

EXHIBIT 1

From: Manuel Albers [manuel.albers@nxp.com]
Sent: Wednesday, July 30, 2008 5:53 PM
To: shenderson@mbta.com
Cc: Fluegge.Wolfgang@Scheidt-Bachmann.de; bhoene@scheidt-bachmann-usa.com
Subject: Boston Charlie Card Hack Demo subject at speach at upcoming Defcon conference in August

Scott,

FYI: Today we learned about a conference (Defcon) at which a team of MIT students intends to demo a Charlie Card Hack. Of special concern is the announced intent to release open source tools required to perform the attacks:

<http://defcon.org/html/defcon-16/dc-16-speakers.html#Anderson>

The Anatomy of a Subway Hack:

Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson

Student, MIT

RJ Ryan

Student, MIT

Alessandro Chiesa

Student, MIT

Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of

hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese, Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

Please let me know if we can support you in any way.

Best regards,
-Manuel Albers

Director, Regional Marketing Americas & BU A&I - Sales & Marketing - Identification & NXP Semiconductors
(P) +1.802.497.0888 & (C) +1.401.359.4999 & (F) +1 866.333.2976 & <http://www.NXP.com> & (founded by Philips)

The information contained in this message is confidential and may be legally privileged. The message is intended solely for the addressee(s). If you are not the intended recipient, you are hereby notified that any use, dissemination, or reproduction is strictly prohibited and may be unlawful. If you are not the intended recipient, please contact the sender by return e-mail and destroy all copies of the original message.

EXHIBIT 2



COMMUNITY

SCENE

RESOURCES

ARCHIVES

BLOG



OFFICIAL DEFCON FAQ v0.95

[NOTE: Before this
FAQ goes production
1.0 it will be split into
two, one for general
DEF CON questions,
and another for the

What is DEFCON?

DEFCON is one of the oldest continuous running hacker conventions around, and also one of the largest.

How did DEFCON start?

Originally started in 1993, it was meant to be a party for members of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U.S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the

member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and

remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places.

There as a

SummerCon in the summer, a HoHoCon in the winter, a

PumpCon during

Halloween, etc. I

didn't want any

association with a time

of year. If you are a

Phreak, or just use

your phone a lot you'll

notes "DEF" is #3 on

the phone. If you are

into military lingo

DEFCON is short for

"Defense Condition."

Now being a fan of the movie War Games I took note that the main character, David Lightman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEFCON is all about.

DEFCON Press:
through the prism of the media
DEFCON Pics: visual evidence, thousands of pictures, some NSFW
DEFCON Groups:

Local groups that meet
DEFCON Media
archives: Speeches
from DC 1 to the
present, captured
Google: always a good
research starting point
Just remember,
DEFCON is what you
make of it.

When and where is
DEFCON?

DEFCON is generally
in the last week of July
or first week of August
in Las Vegas. DEFCON
16 will be held August
8-10 at the Riviera
Hotel & Casino in Las
Vegas. Many people
arrive a day early, and
many stay a day later.

Isn't there a
DEFCON FAQ
already?

Yes, an unofficial one.
It's quite humorous,
somewhat outdated,
sometimes
informative, and
DEFCON takes no
responsibility for its
content. It can be
found at <http://defcon.stotan.org/faq/>

What are the rules
of DEFCON?

Physical violence is
prohibited. We don't
support illegal drug
use. Minors should be
accompanied by their
parent(s) or guardian

doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEFCON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEFCON. Talking about how you are

going to bomb the
RNC convention in
front of an FBI agent is
a Career Limiting
Move!

Is DEFCON
canceled?

No.

What is there to do
at DEFCON?

DEFCON is a unique
experience for each
con-goer. If you google
around you'll find
dozens of write-ups
that will give you an
idea of what people
have experienced at
DEFCON. Trust write-
ups more than media

articles about the con.
Some people play
capture the flag 24x7,
while many people
never touch a
computer at DEFCON.
Some people see every
speech they can, while
others miss all
speeches. Other
activities include
coffee wars, WI-FI
shoot outs, robot
contests, TCP/IP
contests, movie
marathons, scavenger
hunts, sleep
deprivation, lock
picking, warez trading,
drunken parties, spot
the fed contest, charity
dunk tanks, the Black
and White Ball.
Because DEFCON is
what the attendees
make of it, there are

more events than even
we are aware of. Half
the fun is learning
what happened at
DEFCON after the fact!

I'm not a hacker,
should I go to
DEFCON?

Many people have
different definitions of
what is a 'hacker'. I
would recommend
looking at previous
years speeches, and
write-ups from past
attendees - this should
give you a good idea if
DEFCON is for you.
This hacker FAQ
might give you some
insight into the matter
as well. If you do not
have any technical

interests, DEFCON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEFCON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Ssshhh. Don't tell anyone.

What are Goons?

They are the staff at DEFCON. They have many roles including security, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address. Security Goons generally wear red shirt, Speaker and Content Control wear Blue.

How can I help out

or become a Goon?

The staff at DEFCON has grown organically.

All positions have some degree of trust associated with them, so typically new goons are 'inducted' by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work.

Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they

actually do (hint: you may want to enjoy being at DEFCON, not working full-time at it). Last year the network group got a new Goon when a networking engineer was need, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEFCON is not a spectator sport! Before

the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirt and posters. You can build a bot for Robot Wars, practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEFCON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually

every official event at DEFCON started out as an unofficial event.

After DEFCON you can help support the conference by posting links to your DEFCON photographs at defconpics.org, writing a review of your experiences and posting it online (Don't forget to mailing us (press [at] DEFCON dot org) a copy) or just sending us feedback so we can improve in the future. If you ran a contest write it up and we'll link to it. If you have the results of a contest or a new event we'd love to hear about it.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEFCON were conceived by the attendees. The DEFCON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEFCON (space, namely) you generally don't have to ask anyone's permission. Most events are unofficial until they've been going on for a couple of years. Please

let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEFCON dot org] to keep us in the loop.

How can I speak at DEFCON?

You can submit a response to our CFP (call for papers). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers opens March 1, 2008.

I'm press, how do I sign up, why can't I

get in for free (I'm just doing my job)?

Please email [press\[at\]defcon\[dot\]org](mailto:press[at]defcon[dot]org) if you wish press credentials.

Lots of people come to DEFCON and are doing their job;

security professionals, federal agents, and the press. It wouldn't be

fair to DEFCON attendees if we

exempted one group from paying. If you are a major network and

plan on doing a two minute piece showing all the people with

blue hair, you probably shouldn't bother applying for a

press pass - you won't get one. If you are a security writer or from

a real publication
please submit, and
someone will respond
with an answer.

I want to sell stuff,
how do I do this?

If you want a space in
our vendor area, you
need to apply. Because
of limited space and
our attempt to have a
diversity of vendors,
you may not be able to
get a booth. It is wise
to think of staffing
issues - if you are one
person do you want to
spend your entire time
behind a vendors
booth?

What are the

different price rates?

Everyone pays the same: The government, the media, the 'well known hackers', the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

How much is admission DEFCON, and do you take credit cards?

DEFCON costs \$120 USD cash. Do we take credit cards? Are you JOKING? No, we only

accept cash - no checks, no money orders, no travelers checks. We don't want to be a target of any State or Federal fishing expeditions.

Can I pre-register for DEFCON?

No. We used to do this a long time ago, but found that managing the registration list, and preventing one 'Dr. Evil' from impersonating another 'Dr. Evil' too much of a hassle. Seeing how we would only take case in the first place, and things becomes time consuming and easy to abuse. Cash at

the door works every time.

DEFCON is too expensive, how can I afford it?

DEFCON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. Many people have made an art and science out of coming to DEFCON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)

Lodging: Share rooms - some people have up

to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)

Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)

Booze: You don't need to drink. Brew your own and bring it. (It's been done.)

Entrance: \$120 can be saved, mow some

lawns. Try to go to another 3 day event for cheaper than this that offers so much.

We have increased the fees slowly over the years, but also the amount and quality of events have increased.

With a new hotel for DC-14 some costs have increased, and we have to pass those along.

Inevitably people will try to do some math and pretend that DT gets rich each DEFCON - they seem to lack the ability to subtract.

How many people typically attend DEFCON?

There have been roughly 3,000-5,000 attendees in the last few years of DEFCON.

Is there a network at DEFCON?

Yes. It would be fair to describe the network as 'hostile'. It has been described as 'the worlds most hostile network', but such descriptions are just attempts at flattery. It is recommended that if you want to connect to the DEFCON network pretend that you are sharing out your entire hard drive to 5,000 hackers. You may want to bring a 'clean' computer that you

don't mind being infected/hacked/etc. It is considered very poor form to attempt to DoS the network; while the DEFCON staff may not do anything about such attempts it is reasonable to assume that 'peer justice' may be meted out. If you're unhappy about the possible risks associated with connecting to DEFCON networks there are a couple of options: refrain from computer use for a few days or connect using another network elsewhere in Vegas (another hotel or something).

At DEFCON 13 we rolled out a new WiFi network using Aruba gear. If you were inside the coverage area of the DEFCON access points the new network switch would do things like detect rogue APs and attack them, reset or FIN network connections it didn't like, and prevent one user from being able to scan another user. Nothing is foolproof, but it brought a new level of sanity and stability to the network. We plan to do this again for DC-14. Look in the printed program for the correct MAC and IP address of the gateway router.

What is the age limit?

People have brought children to DEFCON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an 'adult' atmosphere (language, booze, et cetera). If you've never been to DEFCON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have consistently cooperated with parents and/or private investigators who are

looking for children that 'ran away from home' to go to DEFCON. You will have to be 18 to reserve a room.

That said I think NullTone ties with the youngest person to attend DEFCON at 13 year old. Years later he is in college and set up the DEFCON Forums. See, DEFCON won't destroy you completely.

What is a DEFCON "Black Badge"?

The Black Badge is the highest award DEFCON gives to contest winners of

winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEFCON for life—potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of

mail continually.
Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

What about having a DEFCON in XYZ city/country?

We've been in the city of sin since DC 1. We are not looking to franchise. It's always fun to see people organize conventions in their local areas, and if you do, we'll include you in our calendar, but not with the name "DEFCON".

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEFCON. This is discussed in quite some depth on the unofficial DC FAQ, as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the Black and White Ball, an annual Saturday night event where everyone shows off nifty attire.

Will the Riviera allow free parking?

Yes. You will be able to park for free

regardless if you have a room at the Riviera.

I looked at a map of the convention space and noticed there are sky boxes. Can I reserve one?

No. If you have any great ideas for what a sky box should be used for, feel free to send us suggestions, but individual attendees will not be able to reserve sky boxes.

How much do rooms at the Riviera cost, and how do I reserve a room?

The Riviera has reservations online or over the phone (800) 634-6753. Room Rates are "flat-fee" based on quantity of occupants. \$98 + tax with 1 or 2 people, \$118 + tax with 3 or 4 people. Priority for room assignment when you say you're with DEFCON is "Deluxe" when making reservations on the phone.

How much is internet access in the rooms of the Riviera?
\$9.00 for 24 hours.
Free (and more dangerous) internet access is available for

free in the convention area.

Will the Riviera broadcast the speeches on their cable system?

No. There will be two DEFCON channels that will provide 'extra' content (short clips, hacker related videos, etc.). It is our intention that everyone who wishes to attend a speech will be able to - this was a primary motivation for moving hotels.

Will we have DEFCON branded poker chips?

You will have to attend DEFCON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. The hotel is very cooperative in attempting to centralize the DEFCON attendees, for their convenience and ours, but there will be non-DEFCON attendees in hotel rooms next to us.

This FAQ didn't answer my

unclear, how can I
get further
information?

There is a forum
discussion thread in
which you can ask
follow up questions.

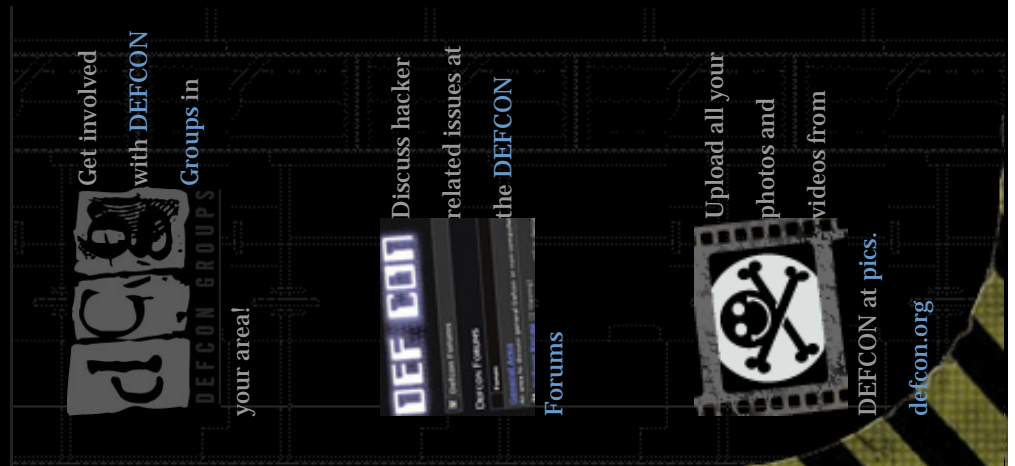


EXHIBIT 3



- [Schedule](#)
- [Speakers](#)
- [Venue](#)
- [Events/Contests](#)
- [Be Prepared](#)
- [FAQ](#)
- [Contact](#)

Schedule

Skyboxes

Place skybox requests with [grifter\[at\]defcon\[dot\]org](mailto:grifter@defcon.org)

206	© 1992-2008 DEF CON Communications, Inc. Main DEFCON Site RSS	210	211/212
	207	208	209




Friday	"Spiders are Fun" party	Hacker pimps		Hardware Hacking Village	Wireless Village	Lockpick Village
Saturday	303 (Skytalks)	Ninja Networks	i-hacked			
Sunday	HAM Radio Testing	Available	Available			










Pre-Con: Thursday, August 7

12:00 - 22:00	Registration - \$120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store Vendor Area Setup: 11:00 - 18:00
18:00 - ???	The Unofficial Defcon 16 Toxic BBQ will be held for its fourth consecutive year. Details of the TBBQ's location can be found at http://www.toxicbbq.com . Sign on to the Defcon Forums and help plan this year's event.
21:00 - ???	theSummit fundraiser for EFF/THF at the Top of the Riv

















Day One: Friday, August 8





08:00 - 22:00	Registration - \$120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store. Vendor Area Hours: 10:00 - 19:00
---------------	--

	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Chillout 101/102
10:00 - 10:50	<p>Welcome by DT & Making the DEFCON 16 Badge with Joe "Kingpin" Grand</p>	<p>Weasel Compliance: The Enterprise Vulnerability Roadmap.</p>	<p>Chema Alonso & Jose Parada Time-Based Blind SQL Injections Using Heavy Queries: A Practical Approach to MS SQL Server, MS Access, Oracle, MySQL Databases and Marathon Tool.</p> 	<p>Brenno J.S.A de Winter Hacking Data Retention: Small Sister your Digital Privacy Self Defense.</p> 	<p>Ben Feinstein The Wide World of WAFs.</p> 	<p>oCTF till 22:00</p> <p>Coffee Wars till 12:00</p> <p>Race to Zero till 18:00</p> <p>Buzzword Survivor till 22:00 Sat</p> <p>DEFCONBots practice during Contest Area hours</p> <p>GH3 Signup till 12:00</p> <p>Badge Hacking Contest till 14:00 Sunday</p> <p>Mystery Challenge till 14:00 Sunday</p>		
11:00	Schuyler	Michael	Ian Angell	Joe Cicero	Panel:	GH3 Free	Warballooning	





11:20	How to make friends & influence Lock Manufacturers.   	Deciphering Captcha 	Security: A Risky Business	E.S.P.	the Name of Science.	The Phreaking Challenge till 17:00	Outdoor Area till 14:00
11:30-11:50		Kolaris Whitespace: A Different Approach to JavaScript Obfuscation.  		Clinton Wong Web Privacy & Flash Local Shared Objects.		Mystery Challenge Wildcard Slot Competition	
12:00 - 12:50		Mike Spindel Captchas: Are they really Hopeless? (Yes!) 	Mark Bristow ModScan: A SCADA MODBUS Network Scanner  	Roger Dingledine Security and anonymity vulnerabilities in Tor: past, present, and future		Scavenger Hunt till 17:00 GH3 Med. Heat 1 Beverage Cooling Contraption Contest	Chillout Area, DJs QueerCon Mixer @ 16:00
13:00 - 13:20	Marc Weber Tobias Open in 30 Seconds	Tom "Strace" Stracener & Robert	Robert Ricks New Tool for SQL Injection with DNS	Jim O'Leary Every Breath you Take.	Greg Conti Could Googling Take Down	GH3 Med. Heat 2 Mystery	






	<p>Cracking One of the Most Secure Locks in America.</p>	<p>"RSnake" Hansen Xploiting Google Gadgets: Gmalware & Beyond</p>	<p>Exfiltration.</p>	<p>a President, Prime Minister, or an Average Citizen?</p>	<p>Challenge begins at 1:05:70 till 14:00 Sunday</p>	
<p>13:30 - 13:50</p>			<p>Morgan Marquis-Boire Fear, Uncertainty and the Digital Armageddon.</p>			
<p>14:00 - 14:50</p>		<p>Nathan Hamiel & Shawn Moyer Satan is on my friends list: Attacking Social Networks.</p>	<p>Kurt Grutzmacher Nail the Coffin Shut,NTLM is Dead.</p>	<p>Magnus Bråding Generic, Decentralized, Unstoppable Anonymity: The Phantom Protocol.</p>	<p>Jan Newger Anti-RE Techniques in DRM Code</p>	<p>GH3 Med. Heat 3</p> <p>Mobile Hacker Spaces Demo in outdoor area till 16:00</p>
<p>15:00 - 15:50</p>	<p>Eric Schmiedl Advanced Physical Attacks: Going Beyond Social Engineering and Dumpster Diving Or, Techniques of Industrial</p>	<p>Wendel Guglielmetti Henrique Playing with Web Application Firewalls.</p>	<p>Kevin Figueroa, Marco Figueroa, & Anthony L. Williams VLANs Layer 2 Attacks: Their</p>		<p>Alex Stamos, David Thiel & Justine Osborne Living in the RIA.</p>	





	Espionage		and their Kryptonite. 				
16:00 - 16:50	David Maynor & Robert Graham Bringing Sexy Back: Breaking in with Style.   	Fyodor NMAP- Scanning the Internet.  	James Shewmaker StegoFS  	Blake Self & Durandal Free Anonymous Internet Using Modified Cable Modems. 	Travis Goodspeed Journey to the center of the HP28.		
17:00 - 17:50	Matt Yoder Death Envelope: Medieval Solution to a 21st Century Problem.	Ben Feinstein Snort Plug-in Development: Teaching an Old Pig New Tricks.  	D.J. Capelis Building a Real Session Layer.  	Vic Vandal Keeping Secret Secrets Secret & Sharing Secret Secrets Secretly. 	Panel: Meet the Feds		
18:00 - 18:50	Fabian "Fabs" Yamaguchi & FX New Ideas for	Guy Martin Sniffing Cable Modems. 	John Fitzpatrick Virtually Hacking. 	Eric Smith & Dr. Shana Dardan. Medical Identity Theft.			Closed for Ball Setup






	Port Scanning Improved. 							
19:00 - 19:20				Nathan Evans De-TOR-iorate Anonymity				
19:30 - 19:50								
20:00 - 20:50				TCP/IP Drinking Game		Forum Meet @ 20:30 in Q&A 5 (room 103) till 22:30	Black Ball till 3:00 Sat.	
21:00 - 21:50	Movie Night With DT: Premiere of "Hackers Are People Too"			Hacker Jeopardy				
22:00 - 22:50	Movie Night With DT: Appleseed: Ex Machina					Club QueerCon in Skybox 211 till ???		
23:00 -								


Day Two: Saturday, August 9

08:00 - 22:00	Registration - \$120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the Vendor Area at the J!nx Hackwear Booth Vendor Area Hours: 10:00 - 19:00							
	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Chillout 101/102
10:00 - 10:50	David Weston & Tiller Beauchamp RE:Trace: The Reverse Engineer's Unexpected Swiss Army Knife. 	Nelson Murilo & Luiz "efffn" Eduardo Beholder: New WiFi Monitor Tool. 	Don Blumenthal Working With Law Enforcement.	Joe "kingpin" Grand & Zoz BSODomizer. 	G.Mark Hardy A Hacker Looks at 50.	oCTF till 22:00 Øwn the Box in oCTF Area during oCTF Hours	Skytalks in Skybox 206 till 18:00	
11:00 - 11:50	Matt Weir & Suhir Aggarwal Password Cracking on a Budget. 	Thomas d'Otreppe de Bouvette "Mister X" & Rick Farina "Zero_Chaos" Shifting the Focus of WiFi Security: Beyond Cracking your neighbor's	Scott Moulton Forensics is ONLY for Private Investigators.	Cameron Hotchkies Under the iHood.	Ferdinand Schober Gaming- The Next Overlooked Security Hole.	GH3 Free Play Gringo Warrior till 18:00	Warballooning Demo in Outdoor Area till 14:00	

		<p>WEP key.</p> 					
12:00 - 12:50	<p>FX Developments in Cisco IOS Forensics.</p> 	<p>Matt "DCFLuX" Krick Flux on:EAS (Emergency Alert System)</p> 	<p>John "Jur1st" Benson. When Lawyers Attack! Dealing with the New Rules of Electronic Discovery.</p>	<p>Jay Beale Owning the Users with Agent in the Middle.</p> 	<p>"Ne0nRa1n" & Joe "Kingpin" Grand Brain Games: Make your own Biofeedback Video Game.</p> 	<p>Scavenger Hunt till 18:00 GH3 Hard Heat 1</p>	Chillout Area, DJs
13:00 - 13:50	<p>Adam Bregenzer Buying Time-What is your Data Worth? (A Generalized Solution to Distributed Brute Force Attacks.)</p> 	<p>Alexander Lash Taking Back your Cellphone.</p> 		<p>Luciano Bello & Maximiliano Bertacchini Predictable RNG in the Vulnerable Debian OpenSSL Package, the What and the How.</p> 	<p>Ian Clarke Hacking Desire.</p> 	<p>DEFCONBots GH3 Hard Heat 2 The Phreaking Challenge till 17:00 EEE PC Mod Workshop meetup till 15:00</p>	












<p>14:00 - 14:50</p>	<p>Panel: All your Splits (and Servers) are belong to us. </p>	<p>Major Malfunction Feed my SAT Monkey.  </p>	<p>Panel: Ask the EFF: The Year in Digital Civil Liberties Panel</p>	<p>SensePost Pushing the Camel through the eye of a needle.  </p>	<p>Lyn Tuning Your Brain.  </p>	<p>GH3 Expert Heat</p>	<p>Mobile Hacker Spaces Demo in outdoor area till 16:00</p>
<p>15:00 - 15:50</p>		<p>Zac Franken Is that a unique credential in your pocket or are you just pleased to see me?</p>		<p>Mati Aharoni BackTrack Foo- From bug to Oday.  </p>	<p>Phreakmonkey & mutantMandias Urban Exploration- A Hacker's View.</p>	<p>GH3 Finals Med. GH3 Finals Hard @ 15:30</p>	
<p>16:00 - 16:20</p>	<p>Michael Brooks CSRF Bouncing.  </p>	<p>Mike Perry 365-Day:Active https cookie hijacking.   </p>	<p>Panel: Commission on Cyber Security for the 44th Presidency</p>	<p>atlas VulnCatcher: Fun with Vtrace & Programmatic Debugging.  </p>	<p>Lee Kushner & Mike Murray Career Mythbusters: Separating Fact from Fiction in your Information Security Career.</p>	<p>GH3 Finals Expert</p>	
<p>16:30 - 16:50</p>		<p>MD Sohail Ahmad, JVR Murthy & Amit Vartak</p>					

		<p>Disorder in Wireless LANs.</p> 					
17:00 - 17:20	<p>Felix "FX" Lindner Toying With Barcodes</p>	<p>NYCMIKE The World of Pager Sniffing/ Interception: More Activity than one may suspect.</p>	<p>Don Blumenthal What to do when your Data winds up where it shouldn't.</p>	<p>David Byrne Grendel-Scan: A New Web Application Scanning Tool.</p> 	<p>Christopher Tarnovsky Introducing Momentary Faults Within Secure Smartcards/ Microcontrollers.</p> 		
17:20 - 17:50		<p>Fouad Kiamilev & Ryan Hoover Demonstration of Hardware Trojans.</p> 					
18:00 - 18:50	<p>Paul F. Renda The True Story of the Radioactive Boyscout: The first Nuclear Hacker & how his work relates to Homeland</p>	<p>Scott Moulton Solid State Drives Destroy Forensic & Data Recovery Jobs: Animated!</p> 	TBA	<p>Renderman How can I pwn thee? Let me count the ways.</p>			Closed for Ball Setup

	Security's model of the dirty bomb. 							
19:00 - 19:50	Movie Night With DT: 25th Anniversary Showing of Wargames							
20:00 - 20:50	Followed by a fireside chat with David Scott Lewis, IT & green tech			LeetSkills Talent Competition				
21:00 - 21:50	entrepreneur, model for David Lightman			Hacker Jeopardy				White Ball till 3:00 Sunday
22:00 - 22:50	Movie Night With DT: Three Days of the Condor							
23:00 - ????								

Day Three: Sunday, August 10

08:00 - 12:00	Official DEFCON Store in the Vendor Area at the J!nx Hackwear Booth Vendor Area Hours: 10:00 - 15:00							
	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Room
10:00 - 10:20	<p>Bruce Potter Malware Detection through Network Flow Analysis.</p> 	<p>Brian K. Edwards Markets for Malware: A Structural Economic Approach</p>	<p>Tony Howlett The death of Cash: The Loss of anonymity & other danger of the cash free society.</p>	<p>Christer Oberg, Claes Nyberg, & James Tusini Hacking Open VMS.</p> 	<p>Stefan Frei, Thomas Duebendorfer, Gunter Ollman & Martin May Exploiting A Hundred-Million Hosts Before Brunch</p>			
10:30 - 10:50		<p>Ryan Trost Evade IDS/IPS Systems using Geospatial Threat Detection.</p> 	<p>Peter Berghammer The Emergence (and use) of Open Source Warfare.</p>		<p>JonM Ham for Hackers-Take back the Airwaves.</p> 			
11:00 - 11:50	<p>Rick Hill War Ballooning-Kismet Wireless "Eye in the Sky"</p> 	<p>Dan Kaminsky TBA</p>	<p>Sandy Clark "Mouse" Climbing Everest: An Insider's Look at one state's Voting Systems.</p>	<p>N.N.P. VoIPER:Smashing the VoIP Stack while you sleep.</p> 	<p>Nick Harbour Advanced Software Armoring and Polymorphic Kung Fu</p> 			

								
12:00 - 12:20	<p>Simon Howard Race-2-Zero Unpacked.</p> 	<p>Teo Sze Siong & Hirosh Joseph Let's Sink the Phishermen's Boat!</p> 	<p>Doug Farre Identification Card Security: Past, Present, Future.</p> 	<p>Jay Beale They're Hacking Our Clients! Introducing Free Client-side Intrusion Prevention.</p>   	<p>Valsmith & Colin Ames MetaPost-Exploitation</p>  			
12:30 - 12:50		<p>Renderman 10 Things that are Pissing me off.</p>						
13:00 - 13:50	<p>Thomas Wilhelm Mobile Hacker Space.</p> 	<p>Anthony Martinez & Thomas Bowen Toasterkit, a Modular NetBSD Rootkit.</p>  	<p>Zack Anderson, RJ Ryan & Alessandro Chiesa The Anatomy of a Subway Hack: Breaking Crypto RFID's & Magstripes of Ticketing Systems.</p>  	<p>Paul Craig Compromising Windows Based Internet Kiosks.</p>  	<p>Jonathan Brossard Bypassing pre-boot authentication passwords</p>	<p>The Phreaking Challenge till 14:30</p>		








<p>14:00 - 14:50</p>	<p>Panel: Internet Wars</p>	<p>Michael Ligh & Greg Sinclair Malware RCE: Debuggers and Decryptor Development.</p> 	<p>Mike Renlund The Big Picture: Digital Cinema Technology & Security.</p>	<p>Panel: Black vs. White: The complete life cycle of a real world breach.</p> 	<p>DAVIX Visualization Workshop</p>	<p>Mobile Hacker Spaces Demo in outdoor area till 16:00</p>	
<p>15:00 - 15:50</p>	<p>Jason Scott Making a Text Adventure Documentary.</p> 	<p>Igor Muttik Good Viruses. Evaluating the Risks.</p> 	<p>Taylor Banks & Carric. Pen-Testing is Dead, Long live the Pen Test.</p>				
<p>16:00 - 16:50</p>		<p>Chris Eagle & Tim Vidas Next Generation Collaborative Reversing with IdaPro &CollabReate.</p> 	<p>Tottenkoph, Rev & Philosopher Hijacking the Outdoor Digital Billboard Network.</p> 	<p>Iclee_vx Comparison of File Infection on Windows & Linux.</p> 			
<p>17:00 - 17:50</p>	<p>Awards Ceremonies hosted by Dark Tangent</p>						

EXHIBIT 4

The Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson *Student, MIT*

RJ Ryan *Student, MIT*

Alessandro Chiesa *Student, MIT*

In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese, Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

José Parada is an IT Pro Evangelist in Microsoft. He is a very famous speaker in Spanish conferences about IT Infrastructures, Microsoft Technologies and Security. He has been working in the Microsoft Technet Program from 2005 delivering conferences, webcasts and technical information.

[Top of page](#)

The Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson *Student, MIT*

RJ Ryan *Student, MIT*

Alessandro Chiesa *Student, MIT*

In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese, Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

[Top of page](#)

Digital Security: a Risky Business

Ian O. Angell *Professor of Information Systems. London School of Economics*

In this talk Professor Angell will take the devil's advocate position, warning that computer technology is part of the problem as well as of the solution. The belief system at the core of computerization is positivist and/or statistical, and that itself leads to risk. The mixture of

EXHIBIT 5

Schematic Illustrating the MBTA's Fare Media System

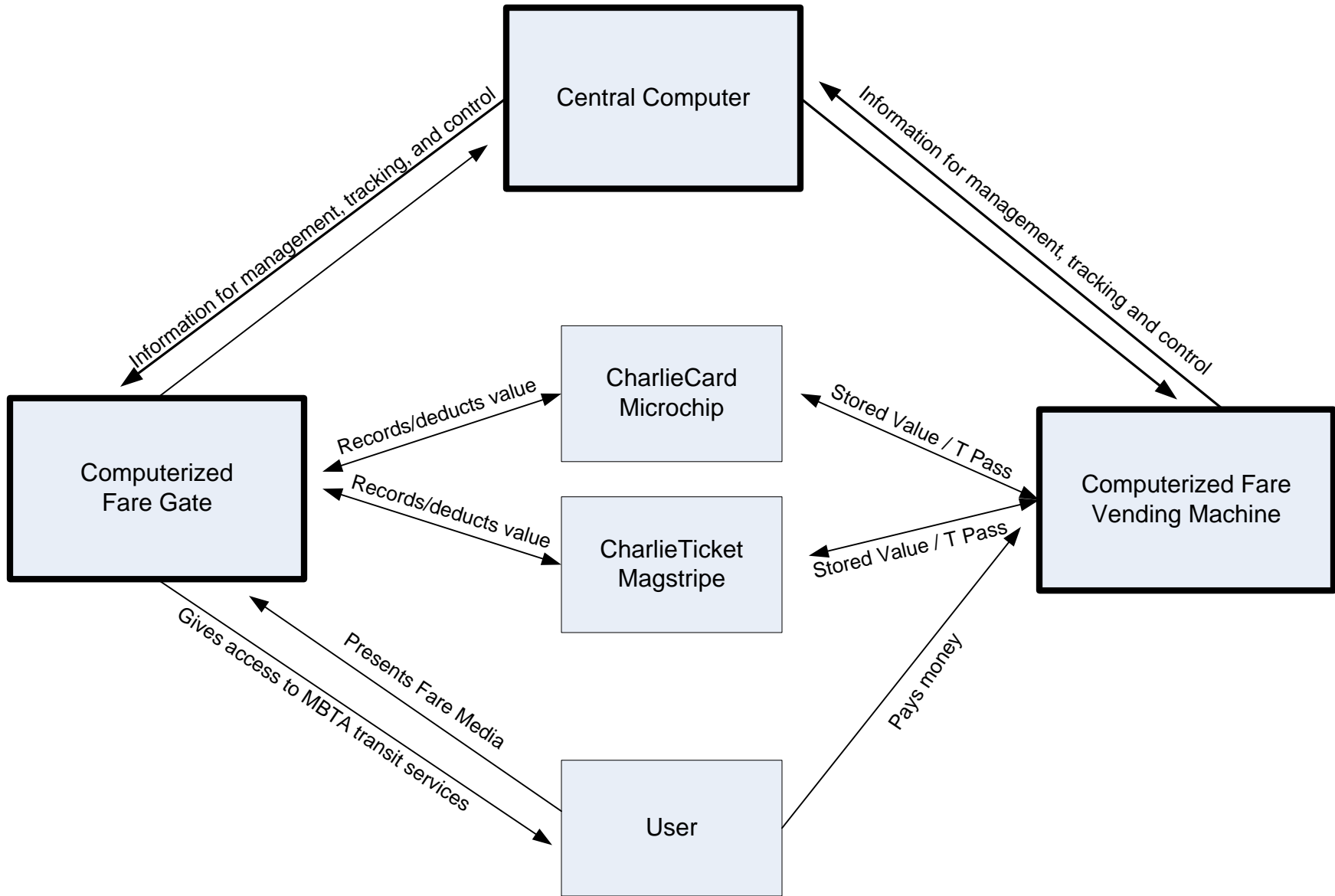


EXHIBIT 6

~~Original~~[Current](#) Version

The Anatomy of a Subway Hack:

Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack ~~Anderson~~[StudentAndersonStudent](#), MIT

RJ ~~Ryan~~[StudentRyanStudent](#), MIT

Alessandro ~~Chiesa~~[StudentChiesaStudent](#), MIT

~~Want free subway rides for life?~~In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We ~~go over social engineering attacks we executed on employees~~[survey 'human factors' that lead to weaknesses in the system](#), and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote ~~to perform~~[in the process of researching](#) these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese, Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

~~#5526763_v1~~[#5526763_v2](#)

Document comparison done by Workshare DeltaView on Thursday, August 07, 2008
5:11:58 AM

Input:	
Document 1	interwovenSite://BOSDMS/Active/5526763/1
Document 2	interwovenSite://BOSDMS/Active/5526763/2
Rendering set	standard

Legend:	
<u>Insertion</u>	
Deletion	
Moved from	
<u>Moved to</u>	
Style change	
Format change	
Moved deletion	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	7
Deletions	11
Moved from	0
Moved to	0
Style change	0
Format changed	0
Total changes	18

EXHIBIT 7

July 14, 2008 9:12 AM PDT

Column: The man who changed Internet security

Posted by [Robert Vamosi](#)

[14 comments](#)

Programming note: *As of Friday, July 11, 2008, Defense in Depth will now only carry my weekly column plus additional commentary on the state of computer security. My security news blogs will instead appear under the [CNET News Security banner](#) going forward. And my CNET News Security Bites podcasts can be found at [here](#). All of these can be subscribed to via RSS.*

While security researcher Dan Kaminsky still won't comment on the specific nature of a [flaw within the Domain Name System](#)--for fear that criminal hackers might exploit it before the worldwide network of name servers worldwide and client systems that contact them can be updated--he nonetheless went public on July 8 with some details, backed by simultaneous patch releases from Microsoft, Cisco, and others.

There have been other multiparty patch releases, but never has there been one on such a massive scale. It took someone with the gravitas and reputation of Kaminsky to pull together the affected parties.

What he and others he took into his confidence did over the last few months was not only responsible but extraordinary. The flaw that Kaminsky discovered could allow criminal hackers to guess the transaction ID of any request to a DNS server for a particular domain, such as one used for a bank or an e-commerce site, and then redirect that request to another site, a phishing site. It would do so silently, evading most anti-phishing technology because

[Ad Feedback](#)



About Defense in Depth

Covering computer viruses and computer crime, Robert Vamosi goes beyond the hype to provide you with expert interviews of the top security researchers, as well as offeri the hands-on, nontechnical advice you'll need to stay safe online.



[Subscribe via RSS](#)

[Click this link to view as XML.](#)

the change would be made not at the desktop level but at the DNS server itself. Certainly this is big, and certainly one would want to get the news out as soon as possible--but Kaminsky took the time to inform the proper vendors and authorities and, only after they were ready with patches, did he disclose some of what he'd discovered.

That isn't to say what Kaminsky did was perfect; he himself admits there are lessons to be learned and improved upon the next time this happens. Whether you agree with the severity of the flaw Kaminsky disclosed last Tuesday, I do think all future vulnerability disclosures could benefit from his example.

Kaminsky, director of penetration testing at IOActive, is no stranger to vulnerabilities. Over the years he's found a fair share and says that in the case of the DNS flaw he wasn't looking for it. In this week's [Security Bites podcast](#), Kaminsky told me that after three days of testing he knew he had something important. At that point, early in 2008, he had a few options.

One was to tell the vendor (or, in this case, vendors) directly. [Ari Takanen of Codenomicon](#) told me he prefers that security researchers keep vulnerabilities between them and the vendor. Vendors, Takanen said, have their own development cycles, and for a researcher to burst into a room or go public and demand that everyone work on his or her vulnerability is unrealistic. While Kaminsky was willing to work with the vendors, he wasn't willing to give them forever.

Another option was to sell the vulnerability to a third party like TippingPoint's [Zero Day Initiative](#). ZDI acts as the middleman, talking with the vendor and communicating with the researcher. The advantage here is that a researcher with no connections to the affected vendor can communicate the problem clearly.



Dan Kaminsky at DefCon in 2006.
(Credit: Declan McCullagh/CNET News)

Add this feed to your online news reader

Defense in Depth topics

- Antivirus
- Networking
- Audio and video
- Phishing
- Tools and books
- Rootkits
- Browsers and extensions
- Security
- Chat and e-mail
- Spyware
- Criminal Hackers
- Storage
- Mobile
- Uncategorized

ZDI has been credited with several vulnerabilities, such as those announced by Apple and Microsoft. Kaminsky has no qualms with those who opt for this method, although he said he didn't understand why a company would pay for this information. (I know the answer: TippingPoint uses the vulnerability data it purchases to protect its customers first, thereby giving it a competitive advantage in the vulnerability assessment space).

Another option for Kaminsky was to go public, to announce the vulnerability and publish details, including an exploit, on, say, Bugtraq. A few researchers have gone this route, but often as a last resort after getting a cold shoulder from the vendor. A few researchers have published flaw details

Most popular stories

first without contacting anyone, taking both the public and the vendor by surprise. But such moves are unwise since they give the bad guys all the information they need while everyone is vulnerable.

Kaminsky provides the only of cracking DNS
IKEA to sell solar panels?

Photos: Microsoft from the OS looks like show
Images: Scientists develop eye camera

Finally, as Kaminsky found out, the upside of selling your vulnerability to the criminal underside of the Internet.

Black Hat a sure bet to be big, bold in Vegas

With the DNS flaw, Kaminsky was in a very weird position. What he found wrong with DNS, the servers that translate a Web site's common name to its IP address, wasn't just within one vendor's product, it cut across various products, from various vendors. He said he consulted with DNS expert Paul Vixie, and together they decided they had to convene a meeting, and do so within a few weeks of the discovery.



Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure.

That meeting occurred at Microsoft's Redmond, Wash., headquarters on March 31, 2008. There, representatives from 16 vendors sat down and listened to Kaminsky's pitch. After deciding this was a real and exploitable problem, the vendors decided they would have little choice but to agree to release simultaneously their respective patches.

At some point, July 8, 2008, was agreed upon as the date,

EA, Paramount announce 'Godfather II' video ga
Posted in Geek Gestalt by Daniel Terdiman

August 8, 2008 5:35 AM PDT



Between a rock and YouTube, video execs see promise

Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT



Targeted for hacking by reporters at my table

Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT

[All News.com headlines »](#)

perhaps because it coincided with Microsoft's monthly Patch Tuesday. The date was significant in other ways: for example, it fell roughly 30 days before Kaminsky was scheduled to speak at Black Hat in Las Vegas.

Between March and July, there was considerable back and forth among Kaminsky and the vendors, and then, as the date neared, he decided to share the details with a few others.

In retrospect, Kaminsky confessed that he really should have told more people. He had gone through great pains to inform the DNS community, the specific vendors, and few researchers. He did so to keep word from getting out.

But within hours of making his announcement, Kaminsky faced a chorus of public ridicule by other security researchers, most hearing about the flaw for the very first time. The complaints, at times, trivialized the announcement, with fellow researchers citing that similar claims had been made against DNS [3 to 10 years before](#) or [even longer](#). Some suggested Kaminsky was simply trying to advertise his talk at Black Hat next month.

Most vocal was Matasano Security researcher Thomas Ptacek, who [blogged his doubts](#). But Kaminsky called Ptacek and he retracted his comments. He now says, "Dan has the goods. Patch now, ask questions later."

Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure. He could have, as Ptacek notes, made thousands of dollars off this DNS thing. Instead, Kaminsky has set a high mark for future disclosures. He has changed Internet security, and done so for the better of us all.

TOPICS: [Security](#)

TAGS: [security](#), [column](#), [Security Watch](#), [Dan Kaminsky](#), [DNS patch](#)

BOOKMARK: [Digg](#) [Del.icio.us](#) [Reddit](#) [Yahoo! Buzz](#)

Featured blogs

[Beyond Binary](#) by Ina Fried

[Coop's Corner](#) by Charles Cooper

[Defense in Depth](#) by Robert Vamosi

[Geek Gestalt](#) by Daniel Terdiman

[Green Tech](#)

[One More Thing](#) by Tom Krazit

[Outside the Lines](#) by Dan Farber

[The Iconoclast](#) by Declan McCullagh

[The Social](#) by Caroline McCarthy

[Underexposed](#) by Stephen Shankland

Recent posts from Defense in Depth

[Black Hat 2008: Notes from the field](#)

[Column: Finally, ID fraud protection that works](#)

[Column: Will you be ditching your antivirus app anytime soon?](#)

[A real simple answer to password protection](#)

[Despite patch, today's systems still vulnerable to 2002 flaw](#)

ADD A COMMENT ([Log in or register](#))

14 comments (Page 1 of 2)

by [inachu](#) July 14, 2008 7:55 AM PDT

I miss the days where most govt agencies had their own BBS.

Using telnet and going into various areas just exploring.

I went from my local library to MIT then onto NIST then onto some tokyo university BBS retracing mysteps it went all the way around the world through nasa then loggen back into my library.

Sad to see we can't do that anymore. No more wild jungle.

[Reply to this comment](#)

by [tekwiz4u](#) July 14, 2008 11:17 AM PDT

It's commendable what he did. He wasn't in it for bragging rights, like most of the hackers out

Resource center from News.com sponsors

Same great protection. Reengineered for speed.

Norton Internet Security™2008



Norton still delivers award-winning protection and now uses

83% less memory and scans 48% faster than the competitor average. [Get a FREE trial today!](#)



[Norton Beats the Competition](#)

See how Norton Internet Security™2008 uses less memory, while scanning and booting faster than the competitor average.

[Norton Protection Blog](#)

Read the latest from our security experts as they help protect people from evolving online threats.

[Protect Your Bluetooth Connection](#)

Don't let fraudsters sink their teeth into your Bluetooth connection.

[Vishing - What you](#)

there. The exploit would have been bad for all of us. But he took it upon himself to be responsible to benefit the greater whole. Good job.

[Reply to this comment](#)

by [n3td3v](#) July 14, 2008 11:28 AM PDT

Media hype and clever marketing for Blackhat security conference.

Let's find out who is making the money, this vulnerability is over hyped.

[Reply to this comment](#)

by [The_Decider](#) July 14, 2008 12:10 PM PDT

Responsible? Only because the parties involved took it seriously.

If they had not and Kaminsky hadn't disclosed it would have been irresponsible. The black hats would have found it eventually leaving everyone at the mercy of them.

Full disclosure is always better than those idiots who think there is any merit to security through obscurity.

[Reply to this comment](#)

by [RobertinOhio](#) July 14, 2008 12:44 PM PDT

As a security professional whom is certified I still do not see the value of this "admiral approach" to

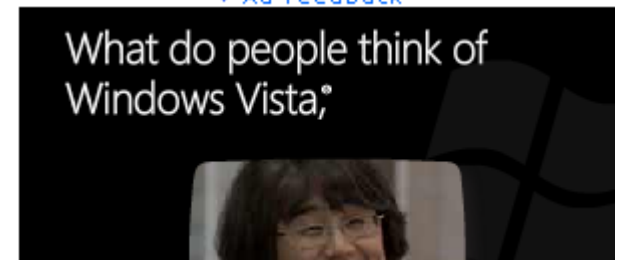
need to know

Meet the latest ID theft scam: Voice Phishing.

Take Norton for a Test Drive Today!

Act now to get your FREE trial of Norton Internet Security 2008.

[Ad Feedback](#)





releasing of security incidents and vulnerabilities. Yeah Dan Kaminsky has made a name for himself in the security community. If he was just some other schmo...then he would have never seen the inside of any vendor's office. My name does not mean jack so I know I am not going to pick up the phone and get a meeting at Cisco or Microsoft in a couple of days to discuss the issue with them. I am going to put my discovery on Bugtraq and if the internet gets shut down in North America as a result...oh well.

BUT...if I do sit on it and a hacker finds the exploit and then I come out afterward, I get nailed for not sharing it. D-amned if I do and d-amned if I don't. The good guys always loose.

Another thing I have learned is usually the hacker will almost always win. All you can do is contain, eradicate, and learn from attacks and exploits to make it harder for them to break in. Not sharing your discoveries from the general public and only with vendors is most certainly NOT the way to resolve these issues however. I do not commend Dan Kaminsky for his actions, he is setting a BAD precedent. One that unfortunately Infragard, another organization with a history of one way traffic with information, follows.

[Reply to this comment](#)

by [DanKaminsky](#) July 14, 2008 2:13 PM PDT

Robert--

The vendors have become pretty good at responding to stuff -- and, of course, if you do find something of technical value, please feel free to contact me and I will be happy to help. I'm trying to find a balancing point between not releasing (which leads to no patches, and/or no deployment of patches) and releasing in a problematic manner (i.e. even those places that are responsible, and do maintain their security, are still hit). Maybe this isn't perfect, but please give me the benefit of the doubt until you know just what I've found.

[Reply to this comment](#) | [View all 2 replies](#)

by [DanKaminsky](#) July 14, 2008 2:17 PM PDT

Decider--

I agree. It's only because the vendors were so amazingly responsive that this path could be taken at all. If they'd been lame, we'd be screaming at them for being so. So, they weren't lame, in all fairness they deserve some appreciation for that.

[Reply to this comment](#)

by [n3td3v](#) July 14, 2008 3:47 PM PDT

Dan Kaminsky is making money out of this there is no doubt.

If he hadn't circled his disclosure around a profiteering security conference I wouldn't bash this **** so much.

Because he has circled his disclosure around a big security conference, I know his motivation is money.

I don't know who he has been shaking hands with and what money has been exchanged, but this is something for the government to wire tap on.

[Reply to this comment](#)

by [mehap](#) July 14, 2008 11:12 PM PDT

So what if he is making/indulging in making money?

Your whole system is geared on making money.


How do you survive mate?

[Reply to this comment](#)

by [DanKaminsky](#) July 15, 2008 3:45 PM PDT

n3td3v--

Dude, did you miss the fact that Defcon is like three days later? Black Hat is just practice for

Defcon  Seriously, the last big talk was Seattle Toorcon. Rickrolling the Internet isn't exactly profit source number one.

[Reply to this comment](#)

1 | 2 | [Next 10 Comments >>](#)

Register to submit a comment

Already have an account? [Log in now](#)

Join the CNET communityTo continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's [Terms of Use](#)

CONTINUE

[Need help? »](#)

Powered by [Jive Software](#)

On TechRepublic: 19 words you don't want in your resume [Log in](#) | [Sign up](#) | [WI](#)



Search: News [Advanced search](#)

- Today on CNET
- Reviews
- News**
- Downloads
- Tips & Tricks
- CNET TV
- Compare Prices
- Blogs
- ad [Click to Save up to \\$300/yr c](#)
- [Business Tech](#)
- [Cutting Edge](#)
- [Green Tech](#)
- [Wireless](#)
- [Security](#)
- [Media](#)
- [Markets](#)
- [Personal Tech](#)
- [Video](#)
- [My News](#)

Sponsored Links

[Lock Down Windows XP](#)

Secure your confidential data. Free security guide download.

www.newboundary.com

[Norton Internet Security](#)

Newest 2008 version available now! Includes AntiVirus™ and Firewall.

www.norton.com

[SAP Security & Controls](#)

Affordable, remote security admin for SAP by The Security Experts

www.sym-corp.com

- [Site map](#)
- [Help center](#)
- [Corrections](#)
- [Newsletters](#)
- [Send tips](#)
- [News.com mobile](#)
- [Content licensing](#)
- [RSS feeds](#)

Search: News

- Popular topics: [CES](#) [Drivers](#) [Games](#) [IE7](#) [iPhone](#) [iPod](#) [iPod Nano](#) [iPod Touch](#) [iTunes](#) [Leopard](#) [Macworld](#) [Nintendo Wii](#) [PS3](#) [Spyware](#) [TVs](#) [Vista](#) [Xbox 360](#)

- [About CNET](#)
- [Today on CNET](#)
- [Reviews](#)
- [News](#)
- [Compare prices](#)
- [Tips & Tricks](#)
- [Downloads](#)
- [CNET TV](#)

Popular on CBS sites: [Fantasy Football](#) [Miley Cyrus](#) [MLB](#) [Wii](#) [GPS](#) [Recipes](#) [Mock Draft](#)

[About CNET Networks](#) [Jobs](#) [Advertise](#)

Visit other CBS Interactive sites

Copyright ©2008 CNET Networks, Inc., a CBS Company. All rights reserved. [Privacy policy](#) [Terms of use](#)

August 7, 2008 9:07 AM PDT

Kaminsky provides the why of attacking DNS

Posted by [Robert Vamosi](#)

[6 comments](#)

LAS VEGAS--Speaking before a packed audience, researcher Dan Kaminsky explained the urgency in having everyone patch their systems: virtually everything we do on the Internet involves a Domain Name System request and therefore is vulnerable.

Expectations were running high before Wednesday morning as [Kaminsky](#), director of penetration testing for IOActive, had revealed little about his [DNS vulnerability](#) up till then. That didn't stop others from trying to [figure it out](#). But that actually helped Kaminsky in the end; it meant during his speech, he was able to skip the [what](#) and go directly to the why.

Security researchers always thought it was hard to poison DNS records, but Kaminsky said to think of the process as a race, with a good guy and bad guy each trying to get a secret number transaction ID. "You can get there first," he said, "but you can't cross finish line unless you have the secret number."

The question is why would someone bother? Well, Kaminsky talked about how deeply embedded DNS is in our lives. Kaminsky said there are three ages in computer hacking. The first was attacking servers (for example FTP and Telnet). The second was attacking the browsers (for example Javascript and ActiveX). We're now about to enter the third age, where attacking Everything Else is possible.

[Ad Feedback](#)



About News - Security

Online security is threatened by more than hacking and phishing attempts. Check here for the latest updates on software vulnerabilities, data leaks, and rapidly spreading viruses--and learn how to protect your systems.



[Subscribe via RSS](#)

Click this link to view as XML.

[Add this feed to your online news reader](#)

We know that if we type a name.com into a browser, the DNS resolves it to its numerical address. But what we don't realize is that same process occurs when we send e-mail or when we log onto a Web site. These also require DNS lookup.

Kaminsky then detailed how various security methods on the Web can be defeated if one owns the DNS. For example, if a site wants to establish a Trust Authority Certificate with the Certificate Authorities, they use e-mail to confirm the identity of the requester. He also said that it's possible to poison Google Analytics and even Google AdSense, which also rely on DNS lookup.

Prior to the patch, the bad guy had a 1 in 65,000 chance of getting it because the transaction ID is based, in part, on the port number used. With the patch, the chances decrease to 1 in 2,147,483,648. Kaminsky said it's not perfect, but it's a good enough start.

[Click here for full coverage of Black Hat 2008.](#)

TOPICS: [Vulnerabilities & attacks](#), [News](#)

TAGS: [Security](#), [Black Hat 2008](#), [Dan Kaminsky](#), [DNS](#)

BOOKMARK: [Digg](#) [Del.icio.us](#) [Reddit](#) [Yahoo! Buzz](#)

Recent posts from News - Security

[Targeted for hacking by reporters at my table](#)

[Black Hat expels reporters in network snooping](#)

[Microsoft to seek credit for finding vulnerabilities](#)

[Wall of Sheep comes to Black Hat](#)

[Is Check Point's security profile the broadest?](#)

News - Security topics

[Corporate & legal](#)

[Privacy & data protection](#)

[News](#)

[Vulnerabilities & attacks](#)

Most popular stories

[Kaminsky provides the why of attacking DNS](#)

[IKEA to sell solar panels?](#)

[Photos: More spins from the Oshkosh air show](#)

[Images: Scientists develop eye camera](#)

[Black Hat a sure bet to be big, bold in Vegas](#)

Latest tech news headlines



[Between a rock and YouTube, video execs see promise](#)

Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT



[Targeted for hacking by reporters at my table](#)

Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT



[Google sours on \\$1 billion AOL investment](#)

Posted in News - Digital Media by Steven Musil
August 7, 2008 9:20 PM PDT

[ADD A COMMENT](#) ([Log in or register](#))

6 comments (Page 1 of 1)

by [One Mark Bliss](#) August 7, 2008 10:04 AM PDT

Actually, the chances decrease, since the one is divided by the increased number. Consider that the concept of chance being used in the article represents the random likelihood that someone will guess the secret code in one attempt.

It seems that a similar confusion exists in another concept nothing to do with chance, namely turning the air conditioning up, or down. Which makes the room colder? In that case it depends on whether the concept being referred to is the amount of the flow of cold air, in which case it would be up, or the numerical representation of temperature, in which case it would be down.

The only way a similar confusion can arise with chance is whether it is couched as the chance of guessing something randomly, or the chance of not guessing it. So, in the article, the chance would only increase if it were the chance of a hacker randomly NOT getting the secret code.

[Reply to this comment](#) | [View reply](#)

by [conobs](#) August 7, 2008 11:20 AM PDT

instead of giging them on symantecs
WHERE IS THE MEAT?
how dos it work?

this would qualify more as a story about a story, not an actual news story
take it up a notch
thx
bob

[All News.com headlines »](#)

Featured blogs

[Beyond Binary](#) by Ina Fried

[Coop's Corner](#) by Charles Cooper

[Defense in Depth](#) by Robert Vamosi

[Geek Gestalt](#) by Daniel Terdiman

[Green Tech](#)

[One More Thing](#) by Tom Krazit

[Outside the Lines](#) by Dan Farber

[The Iconoclast](#) by Declan McCullagh

[The Social](#) by Caroline McCarthy

[Underexposed](#) by Stephen Shankland

Resource center from News.com sponsors

Same great protection.

[Reply to this comment](#)

by [conobs](#) August 7, 2008 11:25 AM PDT

i dont know maybe i am wrong and overly harsh

[Reply to this comment](#)

by [frazmann](#) August 7, 2008 12:55 PM PDT

@conobs - the crux of the hack are that you send a DNS request to a server, knowing that the server will send a request to it's DNS master server to obtain the translation, and then bombard the server with fake responses, hoping to guess the transaction id that it used when making the request. If you get it right before the master server's response arrives then you have planted a fake DNS entry in your server, and the real response is thrown away. If you do this from your comcast account then you can re-direct all your neighbors to a fake google.com that sits on your PC. Seems so simple I'm surprised no-one tried it before....

[Reply to this comment](#)

by [benjaminstraight](#) August 8, 2008 3:14 AM PDT

Good article.

[Reply to this comment](#)

Reengineered for speed.

Norton Internet Security™2008



Norton still delivers award-winning protection and now uses

83% less memory and scans 48% faster than the competitor average. [Get a FREE trial today!](#)



[Norton Beats the Competition](#)

See how Norton Internet Security™2008 uses less memory, while scanning and booting faster than the competitor average.

[Norton Protection Blog](#)

Read the latest from our security experts as they help protect people from evolving online threats.

[Protect Your Bluetooth Connection](#)

Don't let fraudsters sink their teeth into your Bluetooth connection.

[Vishing - What you need to know](#)

Meet the latest ID theft scam: Voice Phishing.

[Take Norton for a Test Drive Today!](#)

Act now to get your FREE trial of Norton Internet Security 2008.

On The Insider: Paris Says the Video Speaks for Itself

Log in | Sign up | WI



Search:

News



- Today on CNET
- Reviews
- News
- Downloads
- Tips & Tricks
- CNET TV
- Compare Prices
- Blogs
- ad ▶ [Click to Save up to \\$300/yr c](#)
- Business Tech
- Cutting Edge
- Green Tech
- Wireless
- Security
- Media
- Markets
- Personal Tech
- Video
- My News

Register to submit a comment

Already have an account? [Log in now](#)

Join the CNET community To continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's [Terms of Use](#)

CONTINUE

[Need help? »](#)

▼ [Ad Feedback](#)



Powered by [Jive Software](#)

- [Site map](#)
- [Help center](#)
- [Corrections](#)
- [Newsletters](#)
- [Send tips](#)
- [News.com mobile](#)
- [Content licensing](#)
- [RSS feeds](#)

Search:

News



Popular topics: [CES](#) [Drivers](#) [Games](#) [IE7](#) [iPhone](#) [iPod](#) [iPod Nano](#) [iPod Touch](#) [iTunes](#) [Leopard](#) [Macworld](#) [Nintendo Wii](#) [PS3](#) [Spyware](#) [TVs](#) [Vista](#) [Xbox 360](#)

On The Insider: Paris Says the Video Speaks for Itself

[Log in](#) | [Sign up](#) | [WI](#)



Search:

News

 [Advanced search](#)

- [Today on CNET](#)
- [Reviews](#)
- [News](#)**
- [Downloads](#)
- [Tips & Tricks](#)
- [CNET TV](#)
- [Compare Prices](#)
- [Blogs](#)
- [ad ▶ **Click to Save up to \\$300/yr c**](#)
- [Business Tech](#)**
- [Cutting Edge](#)**
- [Green Tech](#)**
- [Wireless](#)**
- [Security](#)**
- [Media](#)**
- [Markets](#)**
- [Personal Tech](#)**
- [Video](#)**
- [My News](#)**

[About CNET](#) [Today on CNET](#) [Reviews](#) [News](#) [Compare prices](#) [Tips & Tricks](#) [Downloads](#) [CNET TV](#)

Popular on CBS sites: [Fantasy Football](#) [Miley Cyrus](#) [MLB](#) [Wii](#) [GPS](#) [Recipes](#) [Mock Draft](#)

[About CNET Networks](#) [Jobs](#) [Advertise](#)

Visit other CBS Interactive sites

Copyright ©2008 CNET Networks, Inc., a CBS Company. All rights reserved. [Privacy policy](#) [Terms of use](#)

EXHIBIT 8



Athena Rules of Use (including MITnet)

MITnet, MIT's campus-wide computer network, connects thousands of computers on and off campus, including the Athena workstations, printers, and servers, many student machines in the dorms, and the campus dialup servers. Network connectivity has many advantages which you will discover as you explore Athena, MITnet, and the Internet beyond. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

Similarly, the **Athena-specific end-user facilities** (clusters, workstations, printers, etc.) are provided as an Institute resource, and certain guidelines are necessary to help maintain this resource.

This section summarizes:

- [the rules that apply to all users of MITnet](#) (this includes all Athena users)
- [the rules regarding the appropriate use of Athena-specific facilities](#)

We expect you to follow these rules, and we hope you will help others follow them as well. If you need assistance in dealing with someone willfully violating the rules, send email to stopit@mit.edu.

We appreciate your cooperation.

Summary

The listing below provides only summaries of the rules. For the full text of each rule, please see the following pages.

MITnet Rules of Use

Comply with Intended Use of the System

- 1. Don't violate the intended use of MITnet.**

Assure Ethical Use of the System

- 2. Don't let anyone know your password(s).**
- 3. Don't violate the privacy of other users.**
- 4. Don't copy or misuse copyrighted material (including software).**
- 5. Don't use MITnet to harass anyone in any way.**

Assure Proper Use of System Resources

- 6. Don't overload the communication servers; in particular, don't abuse your electronic mail (email) or Zephyr privileges.**

Additional Rules for Athena Facilities

Comply with Intended Use of the System

A1. Don't violate the intended use of the Athena system.

Protect Athena Equipment

A2. Don't eat, drink, or bring food or liquids into the Athena clusters.

A3. Don't turn the power off on Athena equipment.

A4. Don't reconfigure the cluster, either hardware or software.

Assure Fair Access to Workstations in Athena Clusters

A5. Don't violate the official priorities for the use of workstations; in particular, don't play games or engage in other non-academic activity if the cluster is busy, and don't log on to more than one workstation at a time.

A6. Don't leave your workstation unattended for more than 20 minutes.

A7. Don't make a lot of noise in the Athena clusters.

Assure Fair Access to Athena Printers

A8. Don't violate the official priorities for the use of printers; in particular, don't be a printer hog or use the Athena printers as copy machines.

MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsible, legal, and respectful of privacy. If you have questions or wish further information about any of the MITnet policies outlined below, send e-mail to itpolicy@mit.edu.

All network users are expected to follow these rules. *Violations of the rules can subject the offender to Institute disciplinary proceedings and, in some cases, to state or federal prosecution.*

PLEASE NOTE: Laws that apply in "the real world" also apply in the "virtual" networked computer world (including MITnet). Laws about libel, harassment, privacy, copyright, stealing, threats, etc. are *not* suspended for computer users, but apply to all members of society whatever medium they happen to be using: face-to-face, phone, *or* computer. Furthermore, law-enforcement officials are more computer-savvy than ever, and violations of the law in "Cyberspace" are vigorously prosecuted.

Similarly, Institute policies (as described in MIT's [Policies and Procedures](#), for example) also apply to MITnet users. Other rules may also apply to users of particular facilities connected to MITnet: users of MIT's

academic computing resources are subject to the [Additional Rules for Athena Facilities](#); providers of information to MIT's Campus-Wide Information System (via TechInfo, the World Wide Web, etc.) have specific guidelines (see <http://web.mit.edu/cwis/www/faq/guidelines.html>); other facilities may have their own constraints (check with your local system manager); and external networks to which MITnet provides access may have their own rules to which MITnet users may be subject.

Complying with the Intended Use of the System

It is important that you understand the purpose of MITnet so that your use of the system is in compliance with that purpose.

1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:

- *Don't try to interfere with or alter the integrity of the system at large*, by doing any of the following:
 - permitting another individual to use your account
 - impersonating other individuals in communication (particularly via forged email or Zephyrgrams)
 - attempting to capture or crack passwords or encryption
 - destroying or altering data or programs belonging to other users
- *Don't try to restrict or deny access to the system by legitimate users.*
- *Don't use MITnet for private financial gain.* For example, users are *not* permitted to run a private business on MITnet. (Commercial activity *is* permitted, but *only* for business done on behalf of MIT or its organizations. Cf. Section [13.2.3](#) of MIT's [Policies and Procedures](#): "MIT's computing and telecommunications facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization.")
- *Don't transmit threatening or harassing materials.* (Cf. [Rule 5.](#))

Assuring Ethical Use of the System

Along with the many opportunities that Athena provides for members of the MIT community to share information comes the responsibility to use the system in accordance with MIT standards of honesty and personal conduct. Those standards, outlined in Section [13.2](#) of MIT's [Policies and Procedures](#), call for all members of the community to act in a responsible, professional way.

Appropriate use of MITnet resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

2. Don't let anyone know your password(s).

While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should *never* let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., IS&T staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one. And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, how to change passwords, and how to share information on Athena without giving away your password, see the document [Managing Your Athena Account](#).

3. Don't violate the privacy of other users.

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet, and the operating systems used by Athena and other MITnet systems, encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections [11.2](#), [11.3](#), and [13.2](#) of MIT's [Policies and Procedures](#)). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section [11.1](#) of MIT's [Policies and Procedures](#) notes, "Invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- *Don't try to access the files or directories of another user without clear authorization from that user.* Typically, this authorization is signaled by the other user's setting file-access permissions to allow public or group reading of the files. If you are in doubt, ask the user.
- *Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.* These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.
- Unless you understand how to protect private information on a computer system, *don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves* (e.g., grades, address information, etc.)
- *Don't make any personal information about individuals publicly available without their permission.* This includes both text and number data about the person (biographical information, phone numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.) For instance, it is *not* appropriate to include a picture of someone on a World Wide Web page without that person's permission. (Depending on the source of the information or image, there may also be copyright issues involved; cf. [Rule 4](#)).
- *Don't create any shared programs that secretly collect information about their users.* Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)
- *Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.*

4. Don't copy or misuse copyrighted material (including software).

Many computer programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. You must abide by these legal and contractual restrictions, because to do otherwise may subject you to civil or criminal prosecution.

Copyright-related restrictions may include (but are not necessarily limited to) prohibitions against:

- copying programs or data
- reselling programs or data
- redistributing or providing facilities for redistributing programs or data
- using programs or data for non-educational purposes
- using programs or data for financial gain
- using programs or data without being among the individuals or groups licensed to do so
- publicly disclosing information about programs (e.g., source code) without the owner's authorization

For more information about the legal issues surrounding duplication of software, see the pamphlet "Is it okay to copy my colleague's software?" (To request a copy, send e-mail to sendpubs@mit.edu or call x3-5150.) Some software on Athena is subject to special licensing restrictions; see the document [Summary of Available Athena Software](#). For all other software licensing questions, send email to contracts@mit.edu.

The above prohibitions focus on computer software, but copyright laws apply to *all* material on MITnet. For example, it is inappropriate to copy *any* material owned by others from *any* source (e.g., cartoons, photographs, articles, poems, graphics scanned from a magazine, etc.) without permission of the owner. You should assume that all materials are copyrighted unless a disclaimer or waiver is explicitly provided. (This is particularly true on the World Wide Web; to include information from some other source on a Web page, *link* to it, *don't* copy it. In some cases, even this action may violate copyright or licensing agreements by enabling illegal redistribution of programs or data. If you're unsure, ask the owner.)

5. Don't use MITnet to harass anyone in any way.

"Harassment," according to MIT's [Policies and Procedures](#) (Section [9.5](#)), is defined as:

any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual or group's educational or work performance at MIT or that creates an intimidating, hostile or offensive educational, work or living environment.... Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group.

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to stopit@mit.edu. (If you believe you are in danger, call the Campus Police *immediately* at x3-1212.)

Assuring Proper Use of the System

MITnet's resources, as well as the resources MITnet gives you access to (e.g., Athena, postal servers, bulletin boards, etc.), are powerful tools that can be easily misused. Your use of the system should be consistent with the intended uses of these resources. In particular, you should not overload the system or otherwise abuse the

network.

6. Don't overload the communication servers; in particular, don't abuse your electronic mail (email) or Zephyr privileges.

Electronic mail is a fast, convenient form of communication. It is easy to send electronic mail to multiple recipients, and you can even send a message to many recipients simply by specifying a single list name (i.e., by using a mailing list). But this ability to send messages to many people also makes it easy to misuse the system. The general rule is: *use email to communicate with other specific users, not to broadcast announcements to the user community at large.*

For example, while it is appropriate to use email to have an interactive discussion with a set of people (even 20 or more users) or to use email to send a single copy of an announcement to some "bulletin board" facility with a wide readership (e.g., Network News, or a Discuss meeting), it is not appropriate to use email as a way to broadcast information directly to a very large number of people (e.g., an entire MIT class). This is true whether you include the recipient usernames individually or by using a mailing list: under no circumstance should you use the email system to get a general announcement out to some large subset of the MIT community.

These guidelines are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of email messages at once. When a user sends out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a degradation of service for all users.

These considerations apply to the Zephyr service as well. Zephyr is a central service involving thousands of transactions daily. Using Zephyr to transmit messages to a very large group of people degrades the system performance and is inappropriate.

Finally, the proliferation of electronic chain letters is especially abusive of the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing. Creating or forwarding chain letters may subject you to Institute disciplinary proceedings.

Additional Rules for Athena Facilities

These Rules of Use for Athena Facilities are intended to help members of the MIT community protect the Athena equipment to assure all authorized users effective access to it. These rules supplement the [MITnet Rules of Use](#), which all Athena users are also expected to follow.

These rules apply to all users of Athena facilities, including students, faculty, authorized guests, and even IS&T/Athena staff. (In certain private Athena clusters, some of these rules may be relaxed, or additional rules may be in effect; check with your cluster's system manager).

If you need assistance in dealing with someone willfully violating the Athena rules, feel free to contact the Athena Hardware Hotline (phone: x3-1410, email: hotline@mit.edu), or send email to stopit@mit.edu. (If you believe you are in danger, call the Campus Police *immediately* at x3-1212.)

Complying with the Intended Use of the System

While MITnet is a general-purpose Institute resource in support of all kinds of computing on campus, Athena is more specifically focused on academic computing -- the use of computers in fulfilling the Institute's

educational goals. This special focus is echoed in a more specific intended use of the system.

A1. Don't violate the intended use of the Athena system.

Athena is an Institute resource for authorized MIT community members to use to fulfill educational goals. You should not take any action that violates that purpose. In particular:

- *Don't use Athena resources for non-educational purposes in any way that interferes with their use for educational purposes.* This is especially true at peak times of the year, when demand for Athena workstations and services exceeds supply and *any* use of Athena for non-educational purposes can potentially take resources away from education-oriented users. (Cf. [Rule A5.](#))
- *Don't use any software available on Athena for any non-educational purpose if the license for that software does not permit such use.* In many cases, software available on Athena is licensed for educational use only. Users who would like to make non-educational use of Athena software (e.g., members of sponsored research projects who might like to use Athena's third-party software) must first check the licensing terms for the specific software they are interested in using (these terms are usually included in the locker for the software). If non-educational use is prohibited by the software license, the users must make their own arrangements to obtain licenses for the software that are compatible with their requirements. (Cf. [MITnet Rule 4.](#))
- *Don't use Athena for private financial gain,* as by sale of the use of Athena resources (especially to anyone outside MIT), or by use of the system in support of any profit-making scheme not explicitly intended to serve Institute purposes. (Cf. [MITnet Rule 1.](#))
- *Access to Athena computing facilities is restricted to authorized members of the MIT community. Trespassing is prohibited and violators will be subject to removal and/or prosecution.* Authorized Athena users typically login to workstations using their Athena usernames. Individuals who login as "root" from the initial xlogin screen or otherwise use workstations without identifying themselves as authorized Athena users may be asked for proof of identification by Athena staff members responsible for the maintenance of Athena computing facilities.

Protecting Athena Equipment

Much of Athena's computer equipment is accessible to a large number of people and is consequently vulnerable to overuse and damage. The following guidelines are designed to help protect this equipment. In the event of any damage to the equipment, regardless of cause, please contact the Athena Hardware Hotline (at x3-1410) immediately.

A2. Don't eat, drink, or bring food or liquids into the Athena clusters.

Food crumbs and spilled drinks are the primary cause of equipment damage in the Athena clusters. This damage is produced not only in obvious ways (a spilled cup of coffee), but also in subtle ways (even the cumulative effect of sticky fingers or crumbs can ruin equipment -- keyboards have been damaged at the rate of one per day from food crumbs alone, and mice are equally vulnerable).

A3. Don't turn the power off on Athena equipment.

Turning the power off on Athena equipment (e.g., workstations, monitors, or printers) can permanently damage the hardware. However, if the equipment smells or looks like it is burning, do turn it off and contact the Athena Hardware Hotline.

A4. Don't reconfigure the cluster, either hardware or software.

Moving equipment will often cause damage, or may cause it to be reported as stolen. Permanent damage may

result from even unplugging a keyboard.

Similarly, altering a workstation's filesystem in any way may render the machine unusable, or threaten its usability in other ways. For example, you should not reconfigure any workstation in an Athena cluster to allow remote connections unless you are actually sitting at that workstation. Even an apparently "harmless" change such as this (i.e., changing the access configuration of a workstation) may create major system security problems, and may actually jeopardize MIT's ability to license software for users in the future.

Also, do not remove Athena equipment -- or furniture! -- from any Athena facility. Doing so constitutes theft and will be dealt with accordingly.

If you believe the configuration of a cluster needs to be changed, you can contact the Athena Hardware Hotline.

Assuring Fair Access to Workstations in Athena Clusters

Athena clusters are facilities provided for members of the MIT community to achieve their academic goals. As such, they are subject to principles of use that support those goals -- the chief considerations being fair access to the facilities for the widest possible set of users, and the maintenance of a comfortable working environment. The rules below reflect these considerations as they affect users of the Athena clusters.

These rules are easily summarized: *please show consideration to other users.*

A5. Don't violate the official priorities for the use of workstations; in particular, don't play games or engage in other non-academic activity if the cluster is busy, and don't log on to more than one workstation at a time.

In conformance with Athena's stated purpose, the priorities for use of the workstations in crowded Athena clusters are as follows (cf. [Rule A1](#)):

- **Highest Priority:** course-related work (including theses)
- **Middle Priority:** personal productivity work (including non-course-related text processing, sending mail, exploring the Athena system)
- **Lowest Priority:** recreational computing (including game-playing and general Web-surfing)

Note that games are the lowest priority software on the system -- you should not play games if there are only a few workstations free, or if people are waiting for workstations. If a user needs a workstation for higher priority work while you are playing games, that user can ask you to give up your workstation. (Low priority activities may actually be disallowed entirely during certain times of the year to assure that the use of the clusters is consistent with the academic purpose of Athena. At these times, you are expected to refrain completely from low-priority activities as defined above.)

Similarly, some clusters have workstations which are reserved for specific course use, or which have special features. If you are using such a workstation for other than its special purpose, and someone who needs its unique feature asks you to surrender it, please do so gracefully.

A6. Don't leave your workstation unattended for more than 20 minutes.

If you are using a workstation in one of the Athena clusters and intend to keep using it but must leave it briefly unattended, you *must* limit your absence to *20 minutes or less* and signal your situation to other users by taking one of the following actions:

- leave a note on the workstation indicating the time you left the machine and your intention to return, *or*
- run the screen saver from the **Panel**, *or*
- run another screensaver program which correctly displays the elapsed time.

(If you choose to use a screen-based timer, note that it is a violation of the rules to tamper with the system such that your display never shows that more than 20 minutes have elapsed.)

If you are gone longer than twenty minutes or leave a workstation without a note or a valid countdown screensaver running, another user who needs a workstation is entitled to log you out or reboot the machine to make that machine available.

At certain times of the year, this rule may be adjusted downwards (e.g., the allowable "time away" may be reduced, possibly to 0) to assure that the clusters are being used effectively and that users will not be without a workstation while machines sit idle.

A7. Don't make a lot of noise in the Athena clusters.

Athena clusters are similar to the MIT Libraries in that students who use these facilities have to be able to concentrate to do their work. Please don't play music, shout, or engage in loud conversation in the clusters.

Also, if you use a workstation that has sound capabilities, you are expected to use earphones rather than have the workstation audible to other users in the cluster.

Assuring Fair Access to Athena Printers

Printing is a shared resource; restraint must still be exercised when using Athena printers to ensure fair access for everyone to this important service. This holds especially true when the clusters are busy. Violation of these rules can result in loss of printing privileges.

A8. Don't violate the official priorities for the use of printers; in particular, don't be a printer hog or use the Athena printers as copy machines. The following rules apply to all Athena Cluster printers including those located in the Copytech Centers (Thesis and color printers).

- Don't use printers as copy machines. Print only **one** copy of a document. Use a copy machine to make multiple copies. The only exception is for printing one's completed thesis to the thesis printer. You are allowed to print two copies maximum of your thesis on archival paper. If additional copies are required, consult your departmental secretary.
- Do not overload the printer queue with multiple jobs that will take longer than 20 minutes total to print. Send the jobs in small groups over time and send them when the printer is not busy. Check the default printer queues by typing **lpq** at the `athena%` prompt. For jobs at printers other than the default, the printing commands (**lpr**, **lpq** and **lprm**) accept the **-Pprintername** option.
- Break large or huge jobs that take longer than 10 minutes total to print into smaller sections and send them to the printer individually.
- You are responsible for retrieving any jobs you queue to print. If you no longer want a job or will be unable to retrieve it, please remove it from the queue. Type **lprm -** at the `athena%` prompt.
- Do not remove unused paper from the cluster printers. That paper is provided solely for the use of that particular printer. If a cluster runs out of paper, please notify hotline@mit.edu.

- Color printing is a limited resource; use it sparingly. Color copying services are available in the Copytech centers to make additional copies.
 - Above all, be courteous in your use of the Athena printers. While these rules do not enumerate every possible violation of appropriate use of the printers, they do address the most common questions and concerns.
-

Comments and feedback to olh-suggest@mit.edu.

Last modified: 15 January 2004