

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Shmoo-Fu: Hacker Goo, Goofs, and Gear with the Shmoo

The Shmoo Group
www.shmoo.com



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



What's up Shmoo?

- Howdy & introductions...
- Our festivities will include:
 - IDN Fallout & Homograph Attacks for Personal Identities
 - Super Spy Stuff
 - Revving Up Rainbow Tables
 - Rogue Squadron & EAP Peeking
 - Shooting Your Security Wad
 - Don't Try This at Home
 - And MORE!

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Stickers anyone?



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



IDN Fallout

- At ShmooCon 2005, Eric Johansen dropped the browser bomb regarding IDN issues.
- The press ran with it a bit.
- The folks responsible for IDN ranted for a bit.
- But did anything concrete occur?
- And where are we now?

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



1337 Personal Identities

- So Ericj is now 3ricj, BTW.
- Oh snap. That rhymes.
- Where does the system break down when your name doesn't quite conform?
- Does 3ricj get more fan mail?
- Can the man keep your 1337 identity down?

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

And now... Pablos.



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Super Spy Stuff

- Robots got boring, so Pablos starting hanging out with models after his chic hacker photo shoot in FHM.
- The result was nothing short of spectacular, as the fashionable cell-phone stowaway strifes hot women face were finally addressed.



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

While Pablos discusses the alien technology inner workings of his secret ninja lair, you can stare at this...



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Dan Moniz goes crazy...



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

rainbowtables.shmoo.com

- We think rainbow tables are neat.
- Just for fun, we started hosting rainbow tables that we had generated.
 - LanMan
 - Via Bittorrent
 - FREE
- Some people liked that. Yay!
- Some people didn't...

DefCon 13



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



----- Forwarded message -----

From: Zhu Shuanglei <shuanglei@hotmail.com>
Date: Mar 10, 2005 12:42 AM
Subject: About your shmoo site
To: beetle@shmoo.com

Hi,

I am Zhu Shuanglei, the author of RainbowCrack software. I notice you are offering free BitTorrent links on your website for the rainbow tables. For those guys selling the table without permission from me, they are not welcome. But you are worse.

As you may know, I develop the rainbowcrack tool and release it the the public for free. I just want to introduce the technique to the world and those need it can benefit from this software. If I sell the tables, I am only making some money for my work and for the fee of hosting my website and for my computing resource. This should be quite reasonable. I am not a business man, if I am there will not be the source code or table generation tool free on the net and I can make a lot of money.

Are you feeling you are cool "Because knowing all passwords is cooler than trying to crack one. ;)". All over the world there will be a lot of guys can do what you do, they aren't. Do you know why? To show off prove neither your ability nor your knowledge.

If possible, please keep honour of my intellectual property of this software, and let those need the tables to generate by themself. If everyone act like you there will be no reason for me to develop this software further or develop other useful software. Or I will never release anything useful to the public.

Don't be crazy any more!

Best Regards,

Zhu Shuanglei

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Revving Up Rainbow Tables

- So, badass LanMan tables are online now via Bittorrent, and still for FREE.
- Sorry for the delay!
- Meanwhile, Dan decided to "be crazy" a bit more.
- We don't need your stinkin' code, Zhu!
- And Snax says, "FUCK OFF!"

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

New Wi-Fi kung-fu from Beetle...



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Why oh why do we Wi-Fi?

- Who here has an open wireless network at home? At work?
- Crap! My Tivo can't do WPA. Neither can my PSP. Ummm... does it matter?
- When and where should we Wi-Fi?
 - Coffee Shops? Airports? Hospitals? Banks? Ummm... Nuclear Power Plants?

DefCon 13



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Where did we go wrong? Where are we going?

- Technology of convenience versus the inconvenience of securing it.
- The poor, poor users were left out in the authentication cold.
- Half-ass security standards pass the buck and / or provide defacto insecure options.
- Security acronyms have taken precedence over proper implementation.

DefCon 13





"Choose a Mobile Network with Care."

For a low-priced mobile network, choose FI2G/FINNET.

Club World. More beds, more places, more often.

Hello Switch to Radiolinja for Elisa,
the Vodafone network in Finland.

Hello We've changed our name!
Radiolinja is now called Elisa, the Vodafone network in Finland.

Hello
larger

**"CHOOSE A MOBILE
NETWORK AT RANDOM!"**



Club World. More beds, more places, more often.

Hello Switch to Radiolinja for Elisa,
the Vodafone network in Finland.

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

How the FUCK does the user know?!



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment

Sc in di pr ur Pr (U Nt Vi er lik pr Et ha st to de ex st fr th In "s cc th Pr be de st cc by ev ac sp Sē th pr ac wl er pr th m er to ex Sē er wi ec

Access Point



SSID: "goodguy"

Stronger or Closer Access Point

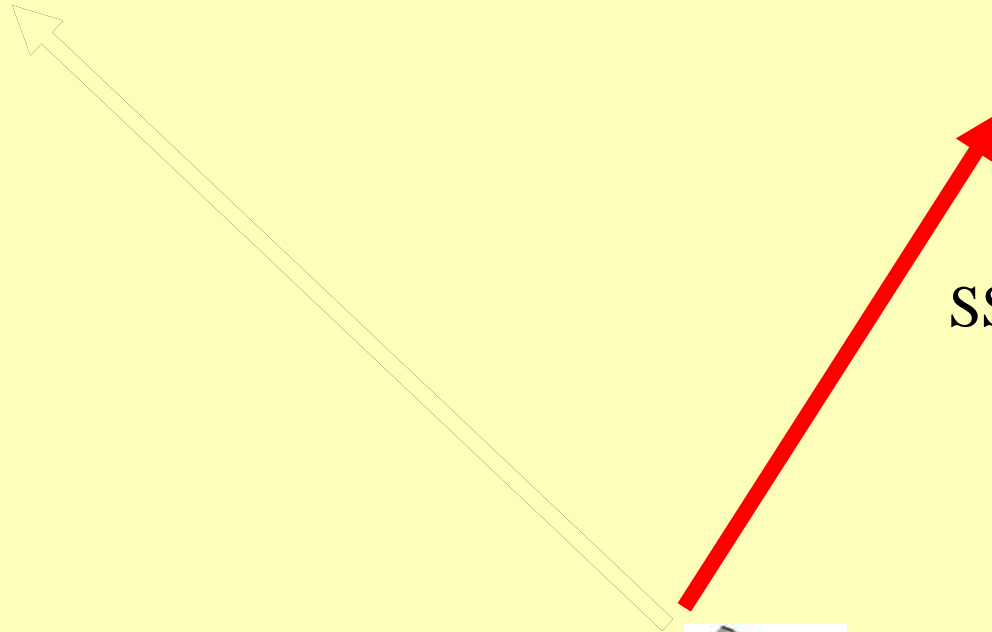


SSID: "badguy"



Wi-Fi Card

SSID: "badguy"



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Rogue AP Attacks

Choose your Wi-Fi weapon...

Normal Gear @
25mW
(14dBm)



Cisco Gear @
100mW
(20dBm)



Senao Gear @
200mW
(23dBm)



Use a 15dBd antenna with a Senao for 38dBd total...

6 WATTS!

VS 25mW?

BAD GUY WINS! NO CONTEST!

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Please sign in - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.hotmail.com

MSN Home | My MSN | Hotmail | Web Search | Shopping | Money | People & Chat

msn Hotmail

Sign-In New Account Sign Up All About Hotmail

What's Hot on MSN

Women: Be better listeners

Kate: Nudity OK with m

Make problem skin lo

Today's hot feature

How to tell b
you're pregn

Hotmail Spotlight

Winnie the Pooh
bumped to #2?

Hotclicks

Stop Spam
Browse with a buddy
Get parental controls
Manage your money
Share photos

MSN Hotmail Upgrade

It's here! New MSN Hotmail e-mail anti-virus protection.
[Learn more.](#)

Do not remember my e-mail address for future sign-in.
(Select this when using a public computer.)

Click Here!

Don't have a .NET Passport? [Get one now.](#)

Forgot your password?

©2004 Microsoft Corporation. All rights reserved. Terms of Use Advertise TRUSTe Approved Privacy Statement GetNetWise



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Con 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Con 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Rogue RADIUS

- Who says rogue APs can't be used against corporate wireless networks?
- There are plenty of ways to screw up EAP.
- FreeRADIUS provides a simple & easy way to accept EAP credentials
 - Integrates nicely with hostapd.
- Can allow for "EAP Peeking"...

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

EAP

Wireless
Wired



Supplicant



Authenticator

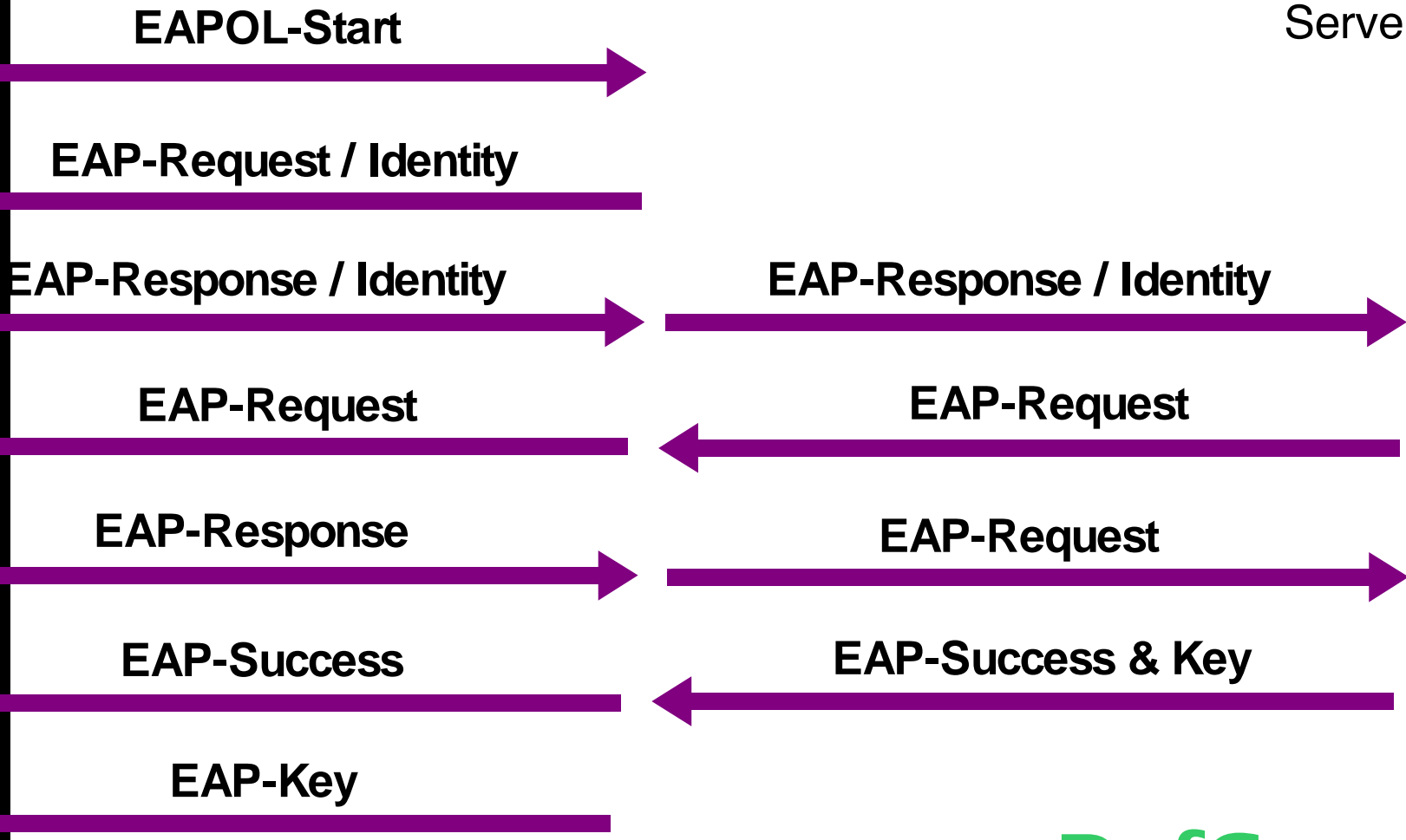


Authentication Server

The system in America...
Some in diss...
prod...
unde...
Priv...
(US...
Note...
Viola...

enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are...
which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



NOTICE TO LAW ENFORCEMENT AGENTS

EAP-TLS

Wireless
Wired

Supplicant
w/ Certificate



Authenticator



Authentication Server
w/ Certificate

802.11 Authentication & Association

802.1x EAP Protocol Exchange

802.1x EAP-TLS Protocol Exchange

EAP-Success

EAP-Success & Key

EAP-Key

DefCon 13



enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can have multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



NOTICE TO LAW ENFORCEMENT AGENTS

EAP-TTLS

Wireless
Wired



Supplicant



Authenticator



Authentication Server w/ Certificate

802.11 Authentication & Association

802.1x EAP Protocol Exchange

802.1x EAP-TTLS Protocol Exchange

Secure Tunnel Established

User Credentials Exchanged

EAP-Success

EAP-Success & Key

EAP-Key

DefCon 13

The system...
Some...
in...
diss...
prod...
unde...
Priv...
(US...
Note...
Viola...
enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statu...
In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such a...
access. There are civil actions which may be taken against law enforcement agents under pri...
fin...
thi...
mu...
email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before se...
equipment.



EAP-TTLS Weakness

NOTICE TO LAW ENFORCEMENT AGENTS

The system...
Some...
in...
diss...
prod...
unde...
Priv...
(US...
Note...
Viola...

enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored" electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which have been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Supplicant



Authenticator



Authentication Server w/ Certificate

Rogue AP + RADIUS



Previous EAP-TTLS Authentication Established

DISASSOCIATED!

802.11 Authentication & Association

802.1x EAP Protocol Exchange

802.1x EAP-TTLS Protocol Exchange

Secure Tunnel Established w/o Remote Certificate Check?

User Credentials Given Up?

DefCon 13



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is liable to recover at least the damages of \$1000 plus legal expenses. Aggravated states may not be able to recover from personal injury if they violate this statute.

In addition, the "stored communications" on this system are protected by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



EAP-TTLS w/ PAP Attack?

Wireless
Wired

Windows XP
w/ SP2



RADIUS
Server

EAP-TTLS w/ PAP
over TLS



Rogue AP w/
Rogue RADIUS
Server

1. Disassociate users.
2. Learn username & password.
3. Disassociate, copy creds to local EAP config.
4. Impersonate victim with legit username & password whenever.

DefCon 13

All Your PAP... Google for targets, if you like. ;)

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

All Your CAs... The "All or None" Vulnerability



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is liable to recover at least \$1000 plus expenses. Aggravated states may not recover from personal liability if they violate this statute.

In addition, the "stored" communications on this system are protected by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Wireless
Wired

PEAP Attack?

Windows XP SP2



RADIUS Server

PEAP w/ MSCHAPv2 over TLS



Rogue AP w/ Rogue RADIUS Server

1. Disassociate users.
 2. Learn DOMAIN and username w/ rogue AP.
 3. Disassociate, seed local password file.
 4. User continuously attempts to re-authenticate.
 5. Repeat #3.
- Authentication success = correct password guessed!

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

EAP Peeking Attack Demo



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Wireless Weaponry for Windows

- But rogue AP attacks require a “sophisticated hacker”, right? Wrong.
- SoftAP + TreeWalk + Apache + ActivePerl = Airsnarf for Windows
 - <http://airsnarf.shmoo.com/airsnarf4win>.
 - “Evil Twin Access Points for Dummies”
- But why only run one rogue AP, when you can run two... or three?

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Windows Rogue AP Attack Demo



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Rogue Squadron Demo



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Heeeeeeeere's Rodney!



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Shooting Your Security Wad

(Never let Beetle title your slides)



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Why is Rodney ranting now?

- Been doing product reviews (public and private)
- Keep seeing some incredibly lame product "features"
- There's a risk of FPGS (Ford Pinto Gastank Syndrome)



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Three Hard Questions?

- Does your product produce an external log?
- Do you have a security incident report mechanism?
- Does your product store it's key material securely?

Why are these hard questions in 2005?



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Don't make things worse

- Text t.b.d.



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Stupid Vendor Tricks

- (things you can't believe a security vendor would try to sell to a security customer.)

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Attacks you should try

- (Things you already knew that you should try on your security infrastructure)

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

How you can make things better

- (We're not the bad guys. We're trying to be educated consumers. Here's some things you can do to help make things better.)
- If you show how one of these possible flaws can be broke, submit to present it at shmoocon 2006)



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Did you want more gear?
Okey dokey.
CowboyM, show 'em what
you got.



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

New Gear Demo



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

And Bruce gets to rant, too!



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Bluetooth Security

- Things have gotten worse, not better
 - Millions more radios than last year
 - Several high profile vulnerabilities
 - Near zero focus from enterprises
- Trifinite.org's work
 - Bloover quite the uber tool

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Bluetooth Security

- Several other attacks via AT commands
 - Dialing, getting data, etc... not good things to do without authentication
- Pairing attacks, known for years, are now being coded and used
- WIDS still seems to equal 802.11 tho...
 - Gonna be a bad year for IT security



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Defending Wireless Networks

- We seemed to have covered a lot of ground on the Offensive.. What about Defense *boom boom* Defense!
- First there was Host Spot Defense Kit (HSDK)
 - Released BH Fed 03
 - Looked for directed rogue AP attacks against your client
 - OS X, Linux, and **Windows** code



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Defending Wireless Networks

- At the time of HSDK, there was NO capability for rogue detection in commercially avail software
- Today, we're still not much better
 - AirDefense Mobile, some other small stuff
 - Rogues are THE BIGGEST threat against enterprise networks
- So, while the industry is still finding their whatnot with both hands, we're making...



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Hot Spot Defense Kit v2

- Enterprise wireless IDS systems look for any attack, not just one directed at a particular client
- When you are on the road (or don't have the "luxury" of an enterprise WIDS) you need the same kind of protection



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Hot Spot Defense Kit v2

- HSDK v 2 aims to be an environmental monitor of sorts
 - Looks for any zip in the wire, not just ones directly effecting the client
 - If you're in downtown Baltimore, and someone starts shooting, you tend to freak out even if they're not shooting at you... wireless shouldn't be any different



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

HSDK v2

- Still under development
- Looking for:
 - Mass auth/deauth/assoc attacks
 - Fake AP signatures
 - Reinjection attacks (hard)
 - The standard rogue detection stuff from v1
- If something is detected, the green ball turns red (step away from the computer)
 - If security software isn't usable, it's useless

DefCon 13



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

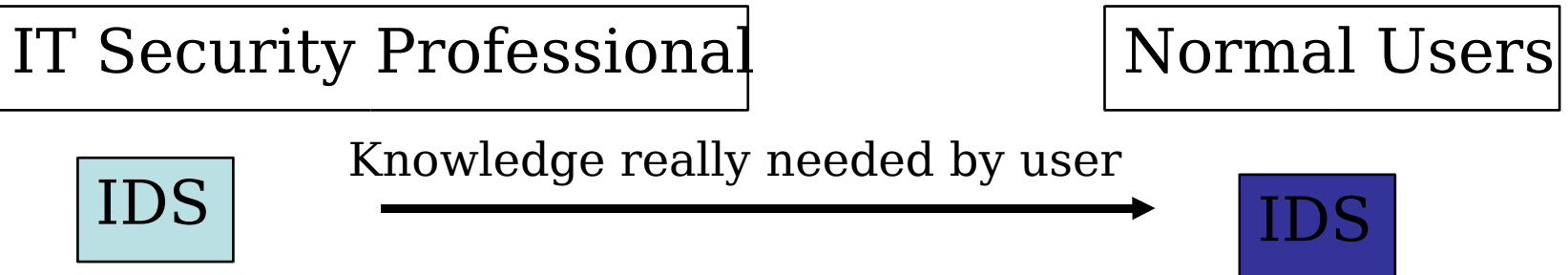
Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Speaking of...

- As security professionals, we sure haven't learned much
 - Security needs to be usable by the users
 - Users need heuristic decisions made for them and presented in red or green balls
 - Security admins need to act like professionals and have a real understanding of their operations



Host and Enterprise
INTEGRITY Monitoring

DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

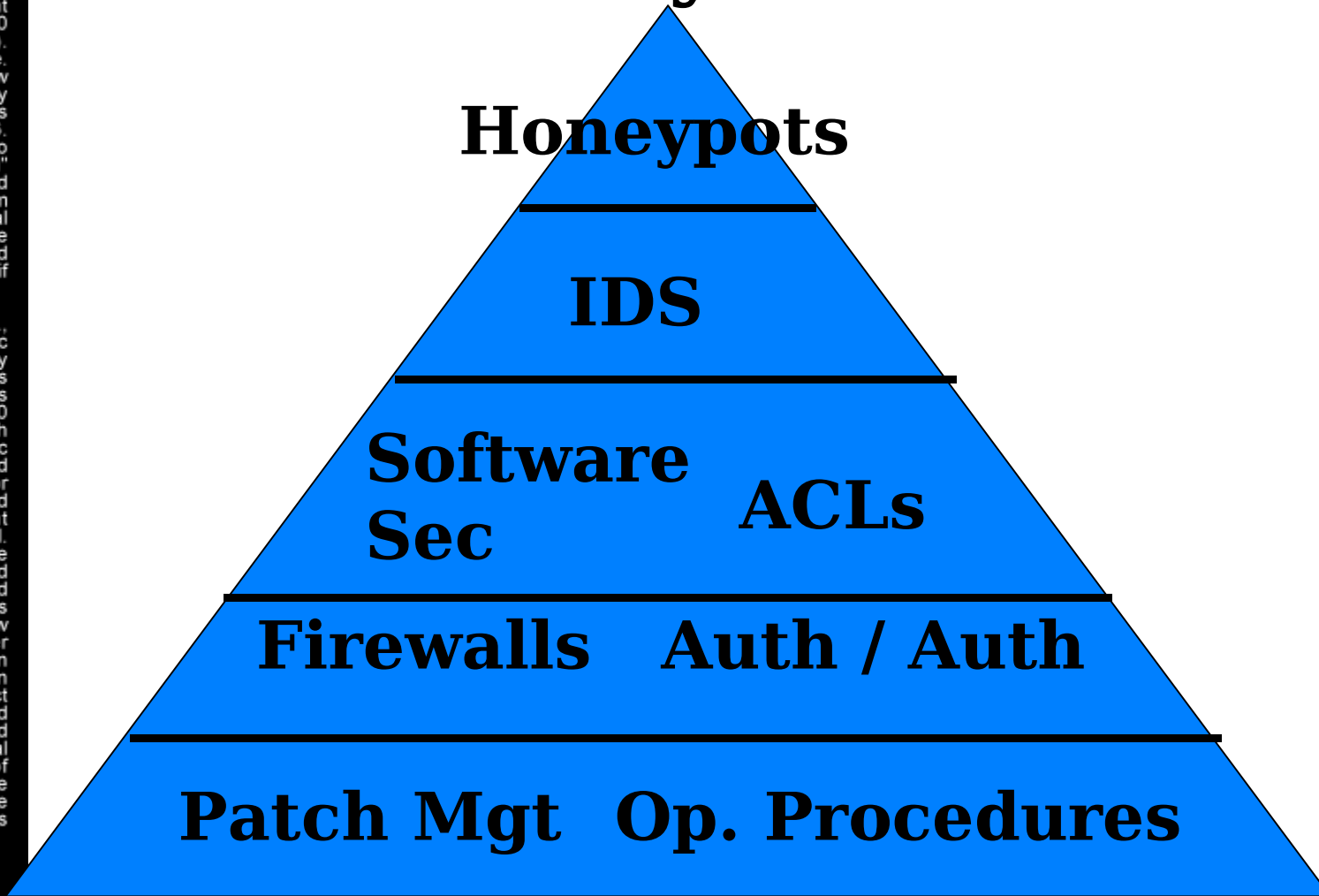
The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Potter's Pyramid of IT Security Needs



Sophistication and Operational Cost



NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Links



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Another Shmoo Announcement Goes Here



DefCon 13

NOTICE TO LAW ENFORCEMENT AGENTS

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.

Thanks! Questions?



DefCon 13