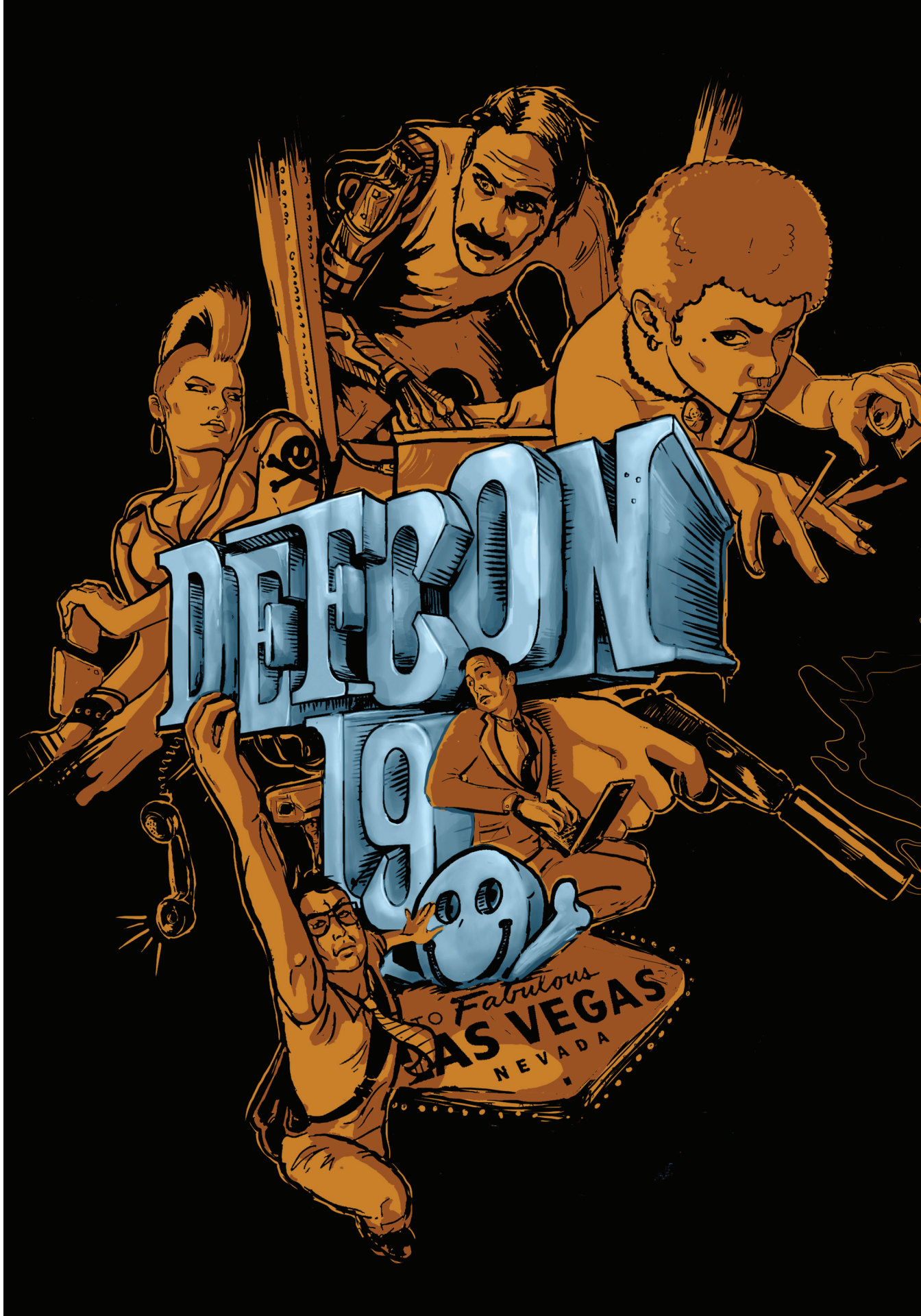
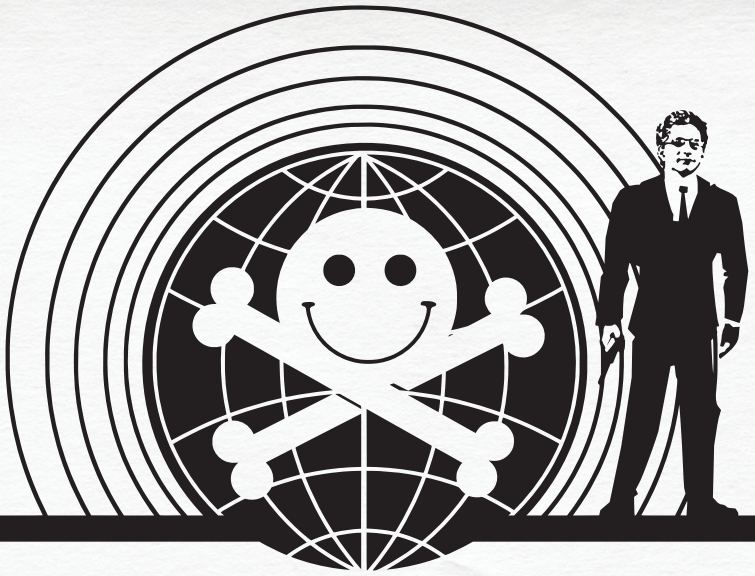

DEFCON
19
Fabulous
AS VEGAS
NEVADA



D.E.F.C.O.N.

For 19 years I have tried to get interesting hackers to tell us what they have been up to, what tools they have built, and how they attack and defend. It turns out that many more people than I imagined were interested in the same stuff. Since the early days the con has evolved to match the technology trends and interests of attendees. The loose spy vs. spy theme of this year is only half a joke, with more nations and criminal groups using cyberspace to gather information and further their own agendas than ever before. I predict another wave of computer security legislation on the horizon, the likes we haven't seen since the DMCA.

For those of you who have been coming for years, as well those of you new to the con, we have lots of surprises for you in store. First off, notice this thing you are holding? Isn't it cool? For the first time we have enough pages to give our font size a +1 so we don't go blind, and rock a first ever DVD to fill with 0days. We are bringing it on site so it will have the most up to date content, instead of stale weeks old presentations. This year it is a single layer, maybe next time a DL?

A new hotel means new adventures. If all works out, by the time you read this we will have tested the DEF CON TV channels and for the first time since we were at the Alexis Park you will be able to kick back in your hotel room and watch most all of the speaking rooms as well as an info channel. Being at the Rio also means more space for contests, speakers, and chill out. We have more music, more pool access, and more speakers.

Some of the other new stuff we are trying this year is a new badge design that is full of clues and hints, that has easy to solve components, as well as the beginnings of a weekend challenge. Without giving to much away the badge, and things around it, are all clues. CTF has grown by two teams, and by next year it will grow again to truly become the world series of hacking contests.

So get involved, make new friends, you will find people are very open and accommodating if you put some thought into your questions and are willing to approach things with an open mind. You don't need to be a lock pick expert to go to the lock pick village, and even if you don't have something to teach I bet by next year you will. "DEF CON is what you make of it" and we have done all we can to give everyone the opportunity to learn, make friends, and enjoy.

Finally, as we are building up to DEF CON 20, our 20th anniversary, we are trying things out that may or may not work. Network coverage areas, floor plans and traffic flow, party locations, and new contest. We want to learn what works best this year so by next we can focus on making DEF CON 20 the con you won't soon forget.

-Dark Tangent

BADGE

"…I don't know what next year will bring. Just expect the unexpected."
– Joe Grand, Final Sentence of the Defcon 18 Badge Description

Grade 1, Commercially Pure Titanium Composition
Titanium 99.67
Carbon 0.08
Iron 0.03
Nitrogen 0.03
Oxygen 0.18
Hydrogen 0.015
(Percentage by weight)

So you've arrived at Defcon. You stood anxiously in line for reg, wondering what the badge will be like this year. Finally it's your turn. Your heart races as you hand over your money and are handed your badge. But something is amiss! Where's the gameboy on a string you waited all year to receive?

That's right, Defcon's not doing electronic badges this year. Electronic badges are so common place at security conferences now it has become passé. So DT asked me to try something different. Percentage wise relatively few people participated in the hack the badge competitions when they were purely hardware based. This year I hope to change that. As a hardware person myself I would have enjoyed creating an electronic badge, but if we did electronic again my good friend Joe may as well have continued with his awesome designs. Moving to a puzzle based reality game will open the playing field to a larger percentage of attendees. As is typical in my contests, each stage has multiple levels of difficulty, from the pretty easy to the "how the hell did they figure that out". Above all I hope the game is enjoyable, and fosters meeting and talking with others.

Made from 0.040" thick Commercially Pure titanium, each Badge weighs approximately .05 ounces. Sheets of material (produced by the Kroll process) were stacked four thick, and fabricated via waterjet (think squirt gun from hell, cutting via erosion). Ti has a linear coefficient of thermal expansion approximately 50% that of stainless steel, making it ideal for use in aerospace and missile applications.

The cut pieces were then deburred via tumbling and antiqued/oxidized by raising their temperature to 1000 degrees in an industrial kiln. The antiquing effect was intended to make the metal look old and worn in support of badge game ambience. All production was done in the United States.

The number of badge designs is not being released as but suffice it to say it is much larger than the standard seven, namely (G)oon, (P)ress, (V)endor, (C)ontest, (S)peaker, (H)uman, and (U)ber. See how many variants you can find.

I've hired a professional actor for the reality game to perform throughout the conference, and added little puzzles here and there for everyone's amusement. Easter eggs accompany all of the mini-puzzles, and overall score will be adjusted in proportion to easter egg difficulty.

Have fun everyone!

Ryan "1o57" Clarke

TOP SECRET

NETWORK

System.output.wifi(ssid)

DefCon – 802.11b/g

DefConA – 802.11a

DefCon-SECURE – 802.1x/wpa2

We're back, with all the wifiz you can take! The DefCon/DefConA SSID's remain open for whatever nefarious activities you have dreamt up. We're bringing back the "secure" wifi for those who want to reduce their risk profile. It's using 802.1x/WPA2 to secure your OTA connection, and keeps your client connection trunked to the firewall and then out to the Internet. Beyond that, good luck

The Rio has allotted us 100Mbps of Internet connectivity. We anticipate this will suffice for all the last minute iOS updates, video streaming, and all other activities that are both planned and unplanned) this year. Enjoy!

Shouts-out to the NOC staff who keep things running every year: Lockheed, Heather, Videoman, effffn, Enki, Mac, Sparky, and DJ t3ase.

Let us know how the network's working for you - noc@defconnetworking.org.

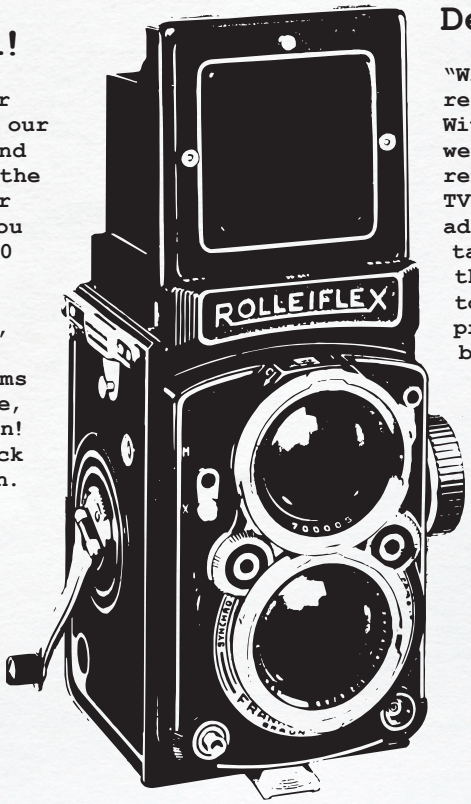
Check throughout con for stats & wrap-up at http://www.defconnetworking.org/.

::HACK UPON XYLEM::

www.defcon.org/1057/ CLASSIFIED

The Hacker Confessional!

This year with better lighting…! Look for our beautiful grey box and green button around the con area. The Hacker Confessional gives you a chance to make a 30 second video that could make it up on DefCon TV. Remember, we're broadcasting through to hotel rooms this year – so please, think of the children! To watch online, check out http://DCTV.defcon.org.



DefCon TV

"With great power comes great responsibility" – Stan Lee. With our arrival at the Rio, we enjoy capabilities which remind us of days past – DefCon TV is back in full force! In addition to broadcasting talks, we've teamed up with the Hacker News Network (HNN) to provide reporting and production facilities. They'll be interviewing speakers, contests, and maybe even you! Look for HNN interviews and reports on DCTV this year throughout the con.

For information or requests email dctv@defconnetworking.org

DEFCON-19 ENTERTAINMENT

SPY VS SPY

FRI BLACK BALL [SHAKEN HARD]

RIO PAVILLION #1: 9PM-5AM

VJ Q-ALBA
Zack Fasel [@zfasel]
Dale Chase
Dual Core
YTCracker
Means+Function
highsage a.k.a. shagghie
DJ Lahbug
Great Scott+Don Vaughn

SAT WHITE BALL [REALLY STIRRED]

RIO PAVILLION #1: 9PM-5AM

Twinkdogg
AnonymousX
DJ SailorGloom {AoE}
REGENERATOR
Miss Jackalope
djdead
LoveBug
Krisz Klink

FRI POOL 6PM-12AM

2-Dub Breaks
Inconspicuous Villain
Ol' Skinny
Traxmyth+Indaskyes
DSTROY
DJ Odyssey

SAT POOL 6PM-12AM

DJ Sinfinity
mauvehed
JSB
Fillmatic
the_audiophile
Alexander King

RESIDENT CHILLOUT DJ [ALL OTHER HOURS OF RIO PAVILLION #1]: KAMPF

DECOR+VISUALS BY: ZEBBLER, KATE VAN REES & JACOB FENWICK
VJING BY: KEVIN @ DESIGN FLAW | SOUND BY: MOBIUS

TOP SECRET

CONTESTS

Gringo Warrior

Noon to 17:00 in the Contest Area

What happens when a good time goes bad? Imagine the following scenario... you are attending a con in Southern California. On a whim (or possibly at the suggestion of Dan Kaminsky) some folks decide to cross the border into Tijuana for a cheap tequila drink-a-thon. You accompany them, but the evening gets way out of control. You awaken in a small room in the back of what appears to be a run-down police station. You become vaguely aware of uniformed individuals speaking to you in a threatening manner. Making references to violation of laws against public drunkenness, your captors describe monumental fines and penalties. They imply that unless you clean out your bank account using your ATM card unless you will face considerable jail time. They slam the door, saying that they're going to give you some time alone to think about their offer.

Your mind races, your brow sweats. Is this really happening? If you comply, what's to stop them from just dumping you in the desert somewhere? Are these people even really police officers? You come to the determination that you have no intention of going along quietly with their plans. Your captors may have confiscated your wallet and passport... but they didn't notice the lockpicks that you were carrying.

Participants in Gringo Warrior will have five minutes to free themselves from handcuffs, escape from their "cell", get past a guard, retrieve their passport from a locked filing cabinet, leave through another locked door, and make their escape to freedom. The course will offer a variety of locks representing a range of difficulty, allowing participation by people of all skill levels. Points will be awarded based on the time of completion as well as the difficulty of locks attempted.The best warrior of all wins the grand prize!

Wall of Sheep

9:00 - 18:00 in the Contest Area

The Wall of Sheep is a Unique and interactive security awareness project that teaches attendees how to secure their devices, monitor traffic on a network and discover plain text protocols ~ Gawk: At the "sheep" captured and placed on the wall, Learn: how to protect yourself, Test: your sheep herding skills & Hope: you're not on the wall! This year the Wall of Sheep will be awarding a prize.

Social-Engineer.Org "The Schmooze Strikes Back - SECTF 2"

Friday 9:30 to 17:00/Sat 10:00 - 17:00/Sun (podcast) 11:00 to 14:00 in the Contest Area

Each contestant is dared to show if they have "the schmooze" by calling target companies to try and obtain "flags" of information from them by using non-malicious methods. Information gathering, reporting, elicitation, pretexting and more are all put to the test in this amazing SE contest.

Defcon Scavenger Hunt

Friday Noon To Sunday Noon in the Contest Area

As one of Defcon's longest running contests the Scavenger Hunt is a competition of will, creativity, smarts and chutzpah as teams search for unusual items and complete insane stunts. With prizes donated by ThinkGeek.com, EvilMadScientist.com, and EVERYONE in the Defcon vendor room, we have thousands of dollars in cool prizes. Come WIN yours! Remember, our "Quick Time" challenges are instant wins and are open to anyone attending the conference so be sure to follow us on Twitter

@defconscavhunt!

Network Forensics Puzzle Contest

Thursday @ 12:00 - Sunday @ 10:00 in the Contest Area

Ann Dercover is on the run, and you're hot on her trail as she travels around the globe hacking companies, stealing intellectual property, launching 0-day attacks and setting up sneaky backdoors. *You are the forensic investigator.* You've got a packet capture of Ann's network traffic. Can you analyze Ann's malicious traffic and solve the crime by Sunday?

Hack Fortress

Friday noon - 20:00, Saturday 9:00 - 20:00 in the Contest Area

Hack Fortress combines elements of two classic contests; a multidisciplinary hacking contest and a Team Fortress 2 LAN party. Calling upon the best of both, Hack Fortress will pit teams of players against one another in a dual-challenge event over the course of two days at DefCon 19.

Separate challenges but both occurring at the same time, teams will consist of two elements battling with their wits and trigger-fingers. One portion of a team will engage in an all-out TF2 bracketed tournament--pitting their best TF2 players against another team's. At the same time, the second element of a team will attempt to tackle the "Hack" challenges based on the "Hack or Halo" competition from ShmooCon.

But, you may be asking yourself, why call this Hack Fortress? It sounds like two separate tournaments. But, you would be wrong, good sir or madam. Very wrong, indeed. For both competitions will have an impact on each other. As players hack their way through the challenges, they will not only earn points for their team but will also be gifting their TF2 players bonuses and perks to give them an edge. A solved challenge may result in 15 seconds of critical hits or something else as devious. The same is also true for the TF2 team--without a flag or point capture in game, it may be impossibly hard to hack through a particular challenge. Without coordination and cooperation between the two elements of a team, neither will be victorious.

So, bring your thinking hats, ready to tackle challenges, and be prepared to take on the very best TF2 players--armed with their own type of hats. Performing exceedingly well in one event is not the course to victory--one must be ready to tackle the enemy on both fronts.

Defcon Radio

Friday at open thru Sunday two hours prior to closing ceremonies in the Contest Area

Defcon Radio is a live Internet radio stream covering all aspects of Defcon during the convention. During the day, open signups will be available online and at the Defcon Radio table to host a show. Topics can be anything involving geekery, but security topics are encouraged. We will also be interviewing speakers,giving updates on contests, and covering other daytime Defcon news.

At night, our feed will switch to the DJs located around the con as our field correspondents hit the parties to cover the sweet groove

action.

Crack Me If You Can

Thursday (23:59) -> Saturday (23:59) in the Contest Area

48 hour contest.Teams of password crackers have 48 hours to crack as many password hashes as they can. The KoreLogic team puts out a large list of hashes of various formats, complexities, etc) and the teams compete for HARD CASH. At last years DEFCON we gave away $1,000 to the various winning teams.

The hashes are created in a way to reward innovation in teamwork, skill, and processing power. The team with the most processing power is not gaurenteed to win, because a large majority of the passwords are not just random strings that can only be found via brute force. Instead, the plaintexts are created based off of patterns seen "in the wild". The teams are expected to take advantage of this fact and use logic to crack these passwords before attempting brute force.

The various hashes used are chosen based on what is seen "in the wild" as well. The teams are not told what the formats will be ahead of time.

The only requirement to have a team is that 1 member be located onsite at DEFCON.

Capture the Packet

9:00 - 18:00 in the Contest Area

CTP "Capture the Packet" is the ultimate traffic analysis competition with live network traffic containing clues, hints, and pieces of the puzzle. In this fast paced skills challenge each team of two will have one hour to sniff/analyze network traffic, decipher clues and solve puzzles to earn points, the winner of each round goes onto the final round where the winner is bestowed the CTP grand prize. Last year many played but only one team walked away the CTP 2010 Winner, will you be next ?

Register at www.CaptureThePacket.com

DEFCON Geo Challenge 2.1

Website will be online 24/7, Booth will be open Fri/Sat 12:00-18:00

What is the Geo Challenge?

The Defcon Geo Challenge is basically urban geo caching with a high tech twist. Contestants will solve puzzles provided by a live contest Website and then submit their answers online via mobile devices. Correct answers will result in GPS coordinates leading them to a disguised geocache. Each puzzle will lead to a cache, each cache will unlock another puzzle. Some caches will be embedded with RFID tokens that can be used to unlock the next puzzle, while some caches may be a puzzle in itself.Rules & Requirements? Teams can consist of no more than 3 people. Each team must have some type of mobile internet device. Smartphones with internet and GPS will work to compete in this contest. Most puzzles and answers can be submitted online, but a few will require a visit to the contest booth. The website should be available the entire con. Registration will be at the Geo Challenge booth, 12:00 noon Friday.

Prizes:

Visit the website to see who has donated prizes for this year's event.

What's new this year?

This year scoring will be based on multiple factors. Points will be awarded for bonus caches, fastest solves, and total puzzles

solved. First to finish will not necessarily be the winner, so make sure to only start your next puzzle when you are able to complete it in one session.The Return of the Geo Challenge. - Why 2.1?

The first Geo Challenge was held at DEFCON 17, we had 30 participants, (2) teams who finished all the puzzles and 1 who came close. We would like to thank Adam Savage from MythBusters not only for his prize donations at DC17, but for accepting our invitation and speaking at the con. What a kick off to a brand new contest! The DC18 Geo Challenge was cancelled due to theft of contest gear that could not be replaced quickly. DEFCON 19 will be the 2nd Geo Challenge, but the 3rd year it has been scheduled. Thus Geo Challenge 2.1
Website: http://www.defcongeochallenge.com
Twitter: DCGeoChallenge
Facebook: DefconGeoChallenge

Arduino 101 - Workspace/Workshop

Friday & Saturday in the Contest Area

Have an Arduino that is just sitting around collecting dust? Ever wondered what it takes to develop Arduino projects? Come by the Arduino 101 workspace for a quick how to, hands on instruction. We will be located directly adjacent to the (Geo Challenge Booth) in the contest area. Sensors, Arduinos, and other modules will be available for your instant learning curve. If you've never touched an Arduino this workspace is for you. We will also explain how some of our Arduino based projects work, what the costs were to create them, and the development process involved in such items. Grab a chair and ask questions, that's what were here for. I myself have only began to delve into the world of Arduino, but it's how fast I was able to get started that prompted me to host this workspace.

Hosted By [Syntax] of DC210

Crash And Compile

Saturday - 20:00 until whenever in the Contest Area

An ACM style programming contest, crossed with a drinking game. What can possibly go wrong?

Beverage Cooling Contraption Contest

Friday at exactly noon.

If there's two things that many hackers know, it's how to enjoy a frosty, refreshing beverage and how to leverage technology to make life better… or at the very least, more entertaining. The Beverage Cooling Contraption Contest asks the question: if you were to be stranded in a hot, dry climate… would you be able to take cans of liquid refreshment sitting at room temperature and turn them into something more palatable?

Teams will put their wits and their fabrication skills to the test in the hope of developing technological contraptions that can accept liquid input (which may range between 70º or over 90º, depending on the Las Vegas sun) and cool said beverage to below 40º in as little time as possible. With bonus points being awarded for cost-efficient, energy-efficient designs as well as creative aesthetic choices, even bystanders are likely to get a kick out of the proceedings. Heh… and if that's not enough encouragement for you, bear in mind that there will be plenty of free beverages available for participants to, ahem, "calibrate their equipment" and so forth. That often leads to an excess of technology output and we have to do something with it… so drop on by and have a good time with us!

15-minute survey for a free t-shirt

9:00 - 21:00 in the Contest Area

The purpose of this research study is to gather information from hackers to obtain increased understanding of hacking from the hackers' perspective. The findings of this study will help the general public better understand how different intentions of hacking might entail different implications for various social groups.

CONTESTS

DEFCON Beard & Championship
Saturday 18:00 in the Contest Area

Due to the growing number of awesome beards at DEFCON and the (popularity?) of the shitshow that is beardsmanship, it's time that folks were recognized for letting their unix beards fly. (see this video, the show is airing august 6th: http://www.youtube.com/watch?v=xfLiZup6PCY)

Open Capture The Flag
Friday and Saturday, 10:00 - 22:00 in the Contest Area

Not to be confused with the original Capture the Flag (CTF), oCTF is a multi-discipline hacking competition for all skill levels from novice to expert. Organized by the Dirtbags, and open to all Defcon attendees. (Formerly known as aCTF or "Amateur Capture The Flag.")

10,000¢ Hacker Pyramid
Friday and Saturday night preceeding Jeopardy 20:00 in Track 1

First night for qualification rounds, second night for semi-final and final rounds

The 10,000¢ Hacker Pyramid is a classic game show take off with the kind of pizazz that only teams composed of average DEFCON Attendees and (in)famous DEFCON Celebrities could possibly bring to the stage. In a series of rounds, 8 teams will vie for the ultimate prize - 10,000 Canadian Pennies! Watch as Dick Clark's worst nightmares come true and a new DEFCON tradition is born. And don't feel bad for the losers - we've got prizes for them too - AWESOME prizes.

Dark Tangent's Tamper Evident Contest
Friday-Sunday in the Contest Area

You will be given a package. This package will have tamper evident seals on it. Some of these products claim to be "Impossible to reseal or reuse". Your goal is to prove them wrong and document your work every step of the way.

Capture the Flag (CTF) - binjitsu 2011
CTF Contest Room
All Con until 14:00 Sun

The following teams have demonstrated their uber prowess by qualifying to participate in the DEFCON 19 Capture the Flag Contest: Binjitsu III, organized by DDTEK.

Out of more than 280 widely international teams, 11 have been selected to battle last year's champions, ACME Pharm, for the CTF title! DEFCON and DDTEK would like to congratulate all of these talented teams and wish them luck!

Hates Irony
sutegoma2
lollersk8ers
IV
European
Nopsled Team
Routards
Plaid Parliament of Pwning
Shellphish
VelociROPtors
int3pids
PLUS@Postech

Defcon Cannonball Run

It was inspired by the Deathrace 2000 caravan but it was decided to have people get there faster. In past years we have had cheaters, police and KTLA News. This year we have no idea what will happen but you will hear rumors at the bar.

Network sniffer shooting game
in the Contest Area

The Schemaverse DEFCON Tournament (When Space elephants attack)
Friday until Sunday afternoon in the Contest Area

Registration will occur at the booth from 9am to 6pm on Saturday.

The Schemaverse is a space-based strategy game implemented entirely within a PostgreSQL database where you compete against other players using raw SQL commands. Use your SQL skills to interactively command your fleets to glory during this weekend-long tournament for the database geeks. Or, if your PL/pgSQL-foo is strong, wield it to write AI and have your fleet command itself while you enjoy the con!

Be The Match Foundation Bone Marrow Drive
in the Contest Area

DefCon Massage
in the Contest Area

Datamatrix Contest
Friday & Saturday in the Contest Area

Datamatrix is a reverse engineering game. At the start of the game, a portion of some source code is published for all the contestants; further portions will be published during the contest.

The program underlying this source code accepts as input a bitstring describing the user ID and an input bitstring of 256 bits. The form factor of the input is a 16x16 matrix (grid) that is colored by users and presented to webcams available at the contests table.

Participants can audit the source code and send input to the program. Depending on the input, the program assigns points to the user. The one that makes the most points wins.

The contest is played exclusively during the Conference. Each player is handled a welcome/invitation/activation Datamatrix at the Contest Table. Also available, will be empty, ready to be filled, Datamatrices. To process a Datamatrix the player should show it to any of the contest webcams that will be sitting at the Contest Table. There will be also a screen showing a point table and some internal data for the players to obtain additional hints as they present the Datamatrices to the system.

The players are expected to analyze the source code, understand how Datamatrices are crafted and come up with ideas to create their own Datamatrices in ways that they obtain the most possible points. The first two players that obtain the biggest quantity of points will be awarded prizes.

EFF's Hack the Vote

Vendor booth hours (9:00 to 17:00)

EFF and Vegas 2.0 proudly present Hack the Vote, an election on e-voting machines. Which candidates wins will be determined by the number of votes and your ability to steal them. How else to best elect the World's No. 1 Hacker? E-voting legal expert Matt Zimmerman and Professor Alex Halderman, noted e-voting security expert, will be judging this contest and have determined that the Accuvote e-voting machines are impenetrable. If states rely on them to vote our democratically elected representatives into office, then surely even an election among the best hackers in the world will be fairly decided by the number of votes cast. We are hoping to host a workshop on Friday that introduces contestants to the machine, so they know how to cast their ballot accurately. Once inside the voting booth, they will have a a set amount of time to punch the right buttons. Specific rules will be provided to contestants. Any suspicious activity, including a final tally that outnumbers votes cast, will be considered illegal, undemocratic, and down right shameful. The voting booth will provide a measure of privacy and whose to say exactly how someone will cast their vote with no one looking over your shoulders. In case this contest doesn't sound judicious enough, we will be charging a poll tax, in the form of a donation to EFF.

Watch The Carnage

Open during Contest Area Hours

View the DefCon network activity as a 3D model, in real time. Take a turn flying through it and trying to find your friends. Try to set off the IDS in such a way that it creates a cool visual effect. Help us answer the question: "Is it really the most hostile network on Earth??"

EFF Fundraiser: Hackers and Guns in Las Vegas – Ya gotta love it.

10:00 – 20:00 in the Contest Area

You've seen it played out numerous times in movies and on TV. A flash bang grenade goes off. SWAT kicks in the door and moves quickly to differentiate between the good guys and the bad guys in the same room. How do they train to effectively recognize and take out the bad guys, while not wasting any of the hostages?

One of the tools they use is a Firearms Training Simulator or FATS system and someone was foolish enough to let us get our hands on one. The system has been very popular in past couple years we've run it and each year we try to kick it up a notch. Stop by and see what we have cooked up for Defcon 19. Hint: Live Targets?

How do you find us? Just listen for the sound of gun fire as you are exploring the con, and that would be us. We will be running the training from 10:am – 8:pm. In addition to the training we will be doing shooting contests where you could win some cool stuff.

So check in to the range and see if you got the skillz to make it through the challenges unscathed. Then the next time you hear a knock at your door in the middle of the night - you'll be ready.

The Skill Drills courseware comprises training drills that focus on the improvement of your student's speed, accuracy, and decision making skills. This courseware was developed by training professionals to focus on hand-eye coordination and has been tested by active Military and Law Enforcement instructors to ensure its training effectiveness. The courseware consists of drills that allow individual combatants to execute training exercises designed to improve target acquisition using laser-based training or Laser Shot's exclusive Live-Fire System Trainer. Each drill allows an instructor to tailor every training session, using adjustable settings such as number of targets, target face time, target speed, and more, for individual skill levels from beginner to expert.

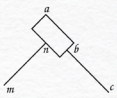
All proceeds go to support the Electronic Frontier Foundation – Leading the fight to protect your personal privacy and digital rights since 1990. More info at EFF.org

Develop for Privacy Challenge Awards

We live in a world of smartphones and other mobile devices that provide amazing services. But these same devices can also collect and share vast amounts of data that can paint a detailed picture about where we go, who we know, what we do and even what we think. Protecting this critical information is more important than ever. But too many users lack the tools that would enable them to take advantage of new technology without losing control of their personal information. The first Develop for Privacy Challenge is our inaugural effort to bridge this gap. We've solicited privacy-enhancing apps from professional and amateur developers, put them in front of a panel of expert judges in the privacy and security space, and selected the best of them to promote and draw attention to issues of online privacy. But the challenge doesn't end there. We need the hackers to take the best apps we get and make them even better. So we'll be announcing our winners at DEFCON and ensuring they are released as open source projects so they can be improved, distributed, and put to use. We hope you'll come check them out and join us in ensuring that the future of mobile devices protects rather than compromises our privacy.

Project 2

Friday 9am-12am
Saturday 9am-12am
Sunday 9am-12pm



Project 2 is active. Look for puzzles everywhere in the con, bring your answers to the terminal in the contest area.

#BloodKode Challenge!

There will be two types of entries into the challenge:

BASIC --- Raffle with normal prizes.

You need to attend the blood drive and donate for BarKode. You will need to bring your proof to a booth at DefCon to sign up, which will then make you eligible to win one of the "normal" prizes. No worries if you have already done so before the challenge, or before the con,just bring in the proof! Please note though we don't want BarKode to get alcohol poisoning so be careful about what you drink before & AFTER donating! ~;-)

EXTREME --- Raffle with AWESOME prizes.

You will need to get your picture taken in the most creative way possible, preferably with a picture or cut out of Barkode with you WHILE you are giving blood & provide proof that it went to Barkode. People who do that will be in the running for the 1st tier prizes (Chris Summer has donated a DEFCON skate board that we will get the DEFCON speakers, goons etc. to sign.) Plus other cool goodies! Please submit your photos on the forums at: https://forum.defcon.org/showthread.php?t=12351

GRAND PRIZE -- There is only 1.

A healthy BarKode! No one should forget that it's not about the prizes: It's about helping out one of our own!

Twitter: #BloodKode

TOP SECRET

EVENTS

theSummit
Thursday at 20:30pm Pavilion 1 (Chillout)

Returning for it's 7th year, Vegas 2.0 is excited to bring back theSummit!

theSummit is a Fund Raiser for the Electronic Frontier Foundation (EFF) on Thursday Night. It features DEF CON, BlackHat, and B/Sides Speakers and Security Specialist from across the globe. Here's your opportunity to put a face to the names you've read about. Ask them a question about there talk, discuss a project your working on, or simply just enjoy a beer with this years 1337.

By attending you are not only offering your self an opportunity to network with this years speakers, but you also helping support one of the most noble organizations, the EFF!

Featuring performances by Dual Core and DJ Jackalope, free beer and mixed drinks sponsored by Google's Digital Liberation Front, door prizes, auction, and general shenanigans.

Start Time: Thursday, August 4th, 2011 at 8:30pm

End Time: Friday, August 5th, 2011 at 4:00am

Location: The Rio Hotel & Casino - Pavilion 1 (Chill lounge)

$40 at the door, Open to all ages

Follow Us on Twitter for Event and Feature Guest Updates:

www.twitter.com/effsummit

Goon band
Friday 20:00 in the Contest Area

The Goon Band rocks the Rio as it returns to Defcon for the third year. Join us Friday night at 8 PM in the Contest area for the best way to get the evening's parties started. We've got more songs than ever, a full size stage, and tons of space for moshing, or just hanging out. Just be sure to take off your badge first. The Goon Band is Roamer, Rich, GM1, vertig0, and Doc.

Mohawk-Con
10:00 – 20:00 in the Contest Area

Get your head buzzed and donate to a non-profit of your choice. EFF? Hackers for Charity? Maybe you'd like to help out your local hackerspace. We could say we're making a statement about how punk values reflect the fight for digital freedoms but we'd be full of it. We do it because it's fun and to support the scene.

Forum Meet

Queercon
Fri and Saturday: Mixer 16:00 in DJ/ Chillout, Friday 22:00 in Rio Pavilion 4

Queercon is BACK! For the eighth year in a row, bigger and better, we're out at the Rio and ready for fun!

Looking for a safe place where you can relax, cut loose, and meet people like yourself? Both Friday and Saturday afternoon at 4PM, join us for a laid-back pre-funk in the DJ Chillout area (Pavilion 1). Come drink, socialize, and swap stories.

On Friday night starting at 10PM in Rio Pavilion 4, we'll turn up the bass for the hottest dance party EVAR! We have an amazing space, Ninja magic, international headliner DJs, and a top-notch system to keep the music

going all night long. Best of all, it's FREE! All GLBTQ+friends are welcome. YOU ARE MADE OF AWESOME AND WE LOVE YOU!

Forum Meet
Friday 19:00 in Pavilion 3

The "Forum Meet" offers the Defcon online community the opportunity to meet and put a face to the names and avatars they see year round on the Defcon forum. It's a place to see old friends and make new ones. If you are a forum participant or "lurker" stop by and say hello.

If you are new to Defcon this is an excellent opportunity to become part of the year round Defcon experience. This event gives you, the new Defcon attendee an opportunity to join in, and gives you a chance to ask questions about the Con that you may not have other opportunities to get answered elsewhere.

It's the place to meet other likeminded individuals in a casual easy going atmosphere, no loud music or flashing lights. A place conducive to just talking and having good conversations.

The "Forum Meet" is not meant to be a "Destination" It is a "starting point" a place to meet people with similar interests and then go explore all that Defcon in Vegas has to offer!

Hacker Karaoke
Thursday 21:00- 2:00
Friday 22:00 - 2:00 On the Contest Stage

Want to BE the performer? Well trot your happy ass down to Hacker Karaoke, DEFCON's first on-site karaoke experience where you can be a star, e don't know it. Don't want to be a star? At Hacker Karaoke you can also in making an utter fool of yourself. Join Bascule and OverDose as we p casbah in "Rock the Casbah".

DEF CON 101

Thursday 13:00 - 15:00 in Track 1

DC101 is the Alpha to the closing ceremony's Omega. This is the place to go to learn about the many facets of Con and to begin your Defconian Adventure. Whether you're a n00b or a long time attendee, DC101 can start you down the path toward maximizing your DefCon Experiences.

As in the past, some DefCon veterans will give a glimpse into their own journey, speaking about how they got involved with the community while giving you some tips on how to do the same.

We'll be hearing from Nikita (one of the few full-time DefCon employees), Roamer (head vendor goon and a fountain of DefConian Knowledge), Lockheed (DefCon Network Architect and head of the NoC team), GM1 (a security team leader, toxic bbq organizer and a member of the goon band), and pyr0 (jack-of-all-trades at DefCon including contests). After a ten minute intermission we'll be right back...

DefCon 101 is Sponsored by Runnerup, HighWiz and the letters F, A, and G.

The Mini-Games will be back again this year!

Lost has a badge related surprised during his mini-game time.

Siviak, Eris Vandal and their Scavenger Hunt cohorts will be back running their mini-game.

The DefCon 101 speakers : Nikita, Roamer, Lockheed, GM1, Pyr0, HighWiz.

DefCon 101 Helpers: Xodia and Ripshy

Most of the speakers at DefCon 101 also believe that using your real name when presenting at DefCon is kinda lame.

VILLAGES

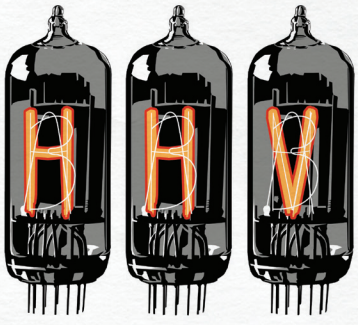
Lockpicking Village

Are you interested in learning more about the mystery behind locks and tools to open them? Are you curious as to how they work, how we use them, and how they can be opened without keys? Perhaps you are already a seasoned picker and want to show off your skills! Stop by the Lockpick Village to learn, practice, or show off!

The Lockpick Village is a fun physical security demonstration and participation area run by The Open Organisation Of Lockpickers, a non-profit organization. Workshops and talks will be held throughout the day covering topics for novices and experts alike. Learn about the history behind mechanical locks, experiment with exotic lock designs, and test your skills against your friends and compete head to head in a multitude of exciting contests!

TOOOL members and other experts will be on hand with plenty of trial locks, picks, shims, and other devices. By exploring the construction and flaws of mechanical lock designs, you can learn how to apply the hacker mindset in order to manipulate locks open in non-destructive ways. Fun for hackers, tinkerers, and professionals alike, the Lockpick Village is the place to gain a much stronger understanding about the role locks play in our physical security today. Don't have any tools yet? Visit the TOOOL table in the vendor area to get some shiny new picks from the only place where 100% of all profits go directly towards the lockpicking community!

Hardware Hacking Village



A place for teaching, learning and experimenting, the HHV has seen unprecedented growth since inception by Russ Rogers (Vertigo) and Ryan Clarke (LostboY) several years ago. As a general rule people trust their hardware (it's common place to reformat a drive, not so common to replace chips, etc.) often allowing hardware vectors to go unnoticed by attackers and defenders alike.

We invite everyone to stop by the HHV and play with some hardware, sit in on a mini-lecture, or help teach others with your mad hardware skills. Come burn some parts just to learn the smell (so you can identify failures in your own work)!

This year we will have mini workshops with people such as Joe Grand, Jon Williams, LosT, and the Null Space Labs just to name a few! We have lots of hardware to give away, and stuff for you to play with and learn on. Hardware kits will also be for sale at the Defcon SWAG booth and in the vendor area. If you've never had experience with hardware, pick up a kit and bring it to the village, we will have people ready to help you get started, so when you return home you can continue on your path to hardware bliss!
See you at the HHV!

Wireless Village

Friday 10:00 - 20:00
Saturday 10:00 - 20:00
Sunday 10:00-12:00
Closed at 12:00 - 15:00 for the Amateur Radio Exams

The Wireless Village is going to be covering all things associated with wireless communications, especially the areas of Amateur Radio, 802.11, RFID, and Bluetooth. The focus is being placed on education with a four hour course, 1030-1230 Friday and Saturday, designed to teach attendees the information needed to pass the FCC Element Two license exam and receive their Amateur Radio Technician Class license. There will be presentations on the various components that make up 802.11 as well as mini-contest involving WEP, WPA/WPA2 cracking. Some of the subject to be covered are the differences in the various modes (802.11a/b/g/n), aircrack-ng, airdrop-ng, etc. as well as things you can do to make your home wireless network more secure. We are planning to have demonstrations on bluetooth and RFID.

DEFCON Kids will have two rooms focused on content for beginner hackers age 8-16. There will be a classroom for kids to participate in demos and workshops, such as learning how to open Master locks, Google Hacking, making Electronics, Social Engineering, coding in Scratch and Communicating in Code. There will be a workstation room for kids to participate in hacking activities anytime throughout the two days, including a Codebreaking Museum, a Maker-bot and the Hardware Hacking Station. The rooms are on a first-come, first-serve basis. There will also be contests just for kids, including social engineering and lockpicking. Follow us on Twitter @DefConKids or online at www.defconkids.org for last minute updates.

Classromm Schedule: Amazon M Room

Saturday

10:00 — **Meet the Keynote**
By Steven Levy

11:00 — **The History and Future of DEFCON + Tips**
By The Dark Tangent, Founder of DEFCON &
Jennifer Granick, Attorney at Zwillinger Genetski

12:00 — **Solving Puzzles**
By Marc Weber Tobias & Tommie Blackwell

13:00 — **The Wall of Sheep Workshop**
By CedoxX & FS

14:00 — **Secrets Revealed**
By Jennifer Wilcox
National Cryptologic Museum, NSA

15:00 — **Google Hacking**
By Johnny Long

16:00 — **Meet the Feds**
By Christopher Cleary, former Cyber Command;
Jerry Dixon, former DHS;
Jon Iadonashi, former Navy;
Rich Marshall, DHS;
Tony Sager, NSA;
Linton Wells, NDU

17:00 — **Social Hour**
By CyFi , cofounder of DEFCON Kids

Sunday

10:00 — **Hardware Hacking**
By Joe Grand

11:00 — **When You Can't Remember Your Locker Combination – Workshop and Contest**
By Deviant Ollam & Christina "Fabulous" Pei

12:00 — **Snapkit Electronic**
By Chris Hoff

13:00 — **Kids Capture the Packet**
By CedoxX & Riverside

14:00 — **Communicating in Code**
By Leigh Honeywell

15:00 — **Coding in Scratch**
By Chris Hoff

16:00 — **Social Engineer Your Future**
By Chris Hadnagy & Jim O'Gorman

17:00 — **Social Hour**
By CyFi , cofounder of DEFCON Kids

18:00 — **General Awards Session**

WorkStation Schedule: Amazon K Room

Saturday, 11:00-16:00

Lock Picking Station

Sunday, 11:00-16:00

Hardware Hacking Station

Saturday and Sunday, 11:00-16:00

Codebreaking Museum, NSA
Makerbot
Coded-Pen-Pal Sign Up
CyptoSculpture

DEFCON CTF SCORING

Scoring a CTF is a challenging proposition. In order to become a master of binjitsu, it is essential to understand how you will be measured.

True binjitsu masters understand that the path to enlightenment may only be achieved by maintaining the delicate balance between the offensive and the defensive arts. This year CTF scoring follows the approach introduced last year for measuring what is happening in the game and is designed to reward offensive as well as defensive excellence. Services constitute the heart of the CTF game. Each team must attack and defend identically configured servers, each running some number of custom services. The idea is to analyze the custom services for vulnerabilities and to develop both an attack and a defense strategy for each service. By exploiting a service an attacker gains access to privileged information which is generally referred to as a key (aka flag, aka token). Keys may be readable (steal information), writable (corrupt information), or both. Teams demonstrate that they have stolen information by turning stolen keys into a key submission server. Teams demonstrate that they can deface a service by overwriting keys with a replacement key unique to the attacker. For both of these activities, teams are awarded points. In order to keep things interesting, keys are periodically updated by the contest organizers, allowing teams to demonstrate that they can maintain continued access to their victim's data through submission or corruption of the new key values. Additionally the period during which teams may submit stolen keys is finite (for example within 30 minutes following the steal) in order to reduce the effects of key hoarding (displayed score not representative of actual score) and key sharing (where teams obtain keys by trading with other teams rather than via attacking other teams).

Rather than simply awarding a point per stolen or overwritten key, the scoring system treats keys as commodities (such as diamonds). The following factors are taken into account when deriving a team's overall score:

1. The more keys that are stolen/overwritten for a particular service, the less each key is worth.

2. Teams earn more points for demonstrating diversity of attack across a given service. In other words, teams can score points for attacking the weakest defender, but they can earn far more points by demonstrating that they can attack across all other teams as well. 3. The longer a team's attacks go unnoticed, the longer that a team remains the sole possessor of an 0-day, the more points a team can accrue for a given service (effectively cornering the market on that commodity)

Teams are awarded points as follows:

1. For a given service up to 1800 points are available for distribution to the teams. 900 points for reading keys from their 9 opponents and 900 points for overwriting keys of their 9 opponents.

2. For a given attacker, a given victim V, and a given service S, the attacker's partial score for the stealing keys from the service is their percentage (0-100) of all keys stolen from V via service S.

3. For a given service S, an attacker's score for service S is the sum of the their partial scores (across all of the other teams) for that service.

4. A team's overall raw score is the sum of its scores across all services in the game.

5. A team's raw score is then multiplied by a measure of the availability of the team's services for the duration of the game. Note that availability does not imply the service is unexploitable, so the team may not in fact be defending the service.

One example of a partial score awards a team 100 points if they are the only team to steal keys for service S from victim V, even if the attacker steals only one key. Thus this is a very valuable key. In another example team 1 may have stolen 400 keys, team 2 300 keys, team 3 200 keys, and team 4 100 keys from service S on victim V. In this second case, the teams are awarded 40, 30, 20, and 10 points respectively. In this case, individual keys are worth less because keys for this service are common.

Item 5 above is meant to ensure that a team does not simply shut down all of its services in order to achieve a perfect defense (and make a boring game for everyone else).

An interesting effect that may be observed under this scoring system is that a team's score may actually decrease from time to time. For example, the first team to submit a key for a service/victim will have the one and only key submitted and therefore a partial score of 100 (percent) for that service. If a second team submits a key for the same service/victim each team's partial score will now be 50 points and the first team will see a decrease in their score owing to the fact that their 0-day is no longer as valuable as it once was. On the other hand if the first team manages to capture 99 keys before the second team submits their first key, the first team will see their score drop almost imperceptibly from 100 to 99 while the second team's score will be only 1. This situation reflects the first team's early entry into the market for these keys and their near monopoly on these keys.

Those familiar with the "breakthrough" system of past CTFs, may note that there is no mention of breakthroughs in the description above. We feel that this scoring system rewards 0-day when 0-day is used effectively to build one's hoard of keys ahead of any other team developing their own version of the same exploit. Further this system allows teams to delay the use of their 0-day in order to keep the number of keys in play to a minimum with the associated risk that another team will beat them to the punch. Thus, in addition to testing a team's offensive and defensive skills, this scoring system attempts to make teams consider the strategy of how, when, and where to make use of their 0-day. Additionally it places increased emphasis on keeping exploits stealthy.

In the CTF room each team is assigned a unique color which is reflected by their team banner, tablecloth and on the scoring displays. The contest allows each team to have at most eight players at the table at any time (though some teams likely have additional resources beyond what is visible at the table). Teams are allowed to bring in whatever tools they prefer.

Stop by the CTF room and talk to a DDTEK representative for more details on the scoring system and displays you will see during the contest.

~ur CTF cr3w

DEFCON CTF HISTORY

CTF	DC	Year	winner	host - title / image (number of teams)
1	4	1996	AJ Reznor	goons - ctf
2	5	1997	AJ Reznor	goons - ctf
3	6	1998	SNI	goons - ctf
4	7	1999	ghettohackers	goons - ctf / up to team
5	8	2000	ghettohackers	goons - ctf / up to team
6	9	2001	ghetto+digirev	goons - ctf / up to team
7	10	2002	digirev	ghettohackers - root fu / redhat 6.2 (8)
8	11	2003	Anomaly	ghettohackers - root fu / openbsd (8)
9	12	2004	sk3wl0fr00t	ghettohackers - root fu / windows (8)
10	13	2005	shellphish	kenshoto - war gamez / freebsd 5.4 (8)
11	14	2006	1@stplace	kenshoto - war gamez / solaris 10 (8)
12	15	2007	1@stplace	kenshoto - war gamez / freebsd (8)
13	16	2008	Sk3wl0fr00t	kenshoto - war gamez / freebsd (8)
14	17	2009	vedagodz	ddtek - binjitsu / freebsd (10*)
15	18	2010	ACME Pharm	ddtek - binjitsu / freebsd+debian (10)
16	19	2011	TBD	ddtek - binjitsu / ????? (12)

*well actually 9, as the team “sk3wl0fr00t” was actually ddtek running the game from a team table

Capture the Flag is one of the oldest contests at Defcon dating back to Defcon 4. In the past few years, “capturing the flag” has become a popular moniker for all kinds of contests, and the sheer quantity of CTFs has been increasing steadily. Defcon CTF is one of the (if not the) oldest CTF that continues to run today. Here you can find a brief history of the contest and its evolution.

Defcon 4 was the first time CTF was really formalized into a contest - judges now decided when a points should be awarded. In Defcon 5 and 6, participants could either provide a target or attack provided targets for points, as you might imagine this amount of flexibility led to chaos on the game floor. Over the years, the game has matured and events such as point scoring have largely been automated (heavily in many cases), this maturity is largely a result of having dedicated, non-defcon organizers. Naming the organizer early allows the organizer to dedicate time to game structure and infrastructure.

After a display of dominance in DC7-9, the ghettohackers became contest organizers for three years, before giving the reigns up to Kenshoto. After winning twice (and coming very close to winning several other times) ddtek took over contest organization for DC17 (ddtek is a subgroup of Sk3wl0fr00t). During DC7-9 the contest seemed to be about equally as much about hacking the contest as hacking the game servers

Since DC10, CTF has been about custom services, pwn others’, patch and protect your own. Each organizer has built on this model with technology aimed at preserving a fair game, additional twists such as scoring methods, and ever increasing difficulty. Recent organizers have chosen to keep the game layout secret until the game starts, participants do not necessarily know the scoring algorithm, network structure, or operating systems involved. At its core CTF is meant to test computer and network security. To some, that seems to be a fairly narrow focus area, but most Defcon attendees realize that “cyber security” is actually a very large and diverse field. Services range from poorly implemented or configured crypto, SQL-injection, cross-site-scripting, buffer overflows, timing attacks, heap exploits, malformed network constructs, custom interpreters, the list is truly endless. What will the contest bring this year?

As the contest matured, teams started participating regularly and more desired to play. A method of “qualifying” was implemented similar to the Olympics and other sporting events. For the past several years a qualification weekend has pitted teams against a set of challenges and the clock. Teams with the most points at the end are invited to participate in person at Defcon. There is really no excuse to not participate in quals, if you’re reading this, you should register and participate next year. Phrases like “placing 132nd feels like quite an accomplishment” tend to appear on social networks.

In 2009 ddtek, an unknown name in the community, was announced as the CTF organizer. From the time of organizer announcement, through qualification round, a lot of google-translated IRC, and even through the entire contest during Defcon, nobody suspected that the folks sitting at the sk3wl0fr00t contest table were actually running the game! “Hacking the top hacker contest” seemed like a fun way to introduce ourselves to CTF organization. The yells of “bullshit” from CTF teams during the Defcon 17 awards ceremony were very gratifying.

more info at https://www.defcon.org/html/links/dc-ctf.html

more info at http://www.ddtek.biz

Swing by the CTF Room and see what’s going on. You’ll never really know what it’s about until you dive in.

~vulc@n

PRESENTATIONS

When Space Elephants Attack: A DEFCON Challenge for Database Geeks

Abstrct
Creator, The Schemaverse

The Schemaverse is a vast universe found purely within a PostgreSQL database. Control your fleet of ships manually with SQL commands or write AI in PL/pgSQL so they control themselves while you sit back and enjoy the con. This presentation will help my fellow database geeks to understand the game play mechanics used in The Schemaverse so they can compete in the weekend long tournament.

Bosses love Excel, Hackers too.

Chema Alonso
Juan Garrido "Silverhack"

Remote applications published in companies are around us in the cloud. In this talk we are going to add ICA and Terminal Server Apps to fingerprinting process, automating data analysis using FOCA. It will allow attacker to fingerprinting internal software, internal networks and combine the info in PTR Scanning, evil-grade attacks and command execution trough Excel files. In the end, we are going to play with a tricky feature in security policies about remote excel that will allow hackers to bypass macro restrictions.

Dust: Your Feed RSS Belongs To You! Avoid Censorship!

Chema Alonso
Juan Garrido "Silverhack"

Law around the world is trying to control what is published on the Internet. After wikileaks case and HBGary ownage everybody could see how there are many controls that can be used to close a website, a domain name and to cut the communication between the source and the audience. What happened if someone wants to close your blog? Could you send any message to your audience? In this talk we provide you a new way to publish your RSS feeds using P2P networks as a failover system. Dust is "only" a Reader but could manage P2P Feeds, multiples http feeds from the same source, and the most important feature, can migrate from one feed to multiple ones without any effort for all your attendees.

IP4 TRUTH: The IPocalypse is a LIE

Sterling Archer
Field Agent, ISIS
Freaksworth
Professor, Mars University

There is a long tradition of researchers presenting at security conferences on topics that are embarrassing to a large company or government agency: ATM hacking, router vulnerabilities, Massachusetts toll road RFIDs, etc. Many of these brave researchers risk lawsuits or career ruin to reveal the truth. THIS is the first talk that puts the presenters' very lives in peril. Much has been made of the so-called "IPv4 address exhaustion" problem, also known as the IPocalypse. Industry analysts, networking vendors, regulatory groups, think-tanks, and so on have insisted that migration to IPv6 is the only solution. However, a small group of dissenters insist that threat is exaggerated and, more importantly, that the "migration plan" is merely a scheme to increase revenue for the network equipment manufactures and overpriced consultants.

The full truth is that IPv6 is the result of an international cabal on the verge of controlling the world. For centuries, mystics have prophesied that this "migration" would be the cabal's turning point. Incontrovertible evidence will be presented to convince all in attendance. Numerological analysis, ancient texts, and intercepted communiqués are just a few examples. Due to threats against their families, the presenters have been forced to take on assumed identities and appear only in disguise.

Security When Nano Seconds Count

James "Myrcurial" Arlen
Principal, Push The Stack Consulting

There's a brave new frontier for IT Security — a place where "best practices" does not even contemplate the inclusion of a firewall in the network. This frontier is found in the most unlikely of places, where it is presumed that IT Security is a mature practice. Banks, Financial Institutions and Insurance Companies. High Speed Trading, High Frequency Trading, Low Latency Trading, Algorithmic Trading — all words for electronic trades committed in microseconds without the intervention of humans. There are no firewalls, everything is custom and none of it is secure. It's SkyNet for Money and it's happening now.

Beat to 1337: Creating A Successful University Cyber Defense Organization

Mike Arpaia
Security Consultant/Penetration Tester Intern at Gotham Digital Science LLC.
Ted Reed

A university with no prior CTF experience and no students with significant prior information security experience may find competition a daunting task. Most competitions require a large amount of technical knowledge to set up, along with a fair amount of organization. But how are students with no information security knowledge going to compete in CTF competitions and keep from getting completely owned? Well, the answer is, they're not. The most important step to successful competition is educating oneself.

In this presentation, we describe our efforts as a team of undergraduate students interested in creating our school's cyber defense organization and beginning to participate in CTF competitions. We introduce the methodologies that we used (and continue to use) in order to start educating and motivating bright students about information security and keep them interested.

We will use our personal experience and proven successful tactics to outline the necessary steps to take and to expose the commonly overlooked necessities of starting a cyber defense organization, regardless of if you are a student interested in information security, an advisor looking to motivate students, an alumnus looking to share your passion for information security, etc.

Information security education must continue outside the classroom. Although the demand for information security knowledge is high, the requirements are rigid. While the industry is growing very rapidly, students who do not show passion and dedication to the field, and deep practical knowledge will be quickly left behind. We aim to leave you armed and ready to compete with and learn from some of the best and brightest information security students in the world.

Pillaging DVCS Repos For Fun And Profit

Adam Baldwin
Co-Founder, nGenuity

Distributed Version Control Systems, like git are becoming an increasingly popular way to deploy web applications and web related resources. Our research shows these repositories commonly contain information very useful to an attacker. This talk, which was part of my small contribution to the Penetration Testing Execution Standard (PTES) will demonstrate how to identify these repositories and techniques to pillage just as much information as possible from them. Lastly there will be release of a new W3AF plugin for mercurial repositories including an automated data extraction exploit plugin.

Chip & PIN is Definitely Broken

Andrea Barisani
Inverse Path S.r.l.
Adam Laurie
Aperture Labs Ltd
Zac Franken
Aperture Labs Ltd
Daniele Bianco
Inverse Path S.r.l.

The EMV global standard for electronic payments is widely used for inter-operation between chip equipped credit/debit cards, Point of Sales devices and ATMs.

Following the trail of the serious vulnerabilities published by Murdoch and Drimer's team at Cambridge University regarding the usage of stolen cards, we explore the feasibility of skimming and cloning in the context of POS usage.

We will analyze in detail EMV flaws in PIN protection and illustrate skimming prototypes that can be covertly used to harvest credit card information as well as PIN numbers regardless the type/configuration of the card.

The attacks are believed to be unreleased so far to the public (which however does not mean fraudster are not exploiting them) and are effective in bypassing existing protections and mode of operations.

As usual cool gear and videos are going to be featured in order to maximize the presentation.

Deceptive Hacking: How Misdirection Can Be Used Steal Information Without Being Detected

Bruce "Grymoire" Barnett

There are many similarities between professional hackers and professional magicians. Magicians are experts in creating deception, and these skills can be applied when penetrating a network. The author, with 30 years experience in both security and magic, will explain the basic principles and theories magicians that use to create illusions. This includes definitions of magic terms such as gaff, gimmick, fake, stooge, feint, sleight, bluff, timing, and different types of misdirection. It will be shown that all of these techniques apply to hacking as well. A scenario is presented where normal hacking techniques would be detected and information theft is prevented. The only solution is to use deception and trickery.

Fingerbank — Open DHCP Fingerprints Database

Olivier Bilodeau
Systems architect at Inverse Inc.

The presentation will first take a step back and offer a basic reminder of what passive fingerprinting is and, more precisely, DHCP fingerprinting. Then we will offer defensive and offensive use cases for DHCP fingerprinting. Next, we will cover the goals and resources offered by the new project and some future plans. As part of the announcement, two large fingerprint databases will be made available (both of which were bundled in separate projects: PacketFence and Satori).

We hope this new resource will increase the quality and breadth of current DHCP fingerprint databases and increase adoption for this reliable fingerprinting technique.

PacketFence, The Open Source Nac: What We've Done In The Last Two Years

Olivier Bilodeau
Systems architect at Inverse Inc.

Ever heard of PacketFence? It's a free and open source Network Access Control (NAC) software that's been out there since 2005. In the last two years we had several major releases with important new features that makes it an even more compelling solution.

Trying to appeal to both attackers and defenders, this presentation will cover all of our NAC's secret sauce : Wired / Wireless RADIUS MAC authentication / 802.1X, port-security through SNMP, captive portal redirection techniques, hardware support procedure, voice over IP, FreeRADIUS, Snort and Nessus integration, and quarantine / remediation features. We will continue with the advantages of Open Source when dealing with a NAC. Then we will focus on the last two years of the project, the problems, the missteps and the good, new and shiny stuff. This will include learning about some 802.1X problems, complaining about other vendor's code, looking at our own problems and salivating on some of the technical prowess we recently achieved. Finally we will expose our World Domination Roadmap covering both short-term improvements and potential research projects (and we will beg for help to achieve it).

Hopefully this talk will demystify NACs by explaining in details how our implementation works, give yet another example of why open source rocks and convince those who haven't jumped on the NAC band-wagon to give the free one a try.

Federation and Empire

Emmanuel Bouillon
Security Researcher

Federated Identity is getting prevalent in corporate environments. True, solving cross domain access control to Web applications or services is a nagging issue. Today, unsatisfying traditional approaches based on duplicated user accounts or dangerous trust domain relationships are being replaced by neater solutions. One of them is getting more and more popular not only in academic but in corporate environments as well: Claims-based authorization relying on SAML tokens. This cross domain federated Web SSO solution allows applications or service providers to finely control their access while leaving the burden of users management to their authoritative domains. Authoritative domains also keep full control on what they disclose about their users: Very attractive. However most existing material explains developers how to leverage this technology while keeping them oblivious to the underlying protocols or (many) standards' complexity and intricacies. By taking a radically low level approach, API free, this talk is intended to security pen-testers or architects who have to cope with SAML based access control. The just necessary presentation of the standards involved will be given. Then the two main parts will focus on how to adapt existing tool set to be fully operational against SAML access control and to key aspects that need to be considered prior joining or creating such federation. Most of the points are implementation agnostic and can be applied to Shibboleth, SimpleSAMLPHP or Active Directory Federation Service for instance. As well, the presented tools are Burp Pro Extensions leveraging the Buby framework but can be easily be translated into everyone preferred toolset.

Three Generations of DoS Attacks (with Audience Participation, as Victims)

Sam Bowne
Instructor, City College San Francisco

Denial-of-service (DoS) attacks are very common. They are used for extortion, political protest, revenge, or just LULz. Most of them use old, inefficient methods like UDP Floods, which require thousands of attackers to bring down a Web server. The newer Layer 7 attacks like Slowloris and Rudy are more powerful, and can stop a Web server from a single attacker with incomplete Http requests. The newest and most powerful attack uses IPv6 multicasts, and can bring down all the Windows machines on an entire network from a single attacker.

I will explain and demonstrate these tools: Low Orbit Ion Cannon, OWASP Http DoS Tool, and flood_router6 from the thc-ipv6 attack suite. This deadly IPv6 Router Advertisement Flood attack is a zero-day attack—Microsoft has known about it since June 2010 but has not patched it yet (as of May 4, 2011).

Audience Participation: Bring a device to test for vulnerability to the Router Advertisement Flood! Some cell phones and game consoles have been reported to be vulnerable—let's find out! If your device crashes, please come to the Q&A room so we can video-record it and arrange disclosure to the vendor.

Building The DEF CON Network, Making A Sandbox For 10,000 Hackers

David M. N. Bryan
Luiz Eduardo

We will cover on how the DEF CON network team builds a network from scratch, in three days with very little budget. How this network evolved, what worked for us, and what didn't work over the last ten years. This network started as an idea, and after acquiring some kick butt hardware, has allowed us to support several thousand users concurrently. In addition I will cover the new WPA2 enterprise deployment, what worked, and what didn't, and how the DEF CON team is has mad the Rio network rock!

Kinectasploit: Metasploit Meets Kinect

Jeff Bryner
Owner, P0wnlabs.com

We've all seen hackers in movies flying through 3D worlds as they hack the gibson. How about trying it for real? Now that we've got the kinect, lets hook it up to some hacking tools and see what it looks like to hack via kinect!

Physical Memory Forensics for Cache

Jamie Butler

Physical memory forensics has gained a lot of traction over the past five or six years. While it will never eliminate the need for disk forensics, memory analysis has proven its efficacy during incident response and more traditional forensic investigations. Previously, memory forensics, although useful, focused on a process' address space in the form of Virtual Address Descriptors (VADs) but ignored other rich sources of information. In the past, some techniques of process reconstitution have been auspicious at best and erroneous at worst. This presentation will build upon lessons learned and propose more thorough ways to reconstruct process contents, and therefore a process' address space. By using the methods presented, it will be possible to further reduce the data you care about in an incident response or forensic investigation and to better apply the traditional computer security techniques such as reverse engineering, hash matching, and byte pattern or signature matching such as those provided by ClamAV and VxClass.

Metasploit vSploit Modules

Marcus J. Carey
Enterprise Security Community Manager, Rapid7
David Rude
AKA bannedit, @msfbannedit, Metasploit Exploit Developer
Will Vandevanter
Senior Penetration Tester, Rapid7

This talk is for security practitioners who are responsible for and need to test enterprise network security solutions. Marcus Carey, David Rude, and Will Vandevanter discuss how to use the Metasploit Framework beyond penetration testing to validate whether security solutions are working as expected. Marcus initiated the creation vSploit auxiliary modules that emulate real-world network attacks. This can be used for good and evil purpose. This talk will debut several Metasploit modules designed specifically for testing firewalls, IDS, IPS, and DLP solutions. This presentation will show how to emulate persistent network attacks with vSploit modules which can come in handy if you are a penetration tester.

Lives On The Line: Securing Crisis Maps In Libya, Sudan, And Pakistan

George Chamales
Rogue Genius

Crisis maps collect and present open source intelligence (Twitter, Facebook, YouTube, news reports) and direct messages (SMS, email) during disasters such as the Haiti earthquake and civil unrest in Africa. The deployment of crisis mapping technology is on its way to becoming a standard tool to collect and track ground truth from crisis zones, but very little work has been done to evaluate and mitigate the threat posed by adversaries with offensive infosec capabilities. These platforms can provide responders and humanitarian organizations with the timely, high fidelity situational awareness necessary to direct aid and save lives. Unfortunately, they can also provide hostile national security services and other malicious groups with the information they need to target vulnerable populations, hunt down individuals, and manipulate response operations. In this session we'll setup, operate, attack and defend an online crisis map. Bring your laptop and toolsets because you will have the opportunity to play the bad actor (a technical member of the secret police or terrorist organization) as well as the defender (the response agency, citizen on the ground, and sysadmin trying to keep the server online). The experience will bring together everything we know and love and hate about defending online systems including buggy code, naive users, and security vs. usability tradeoffs and do so in a situation where people are dying and the adversary controls the network. We'll also introduce some not-so-typical concepts like building trust on the fly, crowdsourced verification, and maintaining situational awareness from halfway around the globe. Each step in the process will be based on real-world deployment experiences monitoring everything from local riots to nation-wide revolutions and natural disasters. The lessons learned, vulnerabilities found, and exploits developed during the session will be taken back to the crisis mapping community - enabling them to build more secure systems and more effective, life-saving deployments.

Abusing HTML5

Ming Chow
Lecturer, Tufts University Department of Computer Science

The spike of i{Phone, Pod Touch, Pad}, Android, and other mobile devices that do not support Flash has spurred the growth and interest in HTML5, even though the standard is still evolving. The power of HTML5 allows developers to create almost full-fledged web applications, not just structured content. HTML5's new features has increased the attack surface. It has been demonstrated that the HTML5 offline application cache can be abused. In addition, the support for client-side storage will open up the opportunity for SQL injection attack on client machines. There has been chatter regarding the new attack opportunities that the <audio>, <video>, and <canvas> tags will present, considering they require JavaScript and image-related functions such as SVG. This presentation will demonstrate the issues of HTML5 and how they can be abused and mitigated with good-old techniques. This presentation will also delve into the writing malicious web pages with web workers, abusing cross-origin JavaScript requests, how not to do cross-document messaging, and abusing geolocation.

Familiarity Breeds Contempt

Sandy "Mouse" Clark
University of Pennsylvania
Brad "RenderMan" Haines
Chief research monkey, Renderlab.net

"Good programmers write code, great programmers reuse" is one of the most well known truisms of software development. But what does that mean for security? For over 30 years software engineering has focused on writing the perfect code and reusing it as often as they can, believing if they can just get the bugs out, the system will be secure. In our talk we will demonstrate how the most prominent doctrine of programming is deadly for security. Analysis of software vulnerability data, including a full decade of data for several versions of the most popular operating systems, server applications and user applications (both open and closed source), shows that properties extrinsic to the software play a much greater role in the rate of vulnerability discovery than do intrinsic properties such as the actual software quality. We show that (at least in the first phase of a product's existence), software vulnerabilities have different properties from software defects. Our analysis of attacker tools and popular exploits shows that the attacker's learning curve determines when and which particular products are likely to be attacked. Improvements in those tools affect the frequency of attack, and the ultimate result is point-and-click usability. We will present several examples from both the defender and the attacker perspective illustrating how dangerous familiarity is for security. We will demonstrate that the more familiar an attacker is with your product, the more likely you are to be attacked and the more likely an attacker will succeed.

Look At What My Car Can Do

Tyler Cohen
Department of Defense

This presentation is an introduction to the new world of automobile communication, data and entertainment systems, highlighting the Ford Sync System. The Ford Sync System is a remarkable technological advance that has changed the automobile industry. While hard drives have been used in automobile entertainment applications for some time now, the Ford Sync System is different. It allows the user to interact with the car's communication system in a brand new way. If a vehicle with the Ford Sync system is used to commit a crime or to hide data, how would examiners be able to determine what data might be contained in the Ford Sync System? How does it get there? What forensic process or type of exploitation can be used to determine what traces are left behind on the car's hard drive? This presentation will take the audience through the process of various methods of infilling, hiding, acquiring data, and conducting a forensic exam on the Ford Sync System.

Kernel Exploitation Via Uninitialized Stack

Kees Cook
Ubuntu Security Engineer, Canonical Ltd

Leveraging uninitialized stack memory into a full-blown root escalation is easier than it sounds. See how to find these vulnerabilities, avoid the pitfalls of priming the stack, and turn your "memory corruption" into full root privileges.

The Art and Science of Security Research

Greg Conti
West Point

Research is a tricky thing, full of pitfalls, blind alleys, and rich rewards for the individual and humanity. This talk studies the art and science of conducting security research, from the genesis of your idea through experimentation and refinement to publication and beyond. In this talk you will learn how to generate and select powerful ideas, build upon the work of others, conduct groundbreaking work, and share your results for maximum desired effect. Whether you are a lone researcher or part of a large cabal you will take away ideas and techniques for maximizing the impact of your work, lest it lay dormant or have someone else rediscover your idea several years later.

Internet Kiosk Terminals : The Redux

Paul Craig
Principal Security Consultant — Security-Assessment.com

Paul Craig is the self-proclaimed "King of Kiosk Hacking" You have likely heard of him or his pornographic tool iKAT (Interactive Kiosk Attack Tool). For the last 3 years he has dedicated his life to striking fear into the hearts of Kiosk vendors.

This talk will compromise all of his latest advancements in the field of hacking Kiosk terminals. Multiple platforms, vendors, technologies and more shells than you can shake a stick at. If you have ever wanted to hack that lonely web-browsing computer in the corner of a room, this is the talk for you.

This talk will also showcase a live freestyle Kiosk hacking session, with a truck load of slick ninja techniques and zero-day. Watch out — the King of Kiosk hacking is back in town.

Cipherspaces/Darknets: An Overview Of Attack Strategies

Adrian Crenshaw "Irongeek"
Tenacity Institute and Irongeek.com

Darknets/Cipherspaces such as Tor and I2P have been covered before in great detail. Sometimes it can be hard to follow attack strategies that have been used against them as the papers written on the topic have been academic and abstract. What this talk will attempt to do is step back and give an overview of the topic in a manner hopefully more conducive to the understanding of security practitioners, giving more concrete examples. While little to nothing in this talk will be "new and groundbreaking" it should lead to a better understanding of how encrypted anonymizing networks can be subverted to reveal identities.

Speaking with Cryptographic Oracles

Daniel Crowley
Application Security Consultant, Trustwave - SpiderLabs

Cryptography is often used to secure data, but few people have a solid understanding of cryptography. It is often said that if you are not strictly a cryptographer, you will get cryptography wrong. For that matter, if you ARE a cryptographer, it is still easy to make mistakes. The algorithms might be peer reviewed and unbroken for 15 years, but if you use them incorrectly, they might leak information. Cryptographic oracles are systems which take user-controlled input and leak part or all of the output, generally leading to an attacker being able to defeat the cryptography, in part of in whole. In this talk, methods for finding and exploiting encryption, decryption, and padding oracles with minimal cryptographic knowledge will be discussed.

Taking Your Ball And Going Home; Building Your Own Secure Storage Space That Mirrors Dropbox's Functionality

Phil Cryer

When for-profit companies offer a free app, there is always going to be strings attached. As we have increasingly seen, these strings are often tied to your privacy to enable said third party company to monetize you in some way, but in worse cases your security can be compromised leaving you open to identity theft at best or legal repercussions at worst. One of today's most ubiquitous apps is Dropbox, which operates as a file hosting service that uses "cloud computing" (aka the internet) to enable users to store and share files and folders with others using file synchronization. Sounds harmless enough until you start thinking about how they can do so much for free. Learn about the flaws discovered by security researchers that have caused Dropbox to significantly change their terms of service, and about a group building a free, open sourced option for anyone to use to share and protect their data with. Learn, get involved, help and CYA, because for-profit third party companies are not going to do it for you.

PCI 2.0: Still Compromising Controls and Compromising Security

Jack Daniel
@jack_daniel
James Arlen
@myrcurial
Joshua Corman
@joshcorman
Alex Hutton
@alexhutton
Martin McKeay
@mckeay
Dave Shackleford
@daveshackleford

Building on last year's panel discussion of PCI and its impact on the world of infosec, we are back for more- including "actionable" information. Having framed the debates in the initial panel, this year we will focus on what works, what doesn't, and what we can do about it.

Compliance issues in general, and PCI-DSS in particular, are driving security in many organizations. In tight financial times, limited security resources are often exhausted on the "mandatory" (compliance) at the expense of the "optional" (actual security). We will focus on the information needed to reconcile these issues, and encourage the audience to continue the discussion with us.

Former Keynotes – The Future

Dark Tangent
Rod Beckstrom
ICANN
Jerry Dixon
Team CYMRU
Tony Sager
NSA
Linton Wells II
NDU

Former keynotes keep coming back to DEFCON. Join The Dark Tangent, Rod Beckstrom, Jerry Dixon, Tony Sager, and Linton Wells to discuss the future of cyber security.

Introduction to Tamper Evident Devices

datagram
Lockwiki.com

Tamper evident technologies are quickly becoming an interesting topic for hackers around the world. DEF CON 18 (2010) held the first ever "Tamper Evident" contest, where contestants were given a box sealed with a variety of tamper evident devices, many of which purport to be "tamper proof." All of these devices were defeated, even by those with little experience and a limited toolkit. Like the computer world, many of these devices are overmarketed and it is difficult for the average person to compare different tamper evident technologies.

This talk covers the design and uses of tamper evident devices used in the commercial and government sectors. We'll dig into the nitty gritty of how many of these devices work, the methods by which they can be defeated, and live demonstrations of defeats against common tamper evident devices. Be advised: this talk is for only the stealthiest of ninjas; pirates need not apply.

VDLDS – All Your Voice Are Belong To Us

Ganesh Devarajan Sr.
Security Architect, GoDaddy.com
Don LeBert
Security Engineer, GoDaddy.com

Anytime you want to bypass the system, you tend to have a telephone conversation instead of leaving a paper trail. Data Leakage Prevention (DLP) is on top of the list for most organizations, be it financial or medical industry. In order to overcome this issue we need to devise a new system that can monitor phone conversations. Voice Data Leakage Detection System can be used for tracking Credit card, social security numbers, along with other PII data. An extension of this can be used for tracking Accounting and Financial information that leaves the organization before the information is actually public. This will help spot the people leaking insider information to traders, competitors and other news sources. By utilizing a signature system, each environment can quickly capture sensitive information like Acquisition/ Sale of organization, or honeypot data to find the insider leaks.

Safe to Armed in Seconds: A Study of Epic Fails of Popular Gun Safes

Deviant Ollam
Cluebat Quartermaster

Hackers like guns. Hackers like locks. Hackers like to tinker with guns and locks. And, most of the time, hackers protect their guns with high-quality locks. However, while it's one thing to own a nice gun safe protected by a high security dial, that sort of solution tends to be best for the firearms that one doesn't have in daily use. Many of us who wear a firearm as part of our daily routine opt to store and secure our carry piece in a separate, more easily-accessible way at the end of the day. This talk is an in-depth evaluation of some of the most popular small firearm lockboxes in-use today. Some rely on mechanical locks, others on biometric locks, and some offer a combination of both. But overall, they tend to fail miserably in the face of any dedicated attacker. Come and learn how your favorite gun lockbox might be preventing your toddler from having an accidental discharge, but why it's not at all likely to repel a criminal or even perhaps a curious teenager. Means of both attacking as well as improving upon the lockboxes you already may own will be demonstrated, and audience members will be invited to participate in all sorts of attacks... live and on stage!

Bit-squatting: DNS Hijacking Without Exploitation

Artem Dinaburg
Security Researcher, Raytheon

We are generally accustomed to assuming that computer hardware will work as described, barring deliberate sabotage. This assumption is mistaken. Poor manufacturing, errant radiation, and heat can cause malfunction. Commonly, such malfunction DRAM chips manifest as flipped bits. Security researchers have known about the danger of such bit flips but these attacks have not been very practical. Thanks to ever-higher DRAM densities and the use of computing devices outdoors and in high-heat environments, that has changed. This presentation

will show that far from being a theoretical nuisance, bit flips pose a real attack vector. First the presentation will describe bit-squatting, an attack akin to typo-squatting, where an attacker controls domains one bit away from a commonly queried domain (e.g. mic2osoft.com vs. microsoft.com). To verify the seriousness of the issue, I bit-squatted several popular domains, and logged all HTTP and DNS traffic. The results were shocking and surprising, ranging from misdirected DNS queries to requests for Windows updates. The presentation will show an analysis of 6 months of real DNS and HTTP traffic to bit-squatted domains. The traffic will be shown in terms of affected platform, domain queried, and HTTP resources requested. Using this data the presentation will also attempt to ascertain the cause of the bit-flip, such as corruption on the wire, in requestor RAM, or in the RAM of a third party. The presentation will conclude with potential mitigations of bit-squatting and other bit-flip attacks, including both hardware and software solutions. By the end I hope to convince the audience that bit-squatting, and other attacks enabled by bit-flip errors are practical and serious, and should be addressed by software and hardware vendors.

A Bridge Too Far: Defeating Wired 802.1x with a Transparent Bridge Using Linux

Alva 'Skip' Duckwall
Northrop Grumman, Sr. Cyber Something or other

Using Linux and a device with 2 network cards, I will demonstrate how to configure an undetectable transparent bridge to inject a rogue device onto a wired network that is secured via 802.1x using an existing authorized connection. I will then demonstrate how to set up the bridge to allow remote interaction and how the entire process can be automated, creating the ultimate drop and walk away device for physical penetration testers and remote testers alike.

Virtualization under attack: Breaking out of KVM

Nelson Elhage
KVM, the Linux Kernel Virtual Machine, seems destined to become the dominant open-source virtualization solution on Linux. Virtually every major Linux distribution has adopted it as their standard virtualization technology for the future. And yet, to date, remarkably little work has been done on exploiting vulnerabilities to break out of KVM.

We're here to fix that. We'll take a high-level look at KVM's architecture, comparing and contrasting with other virtualization systems and describing attack surfaces and possible weaknesses. Using the development of a fully-functioning exploit for a recent KVM vulnerability, we'll describe some of the difficulties involved with breaking out of a VM, as well as some features of KVM that are helpful to an exploit author.

Once we've explored the exploit in detail, we'll finish off with a demonstration against a live KVM instance.

I Am Not a Doctor but I Play One on Your Network

Tim Elrod
Security Consultant, Fishnet Security
Stefan Morris
Security Consultant, Fishnet Security

How secure is your Protected Health Information? This talk will expose the world of Health Information Systems with an in depth technical review of their common protocols and technologies. Many of these life-critical systems had once relied on the security provided by air gapped medical networks. Recently, in an effort to realize savings and further share health information, medical systems have moved onto interconnected networks, opening them up to a plethora of attacks. We believe these systems have not had adequate research performed against them due to high cost and relatively low availability. Our talk will not only reveal weaknesses we have discovered in medical protocols but will create a foundation of knowledge for researchers who want to continue investigation of these systems. We will release findings and vulnerabilities that were discovered during the course of this research as well as fuzzers designed to allow penetration testers and researchers to further assess healthcare specific protocols for security vulnerabilities. We will take a look at healthcare specific hardware and discuss vulnerabilities related to these devices including prescription dispensing drug cabinets and the ability to dispense scheduled substances without authentication, authorization, or accounting. Finally, we will discuss how the impact of vulnerabilities on healthcare systems have changed with the introduction of large health information repositories such as the Google Health and Microsoft Health Vault as well as with countless regional and national Health Information Exchanges.

Mamma Don't Let Your Babies Grow Up to be Pen Testers - (a.k.a. Everything Your Guidance Counselor Forgot to Tell You About Pen Testing)

Dr. Patrick Engebretson
Dakota State University
Dr. Josh Pauli
Dakota State University

Always wanted to be a 1337 penetration tester capable of deciphering Kryptos while simultaneously developing your own custom 0-days? Then this is NOT the talk for you. We will however make you laugh by presenting an honest look at the life and times of a penetration tester today. We promise to open your eyes to aspects of the job you may have not considered before (at least we hadn't considered them before we started). Drawn from personal experience, this talk will focus on the myths and realities of penetration testing as a "for-sale" service. We love being penetration testers but we're pretty sure the guidance counselor forgot to mention there was a dark side to all the fun. We got the job with a little knowledge, a couple of lamer exploits, and high expectations. We expected firewalls and IDS to be the only thing standing between us and our beloved shells, but it turns out something far more sinister waited for us. Deadlines, timelines, reporting, scope, budgets, and chubby fingers quickly reared their ugly heads and threatened to smash our dreams. Like all PT'ers before us, we soon found out how important each of these topics are and what a critical role they play in our day-to-day activities. Join us for a unique and humorous 20-minute presentation as we air the dirty laundry about the mechanics of penetration testing and open your eyes to the untold aspects of best job on earth.

Steganography and Cryptography 101

eskimo

There are a lot of great ways to hide your data from prying eyes this talk will give a crash course in the technology and some tools that can be used to secure your data. Will also discuss hiding your files in plain site so an intruder will have no idea that hidden files even exist. These same techniques can also be employed by somebody wishing to transmit messages.

Don't Drop the SOAP: Real World Web Service Testing for Web Hackers

Tom Eston
Senior Security Consultant, SecureState
Josh Abraham
Senior Security Consultant, Rapid7
Kevin Johnson
Security Consultant and Founder, Secure Ideas

Over the years web services have become an integral part of web and mobile applications. From critical business applications like SAP to mobile applications used by millions, web services are becoming more of an attack vector than ever before. Unfortunately, penetration testers haven't kept up with the popularity of web services, recent advancements in web service technology, testing methodologies and tools. In fact, most of the methodologies and tools currently available either don't work properly, are poorly designed or don't fully test for real world web service vulnerabilities. In addition, environments for testing web service tools and attack techniques have been limited to home grown solutions or worse yet, production environments.

In this presentation Tom, Josh and Kevin will discuss the new security issues with web services and release an updated web service testing methodology that will be integrated into the OWASP testing guide, new Metasploit modules and exploits for attacking web services and a open source vulnerable web service for the Samurai-WTF (Web Testing Framework) that can be used by penetration testers to test web service attack tools and techniques.

Get Off of My Cloud: Cloud Credential Compromise and Exposure

Ben Feinstein
Director of CTU Operations & Analysis, Dell SecureWorks Counter Threat Unit (CTU)
Jeff Jarmoc
Security Researcher, Dell SecureWorks Counter Threat Unit (CTU)

An Amazon Machine Image (AMI) is a virtual appliance container used to create virtual machines (VMs) within the Amazon Elastic Compute Cloud (EC2). EC2 instances typically interact with a variety of Amazon Web Services (AWS), and as such require access to AWS credentials and private key materials. In this presentation we will explore how AWS credentials and keys may end up being persisted within an AMI. If persisted within a public or shared AMI, these credentials and key materials may be unintentionally

shared with 3rd parties. We will discuss the different types of AWS credentials and key materials, how they are used to access different Cloud services, and the risks and potential impacts of compromise of this sensitive information. A new tool, "AMIexposed" will be released that can check an AMI for the most common ways AWS credentials and keys are persisted within an AMI. The results of research using AMIexposed against public AMIs will be presented, helping to quantify the scope and prevalence of AWS credentials and keys exposed within public AMIs. We'll also discuss the risks inherent in trusting public AMIs to be free of backdoors, trojans, and other malicious hitchhikers. Results of an experiment demonstrating these risks will be presented. Finally, the talk will propose best practices for utilizing AMIs. These will include specific steps for ensuring you organization's AWS credentials and key materials are not unintentionally persisted within public or shared AMIs, and recommendations regarding usage of 3rd party public AMIs.

Handicapping the US Supreme Court: Can We Get Rich by Forceful Browsing?

Foofus

Using only script-kiddie skills, it may be possible to handicap the outcome of decisions of national importance. This talk presents a walk-though of a project to make more accurate predictions of US Supreme Court case outcomes. That could be a useful thing, if you had something at stake. Conventional techniques for predicting outcomes rely on legal expertise and knowledge of the policy issues at stake in a case and the justices' voting records. Forget all that: we're going to see what we can do with perl and XML transcripts of oral arguments. It's only 20 minutes of your life, but it might equip you to astound your lawyer friends, or make some canny investments.

Getting F***** On the River

Gus Fritschie
Director, Security Engineering - SeNet International
Mike Wright
Senior Security Engineer - SeNet International

Online poker is a multi-million dollar industry that is rapidly growing, but is not highly regulated. There have been "hacks" recently (i.e. weak SSL implementation, superuser account) that have drawn more attention to security in the poker industry, especially as it moves to full regulation in the United States. This talk will cover the technical architecture of online poker, existing security controls, examples of past vulnerabilities, new weaknesses we have discovered in the poker clients and surrounding infrastructure, and next steps of research we are performing in this area.

Cellular Privacy: A Forensic Analysis of Android Network Traffic

Eric Fulton
Director of Research, Lake Missoula Group, LLC

People inherently trust their phones, but should they? "Cellular Privacy: A Forensic Analysis of Android Network Traffic" is a presentation of results from forensically analyzing the network traffic of an Android phone. The results paint an interesting picture. Is Google more trustworthy than the application developers? Are legitimate market apps more trustworthy than their rooted counterparts? Perhaps most importantly, should you trust your passwords, location, and data to a device that shares too much?

UPnP Mapping

Daniel Garcia

Universal Plug and Play(UPnP) is a technology developed by Microsoft in 1999, as a solution for NAT traversal(among other things). This talk explores the exploiting of port mapping services in UPnP/IGD devices from the WAN. It also talks about a tool called Umap to help process the UPnP requests. Attacking UPnP allows attackers to use devices as a proxy that can establish connections to internal and external IP addresses. The software allows scanning internal hosts behind the device NAT, manual port-mapping(WAN to LAN, WAN to WAN) and a SOCKSv4 proxy service that automatically maps requests to UPnP devices. Most UPnP attacks have focused on the exploiting of UPnP from the LAN side of the device, this talk focuses on attacking from the WAN side. Attackers can use these techniques to hide IP addresses and attack internal hosts behind common household gateway devices.

Gone in 60 Minutes: Stealing Sensitive Data from Thousands of Systems Simultaneously with OpenDLP

Andrew Gavin
Consultant, Verizon Business

Got domain admin to a couple of thousand Windows systems? Got an hour to spare? Steal sensitive data from all of these systems simultaneously in under an hour with OpenDLP.

OpenDLP is an open source, agent-based, massively distributable, centrally managed data discovery program that runs as a service on Windows systems and is controlled from a centralized web application. The agent is written in C, has no .NET requirements, uses PCREs for pattern matching, reads inside ZIPs like Office 2007 and OpenOffice files, runs as a low priority service so users do not see or feel it, and securely transmits results to the centralized web application on a regular basis. The web application distributes, installs, and uninstalls agents over SMB; allows you to create reusable profiles, view results in realtime, and mark false positives; and exports results as XML.

OpenDLP also supports scanning databases for sensitive information. It can also perform agentless scans of Windows systems over SMB and UNIX/Linux systems over SSH.

Strategic Cyber Security: An Evaluation of Nation-State Cyber Attack Mitigation Strategies

Kenneth Geers
Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD CoE)

This presentation argues that computer security has evolved from a technical discipline to a strategic concept. The world's growing dependence on a powerful but vulnerable Internet — combined with the disruptive capabilities of cyber attackers — now threatens national and international security.

Strategic challenges require strategic solutions. The author examines four nation-state approaches to cyber attack mitigation.

- Internet Protocol version 6 (IPv6)
- Sun Tzu's Art of War
- Cyber attack deterrence
- Cyber arms control

The four threat mitigation strategies fall into several categories. IPv6 is a technical solution. Art of War is military. The third and fourth strategies are hybrid: deterrence is a mix of military and political considerations; arms control is a political/technical approach.

The Decision Making Trial and Evaluation Laboratory (DEMATEL) is used to place the key research concepts into an influence matrix. DEMATEL analysis demonstrates that IPv6 is currently the most likely of the four examined strategies to improve a nation's cyber defense posture.

There are two primary reasons why IPv6 scores well in this research. First, as a technology, IPv6 is more resistant to outside influence than the other proposed strategies, particularly deterrence and arms control, which should make it a more reliable investment. Second, IPv6 addresses the most significant advantage of cyber attackers today — anonymity.

Bulletproofing The Cloud: Are We Any Closer To Security?

Ramon Gomez

Cloud security has come into focus in the last few years; while many ways to break the cloud have been proposed, few solutions have been put forward. This talk is primarily a conceptual discussion on how cloud providers can and should be (but probably are not) protecting both their own and their clients' assets in their cloud implementations. It will discuss the known issues with cloud, and a readily available proposed solution to some of these issues. The presentation will conclude with a demonstration of an actual implementation of this theory at a cloud hosting provider. An understanding of basic network security technology is required.

Smile for the Grenade! "Camera Go Bang!"

Vlad Gostom
Penetration Tester
Joshua Marpet
Security Evangelist, DataDevastation

Cameras are hugely important to urban and suburban battlefields. Reconnaissance is a must-have for commanders, and a force multiplier for actual combat units. A combat-deployable camera system is being developed or used by nearly every military-industrial manufacturer and government agency, ranging from Throwable Camera Balls to Grenade-style launched cameras. But they're expensive and inaccessible to civilians. Would it be possible to build a combat-deployable camera system that would fulfill the mandates of a tactical combat team, feed information to a strategic command center, and force-multiply "on the cheap"?

Represent! Defcon Groups, Hackerspaces, and You.

Anch
DC503
blakdayz
DC225
Anarchy Angel
DC414
ngharo
DC414
Itzik Kotler
DC9723
Jake "GenericSuperhero"
Black Lodge Research
converge
DCG Coordinator

Fabricating, circumventing, forging, partying, milling, crafting, building breaking — Defcon Groups have risen, fallen, and endured the last 8 years as decentralized and smoldering embers of the local hacker think-tank. This year Defcon sets out to stoke that fire and unite our groups, at and outside of the conference. The talk will consist of a panel of Defcon Groups leaders, uncovering the secrets and follies of several groups: what makes them work, when do they fail, and ultimately .. WTF have these people been doing all this time? Come hear how hackerspaces have influenced these local groups and the cool ways that these groups are propping the hackerspace. What can you break?

Smartfuzzing The Web: Carpe Vestra Foramina

Nathan Hamiel
Principal Consultant, FishNet Security
Gregory Fleischer
Senior Security Consultant, FishNet Security
Justin Engler
Security Consultant, FishNet Security
Seth Law
Principal Consultant, FishNet Security

It can be scary to think about how little of the modern attack surface many tools cover. There is no one best tool for the job and on top of that some tools don't do a great job at anything. Often in the hands of general users the capabilities and limitations are not even thought of during testing. Point, click, done. The attack surface of modern web environments as well as their protection mechanisms have become more complicated and yet many tools have not adapted. Hey, Y2K called and it wants some applications tested.

There is certainly no shortage of vulnerabilities in modern web environments but we should be looking beyond low hanging fruit at this point. In between fully automated scanners and manual testing lies a sweet spot for the identification of vulnerabilities. Some of the juiciest pieces of information are not found by vulnerability scanners but are found by humans creating custom tests. This is why semi-automated testing space is so important. All of this complicated blending of protection mechanisms, services, and RIA technologies means that moving in to the area of semi-automated testing can be fraught with failure. We detail how these failures can be avoided as well as provide a tool that solves some of these problems as well as provides analysis for your own tools and scripts. Your web applications have moved on, don't you think it's time your tools to do the same?

Earth vs. The Giant Spider: Amazingly True Stories of Real Penetration Tests

Rob Havelt
Director of Penetration Testing, Trustwave SpiderLabs
Wendel Guglielmetti Henrique
Security Consultant, Trustwave SpiderLabs

Earth vs. The Giant Spider: Amazingly True Stories of Real Penetration Tests brings the DEF CON 19 audience the most massive collection of weird, downright bizarre, freaky, and altogether unlikely hacks ever seen in the wild. This talk will focus on those complex hacks found in real environments — some in very high end and important systems, that are unlikely but true. Through stories and demonstrations we will take the audience into a bizarre world where odd business logic flaws get you almost free food [including home shipping], sourcing traffic from port 0 allows ownership of the finances a nation, and security systems are used to hack organizations.

The SpiderLabs team delivered more than 2300 penetration tests last year, giving us access to a huge variety of systems and services, we've collected a compendium of coolest and oddest compromises from the previous year to present at DEF CON. Our goal is to show effective attacks and at the same time not the trivial ones that can be found by automated methods. By the end of this presentation we hope to have the audience thinking differently about systems and applications that organizations use every day, and how they may be used against them.

From Printer To Pwnd: Leveraging Multifunction Printers During Penetration Testing

Deral Heiland
Senior Security Engineer, Foofus.net

In this presentation we go beyond the common printer issues and focus on harvesting data from multifunction printer (MFP) that can be leveraged to gain access to other core network systems. By taking advantage of poor printer security and vulnerabilities during penetration testing we are able to harvest a wealth of information from MFP devices including usernames, email addresses, and authentication information including SMB, Email, LDAP passwords. Leveraging this information we have successful gained administrative access into core systems including email servers, file servers and Active directory domains on multiple occasions. We will also explore MFP device vulnerabilities including authentication bypass, information leakage flaws. Tying this altogether we will discuss the development of an automated process for harvesting the information from MFP devices with the updated release of our tool 'PRAEDA'.

Assessing Civilian Willingness to Participate in On-Line Political and Social Conflict

Thomas J. Holt
Assistant Professor, Michigan State University
Max Kilger
Security Researcher

Changes in the social dynamics and motivations of the hacking community are a potential catalyst that when combined with the expanding reliance of critical infrastructure components upon networked control systems may provide the genesis for the emergence of what is being called the civilian cyberwarrior The emerging visibility and salience of cyber-vulnerabilities within large elements of a nation's critical infrastructure is creating opportunities that are facilitating significant potential shifts in the power relationship between individuals and nation states. This paper examines some of these shifts in the social dynamics and motivations in the hacking community, their effects on the traditional power differential between individuals and nation-state actors and discusses the emergence of the civilian cyberwarrior – individuals that are encouraged and emboldened by this transformed power differential to engage in malicious acts against another country's critical infrastructure or even the critical infrastructure of their own country. In particular, this presentation will explore the findings from an international survey of youth to identify the situational and social factors that predict individual willingness to engage in physical and cyberattacks against various targets. The findings will assist researchers, law enforcement, and the intelligence community to proactively anticipate various threat scenarios and develop effective defenses against attacks on and off-line.

An Insider's Look at International Cyber Security Threats and Trends

Rick Howard
Verisign iDefense General Manager

Verisign iDefense General Manager, Rick Howard, will provide an inside look into current cyber security trends with regard to Cyber War, Cyber Hacktivism, and Cyber Espionage. In this presentation Rick will discuss the current capabilities, tactics, techniques and procedures used by various cyber security cartels in key regions around the world. Finally, Rick will describe the idea of a Cyber Security Disruptor; new ideas, technologies and policies that will fundamentally make us change how we protect the enterprise.

Economics of Password Cracking in the GPU Era

Robert "Hackajar" Imhoff-Dousharm
SanDisk Corporation

As this shift to "General Computing" and working in the cloud has accelerated in the last 4 years, so has the ability to take advantage of these technologies from an Information Security vantage point. This could not be more apparent than with the sudden uptick in GPU based password cracking technologies. In this presentation we will explore where the current GPU cracking technologies are, what their cost are to implement, and how to deploy and execute them (with demo). Most importantly, we will demonstrate the "brute force calculator" which can assist with getting your monies worth. Finally, we will explore where the future lays for this medium and what that means for safe passwords moving into the next decade.

Jugaad – Linux Thread Injection Kit

Aseem "@" Jakhar
Founder, null – The open security community (registered non-profit organization)

Windows malware conveniently use the CreateRemoteThread() api to delegate critical tasks inside of other processes. However till now there is no API on Linux to perform such operation. This paper talks about my work on creating an API similar to createRemoteThread() on *nix OSes. The kit currently works on Linux, allocates space inside a process and injects and executes arbitrary payload as a thread into that process. It utilizes the ptrace() functionality to manipulate other processes on the system. ptrace() is an API generally used by debuggers to manipulate(debug) a program. By using the same functionality to inject and manipulate the flow of execution of a program Jugaad is able to inject the payload as a thread.

There is another awesome tool injectSo that injects the whole library into a process, however it leaves traces like the name and path of the injected library which can easily be found by reading the process maps file. Jugaad does an in-memory thread injection and hence is stealthier as there are no traces of any library found in the maps file. It however allocates memory in the process using mmap2 system call which only shows up as allocated memory in maps file but does not reveal anything about the injection. The payload to be executed runs inside the thread and is independent of the kit - you chose your payload, jugaad injects the payload.

The Art of Trolling

Matt 'openfly' Joyce

Trolling is something that today has a very negative connotation on the Internet and in the common usage of the word outside of it. However, for better or worse trolling has long enjoyed a close relationship with hacking be it in the area of information security, or simply in technology development. I intend to delve into the definition of a troll, the history of trolling in human culture (as well as its contributions), and the techniques that are generally exploited by trolls to realize their intended goals. There will be several past projects that I classify as successful trolls that I will use as object lessons in the practical application of the discussed techniques. Trolls span the gaps between hardware and software projects and at times can carry a variety of "payloads".

Black Ops of TCP/IP 2011

Dan Kaminsky
Chief Scientist, DKH

Remember when networks represented interesting targets, when TCP/IP was itself a vector for messiness, when packet crafting was a required skill? In this thoroughly retro talk, we're going to play with systems the old fashioned way, cobbling together various interesting behaviors with the last few shreds of what low level networking has to offer. Here's a few things to expect:

- IPv4 and IPv6 Fragmentation Attacks, Eight Years In The Making
- TCP Sequence Number Attacks In Modern Stacks
- IP TTLs: Not Actually Expired
- Inverse Bug Hunting: More Things Found On The Open Net
- Rebinding Attacks Against Enterprise Infrastructure
- BitCoin: Network Manipulation for Fun And (Literal) Profit
- The Net Neutrality Transparency Engine

DNS might show up, and applications are going to be poked at. But this will be an old style networking talk, through and through.

Hacking Your Victims Over Power Lines

Dave Kennedy (ReL1K)

When performing penetration tests on the internal network in conjunction with physical pentests your always concerned about being located. Let's remove that barrier and perform your penitents over power lines and never be detected. In this presentation we'll cover how you can perform full penetration tests over the power lines and hack into home automation systems. Home automation has been gaining momentum not only in small homes but in large companies and organizations. There's a huge variety of solutions out there both open-source and "proprietary" that provide these solutions to your homes and businesses. Home automation gives us several things for example, full-fledge 85mbps networks, security systems, lights, windows, HVAC, doors, and cameras and they are all generally done through the power lines or through short-wave wireless communications. So let's break it.... During this presentation we'll be going over the non-existence of security over these devices, show proof of concept demonstrations on hacking these devices, and while we're at it, demonstrate how to disable all security mechanisms that use the different protocols like X10.

Tracking the Trackers: How Our Browsing History Is Leaking into the Cloud

Brian Kennish
Founder of Disconnect

What companies and organizations are collecting our web-browsing activity? How complete is their data? Do they have personally-identifiable information? What do they do with the data? The speaker, an ex–Google and DoubleClick engineer, will answer these questions by detailing the research he did for The Wall Street Journal (http://j.mp/tttwsj) and CNN (http://j.mp/tttcnn), talking about the crawler he built to collect reverse-tracking data, and launching a tool you can use to do your own research.

Hacking and Securing DB2 LUW Databases

Alexander Kornbrust
CEO of Red-Database-Security GmbH

DB2 for Linux, Unix and Windows is one of the databases where only little bit information about security problems is available. Nevertheless DB2 LUW is installed in many corporate networks and if not hardened properly could be an easy target for attackers. In many aspects DB2 is different from other databases, starting at the user management (normally no user/passwords in the database) to the privilege concept.

With the latest versions, DB2 LUW became more and more similar to Oracle (views, commands, concepts to make more stuff query-able from the database) and allows even to run PLSQL code from Oracle databases. IBM is also cloning the insecure configuration from Oracle by granting a lot of the PLSQL packages to public.

This talk will give a quick introduction into the DB2 architecture, differences to other relational database systems and the most common DB2 configuration problems.

Showing a lit of available exploits and typical pentester questions (how can I run OS commands, how can I access the network or file system) will also be covered.

This talk will also demonstrate SQL injection in stored procedure code inside of the database (SQL/PL and PL/SQL), how to find, exploit and fix it.

The last part covers the hardening of DB2 databases.

Sounds Like Botnet

Itzik Kotler
Chief Technology Officer at Security Art
Iftach Ian Amit
VP Consulting at Security Art

VoIP is one of the most widely-used technologies among businesses and, increasingly, in households. It represents a combination of Internet technology and phone technology that enhances and expands the possibilities of both. One of these possibilities involves using it for botnet command and control infrastructure and a data exfiltration vector.

The concept of VoIP Botnet is to operate in closed networks with limited access and the potential of censorship using everyday telecommunication and telephony services such as voicemail, conference calls, voice and signaling information.

Moshi Moshi is a proof of concept VoIP Botnet that allows the operator to dial in from a pay phone or mobile phone, and get shell access and exfiltrate data from the bots.


SKYTALKS
ATTACKS CRACKS HARDWARE
WETWARE RF RANTS RAVES
RIO PAVILION 7
FRI & SAT / SUNDAY
9AM-7PM / 9AM-4PM
PYRO
ANCH
TIMMAH
ROAMER
THEPREZ98
WAREZJOE
JOE SCHORR
JASON ROSS
JASON SCOTT
JULIAN COHEN
STEVE PORDON
KEVIN MCGINLEY
CHRIS NICKERSON
WILL VANDEVANTER ...AND MORE
SKYTALKS.INFO
FOR TOPICS & SCHEDULE
DAN DESIGN
ILLUSTRATION MAR SUDUX.COM PHOTO DAN C MENTALSWITCH.COM MODEL JULIA B

This presentation will discuss and demonstrate the use of VoIP technology to create "Moshi Moshi," we also explore some interesting properties of VoIP based botnet.

Additionally, we will discuss mitigating factors and ways that VoIP providers should implement in order to prevent further VoIP abuse.

Panel: Is it 0-day or 0-care?

Jake Kouns
Open Security Foundation
Brian Martin
Project Lead at OSVDB
Steve Christey
Principal Information Security Engineer at MITRE / CVE
Carsten Eiram
Chief Security Specialist at Secunia
Art Manion
CERT
Dan Holden
HP TippingPoint
Alex Hutton
Verizon
Katie Moussouris
Microsoft

Vulnerability Databases (VDBs) have provided information about security vulnerabilities for over 10 years. This has put VDBs in a unique position to understand and analyze vulnerability trends and changes in the security industry. This panel presentation will examine vulnerability information over the past several years with an emphasis on understanding security researchers, quality of research, vendors, disclosure trends and the value of security vulnerabilities. The emotional debate surrounding Full Disclosure has raged on for decades. This panel will use grounded data to discuss salient points of the debate to hopefully determine trends that may influence the debate. Maybe even in a positive fashion!

DCFluX in: License to Transmit

Matt Krick "DCFluX"
Chief Engineer, New West Broadcasting Systems, Inc.

When cell phones, land lines and the internet break down in a disaster, Amateur radio is there. Considered to be one of the earliest forms of Hacking, this talk will take a look at some of the things that can be done if you are a licensed amateur radio operator.

Balancing The Pwn Trade Deficit – APT Secrets in Asia

Anthony Lai
Co-founder and Security Researcher, Xecure Lab
Benson Wu
Founder and Security Researcher, Xecure Lab
Jeremy Chiu
Founder and Security Researcher, Xecure Lab
PK
Security Researcher

In last year, we have given a talk over China-made malware in both Blackhat and DEFCON, which is appreciated by various parties and we would like to continue this effort and discuss over APT attacks in Asia this year. However, case studies are not just our main dish this time, we will carry out technical analysis over the samples. I have worked with 2 Taiwanese researchers and would like to talk about how to automate the APT attack analysis with our analysis engine, Xecure, and give comparison between samples from various Asian countries, giving similarity and difference analysis among them, which could be insightful to the audience. Finally, we will talk about our contribution to the rule and signature to detect APT attack.

And That's How I Lost My Eye: Exploring Emergency Data Destruction

Shane Lawson
Senior Security Engineer, Tenacity Solutions
Bruce Potter
CTO, Ponte Technologies
Deviant Ollam
Co-Owner, The Core Group

Are you concerned that you have become a subject of unwarranted scrutiny? Convinced that the black helicopters are incoming and ruthless feds are determined in to steal your plans of world domination? This talk explores several potential designs for quick and ruthless destruction of data as a last resort, break glass in case of emergency type of situation. Projectiles and chemical warfare will be involved along with other methods. Each method carries risk, reward, and near certainty for bodily harm. You might lose an eye, but you will keep your freedom with these techniques and remain to fight another day.

I'm Your MAC(b)Daddy

Grayson Lenik
Security Consultant Trustwave, Spiderlabs

The field of Computer Forensics moves more and more in the direction of rapid response and live system analysis every day. As breaches and attacks become more and more sophisticated the responders need to continually re-examine their arsenal for new tactics and faster ways to process large amounts of data. Timelines and super-timelines have been around for a number of years but new software and techniques brings them back into play for Incident Response and live analysis instead of static postmortem forensics. Add in identification of anti-forensics techniques and you gain a whole new view on forensic timelines.

Don't Fix It In Software

Katy Levinson
Director, Hacker Dojo

At Defcon 17 when a speaker didn't show a bottle of vodka was offered to whoever gave an impromptu talk. Somebody went up and talked about his robot project. He mentioned that it didn't normally drive straight, and talked about all the software solutions he had tried to fix this. I was reasonably intoxicated and wound up shouting at him over the crowd that it did not drive straight because of his drive base design, and not his software. This led to questions, which eventually led to a rant about all of the dumb things people who are brilliant at in software do wrong in hardware, and then try to fix using more software. Sadly a scoundrel absconded with my vodka, but a goon took me aside, said the information was great, and told me to submit it as a full talk. Now I am.

This talk will cover material assuming the average audience member is a relatively intelligent coder with a high-school physics/math background and has seen linear algebra / calculus before. The intent is to navigate people new to robotics around many lessons my teams and I learned the "hard way," and to give them all the words to look up in wikipedia to help bridge the gap between amateur and novice professional robotics. It will not cover why your Arduino doesn't work when you plugged your USB tx into your RS232 tx.

PIG: Finding Truffles Without Leaving A Trace

Ryan Linn
Senior Security Consultant, Trustwave SpiderLabs

When we connect to a network we leak information. Whether obtaining an IP address, finding our default gateway, or using Dropbox there are packets that can be used to help identify more about our machine and network. This talk and series of demonstrations will help you learn to passively profile a network through a new Metasploit module by gathering broadcast and multicast traffic, processing it, and looking at how the bad guys will use it to own your network. Without sending a packet, many networks divulge significant information about the assets that are attached. These broadcast packets can be used to identify hosts, OS's, and other hardware that is attached. Any skill level can learn how to easily gather and use this information, how to protect your network, and talk about how to extend the framework for new protocols.

Pervasive Cloaking

William Manning
Booz Allen Hamilton

What Cloak? Recent policy proposals from the US Executive seem to call for government support for strong encryption use by individuals and vendors in the name of protecting privacy and anonymity. Yet strong encryption is still considered a controlled resource, requiring explicit permission to import or export from the US. This is also true for other countries. This talk will try to couch these proposals in light of past crypto rules, illuminate some possible ways forward, and touch on the advantages of and weaknesses inherent in a global cyber domain that has interoperable, strong crypto based encryption capabilities for the masses.

We're (The Government) Here To Help: A Look At How FIPS 140 Helps (And Hurts) Security

Joey Maresca

Many standards, especially those provided by the government, are often viewed as more trouble the actual help. The goal of this talk is to shed a new light onto onesuch standard (FIPS 140) and show what it is inteded for and how is can sometimes help ensure good design practices for security products. But everything is not roses and there are certain things that these standards cannot help with or may even inhibit. By examining these strengths and potential weakness, the hope is everyone will have a new opinion of this and similar standards and how they are used.

SSL And The Future Of Authenticity

Moxie Marlinspike

In the early 90's, at the dawn of the World Wide Web, some engineers at Netscape developed a protocol for making secure HTTP requests, and what they came up with was called SSL. Given the relatively scarce body of knowledge concerning secure protocols at the time, as well the intense pressure that everyone at Netscape was working under, their efforts can only be seen as incredibly heroic. But while it's amazing that SSL has endured for as long as it has, some parts of it — particularly those concerning Certificate Authorities — have always caused some friction, and have recently started to cause real problems. This talk will examine authenticity within SSL, shed new light on the current problems, and cover some new strategies for how to move forward.

Hacking .Net Applications: The Black Arts

Jon McCoy
DigitalbodyGuard

This presentation will cover the Black Arts of making Cracks, KeyGens, Malware, and more. The information in this presentation will allow a .NET programmer to do unspeakable things .NET applications. I will cover the life cycle of developing such attacks and over coming common countermeasures to stop such attacks. New tools to assist in the attacks will be supplied. This presentation will focus on C# but applies to any application based on the .NET framework.

Covert Post-Exploitation Forensics With Metasploit

Wesley McGrew
Research Associate, Mississippi State University
National Forensics Training Center

In digital forensics, most examinations take place after the hardware has been physically seized (in most law enforcement scenarios) or a preinstalled agent allows access (in the case of enterprise forensics packages). These scenarios imply that the "subject' (the one in possession of the media) is aware of the fact that their data has been seized or subject to remote access. While penetration testing tools allow for surface-level access to the target filesystem, there is a lot of potential data that is being missed in unallocated space that could be accessed by file system forensic tools such The Sleuth Kit. In this presentation, Wesley will present a new set of tools that will allow forensic examiners and pentesters alike to image remote filesystems of compromised systems, or perform examinations directly on remote filesystem with forensic tools on the attacking machine by mapping remote drives to local block devices. This is the integration of Metasploit with a large body of existing digital forensic tools.

Vulnerabilities of Wireless Water Meter Networks

John McNabb
Researcher

Why research wireless water meters? Because they are a potential security hole in a critical infrastructure, which can lead to a potential leakage of private information, and create the potential to steal water by lowering water bills? It's a technology that's all around us but seems to too mundane to think about. Because a hacker can't resist exploring technology to see how it works and how to break it, because they are there? In this talk the speaker, who managed a small water system for 13 years, will first present an overview of drinking water security, review reported water system security incidents and the state of drinking water security over the past year, and will then take a deep dive into the hardware, software, topology, and vulnerabilities of wireless water meter networks and how to sniff wireless water meter signals.

Battery Firmware Hacking

Charlie Miller
Principal Research Consultant, Accuvant Labs

Ever wonder how your laptop battery knows when to stop charging when it is plugged into the wall, but the computer is powered off? Modern computers are no longer just composed of a single processor. Computers possess many other embedded microprocessors. Researchers are only recently considering the security implications of multiple processors, multiple pieces of embedded memory, etc. This paper takes an in depth look at a common embedded controller used in Lithium Ion and Lithium Polymer batteries, in particular, this controller is used in a large number of MacBook, MacBook Pro, and MacBook Air laptop computers.

In this talk, I will demonstrate how the embedded controller works. I will reverse engineer the firmware and the firmware flashing process for a particular smart battery controller. In particular, I will show how to completely reprogram the smart battery by modifying the firmware on it. Also, I will show how to disable the firmware checksum so you can make changes. I present a simple API that can be used to read values from the smart battery as well as reprogram the firmware. Being able to control the working smart battery and smart battery host may be enough to cause safety issues, such as overcharging or fire.

DEF CON Comedy Jam IV, A New Hope For The Fail Whale

David Mortman
Rich Mogull
Securosis
Chris Hoff
Rational Security
Dave Maynor
Errata
Larry Pesce
Pauldotcom.com
James Arlen
Liquid Matrix
Rob Graham
Errata

We're baaaaaack! The most talked about panel at DEF CON! Nearly two hours of non-stop FAIL. Come hear some of the loudest mouths in the industry talk about the epic security failures of the last year. We'll be covering mobile phones, cloud, money laundering and food cooked on stage to name just a few topics. Nothing is sacred not even each other. Come for the FAIL stay for the crepes!

Blinkie Lights: Network Monitoring with Arduino

Steve Ocepek
Director of Security Research, Trustwave SpiderLabs

Remember the good old days, when you'd stare at Rx and Tx on your shiny new Supra 1200bps modem, and actually know what the heck was going on? Systems tend to talk a lot more nowadays, and somewhere along the line I completely lost track of who mine hangs out with. And I kind of miss my blinkie lights.

But we live in a world of Arduino and cheap LEDs — maybe there's a way to play with electronics, talk about security, and show the kids a thing or two — all at the same time. Imagine if one of those USB toys on your desk could actually give you an indication of which countries you were trading packets with, or alert you to unusually long-running sessions. 'cerealbox' will demonstrate how an 8x8 multicolor LED matrix, Arduino, and a network monitoring program can be used to make an LED-based sniffer for around $60. And if that doesn't sound interesting, just wait until you see Port Scan Inferno.

Ask EFF: The Year in Digital Civil Liberties

Kurt Opsahl
Senior Staff Attorney, Electronic Frontier Foundation
Kevin Bankston
EFF Senior Staff Attorney
Marcia Hofmann
EFF Senior Staff Attorney
Hanni Fakhoury
EFF Staff Attorney
Peter Eckersley
EFF Staff Technologist
Rebecca Reagan
EFF Intake Coordinator

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 surveillance online and fighting efforts to use intellectual property claims to shut down free speech and halt innovation, discussion of our technology project to protect privacy and speech online, updates on cases and legislation affecting security research, 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.

Hacking Google Chrome OS

Kyle 'Kos' Osborn
Application Security Specialist, WhiteHat Security
Matt Johanson
Application Security Specialist, WhiteHat Security

Google recently announced Chrome OS powered computers, called Chromebooks, at Google I/O and the company is getting ready to market them to businesses as well as consumers. What's different about

Chrome OS and Chromebooks, other than the entire user-experience taking place exclusively in a Web browser (Google Chrome), is everything takes place in the cloud. Email, document writing, calendaring, social networking - everything. From a security perspective this means that all website and Web browser attack techniques, such as like Cross-Site Scripting, Cross-Site Request, and Clickjacking, have the potential of circumventing Chrome OS's security protections and exposing all the users data.

Two members of the WhiteHat Security's Threat Research Center, Matt Johansen and Kyle Osborn, have spent months hacking away on Google's Cr-48 prototype laptops. They discovered a slew of serious and fundamental security design flaws that with no more than a single mouse-click may victimize users by:

- Exposing of all user email, contacts, and saved documents.
- Conduct high speed scans their intranet work and revealing active host IP addresses.
- Spoofing messaging in their Google Voice account.
- Taking over their Google account by stealing session cookies, and in some case do the same on other visited domains.

While Chrome OS and Chromebooks has some impressive and unique security features, they are not all encompassing. Google was informed of the findings, some vulnerabilities were addressed, bounties generously awarded, but many of the underlying weaknesses yet remain — including for evil extensions to be easily made available in the WebStore, the ability for payloads to go viral, and javascript malware survive reboot. With the cloud and web-based operating systems poised to make an impact on our computing future, Matt and Kyle ready to share all their never-before-seen research through a series of on-stage demonstrations.

VoIP Hopping the Hotel: Attacking the Crown Jewels through VoIP

Jason Ostrom
Sipera VIPER Lab

This presentation is about the security of VoIP deployed in hotel guest rooms. What it is, why it benefits administrators and users, and how easily it can be broken. The hospitality industry is widely deploying VoIP. Since 2008, we've seen an increase of these rollouts along with Admin awareness of applying the required security controls in order to mitigate this potential backdoor into a company's mission critical data and systems — their Crown Jewels. The method is simple: through VoIP, a malicious hotel guest may gain access into corporate data resources such as a company's sensitive financial or HR systems. This talk will present updated research with a new case study: A Hotel VoIP infrastructure that had security applied. We will explore the missing pieces. How has this risk changed for permitting a hotel guest unauthorized network access, and who should be concerned? An old VLAN attack will be re-visited, with a new twist: how the VLAN attack applies to recent production VoIP infrastructure deployments, and how it can be combined with a new physical method. A new version of the free VoIP Hopper security tool will be demonstrated live, showcasing this new feature. In addition, we will investigate an alternative to CDP for device discovery and inventory control: LLDP-MED (Link Layer Device Discovery - Media Endpoint Discovery). A case study penetration test of a client infrastructure that used LLDP-MED follows , with a comparison to CDP. VoIP Hopper will demonstrate the first security assessment tool features for this advancing protocol. Mitigation recommendations will follow.

Big Brother on the Big Screen: Fact/Fiction?

Nicole Ozer
Technology and Civil Liberties Policy Director, ACLU of Northern California

Can the NSA really do that? Um, yes. Join me at the movies to take a close look at how current technology has caught up with the spy gadgets dreamed up for Hollywood flicks- from old favorites like Brazil to newer additions like Bourne and Dark Knight. Jaunty tin foil hats and movie snacks will be provided!

Getting SSLizzard

Nicholas J. Percoco
Senior Vice President and Head of SpiderLabs at Trustwave
Paul Kehrer
SSL Architect, Trustwave

The world has seen a seismic shift from browser-based web applications to GUI-rich semi-thick client applications running on handheld mobile devices. In the browser world, the industry had placed a great deal of time and energy towards providing users visual cues to indicate the level security and trust that their data being transmitted to the remote server is protected and not falling into the hands of unintended recipients. In the mobile device world, these visual cues are mostly nonexistent, resulting in the inherent trust that the underlying APIs are ensuring a level of security before transmitting a users sensitive data. In our research, we tested the most popular apps on both the iOS and Android platforms. We ran each app through a data transmission assault course that contained various historic, contemporary, and obscure SSL attacks and documented the results. In this presentation, we will discuss and demonstrate flaws at both the application an OS layer that need to be addressed by both the mobile app developers and well the mobile device manufactures. A utility called "SSLizzard" will also be released for use by mobile application developers to test their mobile apps and their behavior against SSL-based attacks discussed in this talk.

Malware Freak Show 3: They're pwning er'body out there!

Nicholas J. Percoco
Senior Vice President and Head of SpiderLabs
Jibran Ilyas
Senior Forensic Investigator, Spiderlabs

Well There's malware on the interwebs. They're pwning all your systems, snatching your data up. So hide your cards, hide your docs, and hide your phone, 'cause they're pwning er'body out there! This may be the 3rd and final installment of the Malware Freak Show series, so we're pulling out all the stops. This year we'll highlight 4 new pieces of malware but the victims are you and the people you know. We will analyze and demo malware found in your place of employment, your watering hole, your friendly neighborhood grocer, and finally your mobile phone. The malware we are going to demo are very advanced pieces of software written by very skilled developers that are target your world's data. The complexity in their propagation, control channels, anti-forensic techniques and data exporting properties will be very interesting to anyone interested in this topic.

This is REALLY not the droid you're looking for...

Nicholas J. Percoco
Senior Vice President and Head of SpiderLabs at Trustwave
Sean Schulte
Software Engineer, Trustwave

Last year, we presented a talk on the implication of malware and rootkits on mobile devices. We focused on the kernel layer of the Android OS stack. With the proliferation of Apps of every size, shape and color being published this year, we focused solely upon the User Interface (UI) of the Android OS. The results of our research yielded a very dangerous flaw that is likely going to require a UI overhaul of the Android OS. Our talk will demonstrate a technique using legitimate and documented APIs to steal credentials and other user information from the most popular Apps in the Android Market. We will demo this technique live and provide a technical walkthrough of the specific methods being used. At the conclusion of our talk, we'll release a Proof of Concept (PoC) built to demo this technique.

Hacking MMORPGs for Fun and Mostly Profit

Josh Phillips
Senior Malware Researcher

Online games, such as MMORPG's, are the most complex multi-user applications ever created. The security problems that plague these games are universal to all distributed software systems. Online virtual worlds are eventually going to replace the web as the dominant social space on the 'Net, as Facebook apps have shown, and this is big business. MMORPG game security is something that is very important to game studios and players, yet bots and exploits continue to infest all major MMORPG's, the creators and maintainers of the next generation of MMORPG's will need to understand software security from the ground up or face failure. The problem extends from software bugs such as item or money duplication, to mechanical exploitation such as botting, which leads to economic forces and digital identity theft. There is upwards of a billion dollars at stake, for both game hackers and game operators. Both Josh and Kuba have explored game hacking from both sides, and this talk presents a pragmatic view of both threats and defenses.

Port Scanning Without Sending Packets

Gregory Pickett
Penetration Tester, Hellfire Security

With auto-configuration protocols now being added to operating systems and implemented by default in your network devices, hosts are now actively advertising their available attack surfaces to anyone listening on the network.

By collecting background traffic on the network, and analyzing it, we can perform a host discovery, a port scan, and a host profile which even includes configuration information; all without sending any packets.

This means that threats both inside and outside your network can assess and target your network hosts silently without leaving a trail.

In this session, we'll start out by covering what makes this all possible, then examine typical network traffic to see what is made available to us, end up using several brand new tools that I have developed to utilize this information in an actual attack against a vulnerable network host, and finally finish our time discussing what you can as a network defender do about it.

My password is: #FullOfFail! — The Core Problem with Authentication and How We Can Overcome It

Jason M. Pittman
Researcher

Authentication is an integral part of our modern, digital lifestyle. It is a universal means of access to our work, to our finances, and to our friends and recreation. Of all the types of authentication available, passwords are still the most common form of authentication in use. Indeed, passwords in one form or another have been utilized since the dawn of computing. This, as this presentation will demonstrate, is not necessarily a good thing.

Simply put, password authentication is full of fail. Furthermore, the level of fail has nothing to do with the length, the complexity, or any other attribute of passwords. The researchers and professionals that have theorized about or created new password schemes- cognitive or picture-based passwords for example- are well intentioned but are only treating the symptoms of an inherently flawed technology.

The purpose of this presentation, then, is to ask discuss why our password authentication is so full of fail, to outline how this fail extends to other authentication methods, and to paint a brief outline of a new paradigm that does not suffer from the same inherent issues.

Sneaky PDF

Mahmud Ab Rahman
Specialist, CyberSecurity Malaysia

Being a most prevalent document exchange format on the Internet, Portable Document Format (PDF) is in danger of becoming the main target for client-side attack. With estimation of more than 1.5 million line of code and loaded with huge functionalities, this powerful document format is suffered with several high impact vulnerabilities, allowing attackers to exploit and use it as malware spreading vector.

Until now, there are thousands of malicious PDF file spreads with little chances of getting detected.

The challenges are obfuscation techniques used by the attackers to hide their malicious activities, hence minimizing detection rate. In order to sustain the survival of malicious PDF file on the Internet, attackers circumvent the analysis process through diverse obfuscation techniques. Obfuscation methods used usually ranges from PDF syntax obfuscation, PDF filtering mechanism, JavaScript obfuscation, and variant from both methods. Because of rapid changes in methods of obfuscation, most antivirus software as well as security tools failed to detect malicious content inside PDF file, thus increasing the number of victims of malicious PDF mischief.

In this paper, we study in the obfuscation techniques used inside in-the-wild malicious PDF, how to make it more stealthy and how we can improve analysis on malicious PDF.

Why Airport Security Can't Be Done FAST

Semon Rezchikov
Morgan Wang
Joshua Engelman

Eight years after 9/11 TSA finally decided to fix their security system. But what has really changed? Homeland Security's science division has been busy lately, and is currently polishing up a project called FAST - Future Attribute Screening Technology. FAST, part of project MALINTENT, is a project of the Department of Homeland Security Behavioral Science Unit, which supposedly can detect whether you want to blow up the plane purely based off of biological indicators. While it was originally slated for completion this year, the project has been delayed due to many technical difficulties. Starting to smell snake oil? Basic statistics and common sense agree! Methodological flaws, numerous exploits and better uses of tax dollars will be discussed.

Whoever Fights Monsters... Confronting Aaron Barr, Anonymous, and Ourselves

Paul Roberts
Editor, Threatpost.com, Kaspersky Lab
Aaron Barr
Former CEO HBGary Federal
Joshua Corman
Research Director, Enterprise Security Practice, The 451 Group
Jericho
Attrition.org

"Whoever fights monsters should see to it that in the process he does not become a monster." - Friedrich Nietzsche.

Aaron Barr returns for the first time in what's sure to be a gritty and frank (and heated) panel. How can we conduct ourselves without losing ourselves? How far is too far - or not far enough? IT security has finally gotten the attention of the mainstream media, Pentagon generals and public policy authors in the Beltway, and is now in mortal danger of losing (the rest of) its soul. We've convinced the world that the threat is real - omnipresent and omnipotent. But recent events suggest that in their efforts to combat a faceless enemy, IT security firms and their employees risk becoming indistinguishable from the folks with the Black Hats. The Anonymous attacks on Aaron triggered core issues. This panel will confront: Aaron, the emerging "cyber industrial complex", the Good, Bad and Ugly of the escalation with chaotic actors like Anonymous and LulzSec, what the U.S. gains (and loses) by making "APTs" the new "Commies" and cyber the forefront of the next Cold War, and how we may fight our "monsters" while protecting civil liberties and the freedoms we enjoy here at home?

What Time Are You Anyway?

Michael Robinson

Computer forensic examiners rely heavily on timestamps during investigations. Timeline analysis is a critical technique in determining what happened and when. In 2005, timestomp.exe was released and this gave non-observant investigators a run for their money. Unfortunately, there are some gaps in what timestomp.exe will do. Observant investigators can identify timestomping and recover from that activity. Good timestomping requires knowing what time values need to get trashed, where these times are stored, AND what supporting artifacts need to be altered. This presentation examines several file systems and operating systems and identifies what needs to be tweaked in order to effectively hide one's tracks.

Owned Over Amateur Radio: Remote Kernel Exploitation in 2011

Dan Rosenberg

Originally considered to be the stuff of myth, remote kernel exploits allow attackers to bypass all operating system protection mechanisms and gain instant root access to remote systems. While reviewing prior work in remote kernel exploitation, this talk will go over some of the challenges and limitations associated with developing remote kernel exploits.

We will discuss in detail the development of an exploit for a remotely triggerable vulnerability in the Linux kernel's implementation of the ROSE amateur radio protocol. In doing so, a number of new kernel exploitation techniques will be demonstrated. In addition, this talk will present a working example of the installation of a remote kernel backdoor. We will conclude with a demonstration of this exploit against a live system and a discussion of future work in kernel exploitation and mitigation.

Build your own Synthetic Aperture Radar

Michael Scarito

Radar is used extensively by the military, police, weather, air travel, and maritime industries - why not you? Come learn how to build a radar imaging system on the cheap! This talk will explain the basics of how radar works as well as how to measure range and velocity of your chosen targets. You will learn how to use synthetic aperture techniques to generate a two- or even three-dimensional image. The hardware and software design will be totally opened up so you can go home and build your own system.

The talk will try to run through the basics pretty fast, so some knowledge of electronics or basic physics might help, but is not required! Regardless of your background, you will see the capabilities of a modern home-built radar system and hopefully get some ideas for your own uses.

Net Neutrality Panel

Michael "theprez98" Schearer
Associate, Booz Allen Hamilton
Abigail Phillips
Senior Staff Attorney, Electronic Frontier Foundation
Deborah Salons
Telecommunications Attorney, Washington DC
Todd Kimball
Geek, burner, hacker, artist, sectwit

Over the last five years, network neutrality has moved from an abstract buzzword to FCC-enacted policy. Supporters and detractors both contend that their opponents position means "the end of the Internet as we know it!" This panel discussion will present a reasoned discussion of the issue from multiple viewpoints. Among the issues to answer: What is network neutrality and can we even agree on a definition? Does the FCC have the authority to enact net neutrality rules? What is the role of Congress in net neutrality? Lastly, what are the future implications for the Internet? This panel discussion will cover the basics of net neutrality, the role of Congress and the FCC in regulating the Internet, and the future legal and policy implications of the FCC's neutrality rules. Is the future of the Internet really at risk?

WTF Happened to the Constitution?! The Right to Privacy in the Digital Age

Michael "theprez98" Schearer
Associate, Booz Allen Hamilton

There is no explicit right to privacy in the Constitution, but some aspects of privacy are protected by the First, Third, Fourth and Fifth Amendments. This presentation will discuss the historical development of the right to privacy, and in particular, the development of the Fourth Amendment; and then compares this historical development to the current digital age. The development of the right to privacy (especially given the historical context of the Fourth Amendment) to our current age requires us to deal with technologically invasive personal searches as airports, searches and seizures of laptops and other computing devices, and how to handle stored communications. It becomes evident very quickly that searches and seizures are not so clear when it comes to bits and bytes...so where do we go from here?

Archive Team: A Distributed Preservation of Service Attack

Jason Scott
textfiles.com

For the last few years, historian and archivist Jason Scott has been involved with a loose, rogue band of data preservation activists called The Archive Team. As major sites with brand recognition and the work of millions announce short-notice shutdowns of their entire services, including Geocities, Friendster, and Yahoo Video, Archive Team arrives on the scene to duplicate as much as they possibly can for history before all the data is wiped forever. To do this, they have been rude, crude and far outside the spectrum of polite requests to save digital history, and have used a variety of techniques to retrieve and extract data that might have otherwise been unreachable. Come for the rough-and-tumble extraction techniques and teamwork methods, stay for the humor and ranting.

Attacking and Defending the Smart Grid

Justin Searle
Senior Security Analyst at InGuardians, Inc.

The Smart Grid brings greater benefits for utilities and customer alike, however these benefits come at a cost from a security perspective. Unlike the over-hyped messages we usually hear from the media, the sky is NOT falling. However, just like any other technology, the systems and devices that make up the Smart Grid will have weaknesses and vulnerabilities. It is important for us to understand these vulnerabilities, how they can be attacked, and what we need to do to defend against those attacks.

This presentation will explore how the increased functionality and complexity of the Smart Grid also increases the Smart Grid's attack surface, or in other words, increases the ways attackers can compromise the Smart Grid's new infrastructures, systems, and business models. We'll discuss several specific attack avenues against the Smart Grid and the recommendations we are making to utilities and vendors to mitigating and blocking these attacks. This will be done without the FUD and over-hyped framing that we usually find in the media and other Smart Grid presentations.

Mobile App Moolah: Profit taking with Mobile Malware

Jimmy Shah
Mobile Security Researcher

Smartphones are a hot new market for software developers. Millions of potential customers, and a large percentage willing to part with a small sum of money for your latest creation. Even a moderately successful app can help fill your pockets. It's hard to ignore for legitimate developers. It's even harder to ignore for criminals.

Things have changed from the old days of malware creation. It's no longer just about proving yourself or testing a new platform by writing proof-of-concepts(PoCs), porting old malware, and learning the idiosyncrasies of the development tools. Now it's about evading detection and taking a profit. Where there's money, crime usually follows.

The presentation is not about attribution, naming names or pointing out the parties responsible. It's about the underlying technology and the methods used, including:

- how actual examples in the wild function
- detection/analysis evasion techniques
- geographical trends in profit-taking malware

Are You In Yet? The CISO's View of Pentesting

Shrdlu

When a CISO pays good money for a thorough pentesting, she wants results. Not necessarily the ones that the pentester had in mind, either. Whether the time allotted is too short, the pentester has to achieve multiple objectives, or they disagree on the severity of the findings, both the CISO and the pentester have to agree on both sides of the engagement. We discuss numerous aspects of voluntary pwnage: the differences between a security assessment and a penetration test, what color of box works best, tweaking the objectives for more targeted results, and ensuring a happy ending.

Hacking the Global Economy with GPUs or How I Learned to Stop Worrying and Love Bitcoin

Skunkworks

In the post 9/11 era when it's nearly impossible to buy a pack of gum without alerting the big three credit bureaus, you may think that anonymity is long gone from the economy. That's where bitcoin comes in. Bitcoin is a decentralized peer-to-peer currency based solely on computing power. It is (mostly) untraceable and highly anonymous, not backed by any banks or companies, and in the words of Jason Calacanis "the most dangerous project we've ever seen". In my talk I'll explain what bitcoin is and isn't, and why this 70+ PetaFLOP network has caught the attention of everyone from The Washington Post and MSNBC to Wikileaks and the EFF.

How Haunters Void Warranties

Reeves Smith
Senior Network Security Eng. Tenacity Solutions Inc.

Halloween makers or how haunters void warranties, social engineer and find the joy of creativity. A short path down to what a community of makers that mod hardware, special effect and mood you in order to scare the shit out of you just one night a year. These people comprise electrical engineers to housewives and personally I've learned to solder better, faster because of it.

SCADA & PLCs in Correctional Facilities: The Nightmare Before Christmas

John J. Strauchs
President of Strauchs LLC
Tiffany Rad
President of ELCnetworks, LLC
Teague Newman
Information Security Professional/Pen Tester

On Christmas Eve, a call was made from a prison warden: all of the cells on Death Row popped open. Not sure why or if it would happen again – especially concerned that these prisoners have nothing to lose in escape attempts — the warden called physical security engineer, John Strauchs, to investigate. Many prisons and jails use SCADA systems with PLCs to open/close doors. The increased voltage in the door lock was caused by a Christmas Eve power surge and the ladder logic used in PLCs flipped the switches to "open." This talk will evaluate SCADA systems and PLC vulnerabilities in correctional and government secured facilities, give examples of existing risks in other industries using PLCs and demo simulations of PLC vulnerabilities utilizing existing and new exploits while recommending solutions.

Steal Everything, Kill Everyone, Cause Total Financial Ruin! (Or How I Walked In And Misbehaved)

Jayson E. Street
CIO of Stratagem 1 Solutions

This is not a presentation where I talk about how I would get in or the things I might be able to do. This is a talk where I am already in and I show you pictures from actual engagements that I have been on. They say one picture is worth a thousand words I show you how one picture cost a company a million dollars and maybe even a few lives. In a community where we focus so much on the offensive I also make sure with every attack I highlight. I spend time discussing what would have stopped me. We need to know the problems but we need more talks providing solutions and that is what I hope people will get from this. I show the dangers of Social engineering and how even an employee with no SE experience can be an eBay James Bond which can cause total financial ruin to a company. These Security threats are real. So are these stories!

Weaponizing Cyberpsychology and Subverting Cybervetting for Fun, Profit and Subterfuge

Chris "TheSuggmeister" Sumner
Security Researcher
alien
Security Consultant
Alison B
Security Researcher

Almost everything we do in life leaves a personality footprint and what we do on social networking sites like Facebook is no exception. During this talk we will examine:

- What it is possible to determine about someone's personality from their facebook activity
- What to look for when you are trying to identify the most pwnable person in a group
- Whether facebook activity can indicate a high probability of having or developing depression
- How you could weaponize 'sockpuppets' by giving them certain personality traits
- Cybervetting and your rights (or lack of rights) to privacy
- Steps you can take to manage or even alter your 'NetRep' (online reputation)

We conducted a research project called 'The Big 5 Experiment' with the objective of determining whether there were any significant correlations between a user's facebook activity and their answers to a personality questionnaire called 'The Big Five Inventory'. The Big Five Inventory was created by Prof Oliver John, to measure personality dimensions known as the Big Five.

Considering the ubiquity of personality tests such as the Myers-Briggs for employee selection and the growing number of companies adding cybervetting to their selection processes, it can only be a matter of time before we see the two activities merge and at what cost to society?

You should leave the talk with an insight into how the Big 5 Experiment results could be used in attack and defense strategies. Should you wish to conduct your own research, related or not, you should also learn from what proved a rather fascinating experience in carrying out the experiment.

Facebook: http://www.facebook.com/onlineprivacy-foundation

Brute Forcing Interactive Voice Response (IVR) Systems

Harish Skanda Sureddy

This talk proposes a concept about brute forcing IVR systems using popular VOIP / calling programs. The technique suggested here can be used to brute force DTMF flavored IVRs including those in the banking sector. The proposed concept attempts to integrate the VOIP program's API with existing speech APIs such as Java Speech API or Microsoft Speech SDK and build an automated IVR brute forcer.

How To Get Your Message Out When Your Government Turns Off The Internet

Bruce Sutherland
Security Researcher

How would you communicate with the world if your government turned off the Internet? Sound far-fetched? It isn't. It already happened in Egypt and Lybia and the US Congress is working on laws that would allow it to do the same. In this talk we'll explore how to get short messages out of the country via Email and Twitter in the event of a national Internet outage. Remember, data wants to be free.

Web Application Analysis With Owasp Hatkit

Martin Holst Swende
Senior Security Consultant, 2Secure AB
Patrik Karlsson
Senior Security Expert, 2Secure AB

The presentation will take a deep dive into two newly released Owasp tools; the Owasp Hatkit Proxy and the Owasp Hatkit Datafiddler. The name Hatkit is an acronym (of sorts) for Http Analysis Toolkit and are tools mainly for people who analyse (hack!) web applications. The tools make extensive use of MongoDB, in particular the advanced querying facilities in available in this database. Prior knowledge of Javascript and Python is an advantage, but absolutely no requirement.

Wireless Aerial Surveillance Platform

Mike Tassey
Security Consultant
Rich Perkins
Senior Security Engineer

Tired of theory? This session has everything you want, big yellow aircraft flown by computers, pounds of highly volatile chemicals, CUDA, 50 Amp electrical circuits and the ability to attack networks, systems and cell phones interactively from a remote location anywhere in the world. We will demonstrate a fully functional open source autonomous aerial wireless hacking platform and explain how to pwn the friendly skies. The talk will cover actual construction and components of the aircraft itself and its mission support systems. From start to finish, we will discuss design concepts, lessons learned and potential pitfalls.

Staring into the Abyss: The Dark Side of Crime-fighting, Security, and Professional Intelligence

Richard Thieme
ThiemeWorks

Nothing is harder to see than things we believe so deeply we don't even see them. This is certainly true in the "security space," in which our narratives are self-referential, bounded by mutual self-interest, and characterized by a heavy dose of group-think. That narrative serves as insulation to filter out the most critical truths we know about our work.

An analysis of deeper political and economic structures reveals the usual statements made in the "security space" in a new context, one which illuminates our mixed motivations and the interpenetration of overworlds and underworlds in our global society. Crime and legitimacy, that is, are the yin/yang of society, security, and our lives. You can't have one without the other. And nobody should know this better than hackers.

This presentation will make you think twice before uncritically using the buzzwords and jargon of the profession — words like "security," "defense," and "cyberwar." By the end of this presentation, simplistic distinctions between foreign and domestic, natural and artificial, and us and them will go liquid and the complexities of information security will remain ... and permeate future discussions of this difficult domain.

As a result, we will hopefully think more clearly and realistically about our work and lives in the context of the political and economic realities of the security profession, professional intelligence, and global corporate structures.

Insecurity: An Analysis Of Current Commercial And Government Security Lock Designs

Marc Weber Tobias
Investigative Attorney and Security Specialist, Security.org
Matt Fiddler
Security Consultant
Tobias Bluzmanis
Security Consultant

Lock manufacturers continue to produce insecure designs in both mechanical and electro-mechanical locks. While these devices are designed to provide secure access control to commercial and government facilities, in fact many do not. Recent disclosures with regard to extremely popular push-button locks have led to an expanded investigation into their technology and security by our research team. As a consequence, it appears that mechanical locks, as well as electro-mechanical locks that are compliant with government standards, may be subject to several different forms of compromise, thereby placing commercial and government facilities at risk.

In this presentation, we will examine specific design parameters that are supposed to provide a high level of protection against covert entry for both commercial and government facilities, but do not.

It would be logical to assume that the electronics and physical hardware within physical access security devices would work together and present a high level of difficulty in circumventing the requirements of these standards. Our research has disclosed that such is not the case in certain devices. Our investigation with regard to a specific manufacturer of extremely popular hardware discloses a lack of understanding with regard to security engineering and an inability to produce hardware that is immune to different forms of attack. We document three serious occurrences of security engineering failures with regard to different product designs, all intended to provide a certain level of security for commercial and government facilities.

We will examine different designs, both mechanical and electronic, and why there is a basic failure in the most basic fundamentals of designing a secure device.

DIY Non-Destructive Entry

Schuyler Towne
Competitive Lockpicker

Ever leave the house without your picks only to find yourself in a situation where you desperately need them? Well, never fear! I'm going to explain how to open everything from cars, to briefcases to safes with objects as common as popsicle sticks and unconventional as palm sanders. Every attack will be fully explained so you understand the underlying mechanisms and how we are taking advantage of mechanical tolerances and design flaws to own these locks.

The Future of Cybertravel: Legal Implications of the Evasion of Geolocation

Marketa Trimble
Associate Professor of Law, William S. Boyd School of Law, University of Nevada, Las Vegas

This presentation discusses the current legal status of evasion of geolocation and the potential liability of the user-evader or provider of an evasion tool. The presentation also projects how the law might develop to treat acts of evasion and what challenges the technical community might face in this area.

The legal community has shown an interest in geolocation for several years; however, until recently it did not seriously consider mandating the use of geolocation to comply with national laws and regulations. Recently, there have been indications that governments will turn to geolocation as a viable means of partitioning cyberspace; geolocation tools should help mimic physical borders in cyberspace. The emerging reliance of legal systems on geolocation creates a need to address evasion of geolocation and reevaluate the legality of acts of evasion.

So far, no legal disputes concerning evasion have been published; however, the ongoing disputes regarding place-shifting technologies, such as the lawsuits against ivi and Justin.tv in the U.S., TV Catch UP in the U.K., and ManekiTV in Japan, indicate that evasion of geolocation is the next in line for legal attention.

The presentation will provide no legal advice but will offer a number of suggestions that should be considered by those who use evasion, are interested in evasion, or are in the process of developing evasion tools. Additionally, it will suggest the types of legal policy issues that are likely to emerge in the near future.

Runtime Process Insemination

Shawn Webb
Security Analyst

Injecting arbitrary code during runtime in linux is a painful process. This presentation discusses current techniques and reveals a new technique not used in other projects. The proposed technique allows for anonymous injection of shared objects, the ability to pwn a process without leaving any physical evidence behind. Libhijack, the tool discussed and released in this presentation, enables injection of shared objects in as little as eight lines of C code. This presentation will demo real-world scenarios of injecting code into end-user processes such as firefox, nautilus, and python.

Network Nightmare: Ruling The Nightlife Between Shutdown And Boot With Pxesploit

Matt "scriptjunkie" Weeks
Researcher

The best techniques for exploitation, maintaining access, and owning in general move down the stack, using low-level code to bypass security controls. Take the preboot execution environment and get bios-level access to the hardware from across the network, outside any control of the on-disk operating system. In this presentation I will detail the pxesploit attack I wrote, releasing a new metasploit-based comprehensive PXE attack toolkit to deliver any payload reliably to many different operating systems. Also new will be the ability to host a PXE attack through a meterpreter session in memory, using it to escalating privileges and own remote networks.

Seven Ways to Hang Yourself with Google Android

Yekaterina Tsipenyuk O'Neil
Principal Security Researcher, HP Fortify Software
Erika Chin
Ph.D. Student, UC Berkeley

According to Google, Android was designed to give mobile developers "an excellent software platform for everyday users" on which to build rich applications for the growing mobile device market. The power and flexibility of the Android platform are undeniable, but where does it leave developers when it comes to security? In this talk we discuss seven of the most interesting code—level security mistakes we've seen developers make in Android applications. We cover common errors ranging from the promiscuous or incorrect use of Android permissions to lax input validation that enables a host of exploits, such as query string injection. We discuss the root cause of each vulnerability, describe how attackers might exploit it, and share the results of our research applying static analysis to identify the issue. Specifically, we will show our successes and failures using static analysis to identify each type of vulnerability in real-world Android applications.

Key Impressioning

Jos Weyers

We've all seen lockpicking explained on several security venues. You might even have tried it yourself. But what if you need to open a lock a number of times? Wouldn't it be great to have an opening technique that would supply you with a working key in the process? A method to do this has existed for quite some time, but until recently it has remained quite unknown. Some time ago impressioning locks got "re-invented" by the lockpick community and the skill evolved to the level now shown at several international championships. What is it? How does it work? What skill is involved? Why is it the most interesting way to open a lock? These questions, and more will be answered in this talk.

Staying Connected during a Revolution or Disaster

Thomas Wilhelm Sr.
Security Consultant, Trustwave's SpiderLabs

During the recent revolutions in Africa and the Middle East, governments have shut down both Internet and Phone services in an attempt to quell communication among demonstrators. In addition, during natural disasters, people have been left without a means of finding out the latest news regarding emergency services. We will discuss methods that can circumvent severed telecommunication infrastructures, including the use of mobile devices to act as ad hoc network access points. At the end of this talk, a new open source project will be announced, with the goal of developing the capabilities to generate spontaneous networks in times of crisis using current cellular phone technology.

Traps of Gold

Andrew Wilson
Security Consultant, Trustwave SpiderLabs
Michael Brooks
Security Researcher

The only thing worse than no security is a false sense of security. And though we know, "you can't win by defense alone", our modern approaches tend to act as though offense and defense are two entirely separate things. Treating security as an issue of quality has gotten us far, however, nearly everyday, some of the largest companies are still being compromised. It's become apparent that with enough time a skillful attacker will always get in. We have created new armaments to fight back. This style of fighting, known as maneuverability, aims to make your opponents expend their own resources while putting yourself in a position of strategic advantage. Using techniques that leverage deception, ambiguity, and tempo we believe we can do better to protect web applications. If time is an attacker's most important resource, let's steal it away from them. But talk is cheap. Not only will we demonstrate real world examples of this system, we encourage you to prove us wrong. An unofficial web application capture the

flag competition, based on deceptive defense techniques, will be made available for testing throughout the conference.

Network Application Firewalls vs. Contemporary Threats

Brad Woodberg
Security Product Line Engineer, Juniper Networks

In the last few years, a so called whole new generation of firewalls have been released by various vendors, most notably Network Application Firewalling. While this technology has gained a lot of market attention, little is actually known by the general public about how it actually works, what limitations it has, and what you really need to do to ensure that you're not exposing yourself. This presentation will examine/demystify the technology, the implementation, demonstrate some of the technology and implementation specific vulnerabilities, exploits, what it can and can't do for you, and how to defend yourself against potential weaknesses.

Phishing and Online Scam in China

Joey Zhu
Staff Engineer, Trend Micro Inc.

Today, Ebay, Paypal and WOW are all popular targets of global phishing. However, phishing in China is different from that in other countries. The Chinese government has already placed a lot of focus on this issue, however, online scams have already gone beyond the traditional scope of phishing. For example, one of the top five phishing targets is CCTV, which is an official Chinese TV station that produces several of the most widely distributed Chinese TV channels. I will explain how hackers get money through CCTV phishing. In the first part of the presentation, I will introduce the event about massive online bank phishing attacks, which target customers of the "Bank of China" at Feb, 2011. Then, I will share information about popular scams, which try to trick people into believe they won the lottery or bought cheap tickets. Finally, I will show a case about Taobao phishing, analyze its framework and the source code behind it.

Vanquishing Voyeurs: Secure Ways To Authenticate Insecurely

Zoz
Cannytrophic Design
Andrea Bianchi
KAIST

Observation is one of the principal means of compromise of authentication methods relying on secret information such as PINs and login/password combinations. Attackers can gather this information via observation, either from without by methods such as shoulder surfing and camera-based ATM skimmers, or from within by methods such as keystroke loggers and button-overlay-based ATM skimmers. Though these vulnerabilities of PIN/password based authentication mechanisms are well known, they have been difficult to correct due to the prevalence and general acceptance of such systems — they are used in essentially all ATMs, mobile device locking mechanisms, and most web-based authentication schemes. It is difficult to avoid at least the occasional use of untrusted public terminals and devices and the unlocking of one's mobile device in public. We therefore present our research into devices and techniques for mitigating the threat of credential compromise when doing so. These include haptic and auditory mechanisms for password entry into public terminals, mobile device tools for turning one's mobile device into an observation-resistant password entry system, and strategies and tools for secure password entry in the presence of keyloggers and other input recording devices. These techniques can successfully evade observation even when one does not have administrative control of the terminal, as in the case of internet cafe computers and public ATMs.

Whitfield Diffie and Moxie Marlinspike

Come watch Whitfield Diffie and Moxie Marlinspike talk about certificate authorities, DNSSEC, SSL, dane, trust agility and whatever else they want to. Moderated by the Dark Tangent and with Q&A from the audience.

Johnny Long and Hackers for Charity

Johnny Long

Picking on charities is just plain rude. Thankfully, that's not what we're about. We're about proving that hackers have amazing skills that can transform charitable organizations.

We're about stepping into the gap to feed and educate the world's most vulnerable citizens. We are virtual, geographically diverse and different.

We've fed thousands of families through our "food for work" program We build computer labs to help students learn skills and land jobs that are key to disrupting poverty's vicious cycle.We provide technical assistance to charities and non-profits that can not afford IT services.We provide job experience and references to our volunteers.

http://www.hackersforcharity.org/

Anonymous Cyber War

Hubris
Strategic Operations, Backtrace Security http://www.backtracesecurity.com/
a5h3r4h
Director of Psychological Operations

This talk will educate listeners on best practices for safety and privacy on the Internet.It aims to demonstrate the improbability of staying anonymous while engaging in group or social activities on the internet, and especially while engaging in criminal activities as a group.

This talk will reveal how Hubris, A5h3r4h, and Backtrace security staged a cyber war against anonymous, using Anonymous' own methods, and how key operatives in anonymous were exposed, scattered and neutralized. In short, how a handful of bored social engineers with no material resources used trolling, social engineering, and the magic of Google to derail an army of out of control btards with a dose of virtual Ritalin.

We will also provide an explanation of how different organizations (and even non-organizations) have their own "signature" beliefs and behaviors and how they can be used against them.

Hacking and Forensicating an Oracle Database Server

David Litchfield

David Litchfield is recognized as one of the world's leading authorities on database security. He is the author of Oracle Forensics, the Oracle Hacker's Handbook, the Database Hacker's Handbook and SQL Server Security and is the co-author of the Shellcoder's Handbook. He is a regular speaker at a number of computer security conferences and has delivered lectures to the National Security Agency, the UK's Security Service, GCHQ and the Bundesamt f̲r Sicherheit in der Informationstechnik in Germany.

Operational Use of Offensive Cyber

Christopher Cleary
former Computer Network Operations Planner from US CYBER COMMAND

This session will discuss the "Art of the Possible" when it comes to "Offensive Cyber Operations" and why it is so important for both military and non-military cyber professionals to understand each others persepctives on "Offensive Cyber Operations". Discussion will focus on the military's planning process and how the potential introduction of offensive cyber operations could effect the process and why information sharing events sessions like "DEFCON" are so important to its eventual success.

Meet the Federal Agent 2.0

Panel

Current Federal Agents that are running operations and investigations now, targeting today's threats to our nation. Meet the Fed at DEFCON 19 will offer the attendee a chance to ask questions about how these Federal Agents got where they are, general investigative issues relative to their current duties and other relevant topics. MTFA 2.0 differs from past panels as it brings a younger, current operations flavor and has less of a leadership/old school feel. The panel will also be smaller than past years since the focus will be specific to credentialed Federal Agents.

Note: Agents will not discuss current investigations nor will they entertain inappropriate questions.

d

MOVIE NIGHT WITH DT

Every year I try to play some favorite moves from different styles. I usually go for a sci-fi live action, an animated or CG generated one, and something totally different. This year I am sticking with tried and true movies, partially because I didn't have time to find really cool new ones, and partially because I haven't shown these before.

Spy Game

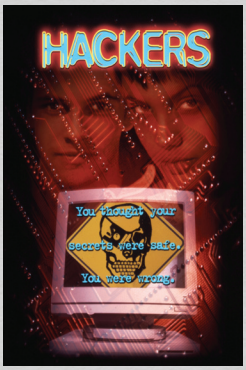
Saturday 19:00 in Track 2

2001 126 Min (R) Rated
With 3 Days of the Condor (A past Movie Night pick) and Sneakers star Robert Redford and Brad Pitt. No real computers here, you as you follow Redford's character you can tell he thinks like a hacker. When I metion this movie to people most don't remember it, so I hope it is a suprise to many of you. Trivia Note: Several scenes were copied / inspired by the book "By way of deception"

Akira - Special Edition

Saturday 21:00 in Track 2

1987 125 Min (R) Rated
This movie defines the anime megaopolis genre. It has been cool for over 20 years and is still cool today. That's why I am showing it to you, you poor deprived souls, who don't even realize it has been the foundation on which sci fi anime was built.



Hackers

Friday 19:00 in Track 2

This movie has a special place in my heart, for several reasons. No,it is not accurate, but it was the first "Hacker" movie that tried tovisually depict hacking in different ways than just a dude at a keyboard. It was at a time when the .com bubble was starting to inflate and hacking was cool. The Net had just come out.
This movie had a hacking contest puzzle associated with it, and ended up becoming the first web site in history to be defaced. This was the start of it all. The characters are all based on real hackers from either the MOD or the LOD. Well, not all, there was no hot female hacker. We can play trivia and see who can guess who was who. Lord Nikon was Lord Neon for example.

Good sound track, some funny lines, and they never caught the people who defaced the site.

WORKSHOPS

New for Def Con 19, Workshops extends the experience of learning to the classroom. Take your time and get it right by getting some hands-on time with hardware, software, and picking the minds of some of the most interesting hackers in their fields. Bring your thinking cap and get ready to be schooled. Registration is on-site, cash-only, limited capacity, first-come, first-served, and opens late Thursday and continues Friday and Saturday.. Sessions start at 10AM sharp, Friday and Saturday, and will go till 7PM.

Embedded system design: From electronics to microkernel development.

Rodrigo Almeida. Universidade Federal de Itajubá.
@rmaalmeida

This workshop consists of a introduction on the embedded systems design. Begin by building a simple electronic embedded system design as a target platform. Talk about the low level side of C language as bit-fields arrays and bit-wise operations, pointers to fixed memory addresses and registers, and how to access the micro-controller peripherals, etc. This will be the base to develop a full embedded micro-kernel using ISO-C, without the standard libraries with some of the standard libraries being coded to suit the low memory requirements.

Friday & Saturday - $200

Car Hacking

Robert Leale
CanBusHack.com

Learn how to better understand the fundamentals of Vehicle Network topology, data, Vehicle

Network Protocols, Diagnostic Protocols, Immobilizer and vehicle data and security. Learn about and see how CAN BUS works and can be used, good and bad. Diagnostic and immobilizer demonstrations and theory. Possible demonstration of a known CAN BUS crack.

Friday - $200

The Art Of Exploiting SQL Injection

Sumit Siddharth, notsosecure
www.notsosecure.com

A full day, hands-on training for you penetration testers, security auditors, administrators, and web developers. Learn advanced exploitation techniques via SQL Injection, an oldie but goodie at 15 years old. It still exists in over 30% of web applications! The training will target MS-SQL, MySQL, and Oracle. Identify, Extract, Escalate, Execute.

Friday - $200

Engineering Crash Course

Justin Karl
Mechanics of Materials Research Group (MOMRG), University of Central Florida

Begin your path towards gaining the knowledge required to actually build projects like vehicles, weaponry, and giant mech suits to scare your friends.Who knew that a very strong base of various types of design-applicable knowledge can, in fact, be developed in one day. Engineering Crash Course will teach the basics of Machine Design, Solid mechanics, Control Systems, Flight, Machining, Materials, and Testing. A final, hour-long, Q&A/brainstorming session of evil genius can't be missed..

Friday & Saturday - $200

Open Source Intelligence Gathering for pen-testing with FOCA PRO

Chema Alonso
@chemaalonso

Learn why and how to use FOCA PRO in a fingerprinting process within a pen-testing project. Fire up a copy of FOCA PRO 2.6 and learn how to combine FOCA with other tools like Evilgrade, Spider Tools, etc. Services, DNS, Google, Bing, PTR Scanning, Thrashing, DLP, and more.

Friday - $200

Mobile Hacking Workshop by HotWAN

Blake Turrentine
HotWAN

http://www.hotwan.com

Prepare to be introduced to multiple smartphone technologies and development environments. Inspect and audit mobile apps, circumvent operating systems, leverage mobile forensics, conduct and witness network-based attacks. Be ready to show your mobile OS skills and talk about your knowledge and research into Mobile Hacking on iOS, Android, APIs, SMS/MMS, MITM, and radio stuff like NFC, CDMA, basebands, and more!

Friday & Saturday - $200

Hacking the Male and Female OS (Men are from Windows, Women are from Linux)

Valerie Thomas, Norwin Technologies
@hacktress09

You wouldn't use the same attacks for different operating systems so why would you use the same social engineering attacks for men and women? The male and female brains are as different as Linux and Windows. This principle applies to male and female targets as well as attackers. Cover the basics, then dive into non-traditional topics such as spycraft, acting, pressure sales, the psychology behind them, and how it all applies to the social engineering that we know and love. Explore the mechanics of the male and female brain and how to attack vectors for each and take it to the streets to put it to the test. This session will be especially useful for aspiring social engineers, those who provide social engineering training, and anyone who wants to learn new twists on some old tricks.

Friday & Saturday - $200

Wi-Fi Security Megaprimer (Beginner to Advanced)

Vivek Ramachandran, SecurityTube
@SecurityTube

Join a highly technical and in-depth treatment of Wi-Fi security. Gain a deep understanding of the principles behind various attacks, not just a quick how-to guide on publicly available tools. Start with the basics by dissecting WLAN packet headers with Wireshark, then graduate to the next level by cracking WEP, WPA/WPA2, and then move on to real life challenges like orchestrating Man-in-the-Middle attacks and taking on the live Wi-Fi CTF!

Saturday - $200

How To Present With Impact

James Arlen, Principal, Push The Stack Consulting
@myrcurial

Ever used more than 4 fonts in a PowerPoint deck or a font size less than 24pt? Ever read your talk from speakers notes? We know the answer is to join this highly interactive workshop during which there will instruction and a whole lot of working together to improve, with the aim of getting from the Idea to the Delivery, with two practice sessions in workshop format including your fellow attendees. Stop producing crap presentations which fail to get your point across. There will be a tool released at this talk that will make you not look like crap nearly as often as you do now. Bring PowerPoint or OOo's Present, and get schooled.

Saturday - $200

Hosting sites as I2P eepSites and Tor hidden services

Adrian Crenshaw, Irongeek
http://irongeek.com

Ever wanted to host something but not have it tied back to you? Don't know what VPS to trust? How about hosting it in I2P or Tor? This workshop will cover how to do these things while discussing some of the pitfalls that may give your identity away. Improve your knowledge of how to host I2P eepSites and Tor hidden services.

Saturday - $200

Binary Instrumentation for Hackers

Gal Diskin, Intel
@gal_diskin

Binary instrumentation is a valuable tool for hackers and security experts. More people in the hacker and security community are paying closer attention to it but it is still relatively unknown and underused, despite it being a valuable tool. Learn the basic concepts of DBI and get started using the Pin binary instrumentation engine. DBI is used for vulnerability detection, pre-patching vulnerabilities, de-obfuscation, taint-analysis and much more.

Saturday - $200

MITM workshop: The League of Extraordinary Middlemen

Rob Havelt & Steve Ocepek, Trustwave
@dasfiregod, @nosteve

Got Layer 2 access? Make local networking "all about you" just by helping to send packets along on their happy way. This workshop is all about man-in-the-middle attacks and how they can be useful for everything from snooping to session takeover. While covering techniques from

ARP Poisoning to the latest SLAAC attack, this workshop will arm attendees with powerful inside knowledge about technology implemented on virtually every Local Area Network.

Friday & Saturday - $200

Friday

Embedded System Design: From Electronics To Microkernel Development

Rodrigo Almeida

Hacking the Male and Female OS (Men are from Windows, Women are from Linux)

Valerie Thomas

Engineering Crash Course

Justin Karl

Mobile Hacking Workshop by HotWAN

Blake Turrental

Vehicle Network Hacking

Robert Leale

The Art Of Exploiting SQL Injection

Sumit Siddharth

How to Present with Impact

James Arlen

Saturday

Embedded System Design: From Electronics To Microkernel Development

Rodrigo Almeida

Hacking the Male and Female OS (Men are from Windows, Women are from Linux)

Valerie Thomas

Engineering Crash Course

Justin Karl

Mobile Hacking Workshop by HotWAN

Blake Turrental

Open Source Intelligence Gathering for pentesting with FOCA PRO

Chema Alonso

802.11 Wireless LAN Security and Hacking

Vivek Ramachandran

Introduction To Binary Instrumentation For Hackers

Gal Diskin

Hosting sites as I2P eepSites and Tor hidden services

Adrian Crenshaw

MITM workshop: The League of Extraordinary Middlemen

Rob Havelt & Steve Ocepek

VENDORS

Ninja Networks

"Ninja Networks returns with their limited edition challenge coins, custom made for DEFCON each year. Once they're gone, they're gone, and never remade. Please note that our most popular designs have always sold out by Saturday. (Note for feds/spooks/etc: We do trade coins. Ask at the booth or track down barkode.)"

LBGFX

Customize T shirts & Stickers on the spot at Defcon 18

MECO

Your source for workstations and networking equipment and then some…
PO Box 939 Snohomish, WA 98291-093
Tel: (425)788-0208 Fax: (360)794-8754
Serving the Industry since 1980

BreakPoint Books

BreakPoint Books is your official conference bookstore on site at DefCon. We'll have all your favorite books for sale and we're conveniently located in the Vendor Area. Make sure to stop by and view the titles in stock and purchase a few written by some of your favorite authors!

Greensector

Stop by our booth for unique limited-run t-shirts designs, DJ mixes, stickers, buttons, post cards & other nick-hacks. Presented this year in 3D!

Security Snobs

Security Snobs offers High Security Mechanical Locks including door locks, padlocks, cutaways, and more.

Irvine Underground

IrvineUnderground.org is a group of people located in and around Irvine, California [www.liveirvine.com] and the major Orange County area. June 2002 marked the group's first meeting which only five attendees showed up for; since the launch date the word has spread bringing in a much larger crowd.

Pwnie Express

Pwnie Express specializes in bleeding edge pentesting hardware, including the first-to-market commercial pentesting dropbox, the Pwn Plug. A full pentesting suite packed into an inconspicuous microserver, the Pwn Plug uses covert tunnels and 3G/GSM cell service to maintain an encrypted, firewall-busting backdoor into your target network.

University of Advancing Technology

The University of Advancing Technology (UAT), in Tempe, AZ, is a private university for geeks that merges the values of the traditional academy with the modern technology campus, a fusion that enhances our ability to fulfill the mission of educating students in advancing technology who innovate for our future.
UAT creates a distinct, non-exclusionary and geek-friendly university in which students learn to value their own uniqueness and the power of technology in education. UAT is home to over 1,200 on-campus and online students and faculty members, and offers 20 undergraduate degrees and five master's degrees. With the understanding that all students learn differently, our synchronic learning methodology represents an evolution of established practices critical to improving knowledge retention and lifelong learning.
UAT is accredited by The Higher Learning Commission and a Member of the North Central Association (www.ncahlc.org). UAT is also recognized by the National Security Agency and the Department of Homeland Security as a Center of Academic Excellence.

No Starch Press

Founded in 1994, No Starch Press is one of the few remaining independent computer book publishers. We publish the finest in geek entertainment—unique books on technology, with a focus on open source, security, hacking, programming, alternative operating systems, LEGO, science, and math. Our titles have personality, our authors are passionate, and our books tackle topics that people care about. New titles for DEF CON include the second edition of Chris Eagle's IDA PRO BOOK; the first edition of METASPLOIT: A PENETRATION TESTER'S GUIDE; and the second edition of PRACTICAL PACKET ANALYSIS. We'll have a few new Manga Guides as well as several new and quite excellent programming titles.

EFF

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the Internet, fight illegal surveillance, support freedom-enhancing technologies, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows.

SerePick

SerePick provides custom, covert tools for the Urban Professional. From Titanium Entry Toolsets to custom and covert polymer handcuff keys, our tools just might save your life.

SimpleWifi.com

SimpleWiFi.com 9500 NW 12 ST #4 Doral FL 33172 ¬†305-798-8505
Alfa and AirWaveData high power USB adapters, Acces Points (AP), Outdoor AP and CPE Ethernet units, Long Range Booster antennas including Yagi Cantenna, Parabolic grid, Patch, dipole, rubber flex, omni-directional and marine types. LMR-400 and other cables plus all kind of connectors.

John Sundman

John Sundman writes and publishes hacker fiction. His newest book, Creation Science will be available at Defcon, along with his classic novels Acts of the Apostles, Cheap Complex Devices, and The Pains.

UnixSurplus

"Home of the $99 1U Server"
1260 La Avenida St Mountain View, CA 94043
Toll Free: 877-UNIX-123 (877-864-9123)

Bump My Lock

We have the best priced Bump Keys, Bump Hammers and lock picks. This year we have even more types of lock picks and greater quantities. If you did not get your bump hammer over the past 2 years get it here today. FREE TRAINING

Gunnar Optiks

GUNNARs are high-performance advanced computer eyewear optimized for viewing any digital screen. GUNNAR Optiks Advanced Computer Eyewear offers the only technical eyewear solution that optimizes visual performance for anyone who spends long hours viewing computers, PDAs or video games. GUNNAR eyewear is designed to minimize eye strain and visual stress, while improving contrast, comfort, and focus. Developed with visual ergonomics in mind and powered by GUNNAR's i-AMP lens technology, GUNNAR eyewear creates a more comfortable and productive visual experience for the avid computer user.

The Hacker Academy

The Hacker Academy is cloud-based training for beginner, intermediate and advanced information security professionals who want more than just traditional "on-line" or recorded training. As a member of The Hacker Academy you can expect the following:

* New content added every month, guaranteed!
* The best instruction in the industry
* High quality videos, demonstrations, and lectures
* Hands-on labs for each and every module. Easy to use and alldownloadable
* 24/7 availability
* Interaction with instructors
* Timely, real-world threats and learning scenarios
* Modules from known guest instructors

* If you want to read, buy a book. If you want to learn from doing, become a member today

ACLU

The American Civil Liberties Union of Northern California works daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country.
ACLU-NC's Demand Your dotRights Campaign highlights the need for modern privacy protections to match the technology we develop and use. We work with users, technologists, businesses, and lawmakers to update legal and practical protections so that users don't have to choose between taking advantage of new technology and losing control of their personal information.
Please stop by our booth in the vendor area to learn more about our campaign and what you can do to help!

Null Space Labs

Electronic devices for the modern hacker.

GhettoGeeks

well we're back at it again, and have been working hard all year to bring you the freshest awesome that we can. If you have been to defcon, layerone,toorcon, phreaknic, or other conferences we have been at, you definitely know what shenanigans we are up to. If you have never seen us, feel free to come by and take a look at what we have to offer. Always fun, always contemporary, GhettoGeeks has some for the tech enthusiast (or if you prefer, hacker)

TOOOL

"The Open Organisation of Lockpickers will have available a wide selection of tasty lock goodies for both the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! All sales directly benefit TOOOL, a non-profit organization."

DIFRWear

Our mission is to give individuals the ability to maintain privacy and ensure security in a world of insecure contactless devices. To fulfill this mission, we realize that individuals require devices that supersede the default, and often inadequate methods of securing RFID tags. We produce stylish clothing and accessories that block RFID and Near Field Communication (NFC) technologies.

PaulDotCom

PaulDotCom Security weekly is a podcast and online Internet TV show discussing the latest information security news, hacking, and vulnerabilities. We bring on some of the industries finest talent for interviews, feature "Technical Segments" that show people how to do things, and drink beer.

HELP A FRIEND

Q: What can you get a hacker that has it all?!?

A: How about some blood & bone marrow!

Lots of people know Barkode. He is one of the masterminds behind the ever popular, invite only, Ninja Networks Party held every year at DefCon. He codes those fantastic badges we all covet so much each year. He's one of only two "ginger" Goons. You know him, or have seen him, or have enjoyed his free booze, or played games on his free badges. You have been helped by him while he was on shift, wearing his bright red Goon shirt. He gave you a smile, a laugh, a wave. You know him, or you know of him.What you don't know is that he is sick. He needs your help now. He has been diagnosed with a very rare, acquired, blood deficiency disease.

Paroxysmal nocturnal hemoglobinuria (PNH), sometimes referred to as Marchiafava-Micheli syndrome, is a rare, acquired, potentially life-threatening disease of the blood characterised by complement-induced intravascular hemolytic anemia (anemia due to destruction of red blood cells in the bloodstream), red urine (due to the appearance of hemoglobin in the urine) and thrombosis.

This happened very quickly. In a matter of a few weeks, he went from healthy to needing a bone marrow transplant to survive. This disease destroys his red blood cells. It is literally killing him from the inside. The only treatment for it is constant whole blood transfusions until a bone marrow match donor can be found and eventually a bone marrow transplant can be performed.

We as a community have, in the past, come together in amazing ways. It was a community of a few hundred people or less that created and attended the first DefCon. This year we will all attend the 19th year. It was local community members and volunteers that created the first "hackerspace" and now there are hackerspaces worldwide participating in global interactive contests and projects. We, as a community, are a powerful bunch when we care and try and do. And we, as a community, need to care now. Try now. DO NOW.

What you can do:

1. Enter the #BloodKode Challenge! (See contest section for info.) Donate Blood onsite at DEF CON! There will be a blood drive held Friday and Saturday From 10:00 to 19:00 in the main lobby next to registration. There will be signs marking it's location. If they get 300 people to donate for Barkode then Jayson E Street and Geo have agreed to get Mohawks, Saturday at 18:00 at the MohawkCon booth.

Bonus: Donate blood on site and MohawkCon will give you a complimentary Mohawk for free! See their booth for more info.

2. Find your local Red Cross location and give blood. Notify your nurse that you want your blood to be a directed donation, a replacement pint, for Matt Lewis at Kaiser Permanente Hospital in Los Angeles. You'll need to mention his date of birth (11/4/1979). You are not donating your blood directly to him so it doesn't matter what type you are. You are directing a replacement donation to the blood bank at the hospital.

3. Consider becoming a member of a bone marrow match organization. DefCon attendees should be familiar with Be the Match Foundation as they were present in the contest room at DefCon 18 and will be returning to DefCon 19.Go visit them in the contest area, a cheek swab is taken, No pain, Your personal information is private and confidential. You can also request a kit be mailed to you and you can do it at home, all postage paid. But the sooner you register the better.

Keep updated at: http://barkodestatus.tumblr.com/ for more ways you can help.

SCHEDULE

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00 – 10:50	**Welcome and The Making of the Badge** Dark Tangent & LosT	**Operational Use of Offensive Cyber** Christopher Cleary	**TBD** **Mikko Hyponnen**	**Balancing The Pwn Trade Deficit** Anthony Lai, Benson Wu, Jeremy Chiu, & PK	**DEFCON Challenge for Database Geeks** Abstrct
11:00 – 11:50	**The Art and Science of Security Research** Greg Conti	**WTF Happened to the Constitution?** Michael "theprez98" Schearer	**Physical Memory Forensics for Cache** Jamie Butler		**DCFluX in: License to Transmit** Matt Krick "DCFluX"
12:00 – 12:50	**SSL And The Future Of Authenticity** Moxie Marlinspike	**Meet the Federal Agent 2.0** Panel	**From Printer To Pwnd** Deral Heiland	**Sneaky PDF** Mahmud Ab Rahman	**Staying Connected during a Revolution or Disaster** Thomas Wilhelm
13:00 – 13:50	**Black Ops of TCP/IP 2011** Dan Kaminsky	**Net Neutrality Panel**	**I'm Your MAC(b) Daddy** Grayson Lenik	**Three Generations of DoS Attacks** Sam Bowne	**Insecurity** Marc Weber Tobias, Matt Fiddler & Tobias Bluzmanis
14:00 – 14:50	**Dust: Your Feed RSS Belongs To You!** Chema Alonso & Juan Garrido	**Former Keynotes - The Future** Panel	**What Time Are You Anyway?** Michael Robinson	**Jugaad – Linux Thread Injection Kit** Aseem "@" Jakhar	**Why Airport Security Can't Be Done FAST** Semon Rezchikov, Morgan Wang & Joshua Engelman
15:00 – 15:50	**And That's How I Lost My Eye** Shane Lawson, Bruce Potter, Deviant Ollam	**Malware Freak Show 3** Nicholas J. Percoco & Jibran Ilyas	**Covert Post-Exploitation Forensics With Metasploit** Wesley McGrew	**Runtime Process Insemination** Shawn Webb	**Hacking Your Victims Over Power Lines** Dave Kennedy (ReL1K)
16:00 – 16:50		**Ask EFF: The Year in Digital Civil Liberties** Panel	**Mamma Don't Let Your Babies** Patrick Engebretson & Dr. Josh Pauli	**Familiarity Breeds Contempt** Sandy "Mouse" Clark & Brad "RenderMan" Haines	**Key Impressioning** Jos Weyers
17:00 – 17:20		**Represent! Defcon Groups, Hackerspaces, and You.** Panel	**Are You In Yet?** Shrdlu	**UPnP Mapping** Daniel Garcia	**The Art of Trolling** Matt 'openfly' Joyce
17:30 – 17:50			**Gone in 60 Minutes** Andrew Gavin	**Kernel Exploitation** Kees Cook	
18:00 – 18:50		**Is it 0-day or 0-care?** PanelW	**Bosses love Excel, Hackers too.** Chema Alonso & Juan Garrido	**Owned Over Amateur Radio** Dan Rosenberg	**IP4 TRUTH** Sterling Archer & Freaksworth
19:00 – 19:50			**We owe it all to the Hackers** Steven Levy		

TOP SECRET

Saturday August 6th. 2011

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00 – 10:50	**Hacking and Securing DB2 LUW Databases** Alexander Kornbrust	**"Whoever Fights Monsters..." Paul Roberts, Aaron Barr, Joshua Corman, Jericho**	**Don't Drop the SOAP** Tom Eston, Josh Abraham & Kevin Johnson	**Assessing Civilian Willingness to Participate in On-Line Conflict** Thomas J. Holt & Max Kilger	**Safe to Armed in Seconds: A Study of Epic Fails of Popular Gun Safes** Deviant Ollam
11:00 – 11:50	**Battery Firmware Hacking** Charlie Miller	**Chip & PIN is Definitely Broken** Andrea Barisani, Adam Laurie, Zac Franken, Daniele Bianco	**Smartfuzzing The Web: Carpe Vestra Foramina** Nathan Hamiel, Gregory Fleischer, Justin Engler & Seth Law	**Traps of Gold** Andrew Wilson & Michael Brooks	**DIY Non-Destructive Entry** Schuyler Towne
12:00 – 12:50	**Hacking and Forensicating an Oracle Database Server** David Litchfield	**Security When Nano Seconds Count** James "Myrcurial" Arlen	**Federation and Empire** Emmanuel Bouillon	**Hacking Google Chrome OS** Kyle 'Kos' Osborn & Matt Johanson	**Attacking and Defending the Smart Grid** Justin Searle
13:00 – 13:50	**Weaponizing Cyber psychology** Chris Sumner, alien, Alison B	**DEF CON Comedy Jam IV** Panel	**Web Application Analysis With Owasp Hatkit** Martin Holst Swende & Patrik Karlsson	**Hacking .Net Applications: The Black Arts** Jon McCoy	**Vulns of Wireless Water Meter Networks** John McNabb
14:00 – 14:50	**Archive Team** **Jason Scott**		**Bulletproofing The Cloud: Are We Any Closer To Security?** Ramon Gomez	**"Get Off of My Cloud"** Ben Feinstein & Jeff Jarmoc	**Staring into the Abyss** Richard Thieme
15:00 – 15:50	**DEF CON Awards**	**Economics of Password Cracking in the GPU Era** Robert "Hackajar" Imhoff-Dousharm	**Abusing HTML5** Ming Chow	**Metasploit vSploit Modules** Marcus J. Carey , David Rude and Will Vandevanter	**Smile for the Grenade! "Camera Go Bang!"** Vlad Gostom & Joshua Marpet
16:00 – 16:50		**PCI 2.0** Panel	**Getting F***** On the River** Gus Fritschie & Mike Wright	**Sounds Like Botnet** Itzik Kotler & Iftach Ian Amit	**An Insider's Look at International Cyber Security Threats and Trends** Rick Howard
17:00 – 17:20		**My password is: #FullOfFail!** **Jason M. Pittman**	**Network Security Podcast Meetup**	**VoIP Hopping the Hotel: Attacking the Crown Jewels through VoIP** Jason Ostrom	**Strategic Cyber Security: An Evaluation of Nation-State Cyber Attack Mitigation Strategies** Kenneth Geers
17:30 – 17:50		**Brute Forcing (IVR) Systems** Harish Skanda Sureddy			
18:00 - 18:20		**Vanquishing Voyeurs: Zoz & Andrea Bianchi**	**Big Brother on the Big Screen: Fact/Fiction?** Nicole Ozer	**Fingerbank** Olivier Bilodeau	**Phishing and Online Scam in China** Joey Zhu
18:30 - 18:50				**Pillaging DVCS Repos For Fun And Profit** Adam Baldwin	**Handicapping the US Supreme Court Foofus**
19:00 - 19:50				**This is REALLY not the droid you're looking for...** Nicholas J. Percoco & Sean Schulte	

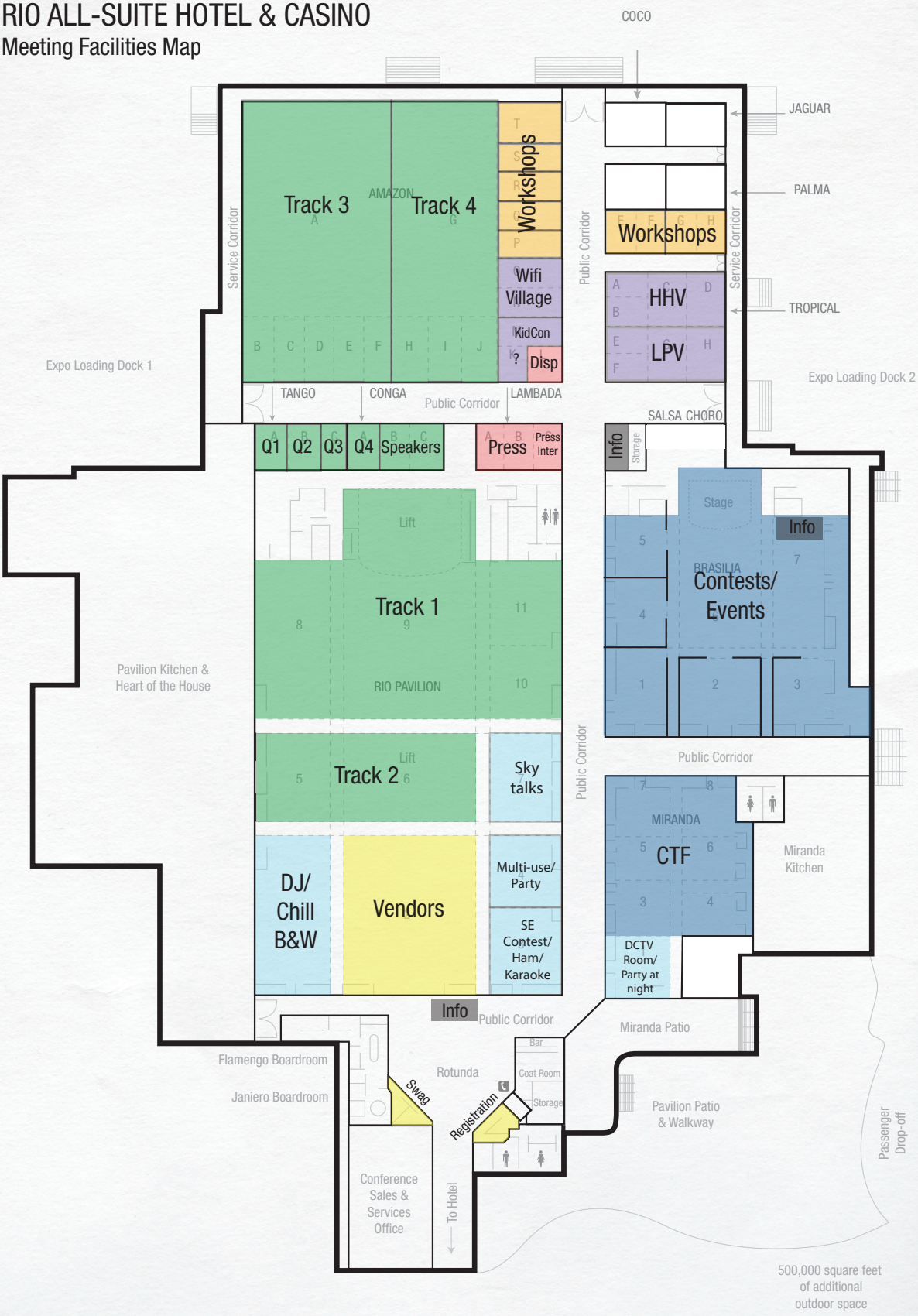
SCHEDULE

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00 – 10:50	**Earth vs. The Giant Spider** Rob Havelt & Wendel Guglielmetti Henrique	**Whitfield Diffie & Moxie Marlinspike**	**PIG: Finding Truffles Without Leaving A Trace** Ryan Linn	**Cellular Privacy: A Forensic Analysis of Android Network Traffic** Eric Fulton	**Look At What My Car Can Do** Tyler Cohen
11:00 – 11:50	**Lives On The Line: Securing Crisis Maps In Libya, Sudan, And Pakistan** George Chamales	**PacketFence, The Open Source Nac: What We've Done In The Last Two Years** Olivier Bilodeau	**Port Scanning Without Sending Packets** Gregory Pickett	**Seven Ways to Hang Yourself with Google Android** Yekaterina Tsipenyuk O'Neil & Erika Chin	**Internet Kiosk Terminals : The Redux** Paul Craig
12:00 – 12:50	**We're (The Government) Here To Help: A Look At How FIPS 140 Helps (And Hurts) Security** Joey Maresca	**A Bridge Too Far: Defeating Wired 802.1x with a Transparent Bridge Using Linux** Alva 'Skip' Duckwall	**Cipherspaces/ Darknets: An Overview Of Attack Strategies** Adrian Crenshaw "Irongeek"	**Getting SSLizzard** Nicholas J. Percoco & Paul Kehrer	**Build your own Synthetic Aperture Radar** Michael Scarito
13:00 – 13:20	**How To Get Your Message Out When Your Government Turns Off The Internet** Bruce Sutherland		**Taking Your Ball And Going Home** Phil Cryer	**Mobile App Moolah: Profit taking with Mobile Malware** Jimmy Shah	**Blinkie Lights: Network Monitoring with Arduino** Steve Ocepek
13:30 – 13:50			**Steganography and Cryptography 101** eskimo		
14:00 – 14:20	**The Future of Cybertravel: Legal Implications of the Evasion of Geolocation** Marketa Trimble	**Network Application Firewalls vs. Contemporary Threats** Brad Woodberg	**Pervasive Cloaking** William Manning	**Hacking the Global Economy with GPUs Skunkworks**	**Kinectasploit: Metasploit Meets Kinect** Jeff Bryner
14:30 – 14:50			**Tracking the Trackers: Brian Kennish**	**Beat to 1337** Mike Arpaia & Ted Reed	**How Haunters Void Warranties** Reeves Smith
15:00 – 15:50	**I Am Not a Doctor but I Play One on Your Network** Tim Elrod & Stefan Morris	**Bit-squatting: DNS Hijacking Without Exploitation** Artem Dinaburg	**Speaking with Cryptographic Oracles** Daniel Crowley	**Deceptive Hacking: Bruce "Grymoire" Barnett**	**Don't Fix It In Software** Katy Levinson
16:00 – 16:50		**Network Nightmare: Ruling The Nightlife Between Shutdown And Boot With Pxesploit** Matt "scriptjunkie" Weeks	**VDLDS — All Your Voice Are Belong To Us** Ganesh Devarajan & Don LeBert	**Introduction to Tamper Evident Devices** datagram	**Wireless Aerial Surveillance Platform** Mike Tassey & Rich Perkins
17:00 – 17:50		**Building The DEF CON Network** David M. N. Bryan & Luiz Eduardo	**Virtualization under attack: Breaking out of KVM** Nelson Elhage	**Hacking MMORPGs for Fun and Mostly Profit** Josh Phillips	**SCADA & PLCs in Correctional Facilities: The Nightmare Before Christmas** Panel
18:00 – 18:50				**Steal Everything, Kill Everyone, Cause Total Financial Ruin!** Jayson E. Street	
19:00 – 19:50	**Awards Ceremonies Hosted By Dark Tangent in Track 1**				

TOP SECRET

RIO ALL-SUITE HOTEL & CASINO

Meeting Facilities Map



NOTES

NOTES

NOTES

NOTES

NOTES

THANK YOU THANK YOU THANK YOU

I would like to thank not only the team that has made DEF CON 19 possible here, but those who have worked all year long to make it possible but for whatever reasons could not be here to enjoy their hard work. To Neil, Nikita, Charel, Zac, LOsT for all the late night work and ideas, Black Beetle, McNamara, Noid, Dan, Ira, cotman, Converge, Will, Kive, L3d.Thank you to everyone listed below, I will not steal the thunder from the teams thanking their members, but instead reinforce them!

And until next year, our 20th anniversary, thank you for supporting DEF CON with your participation, ideas, and energy. See you on https://forum.defcon.org/ for the post game wrap up! -The Dark Tangent

Zac would like to thank: Agent X, Proctor, Major, Eta, FAWCR, Melloman, Roamer, Wad, Doollittle, N0ise, Great Scott, TW, Tyler, Tebrink, Dodger, Charel, Jeff, Nico, Dead Addict, Lockheed, Heather, Videoman, Noid, Pappy, Flea, Arclight, CJ, Evil, SunSh1ne, Verrus, Q, Pyro, Hackajar, LosT, Waz, Vertigo, SheenaR, Preist, Neil, Nikita, Nicole, Kampf, The Uncles: Drew, Jerry, Tony, Vinnie & Trev. Barkode, chin up & get well soon! And most importantly the Defcon Humans, try not to kill anyone guys.

TW and Tyler would like to thank everyone for their hard work in making registration run perfectly. A BIG thanks to Cstone, Crackerjack, Zayne, Matt, 6Q, Aaron, Soua, and Queen.

QM Stores is brought to you by Uncle Ira, Uncle Ira's big-ass truck, ETA, RijilV, Alien, Dodger, Merlin, Major Malfunction, Caffeine, Willpower and Sleep Deprivation. Materials provided to CTF are strictly for rectal use only.

SunSh1ne and Veruus thank the swag crew for all they do: Adam, Fox, GateKeeper, Michelle and Xao.

Roamer thanks the Vendor staff: Wad, AlxRogan, Evil, Redbeard and Latenite. The Goon Band: GM1, vertig0, Doc, and Rich. Wiseacre for his help with the Vendor Diagram. The DC19 Vendors and Joseph Parkes from the Rio.

Got a question? The Information Booth has the answer. Whether or not you like the answer is up to you. But feel free to ask the awesome staff of FAWCR, Melloman, Littlebruzer, Medic, Jenn, Erik, Lipgloss, ACR0NYM, Sweep, Flower, Zookeeper, Littleroo, spottedcoin, Sanchez, Jaffo, Leila T., algorythm, or Puck. The answer is not always 42.

Dispatch wishes to thank the following for another loyal year on the air waves: Doollittle, Jurist, Voltage Spike, Rf, Chuck, Lisa, Aya

Shouts-out to the NOC staff who keep things running every year: Lockheed, Heather, Videoman, effffn, Enki, Mac, Sparky, and DJ t3ase.

Neil thanks Mar, Steve Andrus, y3t1, and Ellen for spectacular artwork. Ping, for all the support and making it all happen! LosT, Charel and Lockheed for all the help! Joseph, Chris and Ryan from the Rio. DT, for letting me do this, as my job! Nikita, I couldn't do it without you.

Nikita would like to thank all the speakers and goons. A special thanks to Neil, Kamph, Highwiz, Dakahuna, Eris, and the others whom don't get thanked enough. PNH and Lukemia can SUCK IT, so thank you everyone who is helping Barkode and Mrs.Gattaca by giving blood or registering for bone marrow donation, if you haven't yet go now!

BIG UPS to the goon entertainment staff Zziks & Krisz Klink; our decor crew Zebbler, Kate & Jacob; our VJs Kevin+co@Design Flaw; our sound guy Mobius; Lock+NOC; Xodia; QM-goons; Charel!; DT!; Neil!; and of course, all of the performers; and any angry SOs, for their support, dedication, and willingness to function on very little sleep for the love of the con!

Pyr0 and his Goons would like to thank all the Contest & Events Leaders for all of their hard work and dedication. Charel for her endless patience and persistence. Neil & Nikita (and youngin') for months of preparation during what has to be the busy time of both of your lives. Zac for his ability to herd cats (and hackers) like no other. The Security Goons for babysitting 10,000 hackers. TheCotMan for his meticulous admin'ing of the DC-Forums, and everyone else that helps make DEF CON happen. Pyr0 would like to personally thank Russr for everything he has done for DEF CON C&E over the last 10 years. Dark Tangent for everything that is DEF CON, including giving all of us a home once a year were we can have our "family reunion". Finally, Rob Bird for his patience putting up with Pyr0 and all of the DEF CON prep during a massive product launch. Shout Outs to: 303 - Security Tribe - DENHAC - Hektik - 23.org - Phenolit - and all the rest of our friends and family.