MSB00010011

Welcome to Defcon 15

Or 0x0F as I like to call it. Just rolls off the tongue.

This year has been a long and strange journey, as it is every year. Oh the stories we could tell. Well, actually we might just do that. We are starting to gather information for a DEF CON Coffee Table book.. think all big and glossy and full of pictures and crazy stories. Once it gets off the ground look for a call for stories and pictures. If you and your crew have something to contribute to the history of DEF CON send it to me. We hope to have it ready for next year!

Now that this is out second year at the Riv we hope to see how it works out. We all have had time to think about the space and how to use it better. One thing I have done is blow up the speaking tracks to a CrAZy five on Friday and Saturday. It's the most speaking ever, so let me know what you think. Also you will notice the most amount of contests ever.. and the first time an integrated mystery contest has happened since 'Find Leeto' at DC 7. There are clues in the program, conference CD, WiFi traffic, all over! Follow the clues...

Friday night there will be a World Premiere of Infest Wisely with the producer and writer here to give us the story behind the making of. Kind of reminds you of the Premiere we had of "Primer" years ago, doesn't it?

This year we continue to grow and evolve as the 'scene' changes, and as always the con is a reflection of what you make of it! When you get home don't forget to check in on the forums https://forum.defcon.org/, and upload all your pictures to https://pics.defcon.org/ to share the nub. Updated speaker material and PodCast formatted audio and video will be made available in a few months after we have all recovered.

The Dark Tangent

Table of Contents

Ode to the DefCon Badge

170 Hours of total time spent
2 Nights of my honeymoon (oh, how I lament!)
3 Circuit board revisions to get it all right
863,600 Total components bring them to light
6,800 Hackers wearing the badge in all its glory
If you want to learn more, please read this fine story

A matrix of 95 leds (5 columns by 19 row)
Two coin cell batteries make the current flow
Six text cutouts and soldermask colors to show
If you're a human, speaker, goon, vendor, press, or uber bro

On power up the badge will not make a peep
But fear not, that's by design, it is only asleep
Touch the top icon (it's a button, really)
And get a scrolling text message intended for thee

Touch the top icon yet again (just trust me)
And you'll move to the next mode for custom text message entry
Hit the bottom icon to begin your noble quest
Then use either icon to cycle through the list
Tap both icons to save a character to your queue
16 Letters long is the maximum we can do
When you're all done, seek out the solid block
Tap both icons again and on the screen your message will walk

The next mode sets the speed of your inscription
You can change it like a baud rate or a doctor's drug prescription
Select the scroll velocity between the numbers 1 and 5
Which goes from slow and boring to a thrilling autobahn drive
(Remember to tap both icons for the badge to come alive)

Next we arrive at our last badge state (finally)
A special treat known as persistence-of-vision or pov
Wave the badge in front of your eyes in one direction
And a secret message appears magically like the morning's first erection
If all you see is a jumbled mess of bright lights
Try hiding in the darkness, squinting your eyes, or changing those hard-coded bytes
(When your badge is not in use, set the mode back to snooze)

The source code is open and the schematics are free (as in beer)
So now you can be a hardware hacking engineer
Unpopulated footprints for a wireless transceiver and accelerometer
If you don't like how the badge acts, then hack it and make it better
(You might even win some development tools, a t-shirt, or a scarlet letter)

For the blood, sweat, and tears behind the scenes of the defcon badge
Come to my talk on friday morning, it's sort of like the hajj (ok, not really)
Business in front, party in back (yeah, that's a mullet)
I'm joe grand aka kingpin from the l0pht, a hacker not a poet

This year's badge is based around a freescale mc9s08qg8 microcontroller and contains a matrix of 95 surface-mount leds (5 columns by 19 rows) to allow user-customizable scrolling text messages. It requires two cr2032 3v lithium coin-cell batteries. Optional circuitry (fully designed, but unpopulated on the final badge circuit board) supports a freescale mma7260qt triple-axis accelerometer for motion-control applications and mc13191fc 2.4ghz rf transceiver for 802.15.4 Or zigbee applications. It's completely hackable. Wear it, use it, modify it, break it, learn from it.

Complete source code and schematics are on the defcon cd and also available at: http://www.Grandideastudio.Com

The software development environment, codewarrior development studio for hc(s)08 microcontrollers, is available for free (up to 16kb) from: http://www.Freescale.Com/codewarrior

Hardware debugging can be done with the spyder08 module (http://www.Freescale.Com/webapp/sps/site/prod_summary.Jsp?Code=usbspyder08) or p&e micro hcs08 multilink usb-ml-12 (http://www.Pemicro.Com/products/product_viewdetails.Cfm?Product_id=33)

The top three most obscure, obscene, mischievous, or interestingly hacked badges will be recognized and awarded at the defcon award ceremonies on sunday. Yes, it's purely subjective and I'm the judge. If you want your hack considered for the contest, show me your submission by 2pm on sunday. We'll have a table set up in the vendor area with a soldering iron, tools, and extra components for your hardware hacking pleasure, a development station set up for your firmware hacking pleasure, some folks from freescale and e-teknet for your engineering support and social interaction pleasure, and some t-shirts for your styling pleasure.

See you there.
Kingpin

The Network @ DefCon

Got Wifi?

WiFi Connections

802.11b/g – DefCon
802.11a – DefConA

Net access will be available in any of the convention areas (all speaking rooms, CTF, Vendors, Contest area, and the Top of the Riviera). We're planning signal coverage in the main hallways, but please don't create bottlenecks by grouping up along the walls (remember our friend the Fire Marshal?).

Bandwidth for everyone! We've contracted for 10Mb of bandwidth out to the Interweb. Remember to share!

As always, I have to thank the crew who sacrifices their con-time in order to make all this happen: Videoman(8 yrs), Heather(7 yrs), Sqweak (4yrs), effffn (3yrs), Connor (3 yrs), Derek/James/Mike(Rant Radio) (4 yrs), Major Malfunction (333 yrs).

Cheers!
Lockheed
(noc@defconnetworking.org)

p.s.. check out http://www.defconnetworking.org/ for post-con stats & wrap-up.

DefCon TV

This year DCTV is in your hands! Rantmedia, those crazy guys from Canada who've been handling DCTV for the last several years, will be providing a video drop box here at DefCon where you can upload videos from the con, the best of which will be placed on the DCTV network inside the convention. Upload will be via HTTP, FTP, and possibly even Bluetooth (on supported hardware, YMMV). We will also be videoblogging the event, and synchronizing the videos with Youtube as we go. Check the Info Booth for details!

If you have ideas ideas on how to make DCTV more fun next year, we'd love to hear it! Email us at dctv@defconnetworking.org with your ideas!

Amateur Radio

For all you radio geeks!

146.58 (FM Simplex) will be the unofficial Defcon 15 frequency for Amateur Radio enthusiasts.

Black & White Ball

Friday night

Black Ball

Industrial/ ebm / Noize

Dress: your best blacks. Bondage Rubber and Fetish Encouraged

Featuring :
Regenerator
www.regenerator.net

DJs

Patrice

Wintamute

SailorGloom

Great Scott!

Catharsis

Kriz Klink

And more ...

Saturday Night

White Ball

==Geekdom Release party==

Dress: Your finest stormtrooper suit, togas, bedsheets and the likes.

Featuring :
Miss DJ Jackalope // Jungle Chaos
www.dj-jackalope.com

DualCore // Live Nerdcore Set
http://dualcoremusic.com

***Minibosses // NES classics**
http://www.minibosses.com/

DJs

Rustcycle / Electronic live mix
http://www.rustcycle.com

Crashish // DNB

Casey // psytrance

Mitch Mitchem // breakbeat/electroclash

* scheduling tentative
All acts subject to change. please see a complete listing posted throughout DEFCON venues

Speaking Area 5, 20:30

Hello again everyone,

Once again I have been allowed some space in your Defcon program to say hi and represent the Defcon music scene. If you are new here or have only been once or twice, there is quite a lively underground music scene here that you may not have yet discovered. It comes to life through Shagghie's hacked musical badge from last year and the presents he brought for us this year, the PA system that is in the vendor room with the Green Sector crew and their cds, nerdcore from Dual Core, Big Beat Battalion at the EFF Summit, DJ Cmos banging out some housey breaks at a Ninja party, people sharing mp3 files off their laptops....you name it, it's all around you.

I plan to be present in it as well, helping organize what I can, helping out the skybox parties if they need it, letting the word get out that there are people putting on a show in such-and-such a space. I will be out, promoting our fun. I also am headlining the Ball on Saturday night.

Who am I? I'm that that demon DJ girl from the Black and White Ball you have seen since DC8, a DJ who has been spinning records for 11 years, a promoter of parties, a propaganda artist, guerilla marketer, student, girlfriend, and soldier in the information war.

If you want some more information on me, and some free dj sets I have to download, DJ-Jackalope.com is the place to go. For Miss Jackalope swag, I have a booth set up in the vendor room where the glow in the dark booth with the cool tunes is at. One more, don't forget to check out your CD that came with this program at registration.

Last note: don't forget that Defcon is your convention. You make it your own.

Got Pr0n?

Yes? Good for you. Got something more interesting? Compromising pictures of Feds hanging out in DEFCON's back alleys? [Insert 3v1l H4x0r name here] selling warez to script kiddies? The Dark Tangent on Con property during waking hours? Zac looking relaxed? Well don't Bogart the pixels... Share them on the mighty Bluetooth Wall of BLame! If you can 'Tooth it, we can host it... Video, Audio, ASCII Art or plain old-fashioned vanilla camera images are all welcome where you see the sign "DEFCON Wall ofBLame"... don't be Lame... Share the Blame!

DefCon Pics

pics.defcon.org is now live for use.

What is it you ask? Think of it as a repository for all pictures related to DEF CON. It is a place you can upload your pictures and arrange them however you want. Others can comment on them, vote, or put them in their own favorites album.

The idea is that as people change providers there is no long term repository for DEFCON pictures except to the links www.defconpics.org points to. Because they don't mirror the content I wanted to create a free place for people to share their pictures that won't change or go down.

The pics software is integrated with the defcon forums, so if you already have an account there you automatically have an account on pics.defcon.org.

So get busy! Upload those pictures. both http and https connections work. Spread the word! Share those interesting con photos now!

11011000

Unscramble the letters to fill in the blanks using the clues provided.
Use the letters in the circles to fill in the final set of blanks.

ISRLEWSE RNEEHTET — HINT: IEEE 802.11?

□○○□□○□□ □○○□□○○○

TIREN-GXENHACE RIRCERA — HINT: IXC?

□□○○□-□□□○□□○□
□□□□○□□

OLTL UDARF — HINT: RIPPING OFF BELL?

□○□□ ○○□○□

LITESTXEF — HINT: FOUND ON BBS'S?

□□○□□○□□○

CLUED

A [PAPER]CHASE GAME

DESIGN BY PINGUINO
WWW.PENGUINPALACE.COM

HINT: MARGINALLY OBFUSCATED

□□□.□□□□□.□□□□□□□□.□□□□

An IP address is a 32-bit number which is used to identify hosts on the Internet. The address is broken into four octets, or groups of 8 bits. Each octet can have a value of 0 through 255. in binary, The value is denoted by adding the values of the bits in the octet which are set to 1 (or true or on - as opposed to 0 which is false or off).

Bit Position Number	7	6	5	4	3	2	1	0
Value if Set On	128	64	32	16	8	4	2	1

So, an octet of 0000 0010 is equal to 2, while an octet of 0000 0101 is equal to 5.
(For those of you pendantic souls, we are stipulating version 4.)

00011011

New DefCon Contests!

Øwn the box? Own the box!

Are you a defensive ninja? Are your services unbreakable, your builds airtight? Do your countermeasures have countermeasures for counter-countermeasures?

So prove it, bucko... Bet your box on it, on the most hostile network in the world.The first person to take you down walks away with your gear. When you're øwned, you're owned. It's that simple.

For the other side of the fence, the reward is clear... Pick your target, bring your best sploits, own the box, and own the box. A shopping spree for the elite.

CONTEST RULES: Entries will be placed on the DC LAN. See the IP ranges advertised on the ØTB (Øwn The Box, not Off-Track Betting) scoreboard for the available targets. Each target could be just about anything, you'll just have to øwn it to find out. We have everything from high-end server gear and laptops to 386's, a NeXT box, and some other freaky stuff. Targets of special interest ("Øwn a goon, Øwn a presenter, Øwn the DOD") will be marked as such.

DAY 1: At the start of the contest, your access will be as an outsider. Your mission? Compromise the box, any way you can, and find the one-time-pad to decrypt the ciphertext for that defender entry, in the ØTB directory of the con CD. If you own Box 1, your key will decrypt the Box 1 ciphertext. Box 2, well, you get the idea.

Once you have the decrypted ciphertext, find a connection somewhere, and mail it to owned.the.box@gmail.com -- this way we have proof and a timestamp of who got to it first. Defenders are *supposed* to put one time pads in a directory called "owned", but hey, they're giving up their gear, so they *might* decide to make things interesting. Who knows?

DAY 2: Now, it's a whole new ballgame. Everybody gets creds! Every defender entry will give out some level of authenticated access. We didn't say what, and it might be nothing of value, but it might be a lot. You'll just have to log in and find out.

Winning attackers get hardware, for free. You're absolutely not required to share your super-secret Mossad-authored remote kernel-level 0day with the person you øwned, but it would be considered good manners. If you compromise a presenter, you may also be asked to come onstage and talk about how you succeeded.

Successful (and failed) defenders get t-shirts. Everybody else gets to bask in the glory of high-stakes attack and defense with the best defensive aikido and attacker ninjitsu around.

Guitar Hero II Contest

Are you a Guitar Hero? Do your friends think you're l33t and can shred like a rock star? Then prove it! For the first time at Defcon, you will have your chance to pound out a great solo and earn points enough to make it into the finals!

The contest will allow contestants to show their skills playing Guitar Hero II on Xbox 360. Medium, Hard and Expert levels will be offered. Initial heats will be a cumulative score of possibly 2 user-chosen songs. The top 4 from each level will go at it 'tournament' style final, head to head, until only 1 player remains.

Signups will be friday, august 3rd, 2007, 11am - 12pm in the contest area. The pre-con signup roster is up in the dc-forums.Entries in the contest will not be taken after 12pm on the friday of con!

Schedule:
FRIDAY
FREEPLAY: Friday, August 3rd, 2007, 11am - 12:30pm, Contest Area
Medium Heat 1: Friday, August 3rd, 2007, 1pm, Contest Area
Medium Heat 2: Friday, August 3rd, 2007, 2pm, Contest Area
Medium Heat 3: Friday, August 3rd, 2007, 3pm, Contest Area (if needed)

SATURDAY
FREEPLAY: Saturday, August 4th, 2007, 11am - 12pm, Contest Area
Hard Heat 1: Saturday, August 4th, 2007, 12pm, Contest Area
Hard Heat 2: Saturday, August 4th, 2007, 1pm, Contest Area
Expert Heat: Saturday, August 4th, 2007, 2pm, Contest Area

FINALS!
Finals Medium: Saturday, August 4th, 2007, 3pm, Contest Area
Finals Hard: Saturday, August 4th, 2007, 3:30pm, Contest Area
Finals Expert: Saturday, August 4th, 2007, 4pm, Contest Area

Clued

Defcon 0xF - 2007 - Las Vegas Riviera. Vaclav is on the run.
Find the words.
Follow the Clues.
Save Vaclav.

How to play: Information is everywhere. Solve the puzzles, solve the mystery.

Brew Wars

The very first Brew Wars will happen this year at Defcon 15.The rules are simple. Just bring twenty four ounces of your home brew to Defcon. The beer will be rated on a scale of 1-10. Each beer will be judged in it's category. The standard of each category of beer is last year's winner of the Great American Beer Festival in the style you have entered.

Phreaking Challenge

"You wanted it, you got it! Announcing the inaugural old skool/new-school Phreaking Challenge. Bring your ear for tones, we'll supply the beige box. Test your elite skillz on several tasks drawn from traditional telephony and VoIP."

Here's how it works:
We'll provide butt sets and phones. You bring a laptop, your ear for DTMF, and all the knowledge you have. Bring a friend and pool your skills.
-You'll complete 3 tasks per round.
-Each task is scored.
-If you're not satisfied with your scores, you can come back and retry the tasks for that round (on that day). One do-over only, though, and only for the first two rounds.
-Round three is a first to the finish set of three related tasks.
-Prepare to clip in, listen well, social engineer, and do a little VoIP hacking.

Toxic BBQ 4

The fourth annual Toxic BBQ will occur August 2nd, 2007, Sunset Park, Las Vegas, NV.

Food Run: 3pm (More Info)
Pre-BBQ Contests & Events: 3pm
BBQ Kickoff: 6pm-Park Closing

What About Weather?
This Event Will Take Place Rain or Shine.

How Much Does It Cost?
The Toxic BBQ is FREE. Contribute something to the BBQ, Such as food, or donation.

Titanium Chef

Cost to Participate:
$40 per team
Prizes for Winners:
OiNK invite for each team member, secret grand prize, refund of entry fee, extreme bragging rights Free giveaways of fun stuff to all participants.

Teams of up to three individuals will put their heads together and engage in heated battle to concoct a delicious dining experience focused around a secret theme ingredient. These hacker chefs will have both their culinary skills and their organizational abilities put to the test in this challenging event. All par-ticipants will gather together a few hours before the Toxic BBQ in order to witness the revealing of the event's secret ingredient, then they will disperse in order to gather supplies, reach Sunset Park, and prepare their food for the judges. Whose cuisine will reign supreme? Will opponents' grill-fu be stronger than you? Participate and find out!

Guess the Flesh

Cost to Participate:
$10 per person
Prizes for Winners:
OiNK invite for first three people to correctly identify all meats Free giveaways of fun stuff to all participants

Have you ever thought to yourself, "Gee, I wish I could dine on the meat of nearly every kind of beast to walk the earth... but I don't own many high-powered firearms, i don't have the money to travel the world, and no government in their right mind would issue me a hunting license?" Well, now your dreams can become a reality. For less than the cost of what passes for a movie and popcorn nowadays, you can have a sample platter featuring eight meats that you aren't likely to see at the supermarket. However, instead of just cooking and randomly giving out samples willy-nilly, this year I have something new planned. I intend to prepare morsels of these meats and plate them in a way that they are not immediately identifiable or distinguishable from one another. Those who are eager to try some new flavors -- and those who think their pallets are up to the challenge — can take a whack at identifying these various animals by taste and texture alone.

DefCon 15 Contests

aCTF 3
"King of the Hill"

Not to be confused with the original Capture the Flag (CTF), aCTF is organized by DC949/ Orange County for amateurs.

We created the accounts for the Local Exploits box and e-mailed the account info out to all the registered teams. If you want to play but haven't registered, check with us at con. As long as things are going smoothly, we'll continue to give out accounts at con after the contest has started, so don't worry if you didn't register... you'll still be able to play.

We will be changing a few things around this year, but the basics will be the same as before. Find a flag, find a way to put your team name on it, and you'll score points for as long as you can keep your flag up there.

As usual, details on the contest will be limited, however we will say that we're branching out a bit more this year. Hacking isn't just about buffer overflows and running metasploit, it's really about one upping someone (or everyone) else. It's about figuring out how things work and taking them apart and putting them back together to do something different, customizing things to make them do things they were never intended to do, and just generally learning how to beat the system.

CTF

Capture the Flag: The qualification round for this years CTF is complete. More than 150 teams were actually submitting answers which means that participation for this year was more than double the previous high water mark (as far as we're aware). Results may be found at http://www.kenshoto.com as always.

This years challenges came in a wide range of technologies and difficulties. No single team actually solved them all... Additionally, this years level of international participation was staggering...

The MUD for this year will remain up for teams to ask questions and hopefullly collaborate with each other about how they came to solutions for some of the harder challenges. Additionally, we will be putting most if not all of the challenges back online for a while so everybody can sharpen up... Stay tuned...

VISIT THE CTF ROOM TO SEE THE TEAMS IN ACTION!

CTF 2007 Qualifiers Final Scores
1 loller skaterz dropping from rofl copters! (6600) -Stepped Down
2 sk3wl of r00t (6500) -Qualified For Defcon
3 Song of Freedom (6100) -Qualified For Defcon
4 Mighty Morf'n Power Haxor (6000) -Stepped Down
5 FEDNAUGHTy (5900) -Qualified For Defcon
6 [0x28]Thieves (5900) -Qualified For Defcon
7 Routards (5800) -Qualified For Defcon
8 Osu, Tatakae, Sexy Pandas! (5800) -Qualified For Defcon
9 our wives are pissed (5400) -Qualified For Defcon
10 ShellPhish (5400) -First Alternate

The LosT@ Con Mystery Challenge

The LosT@Con Mystery Challenge returns to Defcon 15- will you complete the challenge?

The mystery challenge is just that—a mystery. Details of the contest are not given until the contest starts. So take the dare, and enter a contest where you are flying blind.

So you heard about the challenge, and think you can compete? Search for hints and clues carefully, even prior to Defcon.

Suggested Skillset for success:
-Physical security (Lockpicking, literal hacking, etc)
-Electronics (reading schematics, breadboard prototyping, etc)
-Puzzle and Riddle Skills
-Coding, networking, hacking...
-???

Coffee Wars

Submit your beans and become a part of our mighty quest; we'll make sure you get a steaming cup of the very same brew we're savoring. 8th year! Organized by Shrdlu and Foofus.

LPCON5
Lockpicking Contest

Once again, DEFCON will be hosting the CON within a CON. Lock Picking has gotten a great deal of interest over the last 5 years and the contests have proven to be very popular. Once again LPCON will be composed of two primary events. The timed Lock Picking SkillZ Contest and the Lock Picking Points Contest. In addition, LPCON will be running the Lock Picking Village in the Skyboxes. Their will be opportunities to listen to talks, demonstrations, and to practice your skillz on multiple different types of locks from easy to very hard.

The timed Lock Picking SkillZ event will be composed of three elimination rounds consisting of multiple 6-contestant heats over two days. This event is held on the contest floor. The final event will be a competition among the 4 fastest times and will be done on the now infamous "Tower of Terror". Rules will be posted on http://www.securitytribe.com/~doc/lpcon5.

The primary rules are:
you must use manual picks (plug spinners are ok) and no destroying the locks. Check the schedule for time and location, but the plan is for 1pm-4pm on Friday and Saturday for this event. Please signup either by emailing doc-lpcon at hotmail dot com or by stopping by the Lock Picking Village Friday morning before 12 noon.

The second event is the Lock Picking Points Competition. Here you will earn points based on different locks that you pick in the Lock Picking Village. Some will be easy, some hard and the lock picking team will track your scores throughout DEFCON with a prize awarded to the top point getters. You can only get points for each lock once. Sign up for this competition in the Lock Picking Village anytime while we are open.

Lock Field Stripping Competition: Contestants will have opportunity to disassemble and reassemble locks as quickly as possible. There is expected to be 4 Rounds of competition and everyone is welcome to participate. Locks grow increasingly complex with each round. Competitors should expect to see: Master Wafers, Sidebars, Control sleeves, etc. Competitors must COMPLETELY disassemble each lock in each round, display their disassembled lock to a judge, then reassemble.

If the appropriate key no longer operates the lock, they are automatically disqualified. The slowest competitors will be eliminated each round, the exact number eliminated will depend on the number of participants. Participants will be expected to pick or shim their locks open, shims and picks can both be provided if needed. Everyone will receive a cardboard pinning tray to help them avoid losing parts. If, after 5 minutes, anyone has been unable to pick or shim their lock, a key will be provided for disassembly.

The final round will consist of the top 2 competitors from the previous rounds.

Both will be attempting to pick/shim a high security lock to be revealed at the event. If they desire, specialized tools will be provided to each competitor to help in the picking process.

Each competitor gets to keep their first round lock, just for participating, and the first and second place winners will receive prizes.

Don't have picks? No Problem – picks will be available for sale by vendors in the vendor area. You should be able to find picks with LockSport International (LSI) or Toool-USA Please help support the team that puts all the work into making the lock picking activities possible by planning to get your LPCON 5 t-shirt or other commemorative items.

DEFCON Bots

The DefconBots contest pits two fully autonomous robotic guns against each other in a challenge to see who can shoot down the most targets in a shooting gallery the fastest.

Scavenger Hunt

Scavenger Hunt- The scavenger hunt IS on! Get thee to the Info Booth to get started!

"I heard it's 150 points if they get the bed out of Cotman's room and make him sleep on a cot."-astcell
Nuff Said.

Hacker Jeopardy

Is back again this year! (Like we could stop it) Check it out 22:00 to 01:00 in speaking area 2 Friday and Saturday Night! Finale starts at midnight Saturday!

TCP/IP Drinking Game

Javaman— Adam O'Donnell will be guest hosting the TCP/IP drinking game this year. See the game in action Saturday Night at 21:00 in Speaking area 3!

(Wardriving) Wireless Contest

Announcing The DefCon 15 Wireless Contest (queue Thus Spake Zathrustra)

Are you a freq-geek? Think your WiFiFu is hot? Get high from sniffing packets on the ether? Think you're a great lover? We can't help you with the last one, but get ready because here's your chance to prove the rest of those outlandish claims to the world.

Compete in the Wireless Contest, and we can validate you self esteem, at least in the geeky stuff.

The Wireless Contest, following the format for the past few years, will be a series of "Mini-Contests". You can compete in only a single mini-contest or all of them. We recommend that teams be formed to fill in different skill areas.

"Beverage" Cooling Contraption Contest
Take a room-temperature beer and cool it down to proper drinking temperature! Well...It's a little more complicated than that.... Check it out from 12:00 to 14:00 in the Contest Area.

Beverage Cooling Contraption Contest

Take a room-temperature beer and cool it down to proper drinking temperature! Well...It's a little more complicated than that.... Check it out from 12:00 to 14:00 in the Contest Area.

Spot the Fed

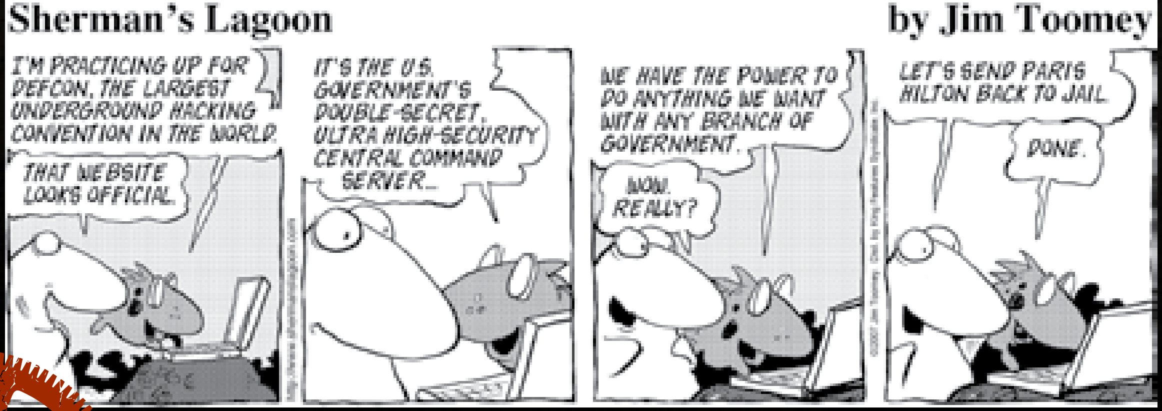
Of course you know they walk among us, these badge-wielding, security-clearance having dot gov types. You've got the warning signs down, from the haircut to the tucked in shirt, from the shifty eyes to the sun-kissed skin. There's really only a few questions left. Do you have the stones to make your suspicions public? Do you have a line of questioning that will force your quarry's hand? Can Priest make your target crack and win you the rare and coveted "I Spotted the Fed" t-shirt?

To get in the game, you need to alert Priest of your discovery. He can be reached in person, via the Goon team, or through the info booth. If you get Priest and point the FED out to him, and you have the stones to do it, get the FED up on stage for a crowd vote on whether they quality or not!

As always, we are not looking for "pseudo-feds." There are more than enough gun and badge types with arrest powers for this contest, so civilian contractors and off-duty military don't qualify.

Spotted Feds
In return for the good-natured ribbing you will receive from the con attendees, those Federales whose covers have been blown receive the equally treasured "I Am the Fed" shirt. Let the soft, fluffy cotton blend soothe all the hurt away.

Un-spotted Feds
Are you a Fed so crafty you remained unspotted? Did you get the DC pallor down so well that we think you're one of us? Rumor has it that contacting Dark Tangent directly (I know, good luck) in some quiet place will get you on the mailing list for your own "I Am the Fed" shirt. If you have schwag to trade you need to find Major Malfunction, DT's official Avatar for trading goods. Of course, this might get you spotted, so be stealthy in your movements. Major Malfunction also has access to the list - but if you're as good as you think you are you can definitely find DT.


Sherman's Lagoon
by Jim Toomey
I'M PRACTICING UP FOR DEFCON, THE LARGEST UNDERGROUND HACKING CONVENTION IN THE WORLD.
THAT WEBSITE LOOKS OFFICIAL.
IT'S THE U.S. GOVERNMENT'S DOUBLE-SECRET, ULTRA HIGH-SECURITY CENTRAL COMMAND SERVER...
WE HAVE THE POWER TO DO ANYTHING WE WANT WITH ANY BRANCH OF GOVERNMENT.
WOW. REALLY?
LET'S SEND PARIS HILTON BACK TO JAIL.
DONE.

Events

Dunk Tank

Dead Addict Dunking Jim Christy

"Dunk a fed for Charity!"
12:00-21:00 Friday and Saturday at the outdoor chill out area.
12:00-15:00 on Sunday.

Once again the Dunk Tank will be here, you can dunk a friend or foe to help raise money for the EFF. Please help this government watch dog that is protecting our privacy. One of the EFF's current endeavors is fighting the White House and NSA from tracking who you have conversation with. All proceeds benefit the EFF's fight to protect your digital civil liberties. All contributions are tax deductible and receipts will be available.

theSummit

theSummit is a fund raiser for the EFF and The Hacker Foundation. It will be held Thursday August 2nd, 2007 in the Skyboxes of event center. For more information regarding this event, check out the Official Website: http://www.vegassummit.org/

Forum Meet

Who is this Cotman? Who is this High Wiz person they speak of? What is a Converge and how will it affect me? Come to the Forums meet and Find out! Meet the people you stalk online, and be sure to wear your Avatar badge. :-) So we can hide..I mean recognize you.

6th year anniversary Forum meet will be held- Room 115 Friday night at 20:00-23:00

QueerCon

You're smart, you're cute, and you think boys kissing is hot. Well, we think you're awesome! Join us on fabulous Friday for friends and fun...

>> the mixer <<

4pm-7pm, Skybox 211/212: Kick back, relax, and enjoy great drinks and lively conversation in a casual atmosphere. We'll be giving away free swag, and your first drink is on us! [21+ w/ID to drink, glbtq please]

((club queercon))

10pm-late, Skybox 205: What happens when you combine top-notch underground hacker DJs with a bumping sound system and a crowd of incredibly awesome people like you? Only the most amazing dance party EVAR! :)
[all ages, glbtq+friends]

Wireless Village

The Church of WiFi excitedly presents the Defcon 15 Wireless Village. Topics could include but have no limitation: 802.11x, 802.16, Bluetooth, IR, CDMA, GPRS, Amateur Radio... think it, do it! The sub-con will be home of amazingly super-krad breakouts, demos, contests, and the finest invisible hand-on activities folks can dream up between now and August. http://www.churchofwifi.org . Located in Skybox 209 Friday through Sunday

Lockpicking Village

This is where there have been lockpicking, presentations, impromptu peer-education, sample tools, practice locks, and fun! This event has included local and remote support of people from TOOOL, TOOOL-USA, LSI, and more. Located in Skybox 210 Friday through Sunday

Prototype Hacker Spaces

Hacker Spaces: It's time to make them a reality. That's the goal of the Defcon "Prototype Hacker Space". It's time to clear out your rooms, garages, and basements, get your local hacker scene organized and start building an infrastructure for the future.

Sponsored by the Hacker Foundation as part of the Hacker Spaces Initiative, the PHS is designed to show you what a collective hacker space looks like and provide you with information and inspiration to start your own. Walls of whiteboards, workbenches, tools, server racks, and couches surround a multi-use meeting space with projector, sweet sound system and Nintendo Wii all for public use. Need to quickly solder something? Want to put your desktop on the network and not worry about watching it? Looking for a space to have your DCG meeting? Need to prove your point, show the slides you didn't get to or continue your talk on a 12ft x 12 ft whiteboard? Stop by the PHS!

Throughout the day and night, representatives of the Hacker Foundation will be on hand to explain the various ways hacker spaces could work where you live. We also want to hear about your local hacker space and learn about the ways you're using your space to connect with your community.

We're also raising money! HSI is building a permanent public use hacker space in Washington DC, the first of what we hope will be a nationwide network of hacker spaces. We hope you'll stop by and take part in our WII BOXING TOURNAMENT and consider donating to any of the many projects sponsored by the Hacker Foundation. We will be able to provide receipts for tax purposes on site! Do you have a non-profit hacker project?

The PHS will also serve as the DefCon headquarters for Hackers on a Plane. Nearly 40 people have signed up to take part in this historic event bridging the world's largest hacker conventions, Defcon and CCCamp! Stop by to check out how we're pulling off the world's first transcontinental hacker conference!

Hacker Foundation

DefCon Movie Night

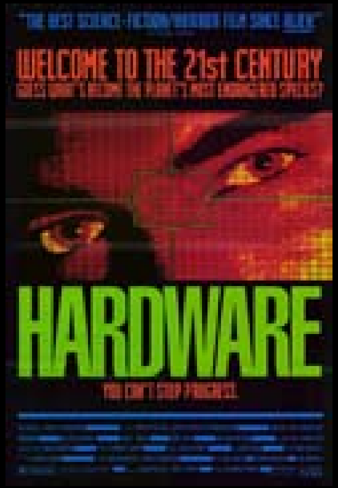
Movie Night will be held in speaking area 1 at 21:00 Friday and Saturday Nights.
Friday- WORLD PREMIERE "Infest Wisely"
Saturday- "Hardware" & "Calamari Wrestler"

Friday:

This year's Defcon Movie Night will feature the WORLD PREMIERE of the new and highly buzz-worthy film "Infest Wisely." The film is centered around the increasingly less science-fictional world of commercial nanotechnology and it's been described this way:

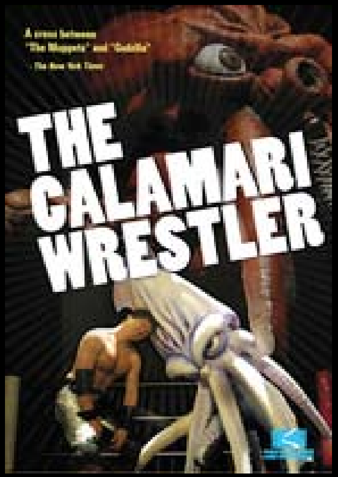
"Infest Wisely asks what would happen if Critical Mass teamed up with the geeks from DefCon to stop commercialized nanotech from taking over our bodies and the world."

It's a feature length movie in seven episodes, each with different directors but all written by novelist Jim Munroe, who will be our special guest for the screening. As always, there's no charge - come join us and support cinema licensed under the Creative Commons. For more information about the film, you can check out its website. http://www.infestwisely.com/


"THE BEST SCIENCE-FICTION/HORROR FILM SINCE ALIEN"
WELCOME TO THE 21st CENTURY
HARDWARE
YOU CAN'T STOP PROGRESS.

Saturday:
For the first movie of Saturday "Night at the Movies with DT" I was digging back to old almost obscure classics. The movie Hardware came to mind. I haven't seen this one in a decade I bet! Hitting Amazon I realize there is a reason I haven't seen it! It isn't available anymore, and I ended up paying $100 buck for a used copy. I hope it plays ok, I'm still waiting for it in the mail as I write this. The movie is definitely lo-fi, keeping in the tradition of last nights premiere, and is best viewed in a slightly altered state. From the movie:

> In the future, a nuclear war has transformed the Earth into a radioactive wasteland where the sea has dried up leaving it as a post-apocalyptic desert. In the desert, A desert scavenger named Nomad discovers a robotic head, arriving in New York City, A space marine named Moses Baxter buys the robotic head from Nomad as a Christmas present for his girlfriend Jill Grakowski, who decides to use it for one of her sculptors. But all hell starts breaking loose, when the robotic head is activated and begins to rebuilt itself. When Alvy, a junkyard dealer discover the robotic head is a Mark 13, a military cyborg of a project that was abandoned. Moses learns Jill's life is in danger, as the Mark 13 cyborg goes on a violent rampage in Jill's apartment as Jill has become the the prime target for extermination.



It's not every movie that can get the stuffy old New York Times to gush, "Goofy, bizzarre, yet surprisingly coherent." Then again, it's not every movie that centers around the exploits of a giant squid that makes his name in the wrestling ring.

There is a plot, but it's fairly bizarre. There are other odd fighting creatures, including something that might be some sort of crawfish.

There is love, and there is betrayal. There is a climactic battle scene for the ages. If there is something more you need from a movie, I don't know if we can be friends.

Defcon movie night is proud to bring you "Calamari Wrestler" - Minoru Kawasaki's entry into the grand tradition of Japanese rubber-suit monster movies. You know in your heart of hearts that a good rubber monster asskicking with subtitles beats a Michael Bay CG crapfest anyday, so join us. More whimsical than "Godzilla", more realistic than "Gamera" and more uplifting and humane than "The Grudge," we feel certain that you'll leave the screening practicing wrestling moves and maybe craving a little Ika Nigiri.

Focus on: Bruce Schneier

We at DEFCON thought it might be wise to forewarn you to be prepared for one of our speakers in particular this year. Bruce Schneier. This year Bruce will be doing a Q&A Session. If you are unprepared for this encounter, expect confusion nausea and shooting pains in the unused part at the back of your brain. Expect to bask and wallow in the reflected glow of his pure leetness. Expect to have your fragile mind blown, reassembled and then mercilessly re-blown.

Though a superhero, Bruce Schneier disdains the use of a mask or secret identity as 'security through obscurity'.

Bruce's Bio reads:

> "Bruce Schneier is an internationally renowned security technologist and CTO of BT Counterpane, referred to by The Economist as a "security guru." He is the author of eight books — including the best sellers "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," "Secrets and Lies," and "Applied Cryptography" — and hundreds of articles and academic papers. His influential newsletter, Crypto-Gram, and blog "Schneier on Security," are read by over 250,000 people. He is a prolific writer and lecturer, a frequent guest on television and radio, has testified before Congress, and is regularly quoted in the press on issues surrounding security and privacy."

But here are some additional "Facts" about Bruce that you should be armed with before it's too late.

Bruce Schneier knows Alice and Bob's shared secret.

When Bruce Schneier wakes up in the morning he passes an encrypted stream.

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone else for days.

If we built a Dyson sphere around Bruce Schneier and captured all of his energy for 2 months, without any loss, we could power an ideal computer running at 3.2 degrees K to count up to 2^256. This strongly implies that not only can Bruce Schneier brute-force attack 256-bit keys, but that he is built of something other than matter and occupies something other than space.

Bruce Schneier writes his books and essays by generating random alphanumeric text of an appropriate length and then decrypting it.

Bruce Schneier can log into any computer just by staring down the prompt.

Most people use passwords. Some people use passphrases. Bruce Schneier uses an epic passpoem, detailing the life and works of seven mythical Norse heroes.

Bruce Schneier is the reason why Leeto is hiding.

When Bruce Schneier observes a quantum particle, it remains in the same state until he has finished observing it.

Bruce Schneier distrusts atomic clocks because the timing attacks are too obvious.

Bruce Schneier can tune an antenna by whistling the desired resonant frequency.

Bruce Schneier does not slow down as he approaches the speed of light, the speed of light slows down as it approaches Bruce Schneier.

Darth Vader doesn't know it, but Bruce Schneier is actually Luke's father.
Bruce Schneier shaves with Occam's razor.

Bruce Schneier wrote the random number generator used to generate thermal noise.

Bruce Schneier, knows if P equals NP.

According to a recent survey, online buyers would trust ssl websites much more if their web browsers replaced the lock icon with a picture of Bruce Schneier. A W3C recommendation is in the works.

Many of these facts brought to you by http://geekz.co.uk/schneierfacts/ .
Visit thier site for more info & Bruce T-shirts.

Presentations

44 Lines about 22 Things That Keep Me Up At Night

Agent X

What keeps a hacker up at night? What issues and projects keep Agent X from getting a good night's sleep? This turbo-rant will present 22 things that make the night seem long and morning far off. Technology challenges, social challenges. Issues with the hacker scene, issues with the way the world works.

kNAC!

Ofir Arkin,
CTO Insightix

Network admission control (NAC), network access protection (NAP), network access control (NAC), and many other acronyms refer to a technology which aim to provide with access control verification before (and after) allowing an element to access the network.

Unfortunately due to the lack of standardization, and the diversity of solutions, many (if not must) NAC solutions suffer form a multitude of weaknesses impacting the deployment, implementation and the overall protection they provide.

The presentation examines various NAC solutions from leading vendors, highlights their weaknesses, and demonstrates how they can be bypassed.

The presentation is an updated presentation, which includes new material, and new unpublished methods to bypass NAC solutions.

Remedial Heap Overflows: dlmalloc style

Atlas

Sometimes even the top dudes need a refresher course. Remedial Heap Overflows is not so much a lesson to the lame, but a refresher for the leet. One day the speaker was approached (in a subway, of course) by a top-notch dude (who has his own posse) and asked how they work. Clearly not even the best of the best always know everything.

Injecting RDS-TMC Traffic Information Signals

(a.k.a. How to freak out your Satellite Navigation)

Andrea Barisani
co-Founder and Chief Security Engineer
Inverse Path Ltd.
Daniele Bianco

RDS-TMC is a standard based on RDS (Radio Data System) for communicating over FM radio Traffic Information for Satellite Navigation Systems.

All modern in-car Satellite Navigation systems sold in Europe use RDS-TMC to receive broadcasts containing up to date information about traffic conditions such as queues and accidents and provide detours in case they affect the plotted course.The system is increasingly being used around Europe and North America.

The audience will be introduced to RDS/RDS-TMC concepts and protocols and we'll show how to decode/encode such messages using a standard PC and cheap home-made electronics, with the intent of injecting information in the broadcast RDS-TM stream manipulating the information displayed by the satellite navigator.

We'll discover the obscure (but scary!) messages that can be broadcast (and that are not usually seen over legitimate RDS-TMC traffic), the limits of standard SatNav systems when flooded with unusual messages and the role that RDS-TMC injection/ jamming can play in social engineering attempts (hitmen in the audience will love this!).

In order to maximize the presentation we'll also demo the injection.

Bridging the Gap Between Technology and the Law

John Benson "jur1st"

The recent case of Julie Amero has cast a bright spotlight on the difference in understanding between the worlds of technology and the law. We will examine adoption of technology within the legal profession, trial court decisions, as well as legislative and appellate decisions which may be inconsistent with generally accepted security measures.

A Journalist's Perspective on Security Research

Peter Berghammer (pfoton)
CEO Copernio: Future Formats

The presentation details the process whereby journalists select, discard, research and ultimately publish security related articles. It outlines the credibility necessary for security researchers to be taken seriously in the presentation of their findings and examines the "blowback" that criminal and kiddie hackers have on the security industry from a journalists perspective. This talk also looks at the current practices of legitimate software companies between secure content (DRM et al), metadata tracking, hardware and software tracking, and the very close parallels between their methods and those of the "hacking" universe.

Analyzing Intrusions & Intruders

Sean M. Bodmer
Savid Technologies, Inc.

Intrusion Analysis has been primarily reserved for network junkies and bit biters. However, due to the advances in network systems automation we now have time to pay more attention to subtle observations left by attackers at the scene of the incident. Century old sciences have enabled criminal investigators the ability attribute attacks to specific individuals or groups.

Teaching Hacking at College

Sam Bowne
Part-time Instructor
City College of San Francisco,
Computer Networking and
Information Technology Department

Last semester I taught a new course in "Ethical Hacking and Network Defense" at City College San Francisco. I had legal, ethical, and practical concerns about this class, so I took several precautions to protect the students from one another, and others from them. The course was a success--it was full and popular, and there were no security problems (at least none that I found out about).

I will show how entropy, a measure of information content defined by Shannon in 1948, can provide useful ways of organizing and analyzing log data.

In particular, we use entropy and mutual information heuristics to group syslog records and packet captures in such a way as to bring out anomalies and summarize the overall structure in each particular data set. I will show a modification of Ethereal that is based on these heuristics, and a separate tool for browsing syslogs.

Our data organization heuristics produce decision trees that can be saved and applied to building views of other data sets. Our tools also allow the user to mark records based on relevance, and use this feedback to improve the data views.

Our tools and algorithm descriptions can be found at http://kerf.cs.dartmouth.edu

Intranet Invasion With Anti-DNS Pinning

David Byrne
EchoStar Satellite

Cross Site Scripting has received much attention over the last several years, although some of its more ominous implications have not. DNS-pinning is a technique web browsers use to prevent a malicious server from hijacking HTTP sessions. Anti-DNS pinning is a newly recognized threat that, while not well understood by most security professionals, is far from theoretical.

This presentation will focus on a live demonstration using anti-DNS pinning techniques to interact with internal servers through a victim web browser, completely bypassing perimeter firewalls. In essence, the victim browser becomes a proxy server for the external attacker. No browser bugs or plug-ins are required to accomplish this, only JavaScript, and untrusted Java applets for more advanced features.

If anyone still thought that perimeter firewalls could protect their intranet servers, this presentation will convince them otherwise.

Virtualization: Enough Holes to Work Vegas

D.J. Capelis
University of California, San Diego

Have you tried to firewall a machine from itself? Have you ever tried to protect a machine with a multi-personality disorder? These questions are brought to us by the wonderful technology of virtualization. Though the technology is clearly sexy, security has clearly been an afterthought.
While every product claims isolation, it seems that's only when you don't have an attacker involved. Despite what the press releases say, it's not free to put all your machines on the same hardware. We'll be brushing aside the dust and trying to figure out part of the cost.

Panel 1: Meet the Fed

Jim Christy DoD
Jerry Dixon DHS
Tim Fowler NCIS
Andy Fried IRS
Barry Gundy NASA
Bob Hopper NW3C
Jon Iadonisi DoD
Mike Jacobs SRA
Tim Koshiba FBI
Bob Lentz DoD
Kevin Manson DHS FLETC
Rich Marshall NSA
Ken Privette Postal IG
Keith Rhodes GAO
Linton Wells NDU

This year we will have so many feds representing their federal agencies that we will have to break it up into two separate panels:

IA Panel: Information Assurance, CERTS, first responder's organizations from agencies including DC3, DHS, SOCOM, NSA, OSD, NDU, and GAO.

LE Panel: and Law Enforcement, Counterintelligence agencies including DC3, FBI, IRS, NCIS, NASA, NWC3, US Postal IG, FLETC, and RCMP.

Agencies that will have representatives include: Defense Cyber Crime Center (DC3), FBI, IRS, NCIS, NASA, DHS, National White Collar Crime Center (NWC3), Special Operations Command (SOCOM), NSA, US Postal IG, Office of the Secretary of Defense, National Defense University, Federal Law Enforcement Training Center (FLETC), and the Government Accountability Office (GAO).

For years Defcon participants have played "Spot the Fed" For the 2nd year, the feds will play "Spot the Lamer" Come watch the feds burn another lamer.

Panel 2: Meet the VCs

Patrick Chung
Partner, NEA
Maria Cirino
Co-Founder and Managing Director, .406 Ventures
Mark McGovern
Tech Lead, In-Q-Tel
Dov Yoran
Partner, Security Growth Partners

2007 held numerous watershed events for the security industry. Innovation is needed and the money is there. Come to this session and meet the VCs actively investing in security, web, and mobile applications. Learn how VCs see the future, what they are looking for, and how best to utilize them to further your innovations. This session will conclude with a announcement about the Black Hat/DEFCON Open, a business plan competition focused on innovations in security; winners will be announced at Black Hat 2008 and DEFCON XVI.

Computer and Internet Security Law - A Year in Review 2006 - 2007

Robert W. Clark
Counsel,
Dept of Navy Office of General Counsel

This presentation reviews the important prosecutions, precedents and legal opinions of the last year that affect internet and computer security. We will discuss the differences between legal decisions from criminal cases and civil lawsuits and what that means to the security professional. Additionally, we look at topics such as: email retention and discovery; active response; use of CFAA as non-competition methods; identity theft and notification issues; legal aspects of emerging technologies; lawsuits involving IT corporations (Google, Yahoo, Apple, Microsoft); and of course, the NSA surveillance litigation. As always, this presentation is strongly audience driven and it quickly becomes an open forum for questions and debate.

Satellite Imagery Analysis

Greg Conti
Lieutenant Colonel,
United States Military Academy

Satellite imagery was once restricted to organizations like CTU, but now it is freely available to us all via powerful free online tools and commercial services. In this talk we will look at commercial collection platforms and capabilities, orbital mechanics and a variety of imagery analysis techniques. We will analyze examples from interesting places around the world and explore issues surrounding the future of satellite surveillance.

Securing Linux Applications With AppArmor

Crispin Cowan
Director of Software Engineering,
SUSE/Novell

The core of the security problem is that most software contains latent bugs, and many of these bug can be exploited by attackers to cause the software to do something undesirable to the victim's computer. To block this threat, one can either use only perfect software (of which there is a shortage :) or use a security system to control what software may and may not do. The problem is that such systems are historically very difficult to use.

AppArmor is an application security system that directly attacks the ease of use problem, making it possible for widespread adoption by developers, system administrators, and users. AppArmor provides for security profiles (policies) that specify the files that a given program may read, write, and execute, and provides tools to quickly and automatically generate these profiles.
This presentation will briefly introduce the AppArmor system, and then spend much of the time showing how to best use AppArmor to confine applications and protect systems. AppArmor is pure GPL software, and is available for SUSE, Slackware, Ubuntu, Gentoo, and Red Hat Linux.

LAN Protocol Attacks Part 1 - Arp Reloaded

Jesse "x30n" D'Aguanno
Praetorian Global & Digital Revelation

Ever wanted to hijack a connection between machines on a LAN, deny service between a host you're attacking and a log server or intrusion detection system, or maybe wanted to sniff traffic on a switched network? Now you can! Er, wait... You already could with the ARP attacks we all know and love.

While these network attacks are quite effective, they do have their weaknesses, as well as security controls to help prevent them. In this talk I will build on the previous research in this field and introduce new, more reliable attacks against the ARP protocol which are much less identifiable and able to protect against.

CiscoGate

The Dark Tangent

Dark Tangent never speaks at DEF CON because he thinks it is cheating.. but not for the 15th anniversary! Come listen to a behind the scenes account of what really happened during the "Cisco/ISS Gate" fiasco from 2005. Throughout the talk the audience will be asked what they would have done at key points and then learn what I chose to do. A cautionary and comical tale of what happens when communication breaks down.

Hacking Social Lives: MySpace.com

Rick Deacon
IT Specialist

This presentation will discuss how to hack MySpace.com using web application hacking methods implementing minimal tools outside of the internet, a text editor, and a cookie editor. How to find exploits will be discussed, as well as what to do with the exploits. Multiple exploits will be revealed and broken down. MySpace XSS filter evasion will be discussed. Session hijacking using cookies provided from MySpace will be proven and shown using patched exploits.

The live demonstration (with audience participation) will be using a 0-Day MySpace exploit! The methodology and practices used in the presentation will always be relevant to MySpace as well as many other sites containing Cross Site Scripting holes. MySpace is filled with hundreds of unattended and undiscovered Cross Site Scripting exploits. Discussion on how to prevent these attacks and secure sites using web applications will also be touched upon. Also, tips on how to mess with your friends :) Questions and volunteers are encouraged!

Now everyone can have a crack at their friend's MySpace! Just don't ruin anyone's precious social life.

Picking up the Zero Day; An Everyone's Guide to Unexpected Disclosures

Dead Addict

Security researchers around the world have been SLAPPed (strategic lawsuits against public participation) across the face by vulnerable software vendors. Bogus legal threats intended to intimidate and prevent public exposure of vulnerabilities are becoming increasingly common. If the software industry succeeds at silencing these researchers the public, governments, global industries, and end user customers are ill served and increasingly vulnerable. Successful silencing of research does not stop it, this merely drives it into private and underground economies.

While private commercial exploit economies are being launched, and underground exploit economies are flourishing, the independent researchers (including small security shops) are increasingly the source of open and honest security information. Corporate security researchers often have contractual relationships with vendors preventing the public disclosure of critical security vulnerabilities.

It is in this context that vulnerable software vendors attempt (often successfully) to silence hackers through bogus legal threats.

While the debate regarding appropriate disclosure protocols is interesting (although seemingly unending), I'm not going to talk about it. This isn't about designing a disclosure utopia, but how to deal with disclosure as it stands today.

Confrontational approaches serve no one (except perhaps aggressive attorneys increasing their billable hours), and legal threats are demonstrably counterproductive.

I'm going to tell everyone what to do: vendors, customers, hackers, and the press. I'll tell vendors how to handle any disclosure with integrity and their best interests in mind; an admittedly tricky task. I'll remind customers that they have the choice in the products they purchase, and it may be wise to reward those that address security issues responsibly. I'll then give some friendly advice to hackers (no legal advice will be given). Finally I'll address the role of the press and how their reporting can ensure the public interest is served.

Revolutionizing the Field of Grey-box Attack Surface Testing with Evolutionary Fuzzing

Jared DeMott
Vulnerability Researcher
Dr. Richard Enbody
Associate Professor,
Michigan State University
Dr. Bill Punch
Associate Professor,
Michigan State University

Runtime code coverage analysis is feasible and useful when application source code is not available. An evolutionary test tool receiving such statistics can use that information as fitness for pools of sessions to actively learn the interface protocol. We call this activity grey-box fuzzing. We intend to show that, when applicable, grey-box fuzzing is more effective at finding bugs than RFC compliant or capture-replay mutation black-box tools. This research is focused on building a better/new breed of fuzzer. The impact of which is the discovery of difficult to find bugs in real world applications which are accessible (not theoretical).

We have successfully combined an evolutionary approach with a debugged target to get real-time grey-box code coverage (CC) fitness data. We build upon existing test tool General Purpose Fuzzer (GPF) [8], and existing reverse engineering and debugging framework PaiMei [10] to accomplish this. We call our new tool the Evolutionary Fuzzing System (EFS).

We have shown that it is possible for our system to learn the targets language (protocol) as target communication sessions become more fit over time. We have also shown that this technique works to find bugs in a real world application. Initial results are promising though further testing is still underway.

This talk will explain EFS, describing its unique features, and present preliminary results for one test case. We will also discuss future research efforts.

Unraveling SCADA Protocols: Using Sulley Fuzzer

Ganesh Devarajan
Security Researcher, Tipping Point Inc.

Firstly, I will be covering the basics of SCADA networks and give a general overview of the SCADA protocols namely Modbus, DNP3, ICCP and IEC standards. North America mainly uses Modbus, DNP3 and to an extent ICCP, the European countries use the IEC standards. After the basics I will be getting into the finer details of the protocols as to what function code, internal indication flags does what and how that can be used to attack or take down the SCADA system. I shall as well discuss and demonstrate the current level of security implementation that these sites have.

After enumerating all those I will talk about the SCADA Fuzzer and the framework that has been worked on and how that can be used to determine the flaws in the implementation of various software. This tool can be used to assess the software out there by various vendors and a brief analysis of some of the software out there will be shown. Even though some of the attacks can be detected by the inline devices today, they are more prone to false positives.

I am using the Sulley Framework to fuzz the various protocol implementations. I basically use Sulley to fuzz all the header fields of the various protocols. Sulley is equipped with some of the protocol specific CRC generators (CRC-DNP) apart from the regular ones. I have as well generated various test cases to fuzz the data sections of the protocols, unlike most other fuzzers.

Once the test cases are developed, the tool will be used to determine the vulnerabilities in various implementations and these vulnerabilities will be presented in Defcon. A case study of the various software implementations will as well be presented showing where they are normally vulnerable.
.

Boomstick Fu: The Fundamentals of Physical Security at its Most Basic Level

Panel with
Deviant
Ollam,
Noid,
Frank Thornton (a.k.a. Thorn),
jur1st

It seems that at every con nowadays there is at least one talk dedicated to physical security. Our servers and data can be encrypted and passworded with the latest algorithms, but that doesn't do the trick if someone marches them out the door when we're not looking. In the past, many physical security talks have focused on passive defense: locks that resist picking, safes which resist cracking, etc. However, sometimes an intrusion is detected while in progress... and such intrusions-even physical ones- may require immediate countermeasures.

Many of us in the security community own firearms, but few have ever had to use them in a defensive situation. Others have considered gun ownership but lack any experience or foundation in this area. This panel of experts will provide a comprehensive overview of this highly-charged and often-misunderstood topic. Bring any questions you have about hardware, ammunition, tactics, and the law.

Tor and Blocking-Resistance

Roger Dingledine
Project leader, The Tor Project

Websites like Wikipedia and Blogspot are increasingly being blocked by government-level firewalls around the world. Although many people use the Tor anonymity network to get around this censorship, the current Tor network is not designed to withstand a large censor.

In this talk I'll describe our plan for extending the Tor design so these users can access the Tor network in a way that is harder to block.

01110011

01111001

Trojans: A Reality Check

Toralv Dirro
Avert Labs EMEA Security Strategist,
CISSP, McAfee
Dirk Kollberg
Virus Research Lead EMEA, McAfee

Today there is a lot of hype around some new proof-of-concept technology or around politically motivated trojans, etc. This talk will deliver a reality check, give an idea what kind of malware the McAfee Research organisation is actually seeing to be used in the real world and show how the different trojans work, what the impact is. The material used are internal statistics of the various threats sent to or discovered by us, some more detailed analysis to make functionality more transparent and some demo's, screenshots, etc. to make clear how complex the trojans used today in real attacks are. This also gives a very clear picture of how the threat changed now that there is a lot of money involved in using trojans to steal personal data of all kind - from bank details to identities in online games.

Toralv Dirro works for McAfee as Avert Labs EMEA Security Strategist. Working in Virus Research for many years since 1994 at McAfee (Dr Solomon's Software back then) after analysing viruses at the University of Hamburg before that, he got finally got bored with debugging things and focused on Network IPS and Vulnerability Assessment/Management. He recently rejoined the Research team. Toralv Dirro is a well reputed expert on next generation AV Technology and Network Intrusion Prevention and is a frequent speaker on those topics.

Real-time Steganography with RTP

I)ruid Computer Academic Underground

Real-time Transfer Protocol (RTP) is used almost ubiquitously by Voice over IP technologies to provide an audio channel for calls. As such, it provides ample opportunity for creation of a covert communications channel due to it's very nature and use in implementation. While use of steganographic techniques with various audio cover-mediums has been extensively researched, most applications of such have been limited to audio cover-medium of a static nature such as WAV or MP3 file audio data. This presentation details common techniques for use of steganography with audio data cover-medium, outlines the problem issues that arise when attempting to use these techniques to establish a full-duplex communications channel using audio data transmitted via an unreliable streaming protocol, and finally documents solutions to these problems as well as a reference implementation entitled SteganRTP.

Everything You Ever Wanted to Know About Police Procedure in 50 Minutes

Steve Dunker
Assistant Professor,
Northeastern State University

Ever wonder just what rules law enforcement must follow? When do the police have to read you the Miranda Warnings? Who is subject to a Stop and Frisk? When does Double Jeopardy apply. What does a cop actually have to know before they can legally stop you? What is the effect of an Invalid arrest? Just when can the SWAT team kick your door without knocking first? When must an officer have a search warrant?

During the "Ask the Criminal Justice Professor" part of the program I'll answer your "hypothetical" questions concerning police procedure. If I don't know the answer, I'll make something up that sounds good.

The Hacker Society around the (corporate) world

Luiz Eduardo

I will talk about the evolution and differences of the hacking communities around the world. Why and how this affects the hackers being taken to the corporate life, motivations, or just why is it better to stay totally underground. How companies attract and manage hackers, and how they scare them away. Computers are cool now, like the tshirt says, and small kids already know what ip addresses are, how to use netstat, etc. Is security gonna become a commodity? Come on over, let's talk about it. The more diverse the crowd is, the better.

Kernel Wars

Joel Eriksson
Security Researcher and CTO of Bitsec
Karl Janmar
Security Researcher, Bitsec
Claes Nyberg
Security Researcher, Bitsec
Christer Öberg
Security Researcher, Bitsec

Kernel vulnerabilities are often deemed unexploitable, or at least unlikely to be exploited reliably. Although it's true that kernel-mode exploitation often presents some new challenges for exploit developers, it still all boils down to "creative debugging" and knowledge about the target in question.

This talk intends to demystify kernel-mode exploitation by demonstrating the analysis and reliable exploitation of several real-life kernel vulnerabilities. From a defender's point of view this could hopefully serve as an eye-opener, as it demonstrates the ineffectiveness of HIDS, NX, ASLR and other protective measures when the kernel itself is being exploited.

The entire process will be discussed, including how the vulnerabilities were found, how they were analyzed to determine if and how they can be reliably exploited and of course the exploits will be demonstrated in practice.

None of the vulnerabilities that will be used as examples had public exploits by the time they were exploited by us, and includes the (in)famous Windows 2000/XP GDI bug, the FreeBSD 802.11 bug and a local NetBSD vulnerability.

We will also demonstrate a full exploit for the remote OpenBSD ICMPv6 vulnerability found by CORE SDI, and discuss the payload techniques we used for it.

The NetBSD-bug is a new 0-day for Vegas and not the same bug that was disclosed at our BH Europe presentation, and we will also throw in at least one more surprise 0-day to keep things interesting. ;)

More info: **http://kernelwars.blogspot.com/**

Routing in The Dark: Pitch Black

Nathan S. Evans
Ph.D. Graduate student, University of Denver
Christian Grothoff,
Ph.D. Assistant Prof. of Computer Science
University of Denver
There is a pervasive dream about a free Internet which is robust, fully decentralized yet efficient, and which ensures privacy for all users. For seven years, the Freenet project has been the most visible embodiment of this vision. This talk will show that the recent 0.7 release of Freenet—marketed to solve most of the problems—entirely fails to deliver.

Freenet 0.7 promises efficient routing in restricted-route networks, often also called friend-to-friend (F2F) networks or darknets. Our work shows that a crucial step in the routing protocol can be easily subverted by an adversary which is no more powerful than any ordinary node operator. The attack targets a fundamental aspect of the routing protocol; in particular, it does not rely on minor flaws in the Freenet implementation and can thus not be easily addressed.

The goal of this talk is not to destroy the dream of a free Internet. Instead, the talk will educate the audience about pitfalls on the path to utopia, improving our progress to this shared vision by shining a light on certain dead ends.

Estonia: Information Warfare and Strategic Lessons

Gadi Evron Beyond Security

In this talk we will discuss what is now referred to as "The 'first' Internet War" where Estonia was under massive online attacks for a period of three weeks, following tensions with the local Russian population.

Following a riot in the streets of Tallinn, an online assault begun, resulting in a large-scale coordination of the Estonian defenses on both the local and International levels. We will demonstrate what in hind-sight worked for both the attackers and the defenders, as well as what failed. Following the chronological events and technical information, we will explore what impact these attacks had on Estonia's civil infrastructure and daily life, and how they impacted its economy during the attacks.

Once we cover that ground, we will evaluate what we have so far discussed and elaborate on lessons learned while Gadi was in Estonia and from the post-mortem he wrote for the Estonian CERT. We will conclude our session by recognizing case studies on the strategic level, which can be deducted from the incident and studied in preparation for future engagements in cyber-space.

Webserver Botnets and Hosting Farms as Attack Platforms

Gadi Evron Beyond Security

The thousands of servers in collocation centers and hosting farms in the market for an ideal attack bot-herders in the market for an ideal attack platform. Learn how about web server malware which is completely cross-platform, and how ISPs (with varying success) are detecting and responding to frequent attempts by the bad guys to take control.

Panel: Internet Wars 2007

Gadi Evron Moderator
Andrew Fried IRS
Thomas Grasso FBI
Dan Hubbard Websense
Dan Kaminsky IOActive
Randy Vaughn Baylor
Paul Vixie ISC

Continuing our new tradition from last year, leading experts from different industries, academia and law enforcement will go on stage and participate in this panel, discussing the current threats on and to the Internet, from regular cyber-crime all the way to the mafia, and even some information warfare.

In this panel session we will begin with a short introductory presentation from Gadi Evron on the latest technologies and operations by the Bad Guys and the Good Guys. What's going on with Internet operations, global routing, botnets, extortion, phishing and the annual revenue the mafia is getting from it. The members will accept questions on any subject related to the topic at hand, and discuss it openly in regard to what's being done and what we can expect in the future, both from the Bad Guys and the Good Guys.

Discussion is to be limited to issues happening on the Internet, rather than this or that vulnerability. The discussion is mostly technological and operational in nature, although last year attendees chose to ask questions directing the discussion to the legal side of things. Participants are people who are involved with battling cyber-crime daily, and are some of the leaders in the security operations community of the Internet.

Biometric and Token-Based Access Control Systems: Are You Protected By Two Screws and a Plastic Cover? Probably.

Zac Franken

An overview and demonstration of common access control and biometric systems. This will include the key elements of their implementation and includes in-depth technical analysis of their common weakness. I will then demonstrate bespoke hardware developed to perform an attack that renders most access control systems useless.

Greetz from Room 101

Kenneth Geers

Imagine you are king for a day. Enemies are all around you, and they seem to be using the Internet to plot against you. Using real-world cyber war stories from the most tightly controlled nations on Earth, Greetz from Room 101 puts you in the shoes of a king who must defend the royal palace against cyber-equipped revolutionaries. Can a monarch buy cyber security? Are his trusty henchmen smart enough to learn network protocol analysis? Could a cyber attack lead to a real-life government overthrow? Ten case studies reveal the answers. Which countries have the Top Ten most Orwellian computer networks? Come to the talk and find out.

Now imagine that your name is Winston Smith, and that you live in a place called 1984. You don't trust the government, and you don't trust the evening news. You can't send your girlfriend an email because you think that the Thought Police will get it first. Greetz from Room 101 details what Web surfing, email, blogging, and connections to the outside world are like for the half of our planet's population who enjoy little to no freedom online, in places where network security battles can mean life or death. Last but not least, the DEFCON audience will hear about the future of cyber control, and the future of cyber resistance.

The Completion Backward Principle

geoffrey

If you're responsible for the burglar alarm at your facility, do you understand how it's being monitored by the "Data Monitoring Group" flunkees? Are all those alarm conditions real? The Completion Backward Principle covers issues arising from Internet-enabled monitoring of burglar alarm systems, and possible mitigations. Spot The Fed will most assuredly be played at this talk.

Intelligent debugging for VulnDev

Damian Gomez
Researcher, Immunity, Inc.

Anyone who has ever developed an exploit will tell you that 90% of their development time was spent inside a debugger.Like with all software engineering, the actual implementation language of the exploit is somewhat irrelevant. The exploit is merely a solution to a problem that was solved using your debugger of choice.

Because a large percentage of your exploit development time is spent inside a debugger, the need for an exploit development oriented debugging framework becomes apparent. This framework should combine the readability of a GUI, the speed of a command line, and the flexibility of a scripting language.

During this talk we will discuss various topics that are relevant to debugging in the context of exploit development. These topics include protocol analysis, runtime data type analysis, advanced heap structure and flow analysis, and bypassing protection mechanisms.

Multipot: A More Potent Variant of Evil Twin

K N Gopinath
Senior Wireless Security
Researcher/Manager,
R&D Group,
AirTight

This presentation pertains to a discovery of a more potent variant of Evil Twin. We call it Multipot. Multipot consists of multiple APs which are configured with the same SSID and lure WiFi clients into connecting to them. The term Multipot is derived from 'multiple' and 'honeypot'. Multipot can occur naturally in the form of multiple Municipal APs or Metro APs around the victim client, all of which are naturally configured for the same SSID (e.g., GoogleWiFi). Such a natural Multipot can induce non-policy compliant communication from wireless clients of an organization. There can also be a handcrafted or malicious version of Multipot where an attacker can combine it with known Evil Twin attack tools (e.g., KARMA, delegated) and launch a Man-in-the-Middle attack against wireless clients.

The prevalent Evil Twin defenses are ineffective against Multipot. In particular, the prevalent defenses include: i) Taking precaution so that clients are not lured to Evil Twins (e.g., specialized client side software), and ii) since these precautions are not always foolproof or practical, using a Wireless Intrusion Prevention System (WIPS) to block clients' connections to Evil Twins. Most of the current WIPS use deauthentication (deauth) based session containment to defend against this threat. In this presentation, we demonstrate that Multipot renders the deauth based session containment completely ineffective. Multipot provides a glimpse into the complexities of evolving wireless vulnerabilities and their countermeasures.

Making of the DEFCON 15 Badge

Joe Grand

Joe Grand is an electrical engineer, prominent speaker, and prolific inventor with multiple pending patents and over a dozen commercially available products. He is the President of Grand Idea Studio, a San Francisco-based product research, development, and licensing firm, where he specializes in the design of consumer electronics and video game accessories.

Involved in computers and electronics since the age of 7, Joe has had the fortune of being a member of the legendary Boston-based hacker collective L0pht Heavy Industries, testifying before the United States Senate Governmental Affairs Committee under his nom de hack, Kingpin, and being praised as a "modern day Paul Revere" by the Senators for his research and warnings of computer security weaknesses.

Disclosure and Intellectual Property Law: Case Studies

Jennifer Granick
Executive Director,
Center For Internet and Society,
Stanford Law School

The simple decision by a researcher to tell what he or she has discovered about a software product or website can be very complicated both legally and ethically. The applicable legal rules are complicated, there isn't necessarily any precedent, and what rules there are may be in flux.

In this presentation, I will use Cisco and ISS's lawsuit against Michael Lynn (from Black Hat 2005) and HID's cease and desist letter to IOActive (from Black Hat 2006) to discuss major intellectual property law doctrines that regulate security research and disclosure. I will give the audience some practical tips for avoiding claims of illegal activity.

Security by Politics - Why it will never work

Lukas Grunwald CTO of DN-Systems Enterprise Internet Solutions GmbH

This talk will show what happens if security is driven by politics and compromise, also I will cover additional security risks by the new generation of electronic passports.

It will show why it could be possible to produce fake biometric fingerprints from the new generation electronic passports, for example by rogue regimes. The new bogus security attempts to secure the ePassports via EAN (Extended Access Control).

Hardware Hacking for Software Geeks

David Gustin
Software Developer
Ab3nd

This presentation is an introduction to hardware design and reverse engineering, with an eye towards developing an individual laboratory for future exploration. We start by covering the basic tools and setting up a laboratory. In this section, we cover the basic tools, such as soldering tools, oscilloscopes, and logic analyzers. The focus is on getting the tools for low or no cost. From there, we cover the forward engineering process, including various microcontroller designs. Finally, we will go over hardware reverse engineering and its relation to the forward engineering process. There will be demonstrations of low cost oscilloscopes, logic analyzers, and flash dumping tools. These tools will be used against consumer-grade hardware to demonstrate the beginning of a reverse engineering attempt.

This talk assumes slight prior knowledge of electronics on a hobbyist level. The ability to read a schematic will come in handy, but isn't required. Even if you don't have a hobby-level interest in electronics, we hope you will by the end of the presentation.

The Commercial Malware Industry

Peter Gutmann

Malware has come a long way since it consisted mostly of small-scale (if prolific) nuisances perpetrated by script kiddies. Today, it's increasingly being created by professional programmers and managed by international criminal organisations. This talk will look at the methods and technology employed by the professional malware industry, which is turning out "product" that matches (and in some cases even exceeds) the sophistication of standard commercial software, but with far more sinister applications.

INTERSTATE: A Stateful Protocol Fuzzer for SIP

Ian G. Harris
University of California Irvine

We present the INTERSTATE fuzzer to detect security vulnerabilities in VOIP phones which implement Session Initiation Protocol (SIP). INTERSTATE generates an input sequence for a SIP phone which is constructed to reveal common security vulnerabilities. SIP is a stateful protocol so a state machine description of the SIP protocol is used by INTERSTATE to ensure that the entire state space is explored. The input sequence consists of SIP request messages as well as GUI input sequences which are remotely applied to the phone under test. The input sequence is generated to perform a random walk through the state space of the protocol. The application of GUI inputs is essential to ensure that all parts of the state machine can be tested. Faults are injected into SIP messages to trigger common vulnerabilities. INTERSTATE also checks the SIP response messages received from the phone under test against the expected responses described in the state machine. Checking response messages allows for the detection of security bugs whose impact is more subtle than a simple crash. We have used INTERSTATE to identify a previously unknown DoS vulnerability in an existing open source SIP phone. The vulnerability could not have been discovered without exploring multiple paths through the state machine, and applying GUI inputs during the fuzzing process.

Ian would like to give recognition to the following co-authors for their contributions. Thoulfekar Alrahem, Alex Chen, Nick DiGiussepe, Jefferey Gee, Shang-Pin Hsiao, Sean Mattox, Taejoon Park, Albert Tam, and Marcel Carlsson.

Hacking the Extensible Firmware Interface

John Heasman
NGSSoftware

"Macs use an ultra-modern industry standard technology called EFI to handle booting. Sadly, Windows XP, and even Vista, are stuck in the 1980s with old-fashioned BIOS. But with Boot Camp, the Mac can operate smoothly in both centuries."
- Quote taken from http://www.apple.com/macosx/bootcamp/

The Extensible Firmware Interface (EFI) has long been touted as the replacement for the traditional BIOS and was chosen by Apple as the pre-boot environment for Intel-based Macs. This presentation explores the security implications of EFI on firmware-based rootkits.

We start by discussing the limitations of the traditional BIOS and the growing need for an extensible pre-boot environment. We also cover the key components of the EFI Framework and take a look at the fundamental design decisions affecting EFI and their consequences. Next we consider the entry points that an EFI system exposes—just how an attacker may set about getting their code into the EFI environment—taking the Apple Macbook as our reference implementation.

After demonstrating several means of achieving the above, we turn our attention to subverting the operating system from below, drawing parallels wherever possible to attacks against systems running a traditional BIOS.

The final part of this presentation discusses the evolution of EFI into the Unified Extensible Firmware Interface (UEFI), soon to be supported by Windows Server (Longhorn) and discusses the application of the previously discussed attacks to UEFI.

Hack Your Car for Boost and Power!

Aaron Higbee
Managing Partner and co-founder,
Intrepidus Group

What happens when you combine a natural hacker, a computer controlled car, and security consultant's discretionary income spent on a pile of parts? A four cylinder, 2.5 liter, 500hp monster daily driver that runs on pump gas. (Pump gas plus computer controlled methanol injection for that extra umph.)

If you love the smell of gasoline and want to learn about performance tuning and ECU hacking, then this presentation is for you. If you have the dealer change your oil for fear of voiding the warranty, then you may want to skip this presentation. Attendees will be introduced to the tools of the trade and tuning concepts that are meant to squeeze out every last drop of power. Concepts will be backed up by practical examples and advice that the audience member can take away and try on their own (....if they dare). The presentation will cover automotive protocols, sensors, and tuning concepts used in making power. The presentation will cover the role of octane, water injection, and methanol injection as a means of coping with high boost turbocharged applications. Basic knowledge of electronic fuel injection and how a motor works is recommended. An understanding of the mechanics of turbochargers and superchargers is a plus but is not required. The presentation will conclude with car modification laws, CARB, emissions testing, SEMA, and privacy concerns about the data an ECU can store.

GeoLocation of Wireless Access Points and "Wireless GeoCaching"

Ricky Hill
Senior Scientist,
Tenacity Solutions

GeoLocation of 802.11b Access Points is not a trivial task. As wardrivers who've stumbled various networks with a GPS unit will attest, "Netstumbler doesn't provide the real location of access points". Instead, it provides an estimate of where the software thinks they are. Why should this be so? In a comparative sport made popular by the proliferation of portable GPS units, GeoCachers routinely find their "caches" or treasures with amazing accuracy. The Wardriving community should be able to do the same...

This talk is about 802.11b Access Point location. The project's primary goal is to build a novel hardware & software configuration that can be used with wardriving gear and Netstumbler to geoLocate AP's as they're encountered. Various methods of radio location are discussed along with a new game we'll call "Wireless GeoCaching."

The Presentation will include details of the hardware—construction of a rotating, stepper-motor driven directional antenna, and the software: Netstumbler and Visual Basic. Video and photos of the actual GeoLocation/GeoCaching sessions will be shown.
No prerequisite—only an interest in Network Stumbling, GeoCaching and Wireless Technology.

Virtual World, Real Hacking

Greg Hoglund

The Market for Malware

Dr. Thomas J. Holt
Assistant Professor,
Dept. of Criminal Justice,
University of North Carolina

As the world comes to rely on computers and rapidly changing technologies, the threat posed by computer attackers has become increasingly significant. Computer attackers exploit vulnerabilities in systems and circumvent antivirus software to obtain all manner of personal and financial information. However, individuals no longer need to rely on their abilities, as malware and automated tools quickly and efficiently perform attacks for them. Individuals can buy access to sophisticated malware, including bots, Trojans, and worms via markets run in publicly accessible web forums operating out of Eastern Europe, Russia, and other parts of the world. These forums also operate black markets where individuals can sell the data they illegally obtain for profit. Examining these markets can have significant benefit for computer security and law enforcement by identifying the functionality of malware in the wild, and the individuals who create these tools. This presentation will explore the latest tools and materials being sold in active publicly accessible web forums that traffic in malware and personal information.The cost, functionality, and utility of these programs will be explored, as well as the dynamics of sellers and buyers in these markets..

Click Fraud Detection with Practical Memetics

Broward Horne
Software Consultant

"Click Fraud Detection with Practical Memetics" is an evolution of my previous Defcon presentations. The original Meme Miner program and Meme Theory were enhanced for better predictive ability which led to an accidental detection of "Pay-Per-Click" advertising fraud. This presentation includes expanded overview of Meme Theory, real-life example of Botnet click fraud, strategies to detect memetic inconsistencies in network propagation, strategies to deceive existing detection schemes and future "Pay-Per-Click" fraud issues.

See http://www.realmeme.com for more.

Faster PwninG Assured: New adventures with FPGAs

David Hulton

I've been giving talks on how FPGAs are cool for the past couple of years at Defcon, so what's different this year? Well, I'll be releasing a couple of new tools.
BTCrack is a Bluetooth PIN cracker that will allow you to crack 8-digit Bluetooth PINs on an FPGA or 5-digit PINs on your computer in real-time (Longer PINs require a little more time) using a capture of the pairing process.
The other tool, WinZipCrack will let you crack WinZip AES encrypted files by specifying a list of words that you want to try. The FPGA implementation runs an order of magnitude faster than a PC and the tool supports all of the different modes of WinZip encryption. I'll also be releasing a tool that will allow you to convert WinZIP AES encrypted files into normal unencrypted PKZIP files with the correct passphrase (in case any of you have ever tried opening a WinZip AES encrypted file in unix, ugh!).

I'll also be doing a lightning quick demo of the other tools available on the OpenCiphers Project website and will be releasing Virtex-5 LX50 support for the whole toolset with up to 3x performance over the previous cores on the Virtex-4 LX25 as well as full Windows support.

HoneyJax (AKA Web Security Monitoring and Intelligence 2.0)

Dan Hubbard
VP Security Research,
Websense Security Labs

We have all heard of Honeypots and more recently HoneyClients. Now we are introducing the concept of HoneyJax. Once again functionality has beaten our security, and Web 2.0 is in full force. User-created content, radical trust, and social networks have lead to several malicious code attacks and spammers have learned that the web a great compliment to sell there trade.

This session will show provide examples and insights into the problems of Web 2.0 and include one way to assist in the identification and tracking of mis-use of these technologies by deploying HoneyJax's within the operating environment.

One Token to Rule Them All: Post-Exploitation Fun in Windows Environments

Luke Jennings
MWR InfoSecurity

The defense techniques employed by large software manufacturers are getting better. This is particularly true of Microsoft who have improved the security of the software they make tremendously since their Trustworthy Computing initiative. Gone are the days of being able to penetrate any Microsoft system by firing off the RPC-DCOM exploit. The consequence of this is that post-exploitation has become increasingly important in order to "squeeze all the juice" out of every compromised system.

Windows access tokens are integral to Microsoft's concept of single sign-on in an active directory environment. Compromising a system that has privileged tokens can allow for both local and domain privilege escalation.

This talk aims to demonstrate just how devastating attacks of this form can be and introduces a new, open-source tool for penetration testers that provides powerful post-exploitation options for abusing tokens found residing on compromised systems. The functionality of this tool is also provided as a Meterpreter module for the Metasploit Framework to allow its use to be combined with the existing power of Metasploit. In addition, a complete methodology will be given for its use in penetration testing. This will include identifying tokens that can be used to access an otherwise secure target and then locating other systems that may house those tokens. A new vulnerability will also be revealed that appears to have been silently patched by Microsoft. The impact of this vulnerability is that privileged tokens can be found on systems long after the corresponding users have logged off.

Finally, defense strategies will be discussed that can help provide defense in depth to reduce the impact of token abuse as a post-exploitation option.

Homeless Vikings, (short-lived bgp prefix hijacking and the spamwars)

Dave Josephsen
Sr Systems Eng, DBG Inc

BGP Prefix hijacks take the IP addresses of others and make them your own. This talk provides a chilling account of the current use of prefix hijacks by spammers in a successful effort to defeat RBL's. Placed within the context of the history of the spamwar, this talk makes clear the grim future we face if we continue to escalate the spam war into the network layer; namely a future where every spammer on earth can arbitrarily choose and make routable an unallocated ipv4 address (one that the RBL's have never seen) once per day for the next 150 years or so without ever using the same address twice, and never colliding with any other spammer.

Black Ops 2007: Design Reviewing The Web

Dan Kaminsky

Design bugs are really difficult to fix - nobody ever takes a dependency on a buffer overflow, after all. Few things have had their design stretched as far as the web; as such, I've been starting to take a look at some interesting aspects of the "Web 2.0" craze. Here's a few things I've been looking at:

Slirpie: VPN'ing into Protected Networks With Nothing But A Lured Web Browser. Part of the design of the web is that browsers are able to collect and render resources across security boundaries. This has a number of issues, but they've historically been mitigated with what's known as the Same Origin Policy, which attempts to restrict scripting and other forms of enhanced access to sites with the same name. But scripts are not acquired from names; they come from addresses. As RSnake of ha.ckers.org and Dan Boneh of Stanford University have pointed out, so-called "DNS Rebinding" attacks can break the link between the names that are trusted, and the addresses that are connected to, allowing an attacker to proxy connectivity from a client. I will demonstrate an extension of RSnake and Boneh's work, that grants full IP connectivity, by design, to any attacker who can lure a web browser to render his page. I will also discuss how the existence of attacks such as Slirpie creates special requirements for anyone intending to design or deploy Web Single Sign On technologies. Slirpie falls to some of them, but slices through the rest handily.

powf: Passing Fingerprinting of Web Content Frameworks. Traditional OS fingerprinting has looked to identify the OS Kernel that one is communicating with, based on the idea that if one can identify the kernel, one can target daemons that tend to be associated with it. But the web has become almost an entirely separate OS layer of its own, and especially with AJAX and Web 2.0, new forms of RPC and marshalling are showing up faster than anyone can identify. powf intends to analyze these streams and determine just which frameworks are being exposed on what sites.

LudiVu: A number of web sites have resorted to mechanisms known as CAPTCHAs, which are intended to separate humans from automated submission scripts. For accessibility reasons, these CAPTCHAs need to be both visual and auditory. They are usually combined with a significant amount of noise, so as to make OCR and speech recognition impossible. I was in the process of porting last year's dotplot similarity analysis code to audio streams for non-security related purposes, when Zane Lackey of iSec Partners proposed using this to analyze CAPTCHAs. It turns out that, indeed, Audio CAPTCHAs exhibit significant self-similarity that visualizes well in dotplot form. This will probably be the first DEFCON talk to use WinAMP as an attack tool.

Fighting Malware on your own

Vitaliy Kamlyuk
Virus Analyst, Kaspersky Lab

There is always a possibility to get infected by some malware, i.e. by surfing the web and catching the malware that uses some new exploit in your browser. What should you do then? Do you know what is available on Windows system to fight malware? The problem of fighting malware on Windows is the limitation of basically available tools. I am going to show you some tricks that will let you do some complicated actions using ONLY components of Windows system and NO 3rd party tools.

I have been working in Kaspersky Lab for 2 years. I've started as a developer & researcher and at some points worked as unix administrator. Today I am working as virus analyst. This position gave me the knowledge of deep understanding of the majority of modern Windows technologies. As a result I learnt how to do the programming in machine code. My presentation will show you the cases when this knowledge is mandatory. I am going to show how to develop an antivirus solution using Windows notepad and the knowledge of machine code programming. Besides, I am going to show several hacks to perform complicated tasks in limited Windows environment.

SQL injection and out-of-band channeling

Patrik Karlsson

A large number of web applications are still found suffering from improper input validation controls. This is a fact commonly exploited by hackers in order to gain unauthorized access to backend databases and steal sensitive corporate information. As systems are hardened hackers are often forced to rely on blind SQL injection in order to extract information.

The audience will be introduced to out-of-band channeling, an alternate technique which under certain circumstances can be much more efficient in achieving the task. A number of different channels, pros & cons and preventive measures will be presented. Did you know a hacker could steal your corporate secrets by channeling them over DNS?

Hacking EVDO

King Tuna
Wardrivingworld.com

Come and spend 50 minutes with the King, not Elvis, but King Tuna. He is going to give you a peak into EvDo and some of the goodies it has to offer. After a very brief overview of what EvDo is he is going to go into detail about the different hardware options you have, and most importantly, how EvDo cards can be hacked and the advantages of delving into the insides of the card. Can ESN's be moved? Can EvDo be used in monitor mode?

Bring a bag because there will be treats for 100 people with a patch so you can use your EvDo card on your laptop as a client or access point.

Functional Fuzzing with Funk

Benjamin Kurtz

This talk will introduce a simple and incredibly powerful framework for the scripted generation of network traffic: Funk, a new tool for fuzzing arbitrary network protocols written using the Chicken Scheme-to-C compiler. Source code will be provided and explained, so you can start using this framework today for all your network traffic generation needs!

Some familiarity with functional languages like Lisp or Scheme will behelpful, but not required.

Comparing Application Security Tools

Edward Lee
Security Researcher, Fortify Software

If you're going to buy an application security tool, which one will it be? Every vendor likes to talk about how their tools are the best. "We are the market leader!" they all say. But not everyone can lead all the time. I will show how I took half a dozen "leading" application security tools (both static and dynamic) and compared them head-to-head against the same open source application. All of the tools found something, but no two tools find the same thing!

I will break down the different techniques each tool uses and show specifically which bugs each tool finds. The proceedings will include all of the details about the code so that you can add your own tools to the comparison. The presentation gives a methodology for doing detailed tools comparison.

IPv6 is Bad for Your Privacy

Janne Lindqvist
Helsinki University of Technology

In recent years, covert channel techniques for IPv4 and more recently for IPv6 have been published by the scientific community and also presented in DEFCON 14. However, a covert channel that contains a considerable bandwidth has been overlooked, the autoconfigured IPv6 address itself. IPv6 Stateless Address Autoconfiguration is used for autoconfiguring addresses without a server in IPv6 networks. The autoconfiguration mechanism consists of choosing an address candidate and verifying its uniqueness with Duplicate Address Detection. The autoconfiguration mechanism has privacy issues which have been identified before and mitigations have been published as RFC 3041. However, we show that the privacy protection mechanism for the autoconfiguration can be used as a covert channel, and consequently, be used to harm the privacy of the user. The covert channel can be serious threat for communication security and privacy. We present practical attacks for divulging sensitive information such as parts of secret keys of encryption protocols. The scheme can also be used for very effective Big Brother type surveillance that cannot be detected by established intrusion detection systems.

Database Forensics

David Litchfield
Founder, Next Generation Security Software

Since the state of California passed the Database Security Breach Notification Act (SB 1386) in 2003 another 34 states have passed similar legislation with more set to follow.
In January 2007 TJX announced they had suffered a database security breach with 45.6 million credits card details stolen - the largest known breach so far.

In 2006 there were 335 publicized breaches in the U.S.; in 2005 there were 116 publicized breaches; between 1st January and March 31st of 2007, a 90 day period, there have been 85 breaches publicized.

There are 0 (zero) database-specific forensic analysis and incident response tools, commercial or free, available to computer crime investigators. Indeed, until very recently, there was pretty much no useful information out that could help.

By delving into the guts of an Oracle database's data files and redo logs, this talk will examine where the evidence can be found in the event of a database compromise and show how to extract this information to show who did what, when. The presentation will begin with a demonstration of a complete compromise via a SQL injection attack in an Oracle web application server and then performing an autopsy. The talk will finish by introducing an open source tool called the Forensic Examiner's Database Scalpel (F.E.D.S.).

No-Tech Hacking

Johnny Long
Penetration Tester (*snicker*)

I'm Johnny. I hack stuff. I've been at it for quite a while now, and I've picked up a few tricks along the way. I get asked about my tricks all the time, mostly by kids who saw that movie. You know the one. But I've always said no. I've held onto my secrets as part of the pact I made with the hacker underground. I mean I'm allowed to give talks and presentations about hacking stuff, but the secrets... the real super-cool secrets I've had to keep to myself. The head of the underground said so. But I got this email the other day that says I'm THIS close to getting kicked out of the underground. Seems the glare of the public eye has been on me for far too long and I've become a liability. So, I'm going to be proactive. I'm going to quit before they can fire me. I'm coming out of the closet (not that one) and I'm airing all the underground's dirty laundry in the process. That's right. I'm going public with the 'berest of the 'ber. The real ninja skillz are yours for the knowing. Want to know how to suck data off a laptop with nothing but your MIND? Poke your way into a corporate email server without touching a keyboard? You think I'm kidding. I'm not. Want to slip inside a building and blend with the shadows? Even the best slip up with this trick, but don't worry. If your camouflage breaks down, I'll teach you the Jedi wave. Not the one in Star Wars (they stole theirs from the hacker underground), but the REAL Jedi wave that confuses people and makes them ignore you as you bumble around in the high security areas. Or the smoke trick. The one that lets you pass through walls untouched, surrounded by a cool-looking (but smelly) cloud of smoke. How about sucking sensitive data from a corporate network from the parking lot? Without a wireless device. How about blending in with the feds? You can chat with them about... fed stuff, and they'll accept you as one of their own. All this and more. The underground is gonna be sooo ticked off.

Self-Publishing and the Computer Underground

Myles Long
Director of Depravity, cDc communications/ CULT OF THE DEAD COW
Rob "Flack" O'Hara
member cDc's Ninja Strike Force
Christian "RaDMan" Wirth
founder, ACiD Productions

Have you ever considered publishing your own book? Your own DVD? Self-publishing has been a part of the computer underground since its inception, from the Neon Knights to the Syndicate of London's recent book "End of Dayz". This panel will discuss types of self-publishing (both on- and off-line) and their relevance to the computer underground. They will also discuss their personal experiences in self-publishing. Ample time for questions will be available. Learn about the process from people who have gone through it.

Social Attacks on Anonymity Networks

Nick Mathewson

Any attacker can scam one or two users into revealing themselves, but do you know how to talk an entire community of smart hackers into weakening its anonymity?

In spite of progress in traffic analysis, social engineering attacks remain the most effective way to break users' anonymity and one of the best force multipliers for traditional traffic analysis attacks. Why bother doing traffic analysis when you can trick users into isolating themselves using nothing more than an IRC client? I'll discuss social attacks to circumvent and weaken existing anonymity networks, from the obvious to the intricate.

This talk will include analysis of historical attacks against the Mixmaster and Cypherpunk remailer networks, and advice for building and using anonymity tools to resist these attacks.

Technical Changes Since The Last Tor Talk

Nick Mathewson

There hasn't been a talk from the developers of Tor (the popular anonymity network) at Defcon since 2004. Since then, we've revised the protocols, added piles of new features to the software, tightened security, integrated more helper tools, made hard strategic decisions, and suffered growing pains. There have been new attacks, new defenses, new research, and new ideas.

In this talk, I'll present the most important technical changes and developments since you last heard about Tor at Defcon. Time permitting, I'll talk about the big technical challenges we're facing for the next year, some of the more interesting feature proposals we're considering, and some of the more interesting ways that smart programmers can help spread privacy to the world.

It's All About the Timing

Haroon Meer
Technical Director, SensePost
Marco Slaviero
Senior Security Analyst, SensePost

Timing attacks have been exploited in the wild for ages. In recent times timing attacks have largely been relegated to use only by cryptographers and cryptanalysts. In this presentation SensePost analysts will show that timing attacks are still very much alive and kicking on the Internet and fairly prevalent in web applications (if only we were looking for them). The talk will cover SensePost-aTime (our new SQL Injection tool that operates purely on timing differences to extract data from injectable sites behind draconian firewall rulesets), our new generic (timing aware) web brute-forcer and lots of new twists on old favorites. We will discuss the implications of timing on current JavaScript malware discussing XSRT (Cross Site Request Timing)(because we can never have too many acronyms!) and will demonstrate how reasonably effective this is against the "Same Origin Policy".

If you are doing testing today, and are not thinking a lot about timing, chances are you are missing attack vectors right beneath your stop-watch!

How smart is Intelligent Fuzzing - or - How stupid is Dumb Fuzzing?

Charlie Miller
Senior Security Analyst,
Independent Security Evaluators

Dynamic analysis, or fuzzing, is a popular method of finding security vulnerabilities in software. Fuzzing may be used by a developer to find potential problems as part of the quality-assurance process or may be used to find potential exploits in an existing software application. Fuzzing has grown in popularity because it is much easier (and often more effective) to generate and run arbitrary inputs than it is to perform a manual code audit or use software reverse engineering. However, the quality of the fuzzing analysis depends heavily on the quality and quantity of the fuzzed inputs. These inputs, called test cases, are normally constructed in one of two ways: mutation-based or generation-based. In mutation-based fuzzing, known good data are collected and then modified; modifications may be random or heuristic. The advantage of mutation-based fuzzing is that little or no knowledge of the protocol or application under study is required, however it is likely that the collected test cases will only test the most common functionality. Generation-based fuzzing starts from a specification or RFC, which describes the file format or network protocol, and constructs test cases from these documents. Generation-based fuzzing is a much more complete method of fuzzing, but it requires a significant amount of up-front work to study the specification and manually generate test cases. In this talk we analyze the differences between mutation and generation-based fuzzing techniques for the Portable Network Graphics (PNG) format, and quantify the potential advantages gained by using a generation-based approach. Our results show that generation-based fuzzing performs up to 76% better when compared to mutation-based fuzzing techniques for this format.

The Next Wireless Frontier - TV White Spaces

Doug Mohney
Editor, VON Magazine

More unlicensed bandwidth from TV!?!
A long-term push to free up more wireless spectrum is expected to come to fruition this year as the FCC will open up unused TV channels—dubbed "white spaces"— for unlicensed broadband use this fall, with full-blown availability in 2008 once the DTV transition takes place.

Dell, Google, HP, Intel, Microsoft and Philips have joined together in the "White Spaces Coalition" to lobby for a spectrum sensing technology to find open TV channels while Motorola has submitting a more conservative proposal combining a geolocation database with spectrum sensing. Microsoft has gone so far as to submit a prototype device to the FCC to allow the regulatory agency to explore and evaluate cognitive radio and spectrum sensing technologies.

Is more unlicensed wireless bandwidth just around the corner? What is the promise of TV whitespace spectrum? What opportunities will there be to create new software and new devices? What are the "gotchas" in the various proposals? What is the latest information out of the FCC on White Spaces device?

Tactical Exploitation

H.D. Moore
Director of Security, BreakingPoint Systems
Valsmith
Founder, Offensive Computing

Penetration testing often focuses on individual vulnerabilities and services. This talk introduces a tactical approach that does not rely on exploiting known vulnerabilities. Using combination of new tools and obscure techniques, I will walk through the process of compromising an organization without the use of normal exploit code. Many of the tools will be made available as new modules for the Metasploit Framework.

Disclosure Panel

David Mortman,
Moderator CSO-in-Residence, Echelon One
Paul Proctor,
Moderator VP, Gartner
Window Snyder,
Vendor Director of Ecosystem Development, Mozilla Corporation
Steven B. Lipner,
Vendor Senior Director of
Security Engineering Strategy,
Trustworthy Computing,
Microsoft Corp.
John N. Stewart,
Vendor VP & CSO, Cisco Systems, Inc.

Concerns about ethics for security professionals has been on the rise of late. It's time for researchers and vendors to meet up and discuss the issues of ethical behavior in our industry and start setting some guidelines for future research and discussion. Join active analysts, vendors and researchers for a lively discussion.

Re-Animating Drives & Advanced Data Recovery

Scott Moulton
System Specialist
Forensic Strategy Services, LLC.

NEW!! Advanced Data Recovery Material. Even people who think they know everything about a hard drive will be surprised at what they will learn in this presentation. Everyone will learn something new about hard drives and how to perform data recovery. We will lay it on the line and tell all! We will display All NEW Material and Animations on the inner workings of a hard drive. We will discuss rebuilding a hard drive and will teach you what to look for and how to accomplish this task on your own. If nothing else you will be entertained by one of the best animations on hard drives in the style of the History Channel.

(un)Smashing the Stack: Overflows, Countermeasures, and the Real World

Shawn Moyer
Chief Researcher, SpearTip Technologies

As of today, Vista, XP, 2K03, OS X, every major Linux distro, and each of the BSD's either contain some facet of (stack|buffer|heap) protection, or have one available that's relatively trivial to implement/enable. So, this should mean the end of memory corruption-based attacks as we know it, right? Sorry, thanks for playing.

The fact remains that many (though not all) implementations are incomplete at best, and at worst are simply bullet points in marketing documents that provide a false sense of safety.

This talk will cover the current state of software and hardware based memory corruption mitigation techniques today, and demystify the myriad of approaches available, with a history of how they've been proven, or disproved. We'll then walk through some real-world analysis of attacks against vulnerable code, and look at how effective the various protection mechanisms are at stopping them.

As an addition to this talk, I thought I'd put my money where my mouth is, so I'm offering a shiny new server up for "Øwn the box? Own the box!", running two services with known vulnerabilities that, hopefully, are protected by the countermeasures described in the talk. If it's compromised before the talk, the winner should be prepared to come up on stage and share how he/she succeeded.

Protecting your IT infrastructure from legal attacks- Subpoenas, Warrants and Transitive Trust

Alexander Muentz

You think your systems and data are safe from any attack. You fear no script kiddie. You get a +5 against social engineering. Yet a single subpoena can crack your junk open wide. A search warrant might leave you with an empty server room.

The law might be the biggest threat to your users, systems and you. Learn how to plan for and react to search warrants, subpoenas and wiretaps. I'm going to speak about the law in an IT context, make it accessible and relevant. If you manage other people's systems for a living or just are afraid of your own privacy and liberty, you might want to see this.

Windows Vista Log Forensics

Rich Murphey
PhD Chief Scientist, White Oak Labs

Event logging in Windows Vista is quite different in terms of the way events are stored on disk and the way they are used by applications. Vista uses a new encoding of event records that lends itself to much broader flexibility for searching events. This encoding has a direct impact on forensic examination of event logs, which will be discussed in this presentation. The impact of the new application programming interface (API) is no less important. A primary role of the event log is support for debugging and tech support resolution. Such debugging information, in turn, provides significant value to forensic analysis where it indicates chronological traces of user activity. The new API offers far more dependable and detailed capabilities for monitoring. To the degree that this API motivates more pervasive debugging information, Vista event logs may provide greater capability to reconstruct timelines of user activity. During the presentation, sample Vista logs will be examined from a forensics perspective. Finally, the impact of these issues on relevant forensic tools will be explored.

Creating and Managing Your Security Career

Mike Murray
Lee Kushner
President of LJ Kushner & Associates

Careers in information security are often difficult to navigate, with the industry changing more and more radically every year. We're going to talk about the important skills, traits and knowledge that a security pro needs, not just the usual stuff (like "go get a CISSP"), we're going to come from the perspective of two people who spend much of their time talking to hiring managers and companies looking for security stars, as well as talking to those same security stars about their careers, where they're going, what's working for them, and, most importantly, what's not. And we're going to use that information to teach you how to manage your own career to find the job that keeps you challenged, growing, happy and appropriately compensated.

The Science of Social Engineering: NLP, Hypnosis and the science of persuasion

Mike Murray
Anton Chuvakin Ph.D.

Social engineering has traditionally been more of an art than a science, we try different things, and if they work, we continue to use them over and over again. Some of the best social engineers have developed excellent technique even without understanding why what they're doing works. Mike & Anton are skilled communicators trained in NLP, hypnosis, FACS and other sciences of influence, and will present (and demonstrate) some of the cutting edge research on influence and persuasion.

Being in the know... Listening to and understanding modern radio systems

Brett Neilson
Taylor Brinton

"Being in the know" is key to supporting or violating a security infrastructure. Whether you're taking over the Taco Bell drive through or listening in during a presidential visit, being armed with the right information could drastically affect your outcome and ultimately lead to your success. This talk will focus on modern radio systems and the challenges of listening to them. We will provide information on several utilities and resources to aid in reconnaissance efforts as well as provide detailed information about how various types of radio systems function in today's modern world. Lastly we will cover some of the hardware to help make you successful and review some fun things to listen to here in Vegas and to do when you get back home.

Hack your brain with video games

NeonRa1n
Julian Spillane
CEO, Frozen North Productions, Inc

Video games are the most effective and accessible tool for hacking your physical and mental state, yet the potential impact of these technologies has yet to be exploited. In this presentation we will take you on a journey through video games -past, present and future-, dispelling the myths and emphasizing the realities, both positive and dark. We will also explain how different input devices can be used to improve the brain and how to hack together your own input framework to take advantage of these innovative peripherals.

This presentation will focus on the various opportunities of such hardware, especially biofeedback devices, in gaming and the positive effects that these technologies can have on our brains and bodies. We will also be presenting some code for expanding and accepting peripherals outside of the norm; as well as a demo of the technology, Biofeedback Tetris, making use of heart-rate monitoring and a measure of galvanic skin response to enhance game-play.

Digital Rights Worldwide: Or How to Build a Global Hacker Conspiracy

Danny O'Brien
International Outreach Coordinator, Electronic Frontier Foundation

Hackers and tech users in the United States have long benefited from some long-lived institutions that have worked to helped defend and publicise their rights, including but not limited to EFF and DefCon itself. But the legal and political fights over DRM and copyright, privacy invasions, cybercrime round-ups and security scaremongering, are now increasingly international battles. How can hackers across the world build their own institutions, and co-ordinate between them. Headed by Danny O'Brien, EFF's International Outreach Coordinator, co-founder of the UK's Open Rights Group, and inventor of "Life Hacks", this talk will pool advice from activist hackers coming to DefCon from around the world.

Greater than 1: Defeating "strong" Authentication in Web Applications

Brendan O'Connor

With Phishing, Fraud, and Identity Theft at peak levels, banks, credit unions, credit card companies, and other financial institutions are enhancing the security of their website authentication. This talk will cover the new methods of authentication, such as mutual authentication, device fingerprinting, out of band authentication, one time passwords, and knowledge base archives. We will analyze how these controls are intended to function, what they're really doing, and how we can defeat them. We will also evaluate the effectiveness of specific technologies based on their stated purpose: stopping phishing, fraud, and identity theft.

Panel: Ask the EFF

Kurt Opsahl
Senior Staff Attorney
Kevin Bankston
Staff Attorney
Marcia Hofmann
Attorney
Matt Zimmerman
Staff Attorney
Danny O'Brien
EFF Activism Coordinator
Seth Schoen
EFF Staff Technologist

Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as NSA wiretapping (with newly released technical information), using the Freedom of Information Act to dumpster dive with the law, tips and tricks for hacking evoting machines legally, how censorship, surveillance and privacy invasions are spreading throughout the world— and how hackers' can defend civil liberties at home and abroad, threats to freedom from digital TV, and much more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

The SOA/XML Threat Model and New XML/SOA/Web 2.0 Attacks & Threats

Steve Orrin
Dir. of Security Solutions, Intel, Corp.

Organizations that are implementing XML based systems, Web Services, Web 2.0 applications are discovering that there are security challenges unique to them that can surface throughout the various phases of lifecycle. Traditional network and application protection and infrastructure systems lack the functionality, performance, and operational efficiencies needed to provide a secure, cost effective solution. Web Services, SaaS and SOA provide significant benefits and efficiencies to organizations that implement them. However they also introduce new risk structures not seen in other applications or technology solutions before. This session investigates the nature of XML, Web Services and next generation threats, including a new threat model for categorizing and classifying threat types, attack vectors, and risks. The session covers new and evolving attacks and the potential damage and loss that they can cause. These include Payload, Semantic and Structural XML based attacks, as well as some Web 2.0 attacks and next generation worm threats.

OpenBSD Remote Exploit and Other IPv6 Vulnerabilities

Alfredo Ortega Core Security

OpenBSD is regarded as a very secure Operating System. This article details one of the few remote exploit against this system. A kernel shellcode is described, that disables the protections of the OS and installs a user-mode process. Several other possible techniques of exploitation are described. Several other ipv6-related vulnerabilities are described and disclosed.

Breaking Forensics Software: Weaknesses in Critical Evidence Collection

Chris Palmer
Security Consultant, iSEC Partners
Alex Stamos
Founding Partner, iSEC Partners

Across the world law enforcement, enterprises and national security apparatus utilize a small but important set of software tools to perform data recovery and investigations. These tools are expected to perform a large range of dangerous functions, such as parsing dozens of different file systems, email databases and dense binary file formats. Although the software we tested is considered a critical part of the investigatory cycle in the criminal and civil legal worlds, our testing demonstrated important security flaws within only minutes of fault injection.

In this talk, we will present our findings from applying several software exploitation techniques to leading commercial and open-source forensics packages. We will release several new file and file system fuzzing tools that were created in support of this research, as well as demonstrate how to use the tools to create your own malicious hard drives and files.

This talk will make the following arguments:

- Forensic software vendors are not paranoid enough. Vendors must operate under the assumption that their software is under concerted attack.
- Vendors do not take advantage of the protections for native code that platforms provide, such as stack overflow protection, memory page protection), safe exception handling, etc.
- Forensic software customers use insufficient acceptance criteria when evaluating software packages. Criteria typically address only functional correctness during evidence acquisition when no attacker is present, yet forensic investigations are adversarial.
- Methods for testing the quality of forensic software are not meaningful, public, or generally adopted. Our intention is to expose the security community to the techniques and importance of testing forensics software, and to push for a greater cooperation between the customers of forensics software to raise the security standard to which such software is held.

CaffeineMonkey: Automated Collection, Detection and Analysis of Malicious JavaScript

Daniel Peck
Security Researcher, Secureworks
Ben Feinstein Security Researcher, Secureworks

The web browser is ever increasing in its importance to many organizations. Far from its origin as an application for fetching and rendering HTML, today's web browser offers an expansive attack surface to exploit. All the major browsers now include full-featured runtime engines for a variety of interpreted scripting languages, including the popular JavaScript. The web experience now depends more than ever on the ability of the browser to dynamically interpret JavaScript on the client.

We will present a software framework for the automated collection of JavaScript from the wild, the subsequent identification of malicious code, and characteristic analysis of malicious code once identified. Building on the work of several existing client honeypot implementations, our goal is to largely automate the painstaking work of malicious software collection. Our focus is on attacks using JavaScript for obfuscation or exploitation.

We will also discuss the findings based on the deployment of a network of CaffeineMonkeys. The analysis and conclusions will focus on identifying new in-the-wild obfuscation/evasion techniques and JavaScript browser exploits, quantifying the prevalence and distribution of well-known and newly discovered obfuscation and evasion techniques, as well as quantifying the prevalence and distribution of known and newly discovered JavaScript browser exploits.

Securing the Tor Network

Mike Perry
Mad Computer Scientist,
fscked.org evil labs

Imagine your only connection to the Internet was through a potentially hostile environment such as the Defcon wireless network. Worse, imagine all someone had to do to own you was to inject some html that runs a plugin or some clever javascript to bypass your proxy settings. Unfortunately, this is the risk faced by many users of the Tor anonymity network who use the default configurations of many popular browsers and other network software. Tor is designed to make it difficult even for adversaries that control several points in the network to determine where you're coming from or where you're going, yet these "data anonymity" attacks and attacks to bypass Tor can be performed effectively by a malicious website, or just one guy with a Ruby interpreter! To add insult to injury, software vendors seldom consider such exploits and other privacy leaks as real vulnerabilities. Fortunately, there are some things that can be done to improve the security of the web browser and Tor users in general. This talk will discuss various approaches to securing the Tor network and Tor usage against a whole gauntlet of attacks, from browser specific, to general intersection risks, to theoretical attacks on routing itself. Methods of protection discussed will include node scanning, transparent Tor gateways, Firefox extensions (including the dark arts of Javascript hooking), and general user education. Each approach has its own strengths and weaknesses, which will be discussed in detail.

Pen-testing Wi-Fi

Aaron Peterson
Founder,Midnight Research Laboratories

As wi-fi becomes increasingly popular and as more layers of access control are added, the fact that a wireless access point exists becomes less interesting to us. The problem is that manually going through a long list of access points checking for interesting information is tedious at best.

Wicrawl is a tool that will allow you to "crawl" through discovered access points with a series of plugins that implement common tools (nmap, aircrack, etc) to find the accessible, interesting, or relevant ones. This can help with penetration testing, detecting rogue access points, or maybe just finding free internet access. We recently revamped wicrawl to be more targeted towards penetration testing adding a new reporting infrastructure as well as accelerated hardware support, and this will be released at Defcon. A wi-fi finding robot will also make its debut!

Aaron will give a guided tour of this new utility and its capabilities, as well as the plugins. A live demo of wicrawl will be shown. We'll hand out free liveCDs that include the software!

How to be a WiFi Ninja

Pilgrim Matthew Shuchman

As one of the founders of WarDrivingWorld.com, where over the past few years we have sold thousands of WiFi devices and antennas for Pen testing and extended range WiFi, I will be presenting simple, but very effective techniques for extending the range of WiFi beyond the standard 15-30 meter range to 3-5 km, or more using home brew components.

Pilgrim is an ancient hacker who came from the tombs of Egypt. In those days punch cards ruled the world. Well with maturity may come intelligence and he founded WarDrivingWorld and enjoys teaching. He was formerly a government economist, has published business books and articles, and owned a network company. He lives in Florida with his dog Jack and enjoys playing with WiFi for fun and profit.

Stealing Identity Management Systems

Plet

Novell's Identity Manager and related components are become fairly common in large networks. Identity management systems in general bring a number of security implications that are often not well understood. Even when best practices are followed, the system often has vulnerabilities that can be exploited. Since there seems to be little research into hacking identity management systems, the goal of this talk is to bring some recognition to security risks these systems bring to an organization. This talk will look at some of the inherent properties of identity management systems which can make them prone to exploitation, and look at some specific techniques for exploiting certain configurations.

Dirty Secrets of the Security Industry

Bruce Potter
The Shmoo Group

The fox is guarding the hen house, and both the fox and the hens are making a lot of money in the process. Such is the state of the security industry in 2007. For the last 15 years, we have been building security into our networks and applications using concepts like "defense in depth" and "layered security." It turns out, that the attackers are now leveraging our security systems against us. Worse, we have made the security industry a self feeding, self fulfilling prophecy that may actually be causing harm to those we are trying to protect.

Yeah, FUD! So while this may sound fatalistic and like I'm trying to stir up a flame war, I think there are real issues that we need to face when it comes to the next steps in computer security. This talk will uncover 8 dirty secrets of the security industry. Some you will believe, some you will be skeptical of, and some may strike a little too close to home.

Covert Debugging: Circumventing Software Armoring Techniques

Danny Quist
Cofounder, Offensive Computing, LLC
Valsmith Cofounder,
Offensive Computing, LLC

Software armoring techniques have increasingly created problems for reverse engineers and software analysts. As protections such as packers, run-time obfuscators, virtual machine and debugger detectors become common newer methods must be developed to cope with them. In this talk we will present our covert debugging platform named Saffron. Saffron is based upon dynamic instrumentation techniques as well as a newly developed page fault assisted debugger. We show that the combination of these two techniques is effective in removing armoring from the most advanced software armoring systems. As a demonstration we will automatically remove packing protections from malware.

The Inherent Insecurity of Widgets and Gadgets

Aviv Raff
Security Researcher, Finjan
Iftach Ian Amit
Director of Security Research, Finjan
Widgets (or Gadgets) are small applications, which usually provide some kind of visual information or access to a frequently used function. Because widgets are in fact applications, they too can include malicious code. Furthermore, due to the simplicity of legitimate widgets, such as calculators and clocks, they are developed without security in mind.
In this presentation, we will explain the three different types of widgets in detail. We will demonstrate proof of concept of a malicious widget for each of the types and also highlight the attack vectors for exploiting a vulnerable legitimate widget.

Following the demonstrations, we will talk at a high-level about widgets integrated in mobile devices. We'll take a brief look at the Widgets 1.0 paper created by the W3C, and also talk about the similarity between widgets and browser extensions in terms of their inherent insecurity.

The Emperor Has No Cloak - WEP Cloaking Exposed

Vivek Ramachandran
Senior Wireless Security Researcher,
AirTight Networks

We thought The Emperor has No Cloak story was a pure fiction until we came across an announcement three weeks ago. Marketing can sell anything. The question is can an invisible cloak be sold in modern times when most of us can see through it?

The WEP cloaking technique works (or rather, as we argue, does not work) by injecting spoofed WEP encrypted data frames ("Chaff") into the air. These chaff packets may contain random data or encrypted with a key different from the actual WEP key in use and may use only weak IVs. Unmodified WEP cracking tools fail to crack the original WEP key in a chaff-contaminated packet trace. Apart from the fact that WEP cloaking does not address any of the other weaknesses in WEP (such as message modification, replay attacks, shared authentication flaws, packet decoding using ICV etc); there are multiple ways to beat WEP cloaking, which we will disclose during our talk.

We also plan to release a set of tools including a patch for Aircrack which will keep WEP cracking the simple job it's always been - even in the presence of WEP Cloaking. Final verdict on WEP Cloaking: WEP was, is, will remain broken. It cannot be secured by obscuring its flaws.

Beyond Vulnerability Scanning - Extrusion and Exploitability Scanning

Matt Richard
Rapid Response Team, iDefense
Fred Doyle
Labs Director, iDefense

With this presentation we will demonstrate a new tool called eescan that automates extrusion and exploitability scanning using a client/server approach. Eescan will be released under the GPL and utilizes python to create an extensible framework for testing extrusion and exploit defenses.
All network security systems have gaps. Layered security tries to cover the gaps with overlapping protections like firewalls, intrusion prevention, proxies and other mechanisms. How do you really know where the gaps are before the weeds grow through? Vulnerability assessment tools scan for vulnerable systems from an attackers perspective. This technique has value but fails to represent the risk posed by client application usage and attacks. They also fail to assess extrusions - the traffic content allowed to leave a network.

Extrusion and exploitability scanning attempts to find these gaps using an automated scanning framework. The scanning techniques simulate user and attacker behavior from the client perspective to holistically measure the amount of risk in a given security system.

Biting the Hand that Feeds You - Storing and Serving Malicous Content From Well Known Web Servers

Billy Rios
Senior Security Researcher, VeriSign
Nathan McFeters
Senior Security Advisor, Ernst & Young

Whats in a name? How do you know you should "trust" the content you are receiving? In today's World Wide Web, we place a lot of "trust" into domain names. For many, domain names help determine the whether a particular link or file should be trusted, or eyed with suspicion. Domain name trust has even made its way into security systems, considering many of the protections built into our browsers are based strictly on domain names! In this talk, we'll take a look at some simple ways to store and serve malicious content from some of the most popular servers on the Internet.

It's time we rethink the ways we've implemented one of our most treasured Web resources... web mail. We'll bite the hand that feeds us by abusing the very features that make web mail services so popular. We'll show you how to use popular web mail servers as a repository for malicious content and how to serve that content to those surfing the World Wide Web (no email address required!)

MQ Jumping

Martyn Ruks
Senior Security Consultant,
MWR InfoSecurity

Every day billions of dollars pass through middleware, the unglamorous component of most enterprise applications. Middleware may be unglamorous, but even if billions of dollars doesn't interest you, it's bound to attract someone's interest sooner or later. Often security is addressed in the front-end web server and back-end database but the other components are often ignored. The reason for this can be a lack of understanding of the risks or lack of knowledge of the middleware products and how they can be attacked. One important property of a multi-tier environment is the ability to reliably pass data between authorised system components and therefore messaging software is often required. A popular and widely deployed example of such a component is IBM's Websphere MQ (formally MQ Series).

This software can be run across a number of platforms including Microsoft Windows, commercial and Open Source UNIX platforms and IBM's z/OS and i5 Operating Systems. Companies use the technology to pass messages between application components and it is widely deployed across a wide range of industry sectors including Finance, Retail, Healthcare and many others. During penetration tests conducted by MWR InfoSecurity against its clients it has been discovered that the security features provided by the product are either not utilised correctly or are not suitable for their intended use.

This presentation will uncover the truth behind Websphere MQ security as it is deployed in the real world and will look at how the software can be abused by an attacker resulting in remote code execution. The talk will focus on methods for analysing the security controls that can be used to protect an installation of MQ and the limitations of each of them. Following on from this section of the talk a number of methods will be presented for compromising both the message data and the Operating System through the MQ service. This will culminate in a demonstration of some of the attacks presented in the talk, followed by a discussion about the methods that exist for protecting an installation and ensuring that security breaches do not occur.

Vulnerabilities and The Information Assurance Directorate

Tony Sager
Chief,
Vulnerability Analysis and Operations Group,
Information Assurance Directorate,
National Security Agency

The Information Assurance Directorate (IAD) within the National Security Agency (NSA) is charged in part with providing security guidance to the national security community. Within the IAD, the Vulnerability Analysis and Operations (VAO) Group identifies and analyzes vulnerabilities found in the technology, information, and operations of the Department of Defense (DoD) and our other federal customers. This presentation will highlight some of the ways that the VAO Group is translating vulnerability knowledge in cooperation with many partners, into countermeasures and solutions that scale across the entire community. This includes the development and release of security guidance through the NSA public website (www.nsa.gov) and sponsorship of a number of community events like the Cyber Defense Initiative and the Red Blue Symposium. It also includes support for, or development of, open standards for vulnerability information (like CVE, the standard naming scheme for vulnerabilities); the creation of the extensible Configuration Checklist Description Format (XCCDF) to automate the implementation and measurement of security guidance; and joint sponsorship, with the National Institute of Standards and Technology (NIST) and the Defense Information Systems Agency (DISA), of the Information Security Automation Program (ISAP), to help security professionals automate security compliance and manage vulnerabilities. The presentation will also discuss the cultural shift we have been making to treat network security as a community problem, one that requires largescale openness and cooperation with security stakeholders at all points in the security supply chain operators, suppliers, buyers, authorities and practitioners.

Network Mathematics: Why is it a Small World?

Oskar Sandberg
Chalmers Technical University
and Guteborg University

Networks are central do almost everything that hackers do. Be they computer networks, peer-to-peer networks, information networks, or social networks, they are all around us and understanding them is the key to understanding both the strengths and vulnerabilities of our world. The speaker, a mathematician working in the field of complex networks, will introduce the modern mathematics of networks, and how it can be applied to real-world situations.

In particular, we will look at the small-world phenomenon, which says that points in many naturally occurring networks tend to separated in only a few steps. In the case of social networks formed by friendship bonds, this is the famous “six degrees of separation”. We will discuss the relevance of this to the world around us, as well as attempt an understanding of the dynamics of such networks, what makes them special, and why they seem to form naturally without explicit design.

The Church of WiFi Presents: Hacking Iraq

Michael Schearer
“theprez98”

What in the world is a U.S. Navy officer (a Naval Flight Officer, no less) doing in the middle of Iraq? Electronic warfare, of course! The Church of WiFi presents an unclassified presentation of theprez98’s experiences during his 9-month tour in Iraq. Embedded with Army units on the ground, theprez98 brought his expertise in electronic warfare to bear against the biggest threat to coalition forces - the improvised explosive device (IED). He will explore the communications infrastructure and the brief history of the Internet in Iraq. Furthermore, drawing on his background as an EA-6B Electronic Countermeasures Officer, he will explain the counter-IED fight in Iraq. Finally, he will discuss the prospects for the future.

Q & A with Bruce Schneier

Bruce Schneier

Bruce Schneier is an internationally renowned security technologist and CTO of BT Counterpane, referred to by The Economist as a “security guru.” He is the author of eight books— including the best sellers “Beyond Fear: Thinking Sensibly about Security in an Uncertain World,” “Secrets and Lies,” and “Applied Cryptography”—and hundreds of articles and academic papers. His influential newsletter, Crypto-Gram, and blog “Schneier on Security,” are read by over 250,000 people. He is a prolific writer and lecturer, a frequent guest on television and radio, has testified before Congress, and is regularly quoted in the press on issues surrounding security and privacy.

The Executable Image Exploit

Michael Schrenk

The “Executable Image Exploit” lets you insert a dynamic program into any community website that allows references to off-domain images; like MySpace or eBay. By uploading the following line of HTML to a community website, <img src=”http://www.mydomain.com/executable.jpg”> you can launch a dynamic program that masquerades as a static image and capable of reading and writing cookies, analyzing referrer (and other browser) variables and access databases. It is even possible to create an image the causes a browser to execute JavaScript.

Panel: Center for Democracy & Technology Anti-Spyware Coalition

Ari Schwartz,
Moderator Deputy Director,
The Center for Democracy and Technology

Profit and motive for spyware will increase drastically over the next three years. How are federal agencies and corporations planning for this surge? What are next big technological breakthroughs? How can we prepare?

The Edge of Forever - Making Computer History

Jason Scott
TEXTFILES.COM

Too often, “Computer History” gets shoved into a forgotten bin of irrelevancy, devoid of use for lessons and understanding. Even more often, people often fail to realize they’re making history themselves. Jason Scott will walk though the basics of computer history, what to save, how to ensure things last for future generations, or perhaps how to ensure it’s never found again.

A Crazy Toaster: Can Home Devices Turn Against Us?

Dror Shalev
Security Expert,
Check Point Software Technologies

Home networking devices, wireless equivalents, hardware and technology raise new privacy and trust issues. Can home devices turn against us and spy on our home network? Do we care if our toaster sees us naked? This talk will cover a scenario of “Crazy Toaster”. Trojan device under Vista and XP environment, or software with TCP/IP capabilities like routers, media players or access points, that joins a local area network and thus becoming a security hazard.

This “Crazy Toaster” presentation will discuss the steps needed to conduct a Trojan device that exploits users trust in technology. Flaws associated with home networking protocols such as UPnP and SSDP would be presented. The primary goal of the “Crazy Toaster” presentation is to present a new offensive technique by demonstrating the security hazard and design flaws. As home networking becomes more ubiquitous, the scope of this problem becomes worse.

Saving The Internet With Hate

Zed A. Shaw

Utu is the Maori word for a system of revenge used by Maori society to provide social controls and retribution. Utu is also a protocol that uses cryptographic models of social interaction to allow peers to vote on their dislike of other peer’s behavior. The goal of Utu is to experiment with the effects of bringing identity, reputation, and retribution to human communications on the Internet. A secondary goal is wiping out IRC because apparently nobody really likes IRC.

This presentation will cover the protocol’s design, use of cryptography, secure coding practices, and an analysis of it’s adoption and current research results. The presentation is for medium to advanced participants interested in similar open source projects. In the spirit of openness and collaboration and just plain evil, there will be an Utu server running for conference participants to use during the conference. The goal is to present the system, get people thinking, and obtain feedback on the design and implementation.

Cool stuff learned from Competing in the DC3 Digital Forensic Challenge

David C. Smith
University Information Security Officer,
Georgetown University
Mickey Lasky Senior Security Analyst

Last fall, the Department of Defense Cyber Crime Center (DC3) hosted a digital forensics challenge that included interesting puzzles such as physical media reconstruction, data carving, password cracking, and booting forensic images with virtual machines. My team from Georgetown University competed with a shoestring budget against a 140 teams and came in 4th place overall. The presentation will cover the individual challenges, our solutions, and the methodologies we developed to compete with the pros.

Thinking Outside the Console (box)

Squidly1 aka Theresa Verity

Having seen the ads this last holiday season, you think you might know all there is to know about the new crop of console game systems. But are these, and other console game systems, just for fun and games? Could they be used for other purposes?? Yes they can. With the advent of more powerful consoles many systems have the ability to do just about anything - after all they are still computers. Two years ago I gave a presentation at ToorCon discussing the hackability and usability of hand-held game systems. Since then, I have looked at all of the popular game consoles and researched their collective potential as platforms of covert penetration testing. Many of these machines can be easily modified to execute code not originally meant for game systems. In this topic I will discuss how game consoles can be used as another avenue in the penetration of your network...

When Tapes Go Missing

Robert Stoudt

We hear it in the news all too frequently, “26 IRS tapes containing taxpayer information potentially contain taxpayers’ names, SSNs, bank account numbers, or employer information”, “tapes containing customer information were stolen from a lock box... 196,000 names, SSN, etc”, “disappearance of 9 tapes containing payroll information on 52,000 employees, including SSNs and in some cases bank account numbers. The 9th tape contained “less sensitive” information about 83,000 hospital patients.”

With quotes such as “It is important for customers to note that these tapes cannot be read without specific computer equipment and software”, in attempted damage control, it is critical that we understand when such statements are true and under what circumstances they are not.

With this in mind, we will take a look at the little investigated field of tape forensics. We will look at how easy it is to recover data from tape, the limitations of tape data recovery and tape data recovery methods, and of course, steps to protect your company data.

Hacking the EULA: Reverse Benchmarking Web Application Security Scanners

Tom Stracener
Sr. Security Analyst, Cenzic
Marce Luck
Information Security Architect,
A Fortune 100 Company

Each year thousands of work hours are lost by security practitioners as time is spent sorting through web application security reports and separating out erroneous vulnerability data. Individuals must currently work through this process in a vacuum, as there is no publicly available information that is helpful. Restrictive EULAs (End User License Agreements) prohibit examining a signature code-base for common errors or signature flaws. Due to the latter point, a chilling effect and has discouraged public research into the common types of false positives that existing commercial technologies are prone to exhibit.

Reverse Benchmarking is a new species of reverse engineering that involves running a security solution against an application designed to solicit false positives. Unlike testing scenarios that emphasize gathering valid or accurate data, Reverse Benchmarking involves exposing architectural or logical flaws within a web application scanner by employing techniques to trick simple rule-based mechanisms. Running a scanner against a Reverse Benchmark target quickly reveals faulty rules, flawed testing logic, or poorly written or implemented security testing procedures. Additionally, a Reverse Benchmarking application will expose patterns in the propensity of a scanner to report false results, making it easier to spot false positives when they occur in the future.

Reverse Benchmarking opens up new opportunities for studying and improving existing web application security technology by exposing common faults in testing logic that are often the culprit of massive false positives. In turn this facilitates research into a taxonomy of general false positive types, ideally, a schema for mapping particular security tests to a common, generic language. This can provide a framework around which public discussion, research, and documentation of such flaws can occur without violating EULA agreements. We will also discuss the formation of a open community initiative centered around the use of Reverse Benchmarking to study false positive types.

Fingerprinting and Cracking Java Obfuscated Code

Subere

The process of obfuscating intermediate platform independent code, such as Java bytecode or Common Intermediate Language (CIL) code aims to make the source code generated by reverse engineering much less useful to an attacker or competitor. This talk focuses on the examination of fingerprinting particular obfuscators and provides a tool capable of cracking key obfuscation processes performed. As more programming languages use intermediate platform techniques on compiled code, the vision behind this talk is to further provide a methodology in reversing obfuscated applications. The demonstration of the tool developed on a number of cases will show how such a methodology can be put in place for cracking obfuscation techniques.

Creating Unreliable Systems, Attacking the Systems that Attack You

Sysmin
The Hacker Pimps
Marklar
The Hacker Pimps

This presentation focuses on analysis and strategies in dealing with systems that gather information, more specifically, personal information. This talk suggests that we need to start looking at the technology of the future through different a different set of eyes, the ones of a researcher. A new classification method is introduced for the classification of attacks on information gathering systems and strategies are introduced for dealing with this technology. Systems that are unreliable cannot be counted on, so the best defense is a good offense.

Sysmin and Marklar are two of the founding members of the Hacker Pimps, an independent security research think tank. The Hacker Pimps provide research in to areas of information security and privacy. Members of the Hacker Pimps have been speakers at a variety of different security events.

The Church of WiFi’s Wireless Extravaganza

Thorn
The Baby-Eating Bishop of Bath and Wells
Renderman
Sacramental Wine Taste Tester
theprez98
Spoonfeeder Extraordinaire

The Church of WiFi (reformed) returns to Las Vegas bigger and better than ever. Last year we brought you the first pre-computed rainbow tables for faster WPA cracking. This year, we’ve gone overboard and expanded the tables to places and sizes not dared before. Can you say: our own live distro?

And that’s not all: we’re prostelytizing our wireless foo this year by hosting the Wireless Village, a place for tutorials, mini-presentations, and breakout sessions. Of course, we have some new projects to show you and a few more ideas on the horizon. Isn’t it time you converted?

Hacking UFOlogy: Thirty Years in the Wilderness of Mirrors

Richard Thieme
ThiemeWorks
“You’re over the line,” an intelligence professional told Richard Thieme recently. “You know enough to know what’s not true but you can’t know enough to know what is. You’re well into the wilderness of mirrors.”

Hacking one complex system is always in some ways like hacking another. You must see nested levels of the context that others assume and which is therefore invisible, you must see through the story that the system tells about itself, and you must have a means of filtering out disinformation and misinformation while suspending belief in the patterns your own mind suggests along the way. You must never believe what you think until the evidence is compelling. And you must have a way of staying sane when the consensus reality that has knitted you into its tissue is challenged at its core.

Ever since a USAF fighter pilot with the "right stuff" told Richard Thieme (who was then his Episcopal clergyman) in 1978 that "We chase the things and can't catch them" — Thieme has explored this domain with beginner's eyes and an open mind. He has interviewed astronauts and NASA psychologists, physicists and social scientists, and scholars in "the invisible college" who conduct serious research and rigorous historical analysis. He has compared notes with intelligence professionals who believe that the least unlikely hypothesis for some of the data is, as one said, "a cultural intrusion" over many decades.

In this presentation, Thieme shows how "hacking the system" of data, disinformation, and "true believers" in an environment which has been saturated with ridicule since 1952, when critical elements of the government made a decision to debunk reports and those making them, is like hacking any complex system in our world of huge black budgets, appropriate paranoia, psy ops, and obsessive secrecy.

This presentation will make you think. It will make you re-examine your presuppositions about what is real. It will at the least bring you face to face with the possibility that you have been "owned" by the managers of perception who appointed themselves guardians of the Bigger Picture - an awareness that animates all real hackers.

High Insecurity: Locks, Lies, and Liability

Marc Weber Tobias
Investigative Attorney and
Security Specialist
Security.org
Matt Fiddler
Security Specialist - Security.org

There is a lot of hype by lock manufacturers, especially those that sell "High Security" cylinders. Terms like "pick proof" and "bump proof" often accompany UL and ANSI rated locks and cylinders.

If your intent is to protect your home then you can be assured that a lock carrying a UL 437 or ANSI rating is quite sufficient. The rules drastically change however if you are going to rely upon locks to protect high value targets such as cash, sensitive information, munitions, or critical infrastructure components. It is then that you might want to do a bit more research into what really constitutes a high security lock and how they can be compromised in the real world. In this presentation we will dissect and analyze these high security standards. Covert methods of picking, bumping, and certain other bypass techniques will also be presented and demonstrated allowing even the highest rated cylinders to be compromised in well under ten minutes.

Portable Privacy: Digital Munitions for the Privacy War

Steve Topletz
Hacktivismo Member;
Administrator, XeroBank

This talk will discuss the increasing need for portable privacy protection, and the pragmatic tools to accomplish it. A law only gives you consent to exercise a right you must already be able to assert. With the open war on privacy rights, not creating tracks has become more important because of increasing data retention and the risks it exposes.

Steve Topletz from Hacktivismo will present the risks, development framework, and solutions to retain your privacy. The talk will include tools for private communications, encrypted data storage, anonymous commerce, and portable secure computing environments. Steve will also be providing a development pre-release of xB Machine, a new portable secure computing environment. A limited number of free XeroBank anonymous internet accounts will also be provided to attendees.

Locksport: An emerging subculture

Schuyler Towne
Board of Directors, TOOOL US

Locksport is nothing new, but it's recent attention in the media and sudden growth have made it a popular topic. This talk will settle some of the bigger debates about the Locksport community. Are we criminals? Are we having a positive impact on modern security? Who started it? Who's advancing the field? And, why do we do it?
This talk will cover a brief history of locks, but will focus primarily on how the locksport community has grown, it's ethics (and ethical struggles) and it's impact on modern security. You will not learn how to pick locks at this talk, but you will learn how lockpickers have impacted your everyday lives.

So, if you've ever taken an interest in good old physical security, come out and learn about the new generation of hardware hackers. Pick the planet!

Malware Secrets

Valsmith
Offensive Computing, LLC
Delchi

What would you do if you had a massive collection of malware? What secrets could you uncover? This rapid fire presentation seeks to reveal some of these secrets based on the analysis of Offensive Computing's large malware collection. (Over 100,000 samples) What are malware author's commonly using to pack their binaries? What are the rarest packers, and could this indicated a targeted attack? How do Anti-Virus companies generally perform on a data set known to contain a large number of malware? These are the some of the questions we will answer in Malware Secrets.

How I Learned to Stop Fuzzing and Find More Bugs

Jacob West
Manager, Security Research Group,
Fortify Software

Fuzzing and other runtime testing techniques are great at finding certain kinds of bugs. The trick is, effective fuzzing requires a lot of customization. The fuzzer needs to understand the protocol being spoken, anticipate the kinds of things that could go wrong in the program, and have some way to judge whether or not the program has gone into a tailspin. Get this setup wrong, and you end up fuzzing the wrong thing, exercising and re-exercising trivial paths through the program, or just plain missing bugs (as Microsoft did with the .ANI cursor vulnerability). Fuzzing effectively takes a lot of customization and a lot of time.

Proponents of fuzzing often avoid static analysis, citing irrelevant results and false positives as key pain points. But is there a more effective way to channel the energy required for good fuzzing in order to find more bugs faster? This presentation will propose a series of techniques for customizing static, rather than dynamic, tools that will let you find more and better-quality bugs than you ever thought possible.

We compare static and dynamic approaches to testing and look at:

- The fundamental problems involved in fuzzing
- Why static analysis is harder for humans to think about than fuzzing
- Interfaces for customizing static analysis tools
- The kinds of bugs static analysis is good at finding
- Why static analysis is both faster and more thorough then fuzzing
- Where static analysis tools break down

The talk concludes with the results of an experiment we conducted on open-source code to compare the effectiveness of fuzzing and static analysis at finding a known-set of security bugs.

Turn-Key Pen Test Labs

Thomas Wilhelm

Currently, those interested in learning how to professionally conduct Information System Penetration Tests have very little options available to them - they can either illegally attack Internet-connected systems, or create their own PenTest Lab. For those who prefer to avoid legal complications, they really only have the last option - a lab. However, this can be a very complicated and expensive alternative. In addition, scenarios have to be created that actually represent real-world scenarios; for a beginner, this is is a Catch-22 since they don't yet have the experience to even know what these scenarios might look like, let alone design them in a challenging way.

In order to provide a simple way for both beginners and experts to improve their skills in Penetration Testing, I have designed what is, in effect, a Turn-Key PenTest Lab using LiveCDs and minimal equipment requirements. The LiveCDs each represent different scenarios that mimic real-world systems and services, which provide essential challenges to improve critical skills in the field of PenTesting. The LiveCDs are available under the GNU GPL license, and freely available to the public.

Multiplatform malware within the .NET-Framework

Paul Sebastian Ziegler
Tatsumori

Multiplatform Malware - many of us have heard that term. Discussions on this matter arose a few month ago and they didn't cease yet. But while many people have taken interest in this matter there still isn't much of a common sense around. The time has come to change this! In this speech you will learn about:

- The current status of multiplatform malware.
- The possibilities multiplatform malware opens up for an attacker.
- Different kinds of multiplatform malware.
- How to easily implement multiplatform malware using runtime frameworks You will also see a live demonstration of multiplatform malware while it's in action hopping between multiple operating systems with ease.

Multiplatform malware is here to stay. And it will be a blast to computer security once it starts to strike. Many systems we presently consider "secure" will be broken, many basic concepts of security will be circumvented. If we don't want to be on lost stands as defenders once that happens—or if we want to ride the wave as attackers—we'll have to act now. Let's create the common sense the community has long waited for! Let's discover what is possible and where fiction starts! Let's all make this fairly new technique blossom or explode - whichever you prefer.

Z-Phone

Philip R. Zimmermann

The time for secure encrypted VoIP for the masses is upon us. The Zfone Project has come a long way in the two years since Phil Zimmermann demoed a prototype at Black Hat. It's now a family of products, running on Symbian and Windows mobile phones, soft VoIP clients on Mac OS X, Windows, Linux, and in the Asterisk PBX, in both open source and commercial products. Zfone lets you whisper in someone's ear from a thousand miles away.

Phil will be explaining the ZRTP protocol used by Zfone, and demoing it. The ZRTP protocol does not rely on a PKI. It also does not rely on SIP signaling for the key management, and in fact does not rely on any servers at all. This means your VoIP security doesn't depend on VoIP service providers who don't always act with your best interests in mind. ZRTP performs its key agreements and key management in a purely peer-to-peer manner over the RTP packet stream. And it supports opportunistic encryption by auto-sensing if the other VoIP client supports ZRTP.

The law enforcement community will be understandably concerned about the effects encrypted VoIP will have on their ability to perform lawful intercepts. But what will be the overall effects on the criminal justice system if we fail to encrypt VoIP? Historically, law enforcement has benefited from a strong asymmetry in the feasibility of government or criminals wiretapping the PSTN. As we migrate to VoIP, that asymmetry collapses. VoIP interception is so easy, organized crime will be able to wiretap prosecutors and judges, revealing details of ongoing investigations, names of witnesses and informants, and conversations with their wives about what time to pick up their kids at school. The law enforcement community will come to recognize that VoIP encryption actually serves their vital interests.

Book Signings

Mike Schrenk
@ No Starch Press
Friday August 3 @ 15:00
Author of:

Webbots, Spiders, and Screen Scrapers: A Guide to Developing Internet Agents with PHP/CURL

Johnny Long
@ Breakpoint Books
Friday August 3 @ 15:00
Author of:

"Stealing the Network: How to Own a Shadow"

"Google Talking"

"Techno Security's Guide to Managing Risks for It Managers, Auditors and Investigators"

"Asterisk Hacking"

Vendors

Irvine Underground

EFF

Immunity

Jinx Hackwear

MECO

Ghetto Geeks

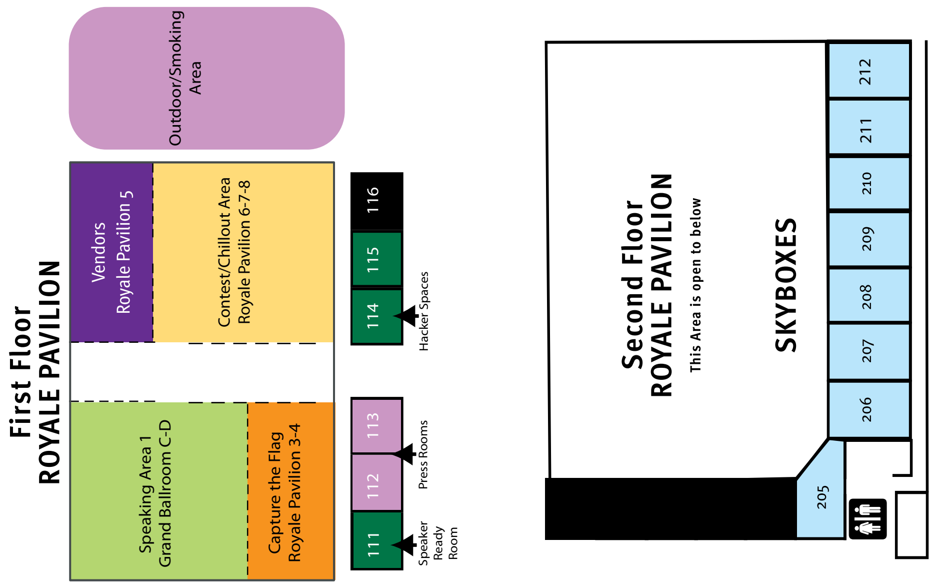
UNIX Surplus

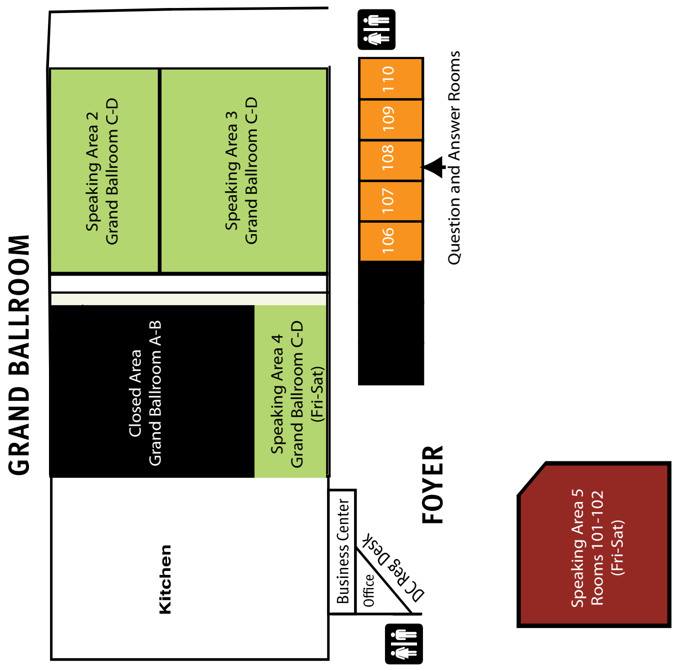
The Sound of Knowledge

E-teknet

UAT

Shadowvex





Pre-Con - Thursday: August 2

12:00 - 22:00	Registration - $100 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store located in the same room as Registration Vendor Area Setup: 11:00 - 18:00
18:00 - ???	The Unofficial Defcon 15 Toxic BBQ will be held for its fourth consecutive year. Details of the TBBQ's location can be found at http://www.toxicbbq.com. Sign on to the Defcon Forums and help plan this year's event.

Day 1 - Friday: August 3

08:00- 22:00	Registration - $100 USD CASH ONLY - Avoid the lines and get your badge early. Registration will be at the West Registration Desk. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store across from Registration. Vendor Area Hours: 10:00 - 19:00

	Track 1	Track 2	Track 3	Track 4	Track 5
10:00 - 10:50	**Joe Grand** Making of the DEFCON 15 Badge	**Church Of WiFi's Wireless Extravaganza**	**Sean Bodmer** Analyzing Intrusions & Intruders	**Jennifer Granick** Disclosure and Intellectual Property Law: Case Studies	**Tony Sager** Vulnerabilities and The Information Assurance Directorate
11:00 - 11:50	**Bruce Schneier** Q & A with Bruce Schneier	**Patrik Karlsson** SQL injection and out-of-band channeling	**David Litchfield** Database Forensics	**Robert Clark** Computer and Internet Security Law - A Year in Review 2006 - 2007Year In Review	**Meet The VCs**
12:00 - 12:50	**Thomas Wilhelm** Turn-Key Pen Test Labs	**Philip Zimmermann** Z-Phone	**Chris Palmer & Alex Stamos** Breaking Forensics Software	**Dead Addict** Picking up the Zero Day; An Everyones Guide to Unexpected Disclosures	**Panel: Anti Spyware Coalition**
13:00 - 13:50	**Jacob West** How I Learned to Stop Fuzzing and Find More Bugs	**Alfredo Ortega** OpenBSD remote Exploit and another IPv6 vulnerabilities	**Scott Moulton** Re-Animating Drives & Advanced Data Recovery	**Steve Dunker** Everything you ever wanted to know about Police Procedure in 50 minutes.	**Disclosure Panel**
14:00 - 14:50	**Danny Quist & Valsmith** Covert Debugging: Circumventing Software Armoring Techniques	**Martyn Ruks** MQ Jumping	**David C. Smith** Cool stuff learned from competing in the DC3 digital forensic challenge	**John Benson** Bridging the Gap Between Technology and the Law	**Bruce Potter** Dirty Secrets of the Security Industry
15:00 - 15:50	**Benjamin Kurtz** Functional Fuzzing with Funk	**Greg Hoglund** Virtual World, Real Hacking	**Rich Murphey** Windows Vista Log Forensics	**Alexander Muentz** Protecting your IT infrastructure from legal attacks- Subpoenas, Warrants and Transitive Trust	**Myles Long, Rob "Flack" O'Hara, & Christian "RaDMan" Wirth** Self Publishing in the Underground
16:00 - 16:50	**H.D.Moore & Valsmith** Tactical Exploitation	**Haroon Meer & Marco Slaviero** It's All About the Timing	**Robert Stoudt** When Tapes Go Missing	**Danny O'Brien** Digital Rights Worldwide: Or How to Build a Global Hacker Conspiracy	**Luiz Eduardo** The Hacker Society around the (corporate) world
17:00 - 17:50	**Damien Gomez** Intelligent debugging for vuln-dev	**Jared DeMott, Dr. Richard Enbody & Dr. Bill Punch** Revolutionizing the Field of Grey-box Attack Surface Testing with Evolutionary Fuzzing	**The Dark Tangent** CiscoGate	**Peter Berghammer** A Journalist's Perspective on Security Research	**Mike Murray & Lee Kushner** Creating and Managing Your Security Career
18:00 - 18:20	**Subere** Fingerprinting and Cracking Java Obfuscated Code	**Charlie Miller** How smart is Intelligent Fuzzing - or - How stupid is Dumb Fuzzing?	**Richard Thieme** Hacking UFOlogy: Thirty Years in the Wilderness of Mirrors	**Sam Bowne** Teaching Hacking at College	**Ofir Arkin** kNAC!
18:30 - 18:50	**Edward Lee** Comparing Application Security Tools	**Ian G. Harris** INTERSTATE: A Stateful Protocol Fuzzer for SIP		**David Hulton** Faster PwninG Assured: New adventures with FPGAs	
19:00 - 19:50	**Meet the Feds**	**Luke Jennings** One token to rule them all	**Aaron Higbee** Hack Your Car for Boost and Power!	**Panel: Ask the EFF**	
20:00 - 20:20	**Johnny Long** No-Tech Hacking	**Toralv Dirro & Dirk Kollberg** Trojans: A Reality Check	**Michael Schrenk** The Executable Image Exploit		
20:30 - 20:50					

Day 2 - Saturday: August 4

08:00 - 22:00	Registration - $100 USD CASH ONLY - Avoid the lines and get your badge early. Registration will be at the West Registration Desk.Official DEFCON Store in the Vendor Area at the J!nx Hackwear BoothVendor Area Hours: 10:00 - 19:00

10:00 - 10:50	**Steve Orrin** The SOA/XML Threat Model and New XML/SOA/Web 2.0 Attacks & Threats	**Paul Ziegler** Multiplatform malware within the .NET-Framework	**Dror Shalev** A Crazy Toaster: Can Home Devices Turn Against Us?	**Thomas Holt** The Market for Malware	**NeonRa1n & Julian Spillane** Hack your brain with video games
11:00 - 11:20		**Valsmith & Delchi** Malware Secrets	**Janne Lindqvist** IPv6 is Bad for Your Privacy		**Pilgrim** How to be a WiFi Ninja
11:30 - 11:50	**Aaron Peterson** Pen-testing Wi-Fi	**Agent X** 44 lines about 22 things that keep me up at night	**Andrea Barisani** Injecting RDS-TMC Traffic Information Signals a.k.a. How to freak out your Satellite Navigation	**Nathan Evans & Christian Grothoff** Routing in The Dark: Pitch Black	
12:00 - 12:50	**King Tuna** Hacking EVDO	**Broward Horne** Click Fraud Detection with Practical Memetics		**Nick Mathewson** Technical Changes Since You Last Heard About Tor	**Mike Murray & Anton Chuvakin** The Science of Social Engineering: NLP, Hypnosis and the science of persuasion
13:00 - 13:50	**K.N. Gopinath** Multipot: A More Potent Variant of Evil Twin	**Vitaliy Kamlyuk** Fighting Malware on your own	**Ganesh Devarajan** Unraveling SCADA Protocols: Using Sulley Fuzzer	**Nick Mathewson** Social Attacks on Anonymity Networks	**Dan Kaminsky** Black Ops 2007: Design Reviewing The Web
14:00 - 14:50	**Doug Mohney** The Next Wireless Frontier - TV White Spaces	**D.J.Capelis** Virtualization: Enough holes to work Vegas	**John Heasman** Hacking the Extensible Firmware Interface	**Roger Dingledine** Tor and blocking- resistance	**Jason Scott** The Edge of Forever - Making Computer History
15:00 - 15:50	**Sysmin & Marklar** Creating Unreliable Systems, Attacking the Systems that Attack You	**Dave Josephsen** Homeless Vikings, (short-lived bgp prefix hijacking and the spamwars)	**Zac Franken** Hacking your Access Control Reader		
16:00 - 16:50	**Ricky Hill** GeoLocation of Wireless Access Points and "Wireless GeoCaching"	**Gadi Evron** Webserver Botnets	**Lukas Grunwald** Security by Politics - Why it will never work	**Zed Shaw** Saving The Internet With Hate	**Plet** Stealing Identity Management Systems
17:00 - 17:50	**Brett Neilson** Being in the know... Listening to and understanding modern radio systems	**Peter Gutmann** The Commercial Malware Industry	**Joel Eriksson, Karl Janmar, Claes Nyberg, Christer Oberg** Kernel Wars	**Mike Perry** Securing the Tor Network	**Panel: Internet Wars 2007**
18:00 - 18:50	**Vivek Ramachandran** The Emperor Has No Cloak - WEP Cloaking Exposed	**Daniel Peck & Ben Feinstein** CaffeineMonkey: Automated Collection, Detection and Analysis of Malicious JavaScript	**Shawn Moyer** (un)Smashing the Stack: Overflows, Counter- measures, and the Real World		
19:00 - 19:50	**David Gustin** Hardware Hacking for Software Geeks	**Kenneth Geers** Greetz from Room 101	**atlas** Remedial Heap Overflows: dlmalloc style	**Steve Topletz** Portable Privacy	
20:00 - 20:50	**Michael Schearer** The Church of WiFi Presents: Hacking Iraq	**Gadi Evron** Estonia and Information Warfare	**Squidly1** Thinking Outside the Console (box)	**|)ruid** Real-time Steganography with RTP	

Day 3 - Sunday: August 5

08:00 - 12:00	Registration - $100 USD CASH ONLY - Avoid the lines and get your badge early. Registration will be at the West Registration Desk.Official DEFCON Store in the Vendor Area at the J!nx Hackwear Booth Vendor Area Hours: 10:00 - 15:00

	Track 1	Track 2	Track 3
10:00 - 10:50	**Dan Hubbard** HoneyJax (AKA Web Security Monitoring and Intelligence 2.0)	**geoffrey** The Completion Backward Principle	**Tom Stracener & Marce Luck** Hacking the EULA: Reverse Benchmarking Web Application Security Scanners
11:00 - 11:50	**Rick Deacon** Hacking Social Lives: MySpace.com	**Deviant Ollam, Noid, Thorn, Jur1st** Boomstick Fu: The Fundamentals of Physical Security at its Most Basic Level	**Oskar Sandberg** Network Mathematics: Why is it a Small World?
12:00 - 12:50	**Aviv Raff & Iftach Ian Amit** The Inherent Insecurity of Widgets and Gadgets	**Schuyler Towne** Locksport: An emerging subculture	**Matt Richard** Beyond Vulnerability Scanning - Extrusion and Exploitability Scanning
13:00 - 13:50	**Brendan O'Connor** Greater than 1: Defeating ""strong"" Authentication in Web Applications	**Greg Conti** Satellite Imagery Analysis	**Jesse D'Aguanno** LAN Protocol Attacks Part 1 - Arp Reloaded
14:00 - 14:50	**David Byrne** Intranet Invasion With Anti-DNS Pinning	**Marc Weber Tobias & Matt Fiddler** High Insecurity: Locks, Lies, and Liability	**Sergey Bratus** Entropy-based data organization tricks for log and packet capture browsing
15:00 - 15:50	**Billy Rios & Nathan McFeters** Biting tha Hand that Feeds You - Storing and Serving Malicious Content From Well Known Web Servers		**Crispin Cowan** Securing Linux Applications With AppArmor
00 - 16:50	Award Ceremonies hosted by Dark Tangent		

DEF CON Shout Outs!

This year over two hundred people helped make DEF CON possible. From printing shirts to helping with the network planning, from words of encouragement to 3am crunch time work, everyone does their part. Below are some of the people that deserve recognition. If you are not mentioned I apologize! Sometimes things get lost in the cracks of the interweb.

I'll start with the 'home team' those that work year round with the back end stuff to make it all possible. Black Beetle, ETA, Nikita, Sleestak, Jameson, Charel, and our counterparts at the Riv. McNabb for the great printing job, Ira for hauling our stuff down to Vegas, Infesteddanigan for last minute network help!

Once everything shows up at the con Zac takes over operations to help make sure all the teams are getting set up on time for a mid Thursday open. Thanks Zac! I think this is the 13th year you have been involved! Once I arrive Thursday night he has things under control and we start to split ops duties, but really our teams run so well that we are a self correcting bunch.

The network, phone, and TV systems are run by the DEFCON Network team of ninjas. We are proud to say they make a hostile environment functional! Each year they increase the bandwidth and access points. The Network and DCTV team would like to send a thanks to: Lockheed, Videoman, Heather, effffn, Sqweak, Connor, Major Malfunction, and the Rant Radio guys: Derek, Cimmerian, Sparky, and Sean Kennedy.

Registraton takes all your money in a smooth and efficient manner! Q and TW would like to thank their team: Rahael, Allen, Tyler Cohen, Carine, Mario, cstone, and Bart plus the crew from Blaine!

Roamer watches over the vendor area, and wants to send out thanks to wiseacre, Phorkus Maximus, AlxRogan, Russ, Security Tribe, wad, panadero, xaphan, libero, tflat and all at NVF.

Russ tries to wrangle all the contests, and through his hard work has helped not only launch the DC Groups but also encourage more participation at the con. It is a team effort and wants to thank Roamer, Pyr0, Dans, Hackajar, wad, panadero, libero, Phorkus, l0stboy, Security Tribe, 303, Black Beetle, SecHor, and all the goons.

Once Uncle Ira drops off the gear the QM stores takes over and manages logistics. QM Stores this year is Major Malfunction, ETA, Generic Superhero, Esteban, and someone that only Q knows the name of… :)
Noid would like to thank all the security Goons who work hard so you don't have to: flea, Queeg, Sky Dog, Carric, CHS, Xinc, Teklord, Chosen1, Cyber, Cy Mike, John D., Kruger, Spahkle, GM1, The Capn, Pescador, Quiet, RiversidE, Vidiot, Luna, Rik, David, Montell, Vect0rX, Pappy, Arclight, h3adrush, dcode, Priest, Kevin E., Justabill, Freshmn, Kampf, Che, Fox Captain, Cjunkie, and Metalhead the Original Goon™, who couldn't make it this year, says "Shouts to all the Goons! , have a juniper mallet for me. See you next year!"

Press coordination by Nico and Crew. Nico would like to thank Bren, Dead Addict, Dirk, and Nicole for managing the press.

All the Speaker Control Goons who make sure the speakers get checked in, get paid, and show up on stage in one piece. This gets more complicated every year as the number of speakers and tracks increase. Agent X would like to thank his team, Nikita, Quagmire Joe, Code24, ArkAngel, Nick Farr, Amish, #2, 5 O'clock Shadow, Bk Delong, Rich Mogull, and Space Girl.

The Black & White Ball has been going on for years, and recently split into a two night affair. Thanks to the hard work of Bink and zziks for pulling this off every year!

Russ rides shotgun on all the contests and would like to call out DC949, Panadero, mel, Kallahar, Doc, converge, Shrdlu, Foofus, Deviant Ollam, Faustus, Thorn, lostboy, Ryan Fox, Shawn Moyer, Siviak, Network Ninjas, Riverside, and Kenshoto for putting on a great CtF!

The DEF CON Forums, https://forum.defcon.org/, is run by a team of ninjas starting with The Cot Man, Converge, Roamer, and the many moderators including octalpus, astcell, Thorn, scroou, Black Beetle, Noid, AlxRogan, The Dark Tangent. For https://pics.defcon.org/ The Cot Man would like to thank: che, Nikita, and renderman.

-The Dark Tangent

00010001LSB