event Log may be due to the machine being powered off and idle during the missing time period. A review of the events leading up to and just after the time gap could provide an indication of the nature of the time gap.

ANCILLARY TIMESTAMPS

A savvy user may manipulate the BIOS clock to hide when certain activities actually occurred to generate an alibi for their activities. But it is possible that they did not account for all activities that occurred under a falsified time. By looking for other unrelated activities that occurred under the falsified time, an examiner may be able to identify an oversight by the users under the incorrect clock and compensate to determine the actual time or discredit the alibi. One common example of such an oversight may be the file and directory timestamps for ancillary data changes by the computer. For example, if the user changed the BIOS clock, and installed hardware or software prior to changing the clock back to an accurate time, hardware driver files or software directory entries in the Program Files folder on the computer may indicate files that were installed during the falsified time. This could lead to an inconsistency where hardware or software was "installed" prior to release from the manufacturer. As another example, a program's activity log may contain timestamps indicating activity prior to the installation date of the program itself. Instances such as these can be useful in establishing the accuracy of the system clock.

SYSTEM RESTORE POINTS

While a discussion of Microsoft System Restore Points is beyond the scope of this article, it should be noted that starting with Windows Me, Windows System Protection automatically creates and saves restore points for the OS to safeguard the running of the computer. Restore points are created whenever actions occur such as installing programs, installing new Windows updates, and use of the computer for 24 hours. These restore points are located in the hidden folder "System Volume Information" on the root of the hard drive. Restore points are named in numerical order of creation. As a result, if the BIOS clock is changed, it is possible to see creation dates of the restore point folders which do no correlate with the order of creation. Table 1 is an example from a real case in which a BIOS clock change was identified via examining restore point creation dates.

Table 1. *Windows System Restore Points Indicating BIOS Clock Manipulation*

	File Created
RP0	01/26/10 04:30:10PM
RP1	01/26/10 04:30:23PM
RP2	01/26/02 04:36:07PM
RP3	01/26/02 04:39:03PM
RP4	01/26/02 04:43:22PM
RP5	01/26/02 05:00:42PM
RP6	01/28/02 10:15:50AM
RP7	02/16/02 09:54:12AM
RP8	02/16/02 09:55:09AM
RP9	02/18/02 02:03:28PM

WINDOWS REGISTRY

The Windows Registry is a treasure trove of information for any forensic investigator. Included among the various system and program settings are many time stamps relating to various system activities. By examining these timestamps, an investigator may identify entries which are out of sequence indicating BIOS clock manipulation. One example would be the User Assist registry entries which provide timestamps with last execution times for various programs on the computer. As described previously, execution times which are inconsistent with program installation dates or other activities on the computer could indicate BIOS clock manipulation.

DATED CONTENT VS. FILE TIMESTAMPS

Lastly, a comparison of dated content along with their file timestamps may provide an indication of clock manipulation. Internet browsing cache files can be a prime example of such dated content. For example, finding a cached copy of a web page discussing the 2012 Ford Mustang that has a file created timestamp in 2010 would generally indicate a suspicious BIOS clock as it would be impossible for the content to have been available at the time indicated by the file timestamp. Using the same concept, certificates, email messages, and anti-virus definition files are other examples of files with dated content which may be compared with their file timestamps to help to indicate BIOS clock manipulation.

SEEING THROUGH THE FRAUDULENT BIOS CLOCK SETTING

In general it is very difficult for an investigator to determine the true time at which an event occurred if the BIOS clock has been manipulated. The operating system assumes the BIOS clock is accurate and does not take measures to verify its accuracy independently. However, it is sometimes possible to find indicators of the actual time or magnitude of clock change despite anti-forensics efforts of a user.

In the example of the Windows System Event Log, a gap in time can provide a sense of how large the

clock change was and provide a maximum bound. For example, if the event entries jump forward from 1/1/10 to 1/1/11, the examiner can posit that the jump was at most one year. It may have been less but is unlikely to have been more based on the latter entries. Similarly if the time values jump back from 1/1/12 to 1/1/11, the examiner could posit that the clock was moved back at least one year. It may have been moved back longer but unlikely to have been less given the new values provided.

In the provided example of Windows Restore Points, one can see in Figure 3 that from point RP1 to RP2, the directory creation date changes from 1/26/10 to 1/26/02. In comparing the time change between the two restore points of 4:36PM to 4:39PM it can be seen that they vary by only a few minutes. In this example, it would be reasonable to conclude that sometime between 4:36PM and 4:39PM on January 26, 2010, the BIOS clock was simply rolled back by exactly 8 years and that many of the activities indicated after 1/26/ 2002 really occurred on the month, day and time indicated but in year 2010 instead of 2002.

Lastly, in the example of dated content not being consistent with their file timestamps, depending on the dates available in the content of the files, very specific differentials between the manipulated clock value and real life may be found. Some content such as stock ticker quotes and news articles which are commonly cached have date and time values included in the content. These values can be used as fairly precise indicators of true time and compared with the file timestamp to determine the clock differential.

As can be seen, the BIOS clock performs a significant role in providing critical data in a forensic computer analysis. The problems presented to an investigator by the anti-forensics technique of clock manipulation can be quite significant. However as shown in the examples provided, there are techniques available to the investigator where clock manipulation can be detected along with ways to determine true time using other available data. While the examples provided are not intended to be an exhaustive list of possibilities, it is hoped that they are useful in helping an investigator form accurate conclusions in their next investigation where a timeline of activities is difficult or confusing to create.

Author bio

David Sun is the founder of SunBlock Systems, an international consulting firm specializing in Computer Forensics and Electronic Discovery. He leads teams of investigators assisting large multi-national corporations with litigation issues related to electronic evidence and discovery. Mr. Sun has taught computer forensics at the University level as well as offered training to various legal and business professionals.

HOW KPMG USES ENCASE® TOOLS

TO SOLVE CLIENTS' E-DISCOVERY CHALLENGES IN CANADA

by Dominic Jaar

Clients of KPMG in Canada turn to us when e-discovery challenges loom and they're not sure they have the internal capability to meet their legal obligations in a cost-effective fashion. What we bring to those clients is our experience providing tested and reliable processes and solutions customized to their particular situations.

What you will learn:

How EnCase eDiscovery helps KPMG in Canada perform remote collection for its clients over their networks.

How KPMG addresses data privacy issues in the European Union (EU) for international companies.

A method of simplifying data transfer, culling, and production.

How EnCase Portable can be used for clients with offices in remote geographic areas.

What you should know:

The basic principles of digital investigation.

How e-discovery relates to forensic investigations.

One of the tools that my information management, e-discovery and forensic technology teams use to meet client expectations is EnCase® eDiscovery from Guidance Software. This article describes some of the ways EnCase eDiscovery and EnCase® Portable can be used and have been used on behalf of our clients in ways both conventional and creative.

ENCASE® FORENSIC CAPABILITIES

First, let me summarize the technological challenges that EnCase eDiscovery make manageable. As readers of eForensics Magazine, you're likely to be familiar with the basic EnCase° Forensic product, which allows for digital investigation and forensic collection. EnCase Forensic is a standard part of most e-discovery professionals' toolkits, to collect *electronically stored information* (ESI) from laptops, workstations, servers, and portable devices like smartphones and USB thumb-drives. KPMG relies on it because it always provided us with a complete job but also because it has the backing of a decade of published court decisions attesting to its acceptability to courts. It is used by law enforcement as well as regulatory, military and intelligence investigators. These days you'll even hear people in the profession say to *EnCase it*, meaning to prepare a digital collection from a computer.

The end result of an EnCase Forensic collection is an EnCase evidence file format consisting of a forensic image file (E01) or a *logical evidence file* (LEF), the second of which is the company's proprietary

virtual container for holding collected ESI in a way that makes it possible to verify that the data contained therein is exactly what was collected.

Created using a highly auditable process, these evidence file formats provide proven chain-of-custody information that is automatically generated at the time of acquisition and continually verified thereafter, as well. Such information cannot be modified or altered within EnCase software, and includes:

- The time and date of acquisition
- The system clock readings of the examiner's computer
- The acquisition MD5 hash value
- The examiner's name.

EnCase software will automatically report a verification error if the Case Info File is tampered with or altered in any way. The EnCase evidence file formats are widely accepted and familiar ESI container formats ingestible into other ediscovery processing and review tools.

ENCASE® EDISCOVERY TECHNOLOGY

If you think of EnCase Forensic as being like a state-of-the-art bicycle, EnCase eDiscovery is more like a high-performance motorcycle. First of all, whereas EnCase Forensic requires that each computer to be searched be opened up and its hard drive connected to a computer running the EnCase Forensic software application, EnCase eDiscovery operates from a single location and reaches out to laptops, workstations and servers over the network and performs its search and collection capabilities remotely and without disrupting the employee using his or her computer, even without the employee being made aware.

Like the EnCase® Enterprise product, EnCase eDiscovery has the capability to reach any endpoint on the client's network, as long as the target machine is turned on and plugged into the network. Its powerful digital search can perform robust pre-collection analytics, i.e. rapidly identifying which files would be collected using a particular set of search criteria, before actually collecting the targeted ESI. And when it comes time to collect, EnCase eDiscovery is equipped to apply identical search criteria against a wide range of endpoints in an automated fashion. Collections can be scheduled or throttled as desired, with the end result being a defensible search and collection and output into the industry-standard EnCase LEF.

When I speak of endpoints on a client's network, of course I'm referring not just to workstations, laptops and file servers, but also e-mail servers and collaborative sites such as SharePoint, which is growing rapidly as a location of choice for key corporate documents and files of every type. EnCase

eDiscovery offers the option of having the resulting LEF with the collected ESI *land* wherever we wish on a network. We just identify an output path, and that's where the LEF is stored.

COVERING THE ENTIRE E-DISCOVERY CYCLE

EnCase eDiscovery software provides oversight of the entire e-discovery process, in that it carries the process through every phase of e-discovery. We use it on behalf of our clients to perform *early case assessment* (ECA) (it offers a web-based viewer that permits searching and filtering, case-specific tagging and commenting on individual e-mails or files, as well as batch coding) and processing. In fact, we at KPMG in Canada have worked and continue to work extensively with EnCase eDiscovery developers at Guidance Software on components of load files that meet our needs and those of our clients.

HOW WE PERFORM COLLECTIONS FASTER AND BETTER – AND SAVE CLIENTS MONEY – USING ENCASE EDISCOVERY

The first advantage of using EnCase eDiscovery is simple math: We can conduct collections across a client's network with a single consultant from a single location. Only one operator is required to perform the collection (or pre-collection analytics). Of course, we spend a good deal of time beforehand in identifying sources of potentially responsive ESI, crafting the search criteria and parameters all in close coordination with the client's legal and IT teams, who may be coordinating legal holds, sending legal hold notices, and possibly contending with privacy considerations (I'll discuss below how EnCase eDiscovery can help with collections that encompass the US, Canada, and Europe).

Unlike collections performed by a team of consultants using one-to-one collection technology, going from machine to machine, a few per day, a single consultant using EnCase eDiscovery can collect from hundreds of custodians across a global network, including from:

- Laptops and workstations, including PSTs residing there
- Peripheral devices such as thumb-drives and external hard drives
- Share drives
- Email stores
- SharePoint
- etc.

Many clients prefer that we conduct these collections from within their corporate firewalls, although, in the appropriate case, we can do so virtually from our KPMG offices. We are able to maintain security, confidentiality, and integrity of the data over the network using EnCase eDiscovery, in large part due to the EnCase evidence file formats, which have been accepted in thousands of courts worldwide. All communications with the servlets have to be authenticated by the EnCase *Secure Authentication for EnCase* (SAFE) server, which provides granular, role-based access that defines which users can connect to which servlets. Integrity is maintained through the EnCase evidence verification process.

The second huge time- and money-saver for our clients comes from the global reach of EnCase eDiscovery. Even if we were to use just a single consultant operating an EnCase eDiscovery collection on a client's network, that single consultant could be conducting numerous simultaneous searches around the world.

Because EnCase eDiscovery can also operate virtually, a single operator can be controlling collections actually launched simultaneously from various locations and jurisdictions around the globe. Each can be scheduled individually to allow for time zones when machines are likely to be turned on. We find that an important advantage of EnCase eDiscovery is that it can search regardless of open applications, which means that if an employee has Outlook® open, for instance, we can still collect email from that custodian.

To give a sense of the scale and reach, a single KPMG in Canada consultant can simultaneously be collecting from 50 or even 100 employees in five separate continents, something that would take at least five consultants using manual collection technology requiring in-person collection. This manual process requires human collection and review of each and every document, email, or other piece of ESI at each physical location.

Our new method represents at least an 80% savings in consultant costs for our clients and the benefit of a standardized approach for all collections.

DATA PROTECTION RESTRICTIONS: COLLECTING EMPLOYEES' DATA FROM THE EU AND US FROM CANADA

EnCase eDiscovery can play a significant role in easing constraints on collection and processing of the personal data of European employees. When *United States* (US) litigation calls for the preservation and production of data collected from European employees, parties struggle to comply with their court obligations versus EU privacy restrictions. The *European Union* (EU) data protection laws call for collection approaches that are the least intrusive feasible method for balancing the legitimate business or legal need to collect the data against the employees' right to privacy, which is considered a fundamental human right. The EU also restricts transfer of personal employee data outside of Europe to

countries who do not have what the EU deem to be *adequate protection* for privacy.

Canada represents a middle ground between the US and Europe when it comes to privacy regulation over collection and processing of employee data. Although located just north of the US, its data privacy laws are much closer to the tough protections by the *European Union* (EU), and the EU data protection officials have declared Canada to have *adequate protections* for those rights, meaning that data collected from European employees legally can more easily be transferred from Europe to Canada.

On the other hand, the US's lax data protection laws have not earned the *adequate protection* designation from the EU, and therefore data collected from European employees is normally prohibited from transfer to the US, unless certain stringent requirements are met, including obtaining the signed written consent of the European employee.

The first of these challenges – collection and preservation of European employees' ESI – can be mitigated through the use of EnCase eDiscovery and EnCase® Enterprise, which offers remote and non-disruptive investigation of any endpoint on a company's network. EnCase technology has been approved for use by data officers and works councils at various companies as a collection tool that is less intrusive of privacy than alternative collection methods. Here are the points emphasized by organizations when seeking approval of data privacy officers and works councils:

- Emphasize that EnCase® Enterprise can enable you to avoid collecting employee personal E-mail or documents. With EnCase Enterprise, your collections will cull the data and preserve only those emails and electronic documents that meet precise search criteria, including keywords and file types. Other documents that do not meet the search criteria – including private personal data ("Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a)," http://en.wikipedia.org/wiki/Data_Protection_Directive.
  See *http://export.gov/safeharbor/index.asp* for an introduction to Safe Harbor principles and self-certification.) – will be left behind.
- *Assure that collections will be done from a jurisdiction with "adequate protection"* (See *http://export.gov/safeharbor/index.asp* for an introduction to Safe Harbor principles and self-certification) *pursuant to EU data protection authorities*. Some works councils are reassured when told that all collections will be done from a jurisdiction that recognizes strict employee privacy, rather than from the US.
- *Emphasize that existing investigative policies already approved by the works council will remain in place*. For example, HR policies relating to the investigation of potential employee wrongdoing had long ago been approved by the works council and will not be affected by the use of EnCase Enterprise technology. That data would go directly to the company's HR team and would be handled the same as before.
- *Permit employees to create a "personal folder."* If employees create a folder in their computer file structure with an agreed-upon folder name in which they can place all of their personal data, EnCase Enterprise's search criteria can be configured to leave that folder untouched, so that none of that data will be collected.
- *Ability to restrict searches by file type*. Employees can be sensitive about certain types of files that may not be of interest to the company – personal photographs, for instance. With EnCase Enterprise, these file types can be excluded.

With its federal privacy mandate, Germany has the most stringent privacy rules in the European Union. For tips on how to obtain German works council approval for use of EnCase, a white paper on the topic is available here.

SIMPLIFYING DATA TRANSFER, CULLING, AND PRODUCTION

Once targeted portions of European employees' data has been collected, US litigants still face the daunting challenge of transferring that data to the US for review, further culling down, and production to adversaries. This is where KPMG in Canada holds a key geographical advantage because

Canada is deemed by the EU to have "adequate protection." This means that employees' personal data lawfully collected in Europe can be transferred more easily to Canada with less EU transfer restrictions.

Using Canada as a privacy "safe zone," US litigants can leverage KPMG in Canada's geographic and EnCase eDiscovery to collect European employees' data remotely from Canada, and then review and process the collected ESI in Canada. EnCase eDiscovery enables us to collect European data from Canada by deploying a collection computer to the client's European network and connecting to this computer using the client's VPN infrastructure.

All communications between EnCase eDiscovery and the collection computer are encrypted to the Advanced Encryption Standard (AES) with a key size of 128 bits. Furthermore, the encryption algorithms used are certified FIPS 140-2-compliant.

Once the data is transferred to Canada, legal teams can review that ESI in Canada and cull it down to the much smaller subset that needs to be produced to adversaries or regulators. Once culled down and ready for production, the organization must now obtain consent from the employees whose data are implicated, which is commonly a smaller number of employees. And at this point, the employee can be reassured that only a fraction of his or her data need be transferred to the US. In some cases none of an employee's ESI will make it through the review process. In most matters, using Canada as the discovery hub between Europe and the US will ease the privacy challenge significantly.

ENCASE PORTABLE

Canada is a country of considerable size, with most major cities and business centers in the southernmost part of the country. KPMG in Canada has a number of clients that operate their businesses in the northern part of the country. Many of these are mining or energy companies and collecting from these remote locations can be complex and expensive.

Historically, we had to fly people to perform collection, which was very time-consuming for the client, particularly when all that was needed, in many cases, was a snapshot of a hard drive or server.

EnCase Portable is another tool that provides not only a key capability to our skill and tool set, but enables a dramatic reduction in the time required to perform certain steps in data collection and processing.

EnCase Portable is a powerful search and collection software for field or remote personnel delivered on a USB device. Even non-specialists can plug the EnCase Portable device with pre-configured datacollection jobs into a USB drive and:

- Scan for evidence without calling in a specialist or seizing computers;
- Perform forensically sound triage and collection;
- Pre-screen evidence to reduce data volumes, allowing forensic professionals to work more efficiently;
- Return the device and the data to professionals for analysis in an encrypted format.

What this means for my team is that we no longer need to fly to remote locations for a simple task, but can use express delivery services to our client locations or use their own internal mail and have the appropriate person at each client site run the data-collection process with our assistance by phone. Then it's a simple matter of returning the EnCase Portable device via delivery service for analysis and processing in one of our KPMG in Canada offices.

We've found that clients prefer this methodology, because they feel actively involved in the process, rather than having a third party come in and disrupt their business processes.

USING ENCASE EDISCOVERY TO PROCESS CLIENTS' ESI

A final value-add for KPMG in Canada's clients is that we are able to process collected ESI using EnCase eDiscovery either at their sites or at our offices. While EnCase eDiscovery is better known for its collection capabilities, it also includes a processing engine for culling, de-duplication, other processing and creation of load files in Concordance, Summation, EDRM-XML or native file formats.

IN SUMMARY

The globalization of business for many corporations and industries has ushered in an era of complexity with regard to international law and data collections. Our decades of dedicated experience at KPMG in Canada and the use of well-established technologies and products like EnCase eDiscovery and EnCase Portable have allowed us to work creatively within the data protection laws of different countries. We now can offer our clients new options in data collection and processing in a way that enables best practices, complete compliance with the laws of every country and region involved, and the most costeffective and non-disruptive means possible.

Author bio

Partner and National Leader, Information Management, eDiscovery and Forensic Technology Services KPMG

LEARN:

- Advancing Computer Science
- Artificial Life Programming
- Digital Media
- Digital Video
- Enterprise Software Development
- Game Art and Animation
- Game Design
- Game Programming
- Human-Computer Interaction
- Network Engineering
- Network Security
- Open Source Technologies
- Robotics and Embedded Systems
- Serious Game and Simulation
- Strategic Technology Development
- Technology Forensics
- Technology Product Design
- Technology Studies
- Virtual Modeling and Design
- Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

University of Advancing Technology
UAT
Learn. Experience. Innovate.

You can talk the talk.
Can you walk the walk?

PLEASE SEE **WWW.UAT.EDU/FASTFACTS** FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.

DIY REMOTE NETWORKED OS X MONITORING

by Israel Torres

Remote access to a machine (or more so machines) is status quo these days; we are creatures of convenience and if we can operate as easily from a remote location as we can at the office we'll take it.

What you will learn:

You will learn how to forensically automate the detection and connection to a target machine on the network, as well as automatically package, transfer and install the watchdog payload to the target system.

What you should know:

You should be familiar with basic scripting and networking.

With so many network connections we have available to us nowadays, remembering all of them – especially test systems seems quite inefficient. If I want to connect to a test system I should be able to by just requesting it and not having to remember the hostname, ip, account name, password, etc. Also if I want to make sure a process is being run (exclusively) and monitor it accordingly it should be conveniently available for me to do so. I will demonstrate what worked best for me to solve these issues nicely.

INTRODUCTION

In short a watchdog is a service that runs to make sure something desired is being accomplished. In this specific case I am interested to make sure a specific process is being sustained during the lifetime of a user being logged in. Mac OS X does not provide something easily available for this through any of it's native controls so I needed to make something quickly for it to work as desired. I start with a proof of concept and have built on it since. Extending it out further has also had me thinking about future builds but this will cover where it currently is as it works perfectly for my specific needs.

I'll begin by referring to the Abstract Workflow of how everything comes together and what is being accomplished along the way (Figure 1).

Within the abstract workflow there is an attacker and a target. In this scenario I am the attacker and the target is the remote machine that I want to detect, locate and connect to. Once a connection has been established I want to copy a payload file (with further instructions) over, and

then install it on the remote system. It is given that I know the authentication credentials necessary for this operation to occur (both as a local and remote user). As stated the primary objective is to update the remote OS X networked machine not knowing the hostname/ip and installing a “conditional watchdog” (Figure 2). The payload deployment model covers the layers of the scripts involved so that in the end only one script is needed to be run to accomplish all the work necessary. This allows for the system to be dynamically discovered, scripts packaged and deployed. Each script calls the next passing parameters to the next.

DEMONSTRATION

This demonstration explains the processes involved to perform the following:

- Detect, locate and login to the known remote machine via ssh
- Use scp/ssh to copy and install the watchdog payload
- Optionally interact within the remote shell.

I know I have a machine on the network, but since it uses DHCP it's IP can change so I don't bother remembering it. Also I am not interested in giving it a static IP since I often reimage it as it is for testing; and some of the things I put on there shouldn't live too long if you know what I mean (i.e. malware testing).

The remote machine also doesn't remain with a consistent hostname as I change it based on what I am doing so i can't rely on pulling the hostname and getting success. Since I also change my network configuration often for these same types of tests I am not entirely sure of what I have going on and usually have to rediscover things along the way and reconfigure them as necessary.

What I do know is that the remote host is on the same network I am on (VLAN) and that it is up and has a few services enabled such as remote screen sharing, file sharing and ssh.

Next up is that the client machine I have (usually another test machine) may or may not have tools loaded on it and may or may not have Internet connectivity to download said tools. For just this case it is always best to have an understanding of how to do this the base vanilla way (applied technique one) as well as how to do it more efficiently with known toolsets available freely (applied technique two). For the following examples we'll go through a vanilla procedure as well as a tooled procedure.

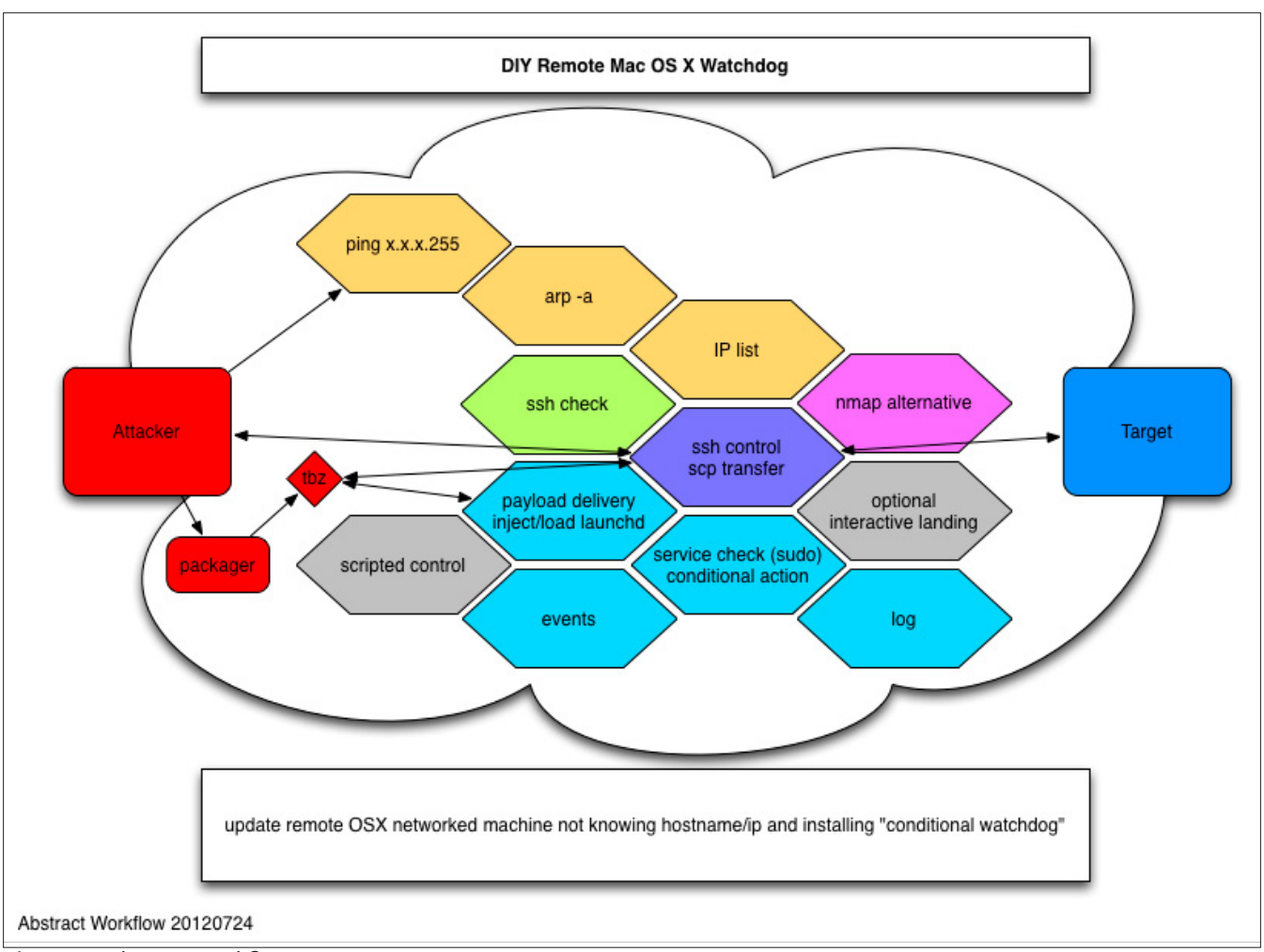


Figure 1. *Abstract Workflow*

APPLIED TECHNIQUE ONE

At this point I open terminal (bash) and perform a simple query to find out what type of network I am on (using interface `en0` – it is good practice to specify the interface especially if you have multiple interfaces).

```
>ifconfig en0
```

the most interesting line is the IPV4 line that has the following information:

```
inet 192.168.2.105 netmask 0xffffff00 broadcast
                  192.168.2.255
```

here I find that my current IP address for interface en0 is 192.168.2.105

```
calculating the subnet (if it isn't obvious)
can be done with this bash one liner:
>C=0;for x in $(echo "0xffffff00" | cut -d x -f 2
| fold -2); do echo -n $((0x$x)); C=$(($C+1)); if
[ $C -lt 4 ] ;then echo -n "." ;fi; done
```

At this point I've discovered the following. My host is on 192.168.2.105 using the subnet mask of 255.255.255.0 and the broadcast address is 192.168.2.255.

The next step I check the arp table using the arp utility displaying all current arp entries (`-a`) on specifically interface `en0` (`-ie`)

```
>arp -a -i en0
```

what returns are two addresses:

```
? (192.168.2.1) at 0:13:10:db:63:7e on en0
ifscope [ethernet]
? (192.168.2.255) at ff:ff:ff:ff:ff:ff on en0
ifscope [ethernet]
```

The first being the test router, and the second being the broadcast address – I know my test machine is online and it isn't appearing on this list. I need to ping the broadcast address and then run arp, one ping will do. Using the switches to bind to the interface (`-b`) and then to exit successfully after receiving one reply packet (`-o`).

```
>ping -b en0 -o 192.168.2.255
PING 192.168.2.255 (192.168.2.255): 56 data bytes
64 bytes from 192.168.2.65: icmp_seq=0 ttl=255
time=0.795 ms

--- 192.168.2.255 ping statistics ---
```

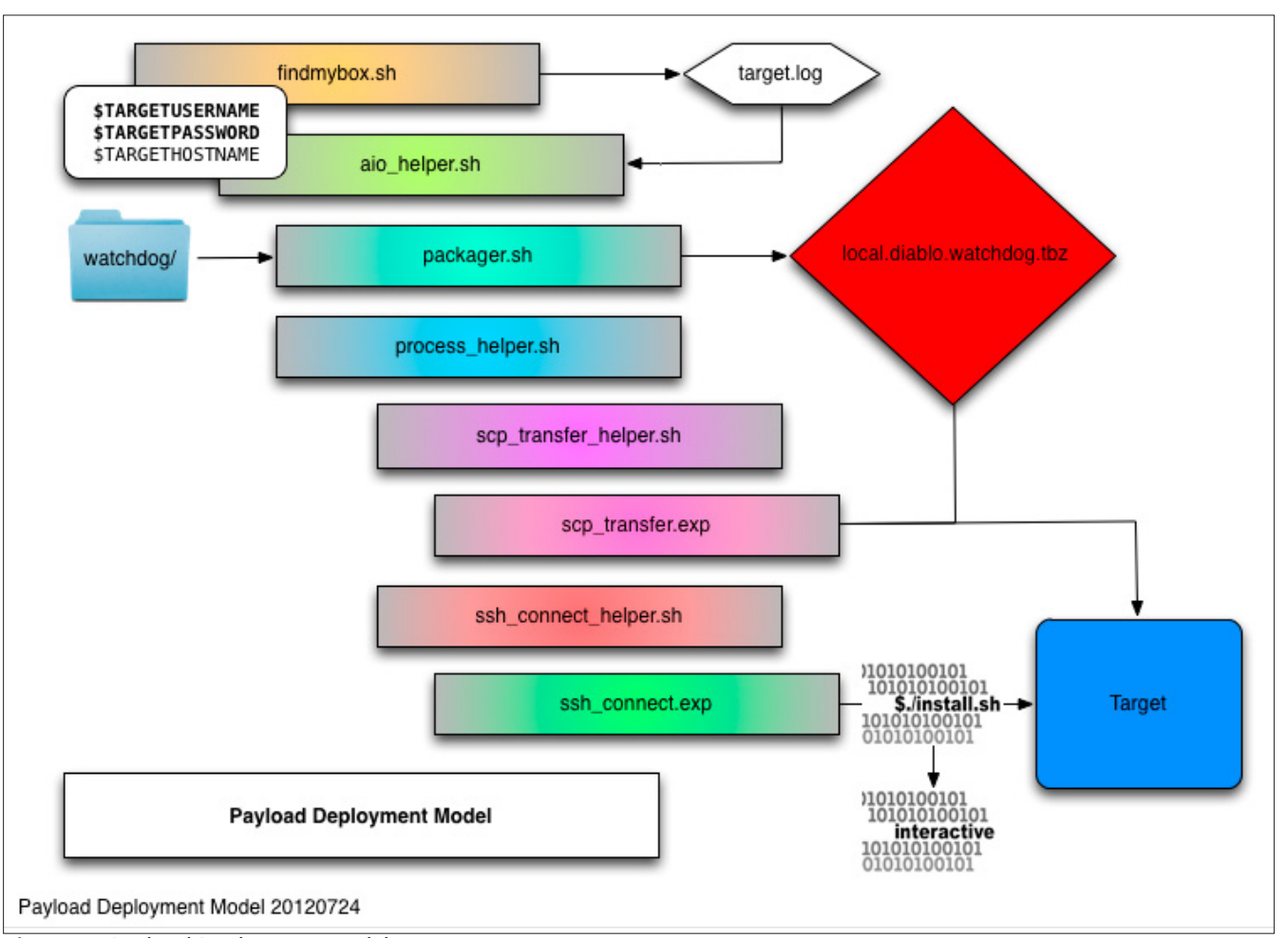


Figure 2. *Payload Deployment Model*

```
1 packets transmitted, 1 packets received, 0.0%
packet loss
round-trip min/avg/max/stddev =
0.795/0.795/0.795/0.000 ms
```

For future sake this can be accomplished in a one-liner:

```
mybroadcast=$(ifconfig en0 | grep  -w inet | cut
-d ' ' -f 6); echo "pinging broadcast ip
$mybroadcast"; ping -b en0 -o $mybroadcast > /dev/
null
```

Now checking arp again, I'll have more (depending on the firewall settings on the host themselves). Since I know my target host doesn't run one while on this network things should work out well.

```
>arp -a -i en0
? (192.168.2.1) at 0:13:10:db:63:7e on en0 ifscope
[ethernet]
? (192.168.2.9) at 0:1b:78:70:27:d1 on en0 ifscope
[ethernet]
? (192.168.2.65) at 0:25:0:ff:55:56 on en0 ifscope
[ethernet]
? (192.168.2.100) at 58:55:ca:d:fa:54 on en0
ifscope [ethernet]
? (192.168.2.102) at 28:cf:da:27:b7:98 on en0
ifscope [ethernet]
? (192.168.2.255) at ff:ff:ff:ff:ff:ff on en0
ifscope [ethernet]
```

Ah, that's much better. I now see 4 additional hosts online. At this stage I could attempt to connect to each host via ssh but a tad smarter way would be to scan for the default ssh port 22 (assuming it is indeed default). Using a for loop, arp and nc (netcat) this can be done in another one-liner that logs the address (in target.log) so I can use it again in the future:

```
L=target.log;for x in $(arp -a -i en0 | cut -d '
' -f 2 | sed 's/[()]//g'); do echo "checking
for ssh daemon on $x:22" && nc -z $x 22 && echo
writing $x to $L && echo $x >> $L; done
```

This results as follows:

```
>
checking for ssh daemon on 192.168.2.1:22
checking for ssh daemon on 192.168.2.9:22
checking for ssh daemon on 192.168.2.65:22
checking for ssh daemon on 192.168.2.100:22
checking for ssh daemon on 192.168.2.102:22
checking for ssh daemon on 192.168.2.112:22
Connection to 192.168.2.112 22 port [tcp/ssh]
succeeded!
attempt to connect to 192.168.2.112
checking for ssh daemon on 192.168.2.255:22
```

voila! that was easy enough so we've identified one host on the network (192.168.2.112) that has the ssh port (22) open. If I had multiple machines I'd either have to compare the ssh-rsa key fingerprint on `~/.ssh/known_hosts` using the command:

```
ssh-keygen -lf ~/.ssh/known_hosts
2048 d3:31:01:67:b4:7d:dd:a0:4e:a6:5c:10:94:29:a
2:f4 192.168.2.112 (RSA)
```

Then compare it with the remote machine to make sure they match:

```
key=tmp-remotessh.key; ssh-keyscan -p 22
192.168.2.112 > $key; ssh-keygen -lf $key; rm $key
```

*note unfortunately `/dev/stdin` on 10.7.4 is seemingly broken to use `ssh-keygen -lf /dev/stdin <<<$key`.

A simple way to automate this via bash script one-liner is:

```
sshlocal=$(ssh-keygen -lf ~/.ssh/known_hosts);
sshremot=$(key=tmp-remotessh.key; ssh-keyscan -p
22 192.168.2.112 > $key; ssh-keygen -lf $key; rm
$key);if [ "$(echo $sshlocal | shasum)" == "$(echo
$sshremot | shasum)" ]; then echo "ssh match
found"; else echo "ssh match not found";fi
```

which returns:

```
# 192.168.2.112 SSH-2.0-OpenSSH_5.6
ssh match found
```

APPLIED TECHNIQUE TWO

In comparison if with nmap installed it all the above 3 lines can be run with this one line.

```
address=$(nmap --log-errors -oG - 192.168.2.1/24
-p 22 -e en0 --open | grep -E 'ssh' | tr -s ' ' |
cut -d ' ' -f 2); echo $address > target.log
```

On that note it's always best to use the right tool for the right job; but always know how to do it without the right tool ;)

Afterwards I follow up with an ssh connector expect script. Expect scripts are used for sessions that don't normally allow for scripted interaction as a shell script would provide. As it is aptly named you expect certain feedback and upon the feedback you can send actions to fulfill the operation. In this case I use them to log me into the remote machines for copying files over using scp and controlling the session via ssh. Certainly I could use a cheap passwordless certificate based login but since I am reimaging these systems a lot it works best for me to use the hardcoded password in the test image than regenerate a certificate. During the

payload deployment workflow the expect script's purpose is to connect to the IP address located in the target.log text file:

```
if [[ -s target.log ]]; then ./ssh_connect.exp
'testaccount' 'testpassword' '192.168.2.112' ;
else echo target.log is empty - exiting; fi
```

I've compiled all these commands into the `./findmybox.sh` script (Figure 3).

To make sure this works as expected I need to make sure the remote machine is configured for ssh access. On Mac OS X 10.7.4 this is done through the system preferences in Sharing (Figure 4).

I'll end up variablizing the target info (`$TARGETUSERNAME $TARGETPASSWORD $TARGETHOSTNAME`) so they are found dynamically they will be automatically processed from beginning to the end.

Now I can find the target machine on the network without having to think about it, next I'll package, transfer and install the watchdog payload.

WATCHDOG SCENARIO

For this practical real-life scenario I had a user that requested playing Diablo III on a Mac, however the user normally doesn't have Administrative access and the controls that Apple offers isn't granular enough to plainly state to allow this game to run. Instead each and seemingly every dependency needs to be added and even then doesn't run as expected.

The simplest thing to do is to use an Admin account to logon on the user's behalf and restrict their actions so they only play the game. Since they don't know the Admin password, they can't change it, create another Admin or really do much without being prompted for an Admin password.

Nonetheless it's always best to keep them on the straight and narrow with a simple DIY watchdog – a service script that makes sure they are in the game state – otherwise perform an action (or set of actions) and logging these actions for later auditing... this is all to be done over ssh; as well as updated (uninstall/install) as needed remotely – transparent to the user. The breakdown to this scenario is as follows:

- GameZ: Diablo 3 on Mac OS X 10.7.4
- AccountY: Admin Account, Battlenet Account
- UserX: Non-Admin User Using Admin Account (not knowing the password to the accounts)

SCENARIO

UserX needs to use *AccountY* to Play the *GameZ*

PRECONDITIONS

- GameZ loads upon account login.
- If GameZ terminates or UserX exits from GameZ the System will perform an action.
- GameZ will be the only thing UserX can use while logged in as AccountY.

VARIABLES

- The system is polling every 60 seconds searching for *GameZ*'s process; this could be increased as deemed necessary.
- The system is checking a specific string (in this case *Diablo III*) which is a meta string (the launcher that encapsulates the game itself); changing the string can make it more granular for a specific known process – this way *UserX* can't just execute the launcher to keep the system up; or run an aptly named while loop in a bash shell to give the appearance that the process is running.
- If process that is expected of *GameZ* is not there; the system will perform an *action* such as shutting down, logging AccountY off, popping up a message, etc.

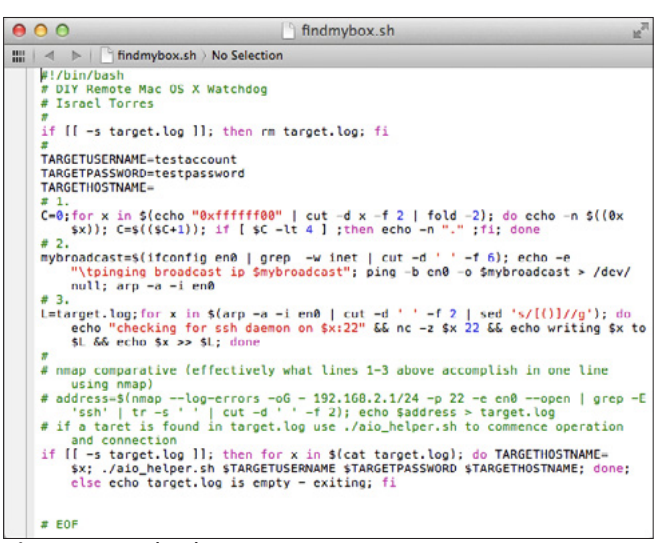


Figure 3. *Findmybox*

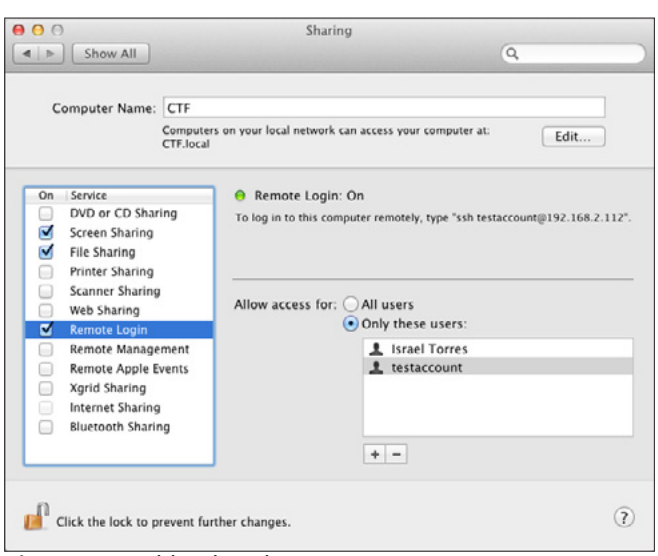


Figure 4. *Enable ssh.psd*

backdoor: remote access is available for the authenticated ssh account to login which puts this polling process on hold and resumes once the ssh account logs off (Figure 5).

After the connection has been made I need to copy the payload just built, and send commands to install and activate it. I created a packager that gets the modified scripts from the watchdog/ subdirectory and archives them into a tarball. This is what get sent across to the `~/` directory using the `scp_transfer.exp` (expect) script after which the `ssh_connectp.exp` (expect) script then executes the unarchiving and installation process. This is where the files are copied to where launchd will access them for that profile [specifically] (`~/Library/LaunchAgents`) and then initiate them to run via *launchctl load*. Once launched it will check every 60 seconds.

Once every 60 seconds the watchdog script checks to see if a MASTER is online (which is what I am when I login via `ssh`) it identifies an external ssh connection (not the current console user) and when the MASTER is flagged will not continue checking – it logs in `system.log` (`/private/var/log/system.log`) which can be viewed to see the "HELLO MASTER" message. (you can verify this once logging into an interactive shell session by running `tail -f /private/var/log/system.log` (Figure 6).

If MASTER is not enabled the watchdog script will then check for the targeted running service. In this case it is *DIABLO III* (string literal) if it is running another process is run via osascript to bring the application into the foreground – this helps if the user is aware of the process requirement and tries to minimize it or even create a fake process from a script named the same name as the process

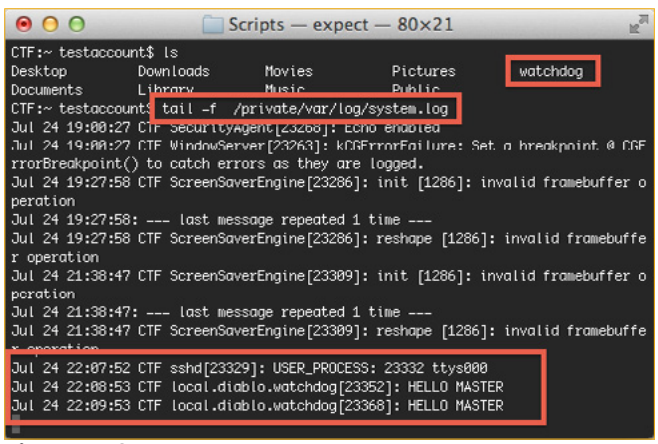


Figure 6. *System Log*

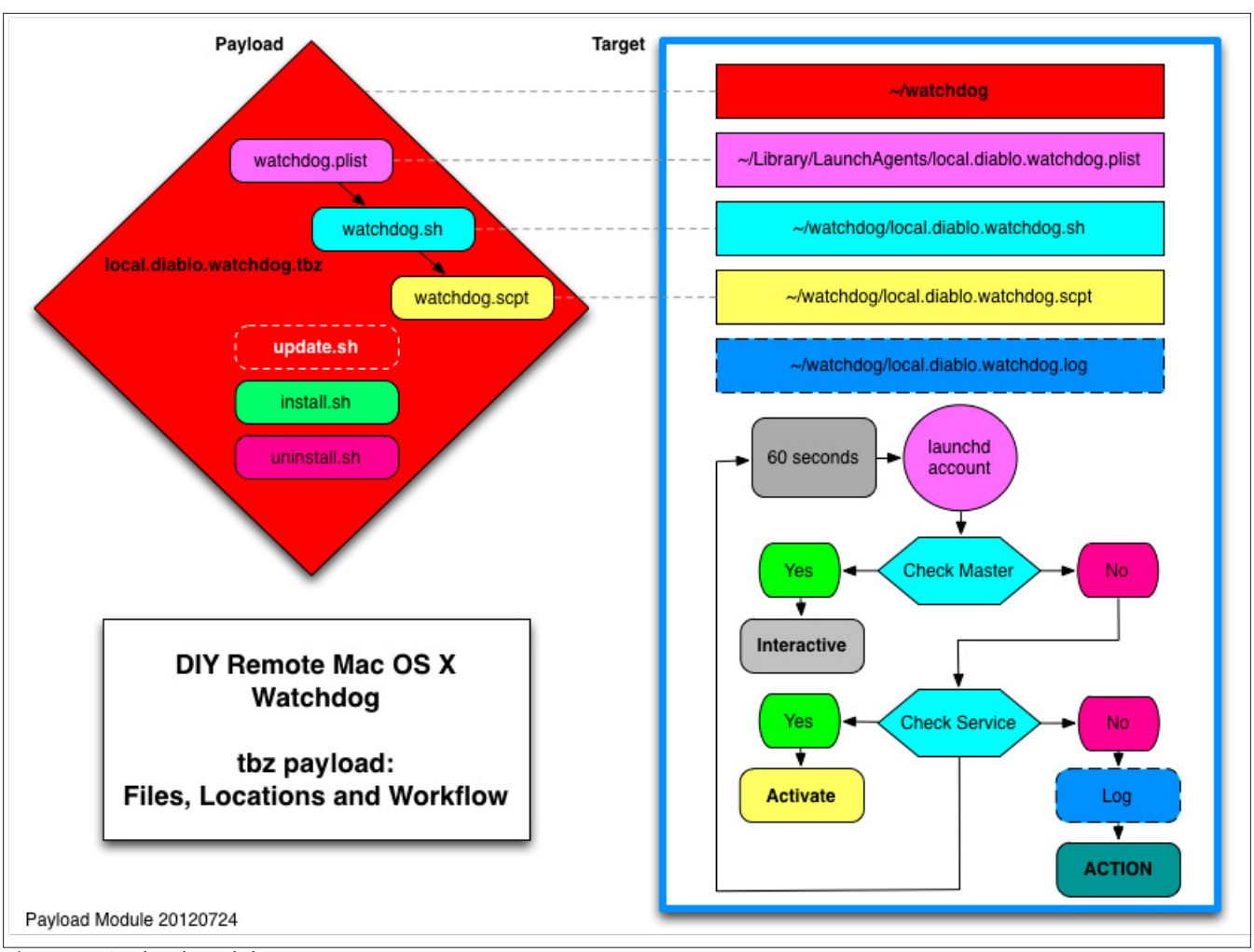


Figure 5. *Payload Module*

(i.e. Diablo III.sh) by calling while(1) and sleeping indefinitely. BTW to create such a fake process I use this simple one-liner that does the trick:

```
echo -e '#!/bin/bash' "\n" 'while [ 1 ]; do echo
running Diablo III fake service; sleep 1000; done'
> Diablo\ III.sh && chmod +x Diablo\ III.sh && ./
Diablo\ III.sh
```

you can validate it by running ps:

```
ps ax | grep -i diablo
```

which will return (Figure 7):

```
8514 s001  S+    0:00.00 /bin/bash ./Diablo III.sh
```

and since the default watchdog script is only looking for *Diablo III* it will satisfy the query. Future builds will hash the binary, and path to make sure it is better derived and prepared for such fakery.

If the targeted service is not running a log will be created in the watchdog subdirectory and the action will be executed – whether it is to logout the console user, shutdown the system, bring up a message box, etc. Naturally using the placement of the plist it the watchdog can be targeted for the profile, or the entire system. Running *man* on launchctl gives the specific paths:

- `~/Library/LaunchAgents`: Per-user agents provided by the user.
- `/Library/LaunchAgents`: Per-user agents provided by the administrator.
- `/Library/LaunchDaemons`: System wide daemons provided by the administrator.
- `/System/Library/LaunchAgents`: Mac OS X Per-user agents.
- `/System/Library/LaunchDaemons`: Mac OS X System wide daemons.

In an interactive shell to see whether or not the process is running as expected you can run the following command:

```
launchctl list local.diablo.watchdog.plist
```

... which will display the source of the plist; otherwise if it isn't loaded it will not show it loaded.

Updating the watchdog is simple enough, easy enough to do during an interactive shell session by calling `~/watchdog/uninstall.sh` – then running `./findmybox.sh` once the local scripts have been modified (located in watchdog/) or by running the remote `~/watchdog/install.sh` script (if you know the scripts are already updated from the previous session – the files will get copied but if you want to restart the service it's simpler to unload and load (which is what the install and uninstall respectively do).

Remember that running the uninstall.sh script will completely remove the remote `~/watchdog/` directory and all the saved log files – if you need to keep them it is easiest to archive them and move them somewhere else (or copying to your local system) then uninstalling otherwise they will get expunged. A non-intrusive update script that does this for you was in the works at the time of this writing for the next revision.

ALTERNATIVE ACTIONS

Alternative actions may be desired such logging out the console user (using same or different account)

```
ps -axu $username | grep -v grep | grep
loginwindow | tr -s ' ' | cut -d ' ' -f 3 | xargs
-n 1 sudo kill -KILL
```

or popping up a message box (Figure 8):

```
osascript -e 'tell app "Finder" to display dialog
                "Unauthorized User Detected!"'
```

For the most part the entire process from start to finish takes only a few seconds (Figure 9). At most under two minutes; I had a hardened Windows 7 machine on the same network and no-

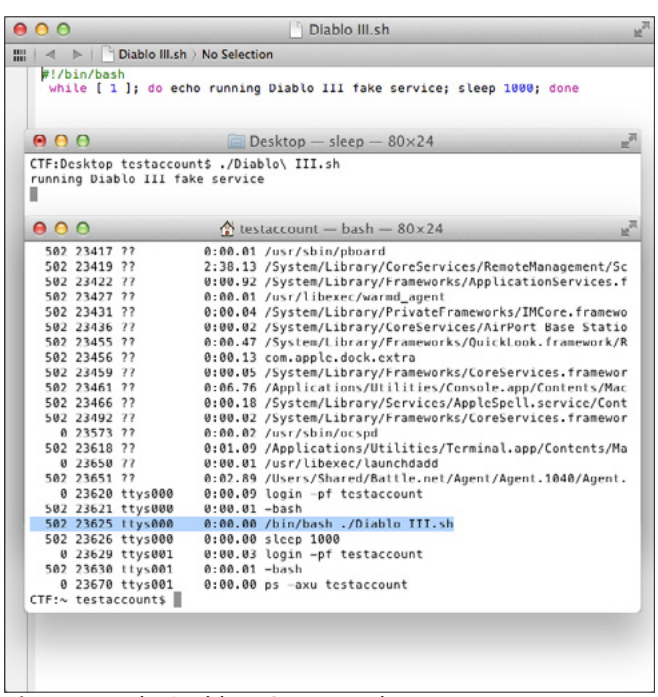


Figure 7. *Fake Diablo III Service.psd*

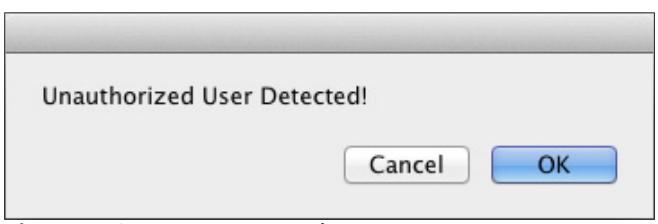


Figure 8. *Popup Message.psd*

ticed that when it was plugged in it would take nc a about a minute to complete it's port 22 (ssh) scan; when it wasn't plugged in it took a few seconds. nmap didn't have an issue with this whatsoever.

FUTURE BUILDS

During research and development of this DIY project. I discovered a few other tasks that will be placed in future builds that didn't make it in this build. Such are the following:

- Advanced Targeted Host Support – Using a switch parameter to isolate a specific host by composite makeup and having to rely on known hostname, ip.
- Hashed Service Check(s) – When finding the associated service to run a hash comparison on the .app to validate it is indeed the service sought and not something easily faked.

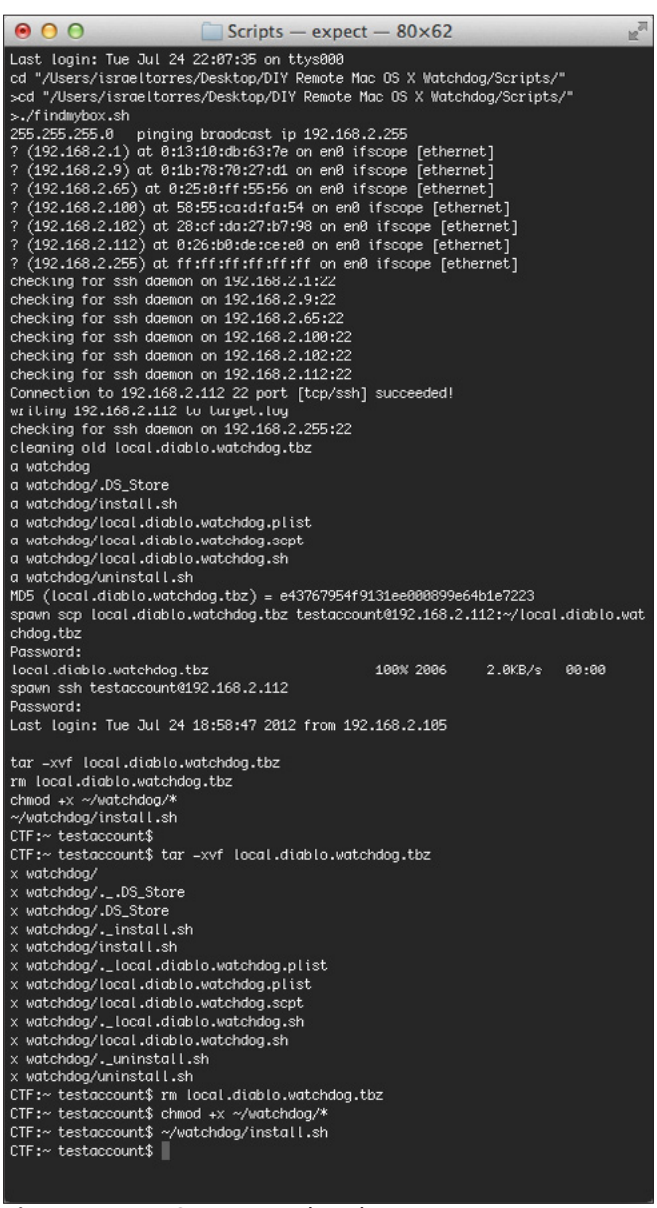


Figure 9. *From Start To Finish.psd*

Notes

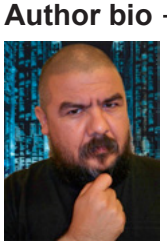
All source code created and tested on:
Mac OS X 10.7.4 11E53
Darwin Kernel Version 11.4.0
GNU bash, version 3.2.48(1)-release
MD5 (Scripts.zip) = c94b8eefce5a1b5e15f71c6b4b3eadaf

- Encrypted Payload(s) – Payloads that would require decoding/decryption prior/during installation. This helps in obfuscation of altering instruction data upon transport or static scans.
- Multiple Payloads – Payloads that can be suited for differing environments, platforms, targets, users, scenarios, etc. Directed upon a small modular script to keep things simple.
- Update feature – Currently you must run `./uninstall.sh` prior to running `./install.sh` to successfully update version the current version to a newer version. Originally I was going to add this intrinsically to the install.sh but thought it better to create an update.sh for optional updates to not change the current operational workflow.
- IRC control feature – Currently operational commands are driven from ssh, however IRC integration (replacement or in addition to) would enable more granular remote control.
- Standalone binary compilation – Currently this is a myriad of shell script built up from the proof of concept for the Mac OS X platform; the build would be more robust and allow for better obfuscation when created as a standalone binary; likely candidates are C or Python.
- Multi-platform support – This was created on a Mac for a Mac, but can be easily modified for *nix systems (if required). Windows on the other hand would be an interesting task.

CONCLUSION

Necessity is the mother of invention and lazyiness is my main motivator when it comes to doing highly repetitive technical tasks. Being able to script them so they work dynamically and serve multiple purposes is always a benefit to everyone. I am hoping what I've demonstrated herein helps you complete your tasks quickly, or given you ideas to make them better.

Author bio



Israel Torres is a security researcher for eForensics Magazine residing in Irvine, California. He spends his free clock cycles writing/coding/hacking freelance, making and breaking ones and zeros, and staying in the digital shadows. He loves PKI/cryptography and prefers poking at Mac OS X. Professionally he serves as a Systems Administrator in Higher Education. E-mail: eforensicsmag@israeltorres.org.

SECURITY IN WIRELESS SENSOR NETWORKS

MAJOR ATTACKS, ENCRYPTION ALGORITHMS AND SECURITY PROTOCOLS

by Deivison Pinheiro Franco

Article is an approach regarding safety analysis in Wireless Sensor Networks (WSNs), which displays components, concepts and operational aspects of security for WSNs. It demonstrates how to operate sensors, process and transmit information based on the processes of decision making, according to processing regions.

What you will learn:

The main vulnerabilities, attacks, encryption algorithms and security protocols for Wireless.
Sensor Networks (WSNs).
Standards and precautions for implementing security in WSNs.

What you should know:

Wireless Sensors Networks concepts.
Components, concepts and operational aspects of enhancing the security of WSNs.
How sensors process and transmit information based on the decision making processes.
Notions of applications, protocols, topologies, routing and management of WSNs.
Situations that a network analyst can find when analyze WSNs.

It's also about how this communication can and should occur in a safe, where they will be approached its main applications, protocols, topologies, routing and management. Taking into account structures, standards and precautions for implementing the same in regard to security in wireless environments. Specifically for distributed sensor nodes arranged in a network and communicating with each other.

Technological advances in the areas of microelectronics and telecommunications bring WSNs – mobile network technologies that enable the integration of sensors in small wireless devices that, by sensing technique, collect data for decision making in a monitored environment.

Ubiquitous computing, also known as pervasive computing, will be based on "invisible" sensors and autonomous elements, which interact with each other to build environments and provide services to its users. The engineering required to build these environments is challenging, in terms of software and hardware. The social issues are also a complicating factor.

Ad hoc networks, or MANET (Mobile Ad hoc NETwork) are wireless networks that do not have a centralized infrastructure. Thus, each node can act as a router, capable of forwarding packets and also run applications. In this context, routing protocols for ad hoc networks must consider certain features that do not occur in a structured network, such as limited resources and dynamic topology. For this reason, use a routing protocol that wastes resources or that does not react well in the face of node mobility, may become unviable.

The basic mode of operation of sensor networks is quite differ-

ent from wireless computer networks due to the high integration of these networks with the physical world. The technological expansion in telecommunications to computer science brought a new set of challenges to overcome. Among these challenges is providing access technologies and the means by which these devices communicate accurately, converging with each other and integrating.

Currently one of the focuses of the research of wireless networks is in the context of mobile ad hoc networks. It is expected that these networks will play an important role in sensing applications, especially where an infrastructured network is not accessible or does not exist. Typical applications for this type of networks include mobile computing in remote areas, tactical communications and for rescue operations in disaster situations.

The critical issue in such networks is their ability to adapt to dynamic changes in topology promoted by the movement of the nodes as an adaptation to topological changes require changes in routing. Routing is linked to route management, and is a crucial aspect to these networks. Due to the high mobility of the nodes, finding a route between the source and the destination and keeping it active, as much as possible, is a complex task. Similarly, finding the node to which a certain message is addressed is difficult in such a network topology.

Wireless Sensor Networks (WSNs) are an essential part of the infrastructure of these environments. They work based on the sensing technique, which is the set of activities performed to obtain information about a certain situation or environment through sensors. The acquired information is used for decision making.

WSN ARCHITECTURE

A WSN is a collection of interconnected sensors that communicate with each other and with the environment, collecting data and transmitting them to a processing center (local or distributed) that will use them to make decisions more appropriate to the monitored situation.

The physical media used to compose the sensors network can be radio signals or infrared light. For economic reasons, this type of interconnection is not feasible with the means of connectivity used in traditional computer networks because the types of applications that run on these networks differ from networks of wireless sensors.

WSN has distributed communication nodes and self-configuration mechanisms in case of failures. Each node is equipped with sensors and can be organized into clusters. A WSN must have at least one sensor, called the sink node or sink, capable of detecting, processing, and making a decision regarding a monitored event and transmiting it to the sensors by broadcast to the network. Figure 1 illustrates a sensor network.

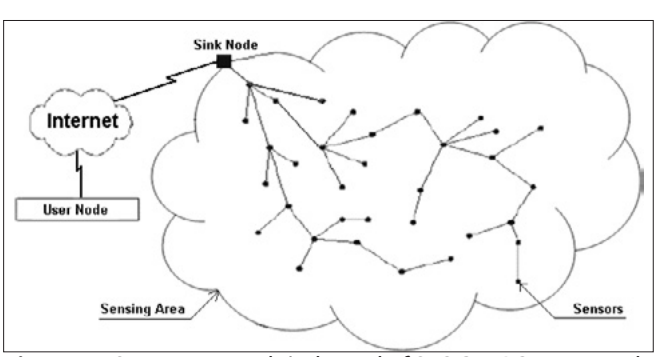


Figure 1. *Sensor Network (Adapted of STOCHERO, 2003 and CAMPISTA, 2003)*

SIMPLIFIED DESCRIPTION OF A SENSOR NODE

Sensors or *Sensor Nodes* (SN) are standalone devices capable of acquiring, processing and communicating information or intelligence regarding a monitored environment. The basic hardware consists of a sensor transceiver, processor, memory, battery and sensor element, which are mounted along the gateways and actuators in the composition of a WSN. Actuators are elements capable of changing values and correct flaws in the monitored environment. The gateways enable communication of a WSN with other networks. Figures 2 and 3 illustrate the basic hardware of a SN and present images sensors, respectively.

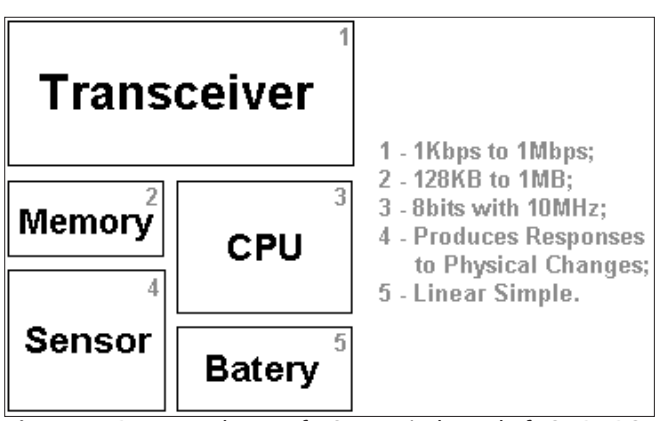


Figure 2. *Basic Hardware of a Sensor (Adapted of LOUREIRO, 2002)*

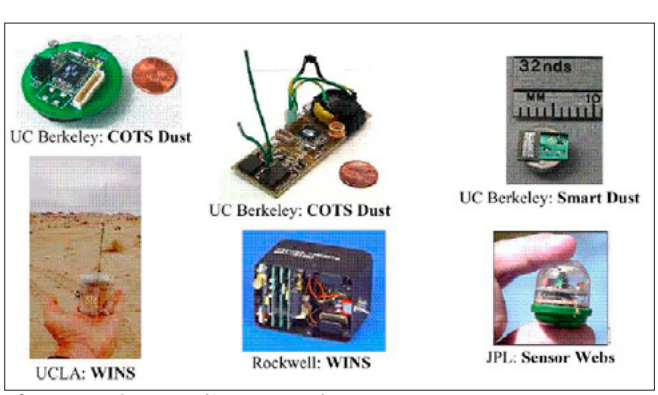


Figure 3. *Sensors (RUIZ, 2004)*

COMMUNICATION INTERFACE

The IEEE 1451 standard defines a communication interface for transducers (elements that are sensors and actuators at the same time), facilitating their development when they should be networked or systems that use various types of communication protocols. Its architecture is shown in Figure 4.

SECURITY

The need to connect to other networks exposes and makes vulnerable a network to attacks and security incidents. For a network that is always available to users, certain requirements must be adopted. In WSNs the SN should be installed and configured according to policies and goals before it goes online, which are determined by your administrator when designing their structure. The security of a WSN is mainly treated before and during installation, for problems with services they consume much energy and incidences of spectrum frequencies similar to those employed by the network may be involved in its operation and affect their lifetime.

Sensor networks use wireless communication, making them more vulnerable to attack, since using this type of communication, the transmission mode is broadcast, and naturally , the network is more susceptible to the action of intruders, who can easily listen to, intercept and alter data traveling across the network.

Some limitations of this type of network, such as processing and low power consumption, make the use of encryption unsuitable, as it requires a more careful processing, using a higher consumption of energy. Thus, providing security in wireless sensor networks becomes a great challenge, requiring security mechanisms that are appropriate to the restrictions of memory, processing and bandwidth existing in this type of network.

REQUIREMENTS

The availability of services to authenticated and authorized users must be constant. To support this, the network must be free of any possibility of denial of service or distributed simply. The DoS or DDos loses air resources and network services because of overload requests.

As the components of the network type are sensors, constant verification of energy usage is necessary because a primary issue for the lifetime of a WSN.

Principles of availability, integrity, confidentiality and authenticity are vital for any network data communication and are achieved through the encryption that is implemented in security protocols. An attacker who attempts to steal the information exchanged by the SN will not have favorable conditions to acquire them it.

The source verification of a data can be done by using protocols that make challenges to the transmitter nodes. These nodes send messages in plain text to the nodes that are being authenticated, encrypt it with a personalized key.

The authenticity is confirmed by the decryption of the sent data to the authenticator mechanism, which verifies if the used key is authentic, from the assigned user, and if the message content is connsistent with the original message transmission.

In WSN cryptographic keys are held by SN. The more keys each node uses, the more private, unique and reliable is the information, ensuring authenticity and eliminating potentially malicious information.

Another verification and validation of the legitimacy mechanism is the exchange of a secret key to compute a message authentication code, but this solution is not secure because the propagation of the messages is in broadcast mode.

The update ensures that information is not copied and inserted in the network. Copied data would be authentic, but not valid. This mechanism is achieved by the periodic use of cryptographic key renovation. The SN resists manipulation and are always updated with any changes within the network.

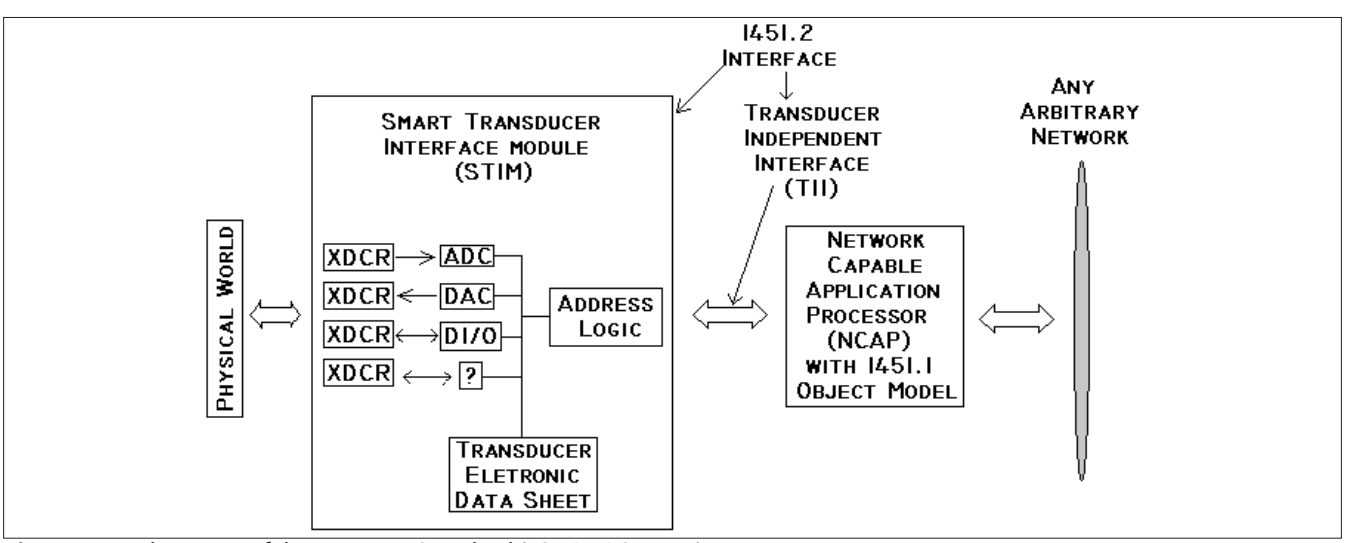


Figure 4. *Architecture of the IEEE 1451 Standard (LOUREIRO, 2002)*

Data integrity ensures communications have not been changed in transit by an adversary. This mechanism is usually implemented by hash functions. Data can be manipulated without the attacker does not even know what it was, because is encrypted. Thus, a data or SN can be manipulated, but without known what it is, not allowing access to their secrets. Depending of the application, this kind of action can be detrimental to the operation of the services and the network.

The nodes should be resistant to manipulation because a malicious user who gains access to a node cannot obtain sensitive information such as, data, code and even cryptographic key or some clue that will lead to such. In possession of such false information a node can be included in the network committing.

The SN should be collaborative, contributing to the functioning of the network, and should not be able to deny forwarding of data packets or control. It is necessary to note the behavior of the network while a SN is idle, because in addition to losing the sync operation and updating of security algorithms, if it falls in and out of this state, it may expend more energy than if it was permanently turned on. If this happens, it will be prevented from exchanging information with the network.

LAW (2002) says that in order to detect an intrusion of this kind of behavior, you would need a mechanism that detects network anomalies through an IDS protocol, but this mechanism is still too sophisticated for its inclusion at current level of development of sensor networks because they demand too great of an expenditure of energy.

LIMITATIONS

Some precautions are necessary to consider a safe communication infrastructure. According to the applicability of the proposed environment which a network is employed, it is necessary to know the objectives and requirements considered to choose the managing application of the information that will be trafficked by its nodes, so as not to overwhelm it.

Encryption algorithms for sensor networks require a compromise between the security provided by the algorithm and the amount of energy it uses. Studies and comparisons have already been made in LAW (2002) between the TEA and RC5. Their decision was to apply to sensor networks.

This is highly relevant because energy is required to encrypt, decrypt, send, receive data and process data, verify and validate signatures that travel over the network. All this results in energy consumption, and its amount stored on a sensor as well as the use of it is its main limitation.

To Akyildiz (2002) another important factor is the behavior during the process in which the sensor is on standby to conserve energy. At this time, the sensors may lose the synchronicty necessary to security algorithm functionality, since there is an exchange of information used in the update process of the keys. If a node loses this information, it may be unable to exchange information with the network. This waiting mechanism should be used carefully, because the sensor moving in and out of this state may expend more energy than if it were turned on all the time.

MAJOR ATTACKS IN WSNS

Considerable vulnerability exists in WSNs due to the wireless communication and the fact that the sensor nodes are in locations without physical security or are not monitored.

The major vulnerabilities related to the physical layer of the OSI model include the interference of the transmitted communication signal, and the damage of sensor nodes. The interference of communication signals transmitted by a node (signal jamming) occurs when an intruder node generates random signals to prevent the communication between the nodes. One way of avoiding this type of interference with the frequencies in use is through the use of spread spectrum signals for encoding. However, the radios that supports encoding spread spectrum are more complex, more expensive and consume more power, which could derail its use in WSN.

An attacker could physically damage a sensor node, so this would negatively effect their task of data collection and/or routing, impairing the functionality of the WSN application.. Further, the node could be replaced by a malicious node to generate attacks to the network or to the information being transmitted. A third possibility is that the information stored on a captured sensor node can be extracted, allowing an attacker to obtain encryption keys or authentication.

To prevent this vulnerability from being exploited, circuits or data protection mechanisms are needed.

The vulnerabilities at the network layer come from problems associated with data routing, since, in WSN, all nodes are routers. The most direct attack on a routing protocol is to change, repeat or fake (spoof) control packets, to create loops, detours, black holes or partitions. Among the major attacks in WSNs, we can enumerate:

SPOOFING

Targeting the control packets responsible for route table information, this type of attack occurs when a malicious node modifies or repeats routing information in the network in order to cause loops, attract or repel traffic, generate error messages and false routes, divide the network, among other damage. This causes information to never reach its destination and always pass through the same node, which will spend a lot of energy sending and receiving it. In this type of attack the malicious

node goes by a sink node, causing the network information passing through it.

SELECTIVE FORWARD
This type of attack is to undermine the functioning of the collaborative network, where a malicious node refuses to forward packets, discarding them. This causes the network to function collaboratively and cannot occur because the fact of the transmission of information to be of type hop-to-hop, where each node must forward packets coming from your neighbors. Thus, a malicious node can act as a black hole, not forwarding incoming data regardless of who received them.

DEVIATIONS
This attack happens when there is a deviation of packets for malicious nodes. The SN neighbors or themselves manipulate the data and make modifications. This vulnerability occurs because the opponents change the routing messages. This causes a node to become accessible to its neighbors as part of their routes, and/or others may reach those notdes by flooding the network with false routes.

SYBIL
Some systems use redundant routes in order to prevent possible threats, should any be affected. In this attack a node may have several identities and impersonate other nodes, which enables the control of the network, using multiple IDs, are replaced by substituting knowledge of alternative routes. In this way, we think it affected a malicious node, which is applying this type of attack; a node is isolated when it should not be.

WORMHOLES
Wormholes are tunnels created by attackers. The messages that enter these tunnels are propagated across the network from one part to another through two malicious nodes that are at the ends of the tunnel. By forging routing metrics, each malicious node will transfer to its neighbors the information that the wormhole is the best path for the transmission of packets and assign the tunnel as the most viable way to forward data. This transmission may be cause flooding and the closer the sink node will undergo further information within this tunnel.

HELLO INUNDATIONS
Hello packets are sent by routing protocols between neighboring nodes to test and verify network connectivity. Thus, a malicious node can send Hello packets deliberately to any node in the network, using any transmitter capable of doing it. The sensors, to receive these packages, identify the node as a neighbor and accept routing information broadcast by it. These routes induce packet forwarding to the malicious node.

SPOOFING OF POSITIVE RECOGNITION
This attack is used with the goal of making it appear that a bad traffic route is secure and suitable for sending packets, or a disabled node is operating normally. This is done when a malicious node sends a positive acknowledgment to a transmitting node, by transfer of a message from the attacker node.

THE RING OF EVIL
The ring of evil occurs when malicious nodes surround a sensor or group of sensors and refuse to forward packets by injecting misinformation in the ring.

In this case, it should be noted that when a network is compromised, or when a node is surrounded by many malicious nodes, it becomes difficult to make create viable solutions.

LOOPS
Loops can be introduced into the network by us intruders. These, in turn, through the propagation of routing information, for the wrong sensors, cause information to be circulated through the network indefinitely, resulting in increased energy consumption in SN until exhaustion.

ENCRYPTION ALGORITHMS AND SECURITY PROTOCOLS FOR WSNS

The purpose of providing security in WSNs brought the need for the creation and implementation of algorithms and techniques to establish secure communication between the various nodes involved in a particular environment. For this to become more efficient, the initial solutions are proposed and directly involved in the layer with the higher incidence of attacks – layer level three – network, with the creation, integration and improvement of security codes directly made in the protocols routing.

Using encryption and secure protocols in WSNs can prevent or reduce the severity of most of the types of attacks presented earlier. However, due to limited resources (energy, processing, and memory) in the existing sensor nodes choosing an algorithm to encrypt and decrypt messages sent by these nodes is not a trivial task. This is because the more complex (in terms of processing and key size) algorithm, provides greater security, but more energy will be spent and therefore the lifetime of the WSNs decrease (Araújo, 2004).

Implementations of routing protocols for ad hoc networks in sensor networks were successful with respect to packet forwarding. However, the question did not meet safety expectations, as this aspect is not native in their algorithms. In addition, implementation of public key cryptography in this

type of network is not feasible since it consumes too much energy resources of the sensors and the network as a whole. Thus, most of the proposed algorithms for secure protocols for sensor networks applies symmetric key encryption, both to save energy and to ensure confidentiality and authentication between sensors and the base station.

Perrig (2001) states that the variables needed to make calculations keys would not fit in the memory of a sensor and that the spread in broadcast, too, is a major obstacle, especially on the issue of key distribution, since it is not a reliable means. However, some studies and research were conducted in order to solve some of these problems.

Changing and incrementing security code level protocols AODV (Ad Hoc On-Demand Distance Vector Routing) and DSR (Dynamic Source Routing) were proposed by Marti et al (2000), which, even with some problems efficiency, succumbed in the creation of two new algorithms: the watchdog and pathrater. The first act promiscuously, which consumes more energy in checking the activities of the network nodes for packet forwarding. The second, based on data provided by the watchdog, acts in measuring the reliability of the transmission rates of the alternative routes to the same destination. But, how the performances of these two algorithms would occur if two nodes are normal and attacking its neighbors at the same time?

As one of the attempts to answer this question Michiardi (2002) proposed a mechanism that forces collaboration between sensors and generalizes the measured transmission rates – CORE (Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks). In this mechanism the neighboring nodes of a particular node collaborate measuring the efficiency of this node in the performance of assigned tasks to him. However, when a given node is estimated it takes to get data generated by it. This, in turn, being under review may change information on their packages. Therefore, there is no guarantee the reliability of the data transmitted. Following are the major cryptographic algorithms and protocols, simple, efficient, low power consuming and memory, developed in order to provide security for wireless sensor networks, so that the process of communication in these networks more efficient and safe.

THE RC5 ALGORITHM

This encryption algorithm was developed in 1994 at the Massachusetts Institute of Technology (MIT) by Ronald Rivest, who called it, initially, “Ron’s Code”.

Because of its high performance because of its simplicity and speed not require much memory consumption of the sensor, the CR5 can be parameterized by word size (block to be encrypted), number of iterations and key size – which can customized to provide different levels of performance

and security, is considered as the most suitable encryption algorithm for WSNs.

THE RC6 ALGORITHM

The RC6 is a variant of the RC5 block cipher type (block cipher), being simple enough to be easily stored and can be implemented in a compact form both in software and hardware. In creating the RC6 its authors wanted to make it more secure against cryptanalysis and faster than RC5, having a difference against the schema key that is generated more leads than in RC5, these derivations are called subkeys. Its main difference with respect to its previous version is that the rotation of RC6 uses variable digits for places determined by the data rather than replacing tables in its encryption process.

THE DES ALGORITHM

Created by Horst Feistel and initially called LUCIFER, DES (Data Encryption Standard) encryption algorithm is the best known in the world. Long used by the U.S. government and most of its banks, this algorithm has undergone some modifications (National Bureau of Standards – NBS), when it received its current name (DES), and may also be called DEA (Data Encryption Algorithm), is widespread and requires a greater capacity for data storage due to tables used in queries, serving as a basis for comparison with other algorithms that require little storage space.

THE TEA ALGORITHM

The TEA – Tiny Encryption Algorithm, was designed and created in 1944 at the University of Cambridge by David Wheeler and Roger Needham in order to be used on platforms that do not have simple or require high processing power.

Its basic principle is one of the simplest encryption, which consists of a large number of iterations with XORs and the sums and subtractions XORs coding and decoding, which reduces its complexity and enhance its performance. Thus, it is estimated that the TEA is at least three times faster than DES.

This algorithm uses the sequence of operations on words instead of wasting energy with hardware operations on bytes or 4 bits. The security provided by it is related to the large number of iterations used and not its complexity.

THE SKIPJACK ALGORITHM

This algorithm was proposed, designed and sponsored by the U.S. government in the '80s, through its National Security Agency (NSA).

Released for use in 1998, SkipJack was created to be used in chips and require little storage space – a necessary condition for providing security in sensor networks, transforming an input block of 64 bits within an output block of 64-bits. The transformation is parameterized by a key of 80 bits and involves performing 32 iterations of a nonlinear function.

THE INSENS PROTOCOL

Assuming that an intruder node affects only its neighbors and not the network as a whole and the possibility of permanent existence of this type of us, INSENS (Intrusion-tolerant routing protocol for wireless sensor networks) is able to identify a node as malicious and not assign the routine tasks of the network.

Beyond the use of path redundancies for the data transmission, because if a route is impaired by the presence of an intruder node, alternative paths may be used, INSENS also limits the type of communication between the sensors being capable of preventing attacks denial of service (single or distributed), making only the base station, or sink node (sink) are authorized to flood the network, which is granted upon authentication so that no sensor node if they do go through. There are also packet filtering and routing by forwarding data to the base station or the sink, which provides the infra-structure WSN, increasing its robustness.

The insertion prevention and dissemination of false routes in the network is done through authentication of routing control information. This is done by the base station which in turn uses processes and propagates the routing tables for the sensors. Thus, the sensors retain the tables received and not inform them. This is somewhat favorable because it minimizes computation, communication, storage and bandwidth required by us, but is unfavorable to the sink, since it will need to increase these same characteristics.

From the moment that a node intruder is identified, all evidence of perceived intrusion on routes that rely on this node is associated with it. This association is performed in the third part of the algorithm. If a node intruder has been identified, the second parameter of the function "Detect intruder" gets the node identified as an intruder. If this parameter is checked, then the signs of intruders are associated with that node.

THE ARIADNE PROTOCOL

The Ariadne (Secure on-demand routing protocol for ad hoc networks) was created primarily for ad hoc networks, but can be used in WSNs. It is a secure protocol that works with on-demand routing preventing the forging and changes information in the routing tables, and we did not malicious employing internally symmetric keys for protection against DoS or DDoS attacks, but even so it is not efficient to attack multiple nodes contiguously.

In this protocol each node algorithm generates a chain of cryptographic keys. However, as mentioned earlier in this topic, memory constraints and energy

consumption of sensors, prevent keys are generated using very long chains which results in a greater expenditure of time and energy into your calculation.

THE SPINS PROTOCOL

The SPINS (*Security Protocols for Sensor Networks*) are a set of specific rules for providing security for WSNs consisting of two protocols: the µTESLA (*Micro Timed Efficient Stream Loss-tolerant Authentication Protocol*) and SNEP (*Sensor Network Encryption Protocol*) – these protocols ensure that data traveling over the network are intact, allowing the base station and the sensors communicate with each other through a secure routing. The first is responsible for the confidentiality and authentication in the network. The second addresses issues of authentication and update the communication between us and the messages broadcast with low overhead.

The SNEP is based on a counter shared between transmitter and receiver used as the initialization vector for the encryption algorithm used in encryption and decryption of data. In this case, encryption is performed by an RC5 algorithm lean due to limitations of the sensors, and therefore more suitable for the WSN. As both participants have the counter and increment after each block of encrypted data, the counter does not need to be sent to each transmission. Thus, to authenticate the transmitter and receiver and maintain data integrity code is used for message authentication.

The µTESLA uses a method for authenticating communication broadcast from symmetric keys for emulating asymmetry that no unauthorized receiver can obtain the key. For that she sends to peer with each node participating in the network parameters necessary for communication to be safe and for the algorithm to work. The authenticity of these parameters is guaranteed by a digital signature. There are proposals that attempt to optimize the process parameters for transmission other than point to point, for a network with many nodes that process would induce a large delay (Liu 2003).

DISTRIBUTION AND MANAGEMENT OF CRYPTOGRAPHIC KEYS

The distribution of cryptographic keys for a group of participants is vital in the formation of WSNs. Therefore, the cycle for the establishment of a key chain or key corresponds to: pre-distribution, transportation, and arbitration agreement.

The pre-key distribution is the distribution of keys by the nodes concerned before the start of communication. This requires that all network nodes are previously known, although not always required that all participating network.

In key transport, exchange keys entities to communicate. The simplest method for this phase is called Key Encryption Key (KEK), which is to encrypt the new key with the shared secret, and only those who possess this secret we can get a new key. In case there is a key for a group previously known, but there is a public key infrastructure, this new key can be exchanged by encrypting it with the public key of the node that will receive it. The arbitration keys use a central arbiter to create and distribute keys between participants, which makes it a specialization of the transport phase. In infrastructured systems, a central point is chosen to play the role of arbitrator. However, in sensor networks, the centralized arbiter function is prohibitive because of the absence of infrastructure and resource constraints.

The key agreement corresponds to the key exchange after the start of the network. Here security between us will be established through asymmetric keys, if they are available. This is necessary to achieve a secure communication within the network, although it is a very costly operation.

Key management is the process in which the cryptographic keys are generated, stored, protected, transferred, loaded, used and destroyed. This management is problematic in sensor networks because they are vulnerable to manipulation due to its limited memory and energy.

To meet the functional requirements and security of most sensor networks must take into account certain requirements such as:

- Do not work with a single key, because due to their lack of protection having a single key is the same as having no key; and
- Respect scalability criteria for adding new nodes can be made at any time without causing excessive increases in the level of processing per node, communication and administrative overhead on the network.

This can be considered two types of schemes for key distribution in sensor networks. A kind open to the entire network and a specific type of node. The open type network team throughout the network node with the same key equates compromise of a single key system with the involvement of the entire network. If there is information theft, the network is completely compromised. The specific type of node determines a single key combination for all who are communicating. There are other proposals for the secure distribution of keys that offer protection on small-scale attacks, increase network security by passing the key through multiple paths and ensure network security even with some nodes compromised.

PROVIDING SECURITY IN BASE STATIONS

In some cases WSNs, besides the drain can make use of an access point, also called a base station, to provide for communication between nodes.

Bibliography

- AKYILDIZ, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E. "A Survey on Sensor Networks". IEEE Communications Magazine, 2002.
- ARAÚJO, Rodrigo Cavalcanti de. "Um Estudo do Impacto do uso de Criptografia em Redes de Sensores sem Fio (RSSFs)". Universidade Federal de Pernambuco – UFPE, 2004.
- CAMPISTA, Miguel Elias M. & DUARTE, Otto Carlos Muniz B.. "Segurança em Redes de Sensores Sem Fio". Universidade Federal do Rio de Janeiro – GTA/UFRJ – 2003.
- CORDEIRO, C. M. & AGRAWAL, D. P.. "Wireless Sensor Netorks", In Mobile Ad hoc Networking, 20º SBRC, 2002.
- HEIDEMANN, J., et al.. "Buiding Efficient Wireless Sensor Networks". In 18Th ACM Symposium on Operating Systems Principles, 2001.
- LAW, Y., et al. "Assessing Security-Critical Energy-Eficcient Sensor Networks". 18th IFIP TC11 Int. Conf. on Information Security. Security and Privacy in the Age of Uncertainty (SEC), 2002.
- LIU, D. e Ning, P. "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks". 10th Annual Network and Distributed System Security Symposium – p. 263-276, 2003.
- LOUREIRO, Antonio A. F., et al.. "Redes de Sensores Sem Fio". Anais do XXII Congresso da SBC, Florianópolis – Santa Catarina, Julho de 2002.
- MARTI, S., et al. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". 6th Annual International Conference on Mobile Computing and Networking, 2000.
- MICHIARDI, M., e Molva, R. "CORE: A COllaborative REputation Mechanism to Enforce Node Cooperation in Móbile Ad Hoc Networks". In Communications and Multimedia Security Conference, 2002.
- MOREIRA, Mauricio Alves. "Fundamentos do Sensoriamento Remoto e Metodologias de Aplicação". Câmara Brasileira do Livro, São Paulo, 2001.
- PERRIG, A., et al. "SPINS: Security Protocols for Sensor Networks", In Seventh Annual ACM International Conference on Mobile Computing and Networks. Mobicom, 2001.

The applications of this type of network demonstrate the necessity of using base stations in some cases, especially in the sensing areas of difficult access. The standard for sensor networks aims to specify the protocol for medium access control layer used in MAC (Medium Access Control) and different physical layers as well as offer two methods of access control: the Distributed Coordination Function – based distributed control and Function Coordination Spot – based on consultation, where the base stations consult the nodes enabling transmission and reception of data, from time to time. During the proposal of its algorithms many authors assume that the base station is a safe spot. The justifications is that by having greater processing can have a more efficient algorithm that derives security. However, even if the base station is subject to attack. Campista (2003) proposes three methods that can increase the base stations security:

ESTABLISHMENT OF MULTIPLE PATHS TO MULTIPLE BASE STATIONS

The introduction of redundant base stations provides protection against attacks to a single one. This strategy can be considered for the route discovery phase and for the data transfer phase.

HIDE THE DESTINATION ADDRESS IN TRANSFERRED PACKETS

By obtaining a packet, an attacker has no way to identify the destination, which could be the base station address.

BASE STATION DISPLACEMENT IN THE NETWORK TOPOLOGY

With that, the base station would not be static, which would hinder its location.

CONCLUSIONS

Security mechanisms inevitably cause processing overhead applying a WSN, and possibly also cause communication overhead due to the increase in size of the messages. However, for some applications, this overhead is acceptable because your security needs. There is still a lot to evolve in this area not only about the safety aspects in particular, but in all matters related to sensor networks. The major limiting factor to this type of network is the amount of energy that is stored and processing capacity of nodes that limit their applications.

Few security algorithms were developed and implemented for these types of networks, allowing much space for research and development in this area. What has been observed is that one should seek a solution that can reconcile the limitations of energy with maximum possible security.

Author bio

Deivison Pinheiro Franco is Graduated in Data Processing. Specialist in Computer Networks, in Computer Networks Support and in Forensic Sciences (Emphasis in Forensic Computing). IT Analyst of Bank of Amazônia. Professor at various colleges and universities of disciplines like: Computer Forensics, Information Security, Computer Networks, Computer Architecture and Operating Systems. Computer Forensic Expert, IT Auditor and Pentester with the following certifications: CEH – Certified Ethical Hacker, CHFI – Certified Hacking Forensic Investigator, DSEH – Data Security Ethical Hacker, DSFE – Data Security Forensics Examiner, DSO – Data Security Officer and ISO/IEC 27002 Foundation.

eCore Techno Solutions

Let us Secure I.T.

HACKING TECHNOLOGIES
Assure Network Security Solutions

Our Services

eCore Techno Solutions

- Cyber Security Lab Consultancy.
- Cyber Crime Investigation & Cyber Law Consultancy.
- CERT(Computer Emergency Response Team).
- Secure Web Penetration Testing & Development.
- Privacy Consulting Practice.
- Medical Compliances.

Hacking Technologies

- Wireless Security Testing & Hardening.
- Network Audit & Risk Analysis.
- Cloud Security Consultancy.
- Network Architecture Assessment.

eCoreSuite

- Data Loss Prevention-Protect sensitive data from leaking.
- Web Filtering-Application,work both on and off network,with no hardware required.
- Employee Monitoring-Record and/or block all computer activities.
- Laptop Data Security-Recover Critical data from lost/stolen laptops.

sales@ecoretechnos.com

SCO 62-63 , 3rd Floor
Sector 17A, Opp Hotel Taj
Chandigarh 160017
INDIA
Office:(0172)461 0064
(0172)400 9111
Direct:+91 9023 63 1234

www.eCoreTechnoS.com
www.HackingTechnologies.com
www.LearnHackingSecurity.com

Featured In

THE TIMES OF INDIA
hindustantimes
The Tribune
The Indian EXPRESS
JOURNALISM OF COURAGE
आज समाज
अमर उजाला
जोश! सच का!
दैनिक जागरण
No. 1
Jagran
पंजाब केसरी
Dainik Bhaskar
दैनिक भास्कर
दिव्य हिमाचल

NETWORK INTRUSION

UNDERSTANDING THE THREAT ENVIRONMENT

by Damon Petralgia

The following article discusses the cyber threat landscape through a non-technical broad approach. It is not meant to be all encompassing and should be an introduction to network intrusion threats for some, whereas for others it should serve as a review. Understanding the current threat landscape and the methods used for network intrusion are crucial to investigators who work to solve criminal acts.

What you will learn:

This article is about the understanding the threat from an investigation standpoint, not from an information security standpoint.

What you should know:

How to hack so that you knew how to prevent it.

Just as any other crime, understanding the crime scene, criminal behavior, motivations, and modus operandi, network intrusion crimes are the same. The most common goal for the intrusion into a network is theft of data. This data may represent intellectual property, trade secrets, financial data including account or credit card numbers, or Identity information. These data types are clear in that they have particular value, however all data has value, even seemingly innocuous data. That must be understood as a universal truth. The data does not need to be super-secret intellectual property or the newest design of a nuclear propulsion system. It can be as simple as a publically available phone number. Obviously some data is more valuable than others, but all data has some intrinsic value. To the criminal or adversary even the seemly innocuous data can be used to leverage more valuable data or provide reconnaissance information. The data is most often the target. In the discussion of network intrusion and online fraud the aggressor or "bad actor" is typically identified as the hacker. Even though this is a slight misnomer as the bad actors will often employ non-technical means to acquire their targets, this article will identify these persons or groups as the hackers. Below is a condensed and simplified matrix of hacker type, motivation and targets. Each cell of the table may have several subsets, however for the purposes of this article this simplified example will be used (Table 1). The target will typically define which hacker type who will be most interested; however the vulnerabilities within the target will define the method of intrusion in most cases. Foreign intelligence and organized criminal enter-

Table 1. *Condensed and simplified matrix of hacker type, motivation and targets*

HACKER TYPE	MOTIVATION / GOALS	PRIMARY TARGET(S)
Foreign Intelligence / Nation-State	Military / Political Advantage	Critical Infrastructure & Military Targets
Terrorist Group	Intended to disrupt, cause chaos, induce fear and uncertainty in a civilian or non-combatant population	Critical infrastructure & corporations
Organized Crime	Profit / organizational power / increased illegal market share	Financial industry and individuals (i.e. ID Theft)
Profit Hacker	Monetary profit	Any
Hacktivist	Activism	Chosen based on belief or rhetoric of group at the time, typically big business, law enforcement or government
Coder / programmer hacker	Profit, create code for specific action (e.g. botnet, worm, virus, Trojan)	Targets specific vulnerabilities to exploit rather than industry – Caveat: each industry has its own subset of inherent vulnerabilities
Recreational hacker	Bragging rights, ego driven	Any
Script Kiddie	Bragging right, acceptance by community	Any

prises are increasingly active and gaining in sophistication in attack methods faster than any other group. As a general rule the Advanced Persistent Threats (APT) (e.g. Stuxnet) are the product of military, foreign intelligence or state sponsorship. The APT has extreme sophistication, however as a general rule, it must contact a Command and Control (C&C) server or staging point outside of the network it is attacking. Of course there are exceptions to this as detailed by the Shamoon attack which destroyed data rather than exfiltrate (steal) data. Additionally some APTs may implement the C&C within the network it is attacking. The APT attacks are extremely difficult to detect. It will enter the network is typically unique ways such as USB device or trusted path. Most times it will not be noticed when entering. The key to detection is the high probability it will contact a C&C outside the network. Therefore, it is careful logging and monitoring of outbound traffic that is essential to discovering the APT attack or infection. To increase the chance of detection of the APT a known baseline of services and traffic should be established. Deviations and anomalies from this baseline should be investigated immediately and thoroughly.Botnets also use the C&C method, but are typically the work of organized crime as opposed to military or foreign intelligence. A botnet is a collection of connected computers controlled by a malicious party. Each compromised computer is known as a "bot". The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC (Internet Relay Chat), HTTP (Hypertext Transfer Protocol) or peer-to-peer (P2P) for example.

The bots will typically report details of the compromised computer to the C&C. The C&C in return will issue updates and other code to further infiltrate the computer, thwart anti-virus and other security measures and steal specific data such as form-data including account numbers and passwords. Again, it is monitoring the outbound traffic which will help to detect this type of attack. Continually at the top of the list of vulnerabilities and attack methods are SQL Injection and Cross-Site Scripting (XSS). The SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of attack, in which SQL commands are injected into the input, or form field within a webpage in order to effect the execution of predefined SQL commands. Cross-Site Scripting (XSS) attacks are another type of injection attack, where malicious script or code are injected into the otherwise trusted web sites. The bad actor or attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Generally the browser has no way to know that the script or code should not be trusted, and will execute the script. The malicious script can be used to ultimately access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. Typically these two vulnerabilities are the result of the underlying coding and programing rather than unpatched operating systems. There are no simple answers or preventions for network intrusions. As preventive and detective measures mature, so do the attack methods. It is the proverbial "cat and mouse" game. Understanding the threat environment is only the beginning, however understanding your adversary may be the key to understanding if and when you are being attacked. Understanding the adversary will allow you to view your network in the way the adversary does enabling you to identify anomalies and weaknesses. Understanding the threat environment is key in the investigation of the attack.

Author bio

Damon Petraglia is the director of a demanding forensic practice and core to the leadership of a highly visible security program. He performs frensic examination and investigation, vulnerability analysis and risk / threat assess-ment, social engineering testing, security architecture review, incident response, and policy and procedure review and development.

ARE ALL SECURE FTP SERVERS SECURE?

by Neil Maher

When discussing Secure FTP Servers, one must first define what is meant by the term. For the purposes of this article, we are defining Secure FTP to mean FTP over SSH, commonly known as SFTP. SSH is used worldwide as an encryption method not only for secure access into a remote Unix or Linux server, but also as a transport protocol for file transfer.

What you will learn:

Help you decide whether your SFTP server is secure by name, or secure by nature.

Some of the differences between the various SSH versions from a security perspective.

Scenarios where a better configured server will provide better security options.

What you should know:

Basic knowledge of SSH key pairs during encryption and authentication of an SFTP session.

So if a Secure FTP Server provides the functionality to connect and transfer files using SSH, then it is secure, right? Wrong.

HANDD Business solutions comes across SSH servers of every conceivable type, from full enterprise *Managed File Transfer* (MFT) solutions like GlobalSCAPE EFT Server or Ipswitch MOVEit DMZ, to all the various types of remote third party host that our customers might be required to connect into in order to transfer files with their trading partners. A business will have no control over what server type their trading partner will use, which means that data is exposed to the risk levels of the host server.

HOW SFTP WORKS

A user initiates a connection to an SFTP server using client software. Examples of client FTP software that support SFTP include CuteFTP, WS_FTP, Filezilla, CoreFTP. Similar to the way that a browser will connect to a website using a URL over HTTP(s) on port 443, the user enters the URL or IP address of the remote server and connects on port 22 (or whichever non-standard port the administrator has configured the server to listen on).

The Server owner generates a private key using algorithms derived from the SSH library relevant to their software version. These algorithms are listed further down this article.

At the same time, a matching public key is generated for client side use. When an SFTP session is requested by the client, the server responds by presenting its public key to the client to identify itself. If the client (the user) accepts the public key, the public

key is then stored client side. The server then proceeds to check the private key against the public key, a process that is known as the Diffie-Hellman handshake. Providing the server is satisfied that the key pair corresponds, it will then use the algorithms in the private key to encrypt the remainder of the session.

Client side, the public key is used to decrypt the session, where algorithms in the public key are deciphered using the client SSH library. The user will then authenticate by whatever means the server administrator requires them to do. Authentication may be anonymous, by username and password, or by a separate SSH key pair generated by the client. The latter authentication method provides a double layer of security, where the client is also encrypting the traffic using its own private key, the server decrypting with the corresponding public key. Public key authentication can be used for system to system file transfer, as no password interaction (or storage of passwords) is required.

All commands passed between server and client, including data, is encrypted during the SFTP session.

VERSIONS

There are several versions of SSH – SSH 1.0, 2.0 and openSSH. Some older servers will use older versions of SSH and older SSH libraries. These libraries will use older algorithms to encrypt traffic, and potentially the keypair used to encrypt the traffic has been in existence for a long time. Let's examine further SSH version one has had a number of vulnerabilities discovered since its inception in 1998, hence the birth of SSH2. Notable vulnerabilities of 1x versions are listed here:

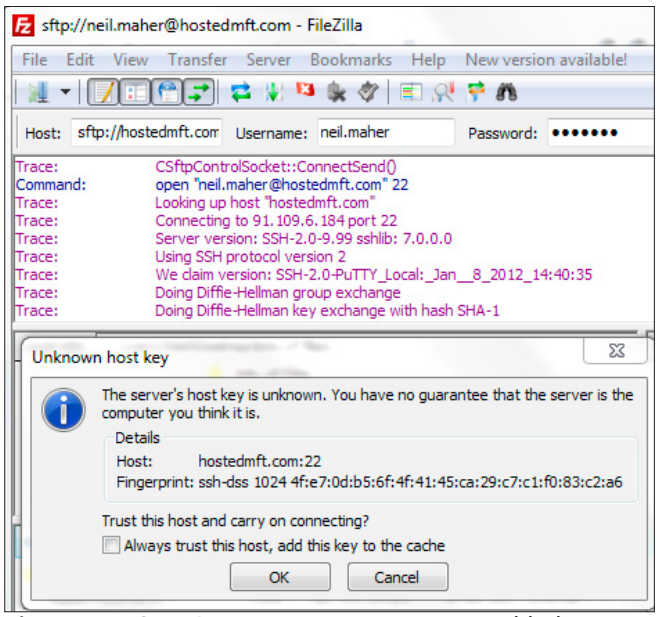


Figure 1. *MOVEitDMZ server is presenting its public key to Filezilla client and performing the Diffie-Hellman handshake*

- Insertion Attack: *http://www.coresecurity.com/content/ssh-insertion-attack*
- Integer overflow vulnerability: *http://www.kb.cert.org/vuls/id/945216*
- Weak CRC allows last block of IDEA-encrypted SSH packet to be changed without notice *http://www.kb.cert.org/vuls/id/315308*
- SSH-1 allows client authentication to be forwarded by a malicious server to another server *http://www.kb.cert.org/vuls/id/684820*

Most servers and clients these days support SSH2, which in itself is a good thing, because SSH2 is not backwards compatible with SSH1. Modern OpenSSH servers will be able to support versions 1 and 2. For additional security, a prospective server owner may consider whether backwards compatibility can be disabled, or whether an SSH2 server might be the better option.

A well configured SSH2 server or client will run in a secure mode that enforces SSH2 connections only – a common name for this mode is FIPS mode, after the FIPS 140-2 standard for encryption. FIPS 140-2 is a US Federal Government standard, and while standards may vary from country to country, in practice organizations elsewhere in the world accept this standard. A server or client running in FIPS mode will terminate connections where SSH1 is still in use.

As discussed above, the SSH libraries contain algorithms used to create the encryption key pair – and some of these algorithms themselves are vulnerable. Again, a server or client running in FIPS mode will disable certain algorithms, dropping connections where the older ciphers are in use.

Finally, the server key pair that is being used to encrypt the traffic could have been around for some time. Is that key pair to be trusted? After all, it's outside administrative control. In a corporate environment, potentially how many hands could a key pair have passed through in 5 years? It's unlikely that an ex-employee who had access is now using that key pair to decrypt traffic maliciously, but it's not impossible. Some MFT Servers will notify when a public key in your key store has reached a certain age – where the practice of generating the key pair server-side and handing out the private key to the clients (not the way it's supposed to be done, but we see it happen a lot in practice) becomes vulnerable.

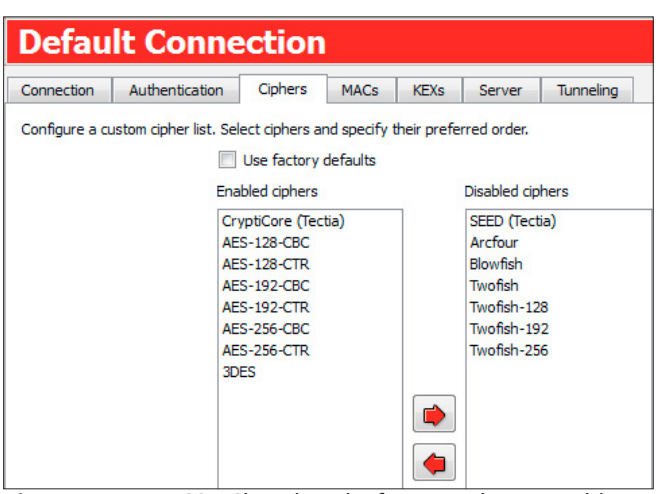


Figure 2. *Tectia SSH Client has the functionality to enable or disable certain algorithms used to generate the SSH Session*

SSH Tectia – the inventors of SSH – uniquely provide a universal key manager to manage SSH keys. The SSH key manager performs a search within the network to discover SSH Key pairs of any version. Administrators are then easily able to apply policies on the keys such as expiry, format etc. Working with an MFT solution, the key manager will ensure that keys are up to date and accessible only to the required persons or applications. More information on SSH key management can be found here: *http://www.handd.co.uk/solutions/SSH-Key-Management/*.

WHY PEOPLE LIKE SFTP

SSH for file transfer is favoured by millions because of its simplicity – it is easier to set up a keypair than to get an SSL certificate generated and signed. The SFTP protocol guarantees integrity, no need to perform CRC checks, it is inherent. For FTP over SSL (FTPS), additional commands have to be passed in order to check file integrity, not all clients and servers support this functionality.

For server owners, there are less firewall ports to open than for FTPS – it is a far easier protocol to incorporate into the network. SSH is easy to administer through a good MFT server, and this article will finish with some steps to ensure security is maintained rigidly.

- SSH1 is obsolete – ensure your technology is using SSH2
- If using openSSH, ensure you are reading the version banner correctly when connecting to a remote host. Remember, openSSH is backwards compatible with SSH1
- Consider disabling or removing entirely older algorithms/encryption ciphers
- If your server is FIPS enabled, use it. If your server is not FIPS enabled, consider changing.
- Renew server keys from time to time – and expect your trading partners to do so too. The risk is multiplied the longer you leave it and the more partners you have. You can't control staff turnover, but you can make keys redundant to a malicious individual.

Author bio

Neil Maher is the Operations Director for HANDD Business Solutions, he has deployed in excess of 500 secure file transfer solutions.

Nevada PI Lic#1948 Expert Data Forensics is a d/b/a ICS of Nevada LLC.
2675 S. Jones St. Suite 207A, Las Vegas NV 89146
PO Box 35006 Las Vegas, NV 89133
T: 702-435-8885 O: 888-355-3888 F: 702-453-8887
[Lic#1498] [Tax ID: 20-4239533]

ExpertDataForensics.com

EXPERT DATA FORENSICS
INVESTIGATORS OF ELECTRONIC EVIDENCE

Digital Forensic & Investigative Services

- First response
- Extraction & preservation of digital contents
- Electronic investigations (Lic#1498)
- Chain of custody
- Expert witness for court/depositions
- Digital data & electronic analysis
- Seizure of digital evidence for forensic purposes
- Investigation of digital evidence
- Recovery of deleted digital content
- Consultation & preventative strategy
- Corporate systems & security analysis
- Data analysis & recovery
- Cell phones & mobile devices data extraction, preservation & analysis
- Retrieve & analyse text messages, emails, images etc.
- Corporate digital crime reconstruction
- Web surfing pattern analysis
- Online hacking, Email investigation
- Authentication of digital data (certificate)
- Password recovery
- Cyber hacking, stalking and activity patterns
- Electronic fraud detection
- Digital corporate sabotage
- Corporate/private infringement
- Employee misuse

Forensic Data Recovery Services

- We specialize in forensic data recovery from computers, cell phones, PDA's
- Data recovery of hard disk
- Data recovery of deleted files
- Digital imaging from electronic device
- Password recovery
- Digital recovery of deleted data contents (emails, txt messages, web chats)

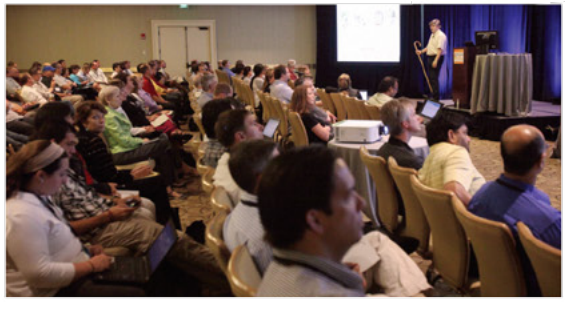
SPTechCon
The SharePoint Technology Conference

March 3-6, 2013 → San Francisco

Get the scoop on SharePoint 2013!

Register Early and SAVE!

The Best SharePoint Training!



Choose from over 90 Classes & Workshops!

Check out these NEW! classes, taught by the industry's best experts!

- How to Install SharePoint 2013 Without Screwing It Up — Todd Klindt and Shane Young
- What IS SharePoint Development? — Mark Rackley
- SharePoint Performance: Best Practices from the Field — Jason Himmelstein
- Creating a Great User Experience in SharePoint — Marc Anderson
- Ten Best SharePoint Features You've Never Used — Christian Buckley
- Understanding and Implementing Governance for SharePoint 2010 — Bill English
- Building Apps for SharePoint 2013 — Andrew Connell
- SharePoint Solutions with SPServices — Marc Anderson
- Lists: Used, Abused and Underappreciated — Wes Preston
- Planning and Configuring Extranets in SharePoint 2010 — Geoff Varosky
- Creating Simple Dashboards Using Out-of-the-Box Web Parts — Jennifer Mason
- Integrating SharePoint 2010 and Visual Studio Lightswitch — Rob Windsor
- Solving Enterprise Search Challenges with SharePoint 2010 — Matthew McDermott
- Getting Stuff Done! Managing Tasks with SharePoint Designer Workflows — Chris Beckett
- SharePoint 2013 Upgrade Planning for the End User: What You Need to Know — Richard Harbridge
- Ten Non-SharePoint Technical Issues That Can Doom Your Implementation — Robert Bogue
- SharePoint MoneyBall: The Art of Winning the SharePoint Metrics Game — Susan Hanley
- Intro to Branding SharePoint 2010 in the Farm and Online — Randy Drisgill and John Ross
- How to Best Develop Requirements for SharePoint Projects — Dux Raymond Sy

Lots more online!

A BZ Media Event

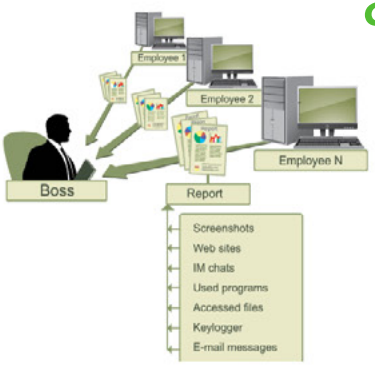
Central Contractor Registration

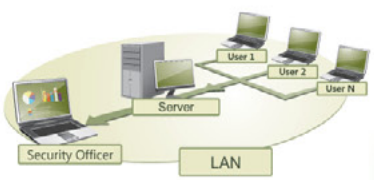
Follow us: twitter.com/SPTechCon

www.sptechcon.com

STAFFCOP

PC monitoring, Corporate Security and Data Loss Prevention Software





StaffCop Standard allows you to monitor all activities on company computers and prevent the unauthorized distribution of sensitive corporate information.

StaffCop will help you:

To locate possible data loss channels and prevent loss
To gain insight into how your employees spend their work time
To increase company and departmentals efficiency

You need StaffCop to:

Gather work time efficiency statistics
Easily control your employees in real-time mode
Improve discipline and motivation of your employees

Who needs StaffCop:

CEO/CTO
Corporate Security Manager
HR Manager
System Administrator

Main Features of StaffCop:

Screenshot recording
Application monitoring
E-mail monitoring
Web site monitoring
Chats/IM activity recording
USB device monitoring
Clipboard monitoring
Social Networks Monitoring
Search Term Tracking
File and Folder tracking
Keystroke recording
System Event Monitoring
Whitelists and Blacklists
PC activities reporting
Stealth installation/monitoring
Strong security
Alert notifications
Remote Install / Uninstall

More Information, Demo Versions, Videos and Technical Guides -

www.STAFFCOP.com

Phone: +1-707 -7098405
Skype: staffcop.com
Email: sales@staffcop.com, paul@atompark.com

Microsoft CERTIFIED Partner