DEFCON 22 2014 Conference Report

Steve Holden (aka "Otto Locke") | TechNewsRadio.com | technewsradio@gmail.com

Administrivia:

- This is my personal report from DEFCON 22 held August 8-10, 2014 in Las Vegas, NV.
- Opinions are my own. I made every effort to make as accurate notes as possible.
- Presentations that I attended in person are marked with a +
- Presentations that I attempted to attend but were full are marked with a o
- There may be more information available at: www.defcon.org & media.defcon.org
- If you want a copy of any of the slides then please let me know.
- At the end of the report there are a bunch of links to BLACKHAT and DEFCON news.

== Day 1 ==

Domain Name Problems and Solutions [Paul Vixie]

- No slides (couple of white paper/articles on CDROM)
- https://twitter.com/paulvixie
- Focus simple SAV (source-address validation)
- DNS poisoning/DDoS threats is a widespread problem
- Reflection attacks are hard to measure based on watching performance on the DNS service device

+ Oracle Data Redaction is Broken (David Litchfield]

- Good intro on SQL Injectable History (SQL, ODBC, Informix, DB2, etc)
- Oracle says their products are unbreakable
- There are a lot of known issues with password management
- Patches from Oracle are not very responsive nor is there a lot of public info on what is fixed and what isn't fixed (good graphic on how they patch - now quarterly)
- Twitter: https://twitter.com/dlitchfield
- At one point their database validation strategy was that all validation was done by the web application server and not within the database. They have changed this but there are two attack vectors - web and then SQL injection
- Good graphic on Microsoft SQL Server Patches (2002 was the worst year) … but now they have a very good track record
- The bugs that David has found should/could/would be found by standard vulnerability and robust security testing.
- What is Oracle Data Redaction: mark sensitive data (Oracle 11/12)
- It can fail though in simple bypass attacks / demos
- SYS.DBMS.REDACT.ADD_POLICY
- demo: data is clear, policy applied, login with standard user, can't see the data, then stand user does XML query on the same data and sees the data
- Trivial example

Meddle Framework for piggy-back fuzzing and tool development [Geoff McDonald]

- Slides are on the CDROM
- Website: http://www.split-code.com/
- Email: glmcdona@gmail.com
- Good overview of fuzzing targets (docs, processes, etc), algorithms/process, and tools
- Tool review: https://github.com/glmcdona/meddle
- Detailed demos

Steganography in Commonly Used HF Radio Protocols [Paul Drapeau & Brent Dukes]

- Slides are on the CDROM
- TWITTER: @pdogg77 @TheDukeZip
- Doing this violates FCC regulations
- Uses commercially available hardware/software
- Why: Enables communication where there is censorship/spying
- Where to hide: protocols, timing, etc.
- Many details on protocol options and research on which ones were better than others.

- They also worked on encrypting the steganography info (but they are not encryption experts)
- They also did some analysis of their injected steganography
- Examples & Source Code links

+ Measuring the IQ of your Threat Intelligence feeds [Alex Pinto & Kyle Maxwell]
- @alexcpsec, @mlsecproject, @kylemaxwell
- No slides
- Basics: What am I able to do? What is my intent against you? [Foes - Viking Style]
- How do you measure this? We look a lot of what they can do but not what they are doing.
- Differences: Signatures vs. Indicators; Data vs. Intelligence, Tactical vs Strategic, Atomic vs. Composite
- It is easy to focus on IP addresses, Domain Names but it gets harder to see Network, Host Artifacts, Tools, and Tactics, Techniques and Procedures (TTP)
- Dig deep on IP address: easy to change, there is a cost in changing though, there maybe pattern (souce code http://github.com/mlsecproject/tiq-test) [Good demo - IP number drives asnumber, asname, country, rhost]
- Maps are not a good way to see TI data from a analysis perspective
- Good demos on what p.values give you when looking at increasing and decreasing data sets
- Tool review COMBINE: on get on gethub [captures the data and converts the data into the right data formats]

Abuse of Blind Automation in Security Tools [Eric (XlogicX) Davisson & Ruben Alejandro (chap0)]
- Slides are available
- A couple of good examples of how to make barcodes and QR codes do non-anticipated stuff
- A couple of examples of taking very small files to make very big data sets because of bad configuration of files 17K file to 17-MBs, etc.
- Two demos showing how you can do similar "messing" with AV, firewall, and IDS systems.
- URLs are also something that can be messed with a lot depending on the server/service technologies
- Twitter: https://twitter.com/XlogicX
- https://twitter.com/_chap0

USB for all! [Jesse Michael & Mickey Shkat]
- Slides are available on CDROM

o The NSA Playset: RF Retroreflectors [Michael Ossmann]
- Slides are available on CDROM
- Slides contain copies of classified documents released on the Internet by Snowden
- Interesting review of what is out there and what the threats are
- Outlines open source / current penetration testing tools can do very similar things
- Presentation has links to more info / consolidate references
- PRESENTER: https://twitter.com/michaelossmann

We Wrapped Samba So You Don't Have To [Lucas Morris & Michael McAtees]
- Slides are available on CDROM

The $env:PATH less Traveled is Full of Easy Privilege Escalation Vulns [Christopher Campbell]
- Slides are on CDROM

Hacking US (and UK, Australia, France, etc.) traffic control systems [Cesar Cerrudo]
- Slides are on CDROM

Detecting and Defending Against a Surveillance State [Robert Rowley]
- Slides are on CDROM

+ Bypass firewalls, application whitelists, secure remote desktops under 20 seconds [Zoltán Balázs]
- Slides are on the CDROM
- Background [root@bt:~# whoami]

- Remote RDP connection scenario [not on the Internet, two factor, no drive mapping, firewall only allows RDP, RDP server as whitelisting] {pretty challenging}
- Good review of what a RED TEAM person could do and then a BLUE TEAM person could do
- Need to get: malware on RDP server, execute the malware, etc.
- Tool review: User Keyboard Event Capture that works with Word (sends ASCII payload and then turn the payload into Binary for execution)
- You can also use this method to accept dialog boxes from AV.
- Applocker Bypass Options: Microsoft documentation tells you how
- With Microsoft Office you can run shell code (examples) however how to do you get out through the super controlled firewall.
- Good example from Lord of the Rings (fish in the barrels)
- There is a framework (WinDivert) for getting a trusted kernel driver
- Good demos
- Links to tools in slides

Investigating PowerShell Attacks [Ryan Kazanciyan & Matt Hastings]
- Draft slides are on the CDROM
- Authors are from Madiant (https://twitter.com/ryankaz42 & @HastingsVT)
- Review of current PowerShell (PS) capabilities and current exploit tools
- There is actually several malware examples
- They researched these malware examples to find out how you can learn more about what these tools are doing and what forensic evidence exists on a compromised system.
- The event logs have a lot of good info of what PS stuff is going on when it is going on (but there are still gaps) [there are some 3rd party apps that help fill the gap] {there are some big logging differences between PS 2.0 and PS 3.0}
- Several demos of: local shell, remote shell, and post exploit
- Other examples to look at for finding evidence: file system, registry

What the Watchers See: Eavesdropping on Municipal Mesh Cameras for Giggles (or Pure Evil) [Dustin Hoffman & Thomas (TK) Kinsey]
- No slides available
- More info: https://khanfu.com/event/38/2610

+Extreme Privilege Escalation On Windows 8/UEFI System [Corey Kallenberg & Xeno Kovah]
- Slides are on the CDROM
- TWITTER: @coreykal, @xenokovah, @jwbutterworth3, @ssc0rnwell
- You can get to RING 3 on Windows (Admin) to RING 0 (full control - SYSTEM, BIOS, FIRMWARE, etc)
- Talk is about going from RING 3 to UEFI (firmware) then make your way back up the rings to 3 from the lower rings
- More info: http://en.wikipedia.org/wiki/Ring_0
- Review of new Windows 8 API / Variables for UEFI
- Review of the open source UEFI code and find the intersection between this code and the APIs from Microsoft
- Review of vulnerabilities that they found
- Review of tools they built
- Demo of the exploit and then a review of what their "watcher" system can do from the firmware level
- The infect the system from Windows and then they show how it is still capable running Linux
- It can inject by seeing things that get into memory (scan for "magic" controller software)
- Demo of the Watcher and then a BIOS kill example (via PING packets)

Client-Side HTTP Cookie Security: Attack and Defense [David Wyde]
- Slides are on CDROM

Am I Being Spied On? Low-tech Ways Of Detecting High-tech Surveillance [Dr. Phil Polstra]
- @ppolstra
- What to look for if you think someone is tracking/looking in/etc on you

- There are many threats (not just a foil hat issue)
- Review on how to detect low light cameras and IR cameras
- Wireless cameras can be found via their comms channels
- There are some mobile apps that can help. You also build a dedicated wifi collection and analysis system (there are also expensive options - some are reviewed in the presentation)
- If you are being tailed or surveyed you need to know a little bit about tactics and watch for patterns
- Audio recording device identification and analysis of pros & cons
- http://beagleboard.org/bone

Saving Cyberspace by Reinventing File Sharing [Eijah]
- Slides are on the CDROM

Veil-Pillage: Post Exploitation 2.0 [Will Schroeder]
- Slides are on the CDROM

An Introduction to Backdooring Operating Systems for Fun and Trolling [Nemus]
- Slides are on the CDROM

Practical Aerial Hacking & Surveillance [Glenn Wilkinson]
- Penetration tester (@glennzw)
- Requirements: high flying, inexpensive, low noise, low visibility, speed, fly pretty far, sensor (video, telemetry, data interception), autonomous flight
- Platform: fixed wing or 'helicopter', camera, gps [size, distance, etc]
- Slides are available on CDROM (but many more slides were in the live brief]
- Flight Controllers (many options, tend to be open source)
- http://www.dronedeploy.com
- Snoopy tool: review, linux savvy, wifi analysis (mac address, name, wigle.net (war driving database))
- RF tools: WIFI, bluetooth, NFC, etc.
- DEMO: Data is visualized in Maltego (Interesting scenario, combo of drones and land based assets and then finds one device at airport, hotel, park)

The Open Crypto Audit Project [Kenneth White & Matthew Green]
- No slides
- POC: https://twitter.com/kennwhite
- More info: https://twitter.com/OpenCryptoAudit

Acquire current user hashes without admin privileges [Anton Sapozhnikov]
- Slides are on CDROM
- POC: https://twitter.com/snowytoxa

Blinding The Surveillance State [Christopher Soghoian]
- No slides
- POC: https://twitter.com/csoghoian

Dark Mail [Ladar Levison & Stephen Watt]
- No slides
- POCs: https://twitter.com/kingladar

Case Studies in Insider Threat [Tess Schrodinger]
- History of traitors, terrorists, etc. [defectors]
- Industrial espionage - two competitors
- Economic espionage - nation states
- SPY, TRAITOR, INSIDER THREATS
- Insider Threat - not always malicious (human error)
- HoneyPot (technical and sexual)

- Sharon Marie Scranage (coup in Ghana, CIA employee, no big issues, seduced in Ghana and then bleed her for info) [Ghana shared the information with many people]
- Several other examples presented in the presentation
- List of other research to look at:
    - Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall -- Eric D. Shaw, Ph.D. and Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology
    - Could A Brain Scan Protect U.S. Troops from Insider Attacks - Patrick Tucker (research Derrell Small - Veritas Scientific)
    - Insider Threat Control: Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time by Todd Lewellen, George J. Silowash, Daniel Costa
- What can you do? - organizational factors (examine), support security, monitoring, education, screening, exit process

Where is the ROP suppose to go? [David Dorsey]
- Slides are on the CDROM

The Secret Life of Krbtgt [Christopher Campbell]
- Slides are on the CDROM

== DAY 2 ==

The Cavalry Year[0] & a Path Forward for Public Safety [Joshua Corman & Nicholas J Percoco]
- Slides are on the CDROM

Hack All The Things: 20 Devices in 45 Minutes [CJ Heres, Amir Etemadieh, Mike Baker, & Hans Nielsen]
- Slides are available on CDROM

Hacking 911: Adventures in Disruption, Destruction, and Death [Christian "quaddi" Dameff, Jeff "r3plicant" Tully & Peter Hefley]
- Slides are available on CDROM

+ Mass Scanning the Internet: Tips, Tricks, Results [Robert Graham, Paul McMillan, & Dan Tentler]
- bin/masscan 0.0.0.0/0 -p443 > watch the scan start on the 4 billion addresses
- reasons to scan: find vulnerabilities, survey, find systems to be patched [deepnet]
- On a 1-Gbps link they see max rate of 500-Mbps coming back (small packet issues)
- There are billing issues … you can get relatively good performance by using multiple VPS at lower rates 150-kpps (packets per second) … and there are ISP complaint issues (fail2bian, snort rules, risk lose peering relationships)
- The tool supports exclude list (but people who get on the list don't want the list published)
- the tool is about 1000 times faster than nmap
- POCs: https://twitter.com/Viss; @ErrataRob
- This tool can be used Load Testing on Firewalls (lots of other things can fall over with this)
- Recommend output to binary and then convert to xml when you need to use the data (saves space)
- Demo: T-Mobile phones have a firewall that stops all the network. You might be able to use Verizon/AT&T but Clear works with a SPOOF SCAN (use the phone to start the scan but use an ISP to actually send the packets)
- Demo: Scanning for VNC (find 100s of no password systems)
- Demo: Heartbleed Vulnerability (NAS devices, cameras, LaCie drives, secure.xxx, honeypots, mainframes
- Demo: http://results.survey.tx.ai [results from a full scan ~3 hours using 300 cloud workers at $0.16 an hour]
- Demo: Scanning 23.0.0.0 is good as it includes a lot of publically available services (aka Amazon, Akami, etc) that don't usually complain

Screw Becoming A Pentester When I Grow Up I Want To Be A Bug Bounty Hunter! [Jake Kouns & Carsten Eiram]
- Slide is available on CDROM

Don't Fuck it Up! [Zoz]
- Slide is available on CDROM

+I Hunt TR-069 Admins: Pwning ISPs Like a Boss [Shahar Tal]
- POC: https://twitter.com/jifa
- Why do you care about TR-069? From the Broadband forum - CPE WAN Mgmt Protocol (specification, many iterations)
- Slides are on the CDROM
- Good summary in the slides on how the SOAP RPC/XML over HTTP is suppose to work between ROUTER and CLIENT (computer, storage, etc)
- List of who have active TR-069 deployed -- 147 million devices online today (there is default open port 7547 related to this protocol)
- What it can do for you? zero-touch config, troubleshooting, upgrade firmware, diagnostics, etc. [A LOT OF POWER IS HERE]
- Review of his router and how TR-069 was hidden by HTML (no way to turn it off)
- Slides also include a detailed ACS CWMP deployment (and this control device is on public internet and controls 1000s of system -- aka all of COMCAST, all of COX, etc)
- If you were a bad ACS: get private data (SSID, MAC address, VOIP, etc), set every parameter (DNS, WIFI, PPP, etc), change firmware
- DEMO: 81% of all ACS scanned were only running HTTP … and completely vulnerable to known threats and capabilities
- DEMO: Review of known ACS source code; found serious problems that let you get to root
- REVIEW: Of two penetration testing success reports on deployed ACS systems (in one situation they ended up owning 500,000 devices)
- What can you do? Audit your own system? Put another router/firewall between you and your provider. Update your router to an open source version? Ask your provider what they are doing.

+ Summary of Attacks Against BIOS and Secure Boot [Yuriy Bulygin, Oleksandr Bazhaniuk , Andrew Furtak & John Loucaides]
- No slides
- History of BIOS to UEFI (icons, colors, etc)
- Good place to start is SPI Flash Write Protection (SMM protection mechanism)
- TOOLS: Intel Security has a tool and MITRE has a tool
- More info: http://www.intelsecurity.com/
- A lot of details on SMM, Secure Boot, etc > all have know attack vectors
- Demo of forensic analysis of SECURE BOOT on and compared with SECURE BOOT off -- found where the variable is stored and can be changed via RING 3
- Secure Boot has an image verification policies -- same attack vector as going around SECURE BOOT … this allows you to boot with whatever you want.
- UEFI does allow compatibility mode where legacy CMS/OS can be supported. This is bad because CMS (easily hackable) can then attack UEFI at the same level.
- There maybe another attack vector where UEFI sees and error, you then say try again, then try again, and then try again (3 times) and then it goes ahead and runs the "error" image

Logging ALL THE THINGS Without All The Cost With Open Source Big Data Tools </buzzwords> [Zack Fasel]
- No slides
- POC: https://twitter.com/zfasel

Cyberhijacking Airplanes: Truth or Fiction? [Dr. Phil Polstra & Captain Polly]
- Slides are on the CDROM

Don't DDoS Me Bro: Practical DDoS Defense [Blake Self & Shawn "cisc0ninja" Burrell]
- Slides are on the CDROM

How to Disclose an Exploit Without Getting in Trouble [Jim Denaro & Tod Beardsley]
- Slides are on the CDROM

+ Secure Random by Default [Dan Kaminsky] {2 hours}
- 15 years of DEFCON - Wow!
- Hard drives are actually mini-computer: serial port (shell, documentation, edit memory, hidden system ports, test output) HDPARN - extremely dangerous - no password to update firmware) - whitepaper with Travis Goodspeed
- S^X (storage XOR execution): there is a ton of places to persistent / keep access / it needs to be part of a discussion (what about your Cloud?)
- Free Internet - big challenge that we know how it works (everything can be broken but can it all be fixed?)
- Random Number Generator: Web Frameworks on serious sites might have 7 password a second | @reversity has a WPS Attack (no entropy but a high 128 bits for encryption - when you key is 32 bits (you can try them all) or you could just use all ZEROs) | need to improve on this
- Dan is working to bring RANDOM to the right library for all the popular languages, systems, services (Liburandy)
- Working on Ryan Castellucci on Story v0.1 - building an encoding option for taking words and building unique (hash) values [enables better password]
- Passphrase (stories, bits on a drive, etc) need to be better - 80 bits is better than 24 bits but remembering 80 bits is nearly impossible (but what about 8 bits from the whole hash) {local stretching}
- Browser 0day: IE still getting tons of attacks (more than Java) in 2013. IE is really COM built into Windows - security was never really considered. All the other browsers have many of the same issues. Google is working on solving this via Type Head. Microsoft is working on Nondeterministic Freeing. There is an option with 64-bit browsers may be able to do something called Iron Heap that never lets memory to be reused.
- DDoS is big again -- 114 >100GB floods in 2014 so far. They are using DNS, NTTP, source addresses, filling stuff up (very damaging) | there is some options BCP38/URPF (not great as you need very high implementation on all networks) | another options is Stochastic Tracing (GRE stream)
- NSA commentary
- More info: http://www.whiteops.com/, http://dankaminsky.com/,

PropLANE: Kind of keeping the NSA from watching you pee [Rob Bathurst, Russ Rogers, Mark Carey, & Ryan Clarke]
- Slides are on the CDROM

Secure Because Math: A Deep Dive On Machine Learning-Based Monitoring [Alex Pinto]
- Slides are not available

NinjaTV - Increasing Your Smart TV's IQ Without Bricking It [Felix Leder]
- Slides are on the CDROM

How Man-In-The-Middle Attacks can help you Evade Monitoring [Ryan Lackey, Marc Rogers, & theGrugq]
- Slides are not available

The Monkey in the Middle: A pentesters guide to playing in traffic. [Anch (MIKE GUTHRIE)]
- Slides are on the CDROM

Advanced Red Teaming: All Your Badges Are Belong To Us [Eric Smith & Josh Perrymon]
- Slides are not not on CDROM but posted to http://www.scribd.com/doc/236525173/DefCon22-All-Your-Badges-Are-Belong-To-Us#download
- POC: https://twitter.com/packetfocus https://twitter.com/infosecmafia

A Survey of Remote Automotive Attack Surfaces [Charlie Miller & Chris Valasek]
- Slides are not available
- POC: https://twitter.com/0xcharlie https://twitter.com/nudehaberdasher
- There is a white paper (slides are very large and probably won't be released)
- The articles on this topic are usually very bad / full of errors
- Goal is to execute code on the car that causes a crash? There are examples of this.

- Review of attack surface: starter/key, tire pressure sensor, remote sensor to open/start car, Bluetooth (!), Radio Data System, Telematics/Cellular/WIFI (!), Internet/Apps (!)
- Cyber Physical: self-parking, lane keep, collision avoidance, etc
- Patching of cars is going to be a big problem
- Demo: Mini-hardware board with attacks inserted into system but then they build a small IPS (intrusion protection system)
- Demo: Jailbreak with Chrysler, Dodge, Ram, Fiat, SRT, Jeep [swapping out of the USB - got caught but after reboot you can put your own USB stick]

Impostor — Polluting Tor Metadata [Charlie Vedaa & Mike Larsen]
- Slides are on the CDROM

VoIP Wars: Attack of the Cisco Phones [Fatih Ozavci]
- Slides are on the CDROM

Detecting Bluetooth Surveillance Systems [Grant Bugher]
- Slides are on the CDROM

Check Your Fingerprints: Cloning the Strong Set [Richard Klafter (Free) & Eric Swanson (Lachesis)]
- Slides are on the CDROM

Manna from Heaven: Improving the state of wireless rogue AP attacks [Dominic White & Ian de Villiers]
- Slides are on the CDROM

+ Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment [Jesus Molina]
- @verifythentrust
- Slides are on the CDROM
- Home automation "abuse" with 200 room home with a 5 star hotel (Starwood in China) -- all rooms have an iPad to control the room and it was connected to the open network at the WIFI … the automation was suppose to be secure but it was not.
- UDP port was used by the iPads and was part of the KNX standard (widespread in Europe and China) - started in 1990
- There are open source clients that allowed for reverse analysis to understand what it does. There is a spec update in 2013 that does have security but you need to pay for the documentation
- There is source code available (tunnel request)
- Hotels just need to be aware of this. The Internet of Things (IoT) is something that is "COOL" but it has some problems

Abusing Software Defined Networks [Gregory Pickett]
- Slides are on the CDROM

Touring the Darkside of the Internet. An Introduction to Tor, Darknets, and Bitcoin [Metacortex & Grifter]
- Slides are on the CDROM

Raspberry MoCA - A recipe for compromise [Andrew Hunt]
- Slides are on the CDROM

Attacking the Internet of Things using Time [Paul McMillan]
- Slides are on the CDROM

+ Getting Windows to Play with Itself: A Hacker's Guide to Windows API Abuse [Brady Bloxham]
- POC: @silentbreaksec & www.silentbreaksecurity.com
- Focus: Not all focused on Metasploit, and add more tools to the mix
- DLL Injection (Black Box): 3 out of 4 are not documented / Code Cave on non-64-bit OSes

- New research: AddMonitor() that is part of spoolsv.exe (only works at Admin level and the DLL needs to be on disk)
- Persistence: Use a service (install - Mandiant report 80%) / run keys / schtasks >> maybe a DLL is better (Process Monitor to start and stop other services and then see the errors. If there is an error then you drop your DLL into the error [VMWARE Tools specific]
- Other persistence example: Print\Monitor\driver from System32 (drop in your DLL)
- DEMOS of the persistence tool
- API HTTP (WinHTTP, WinINet) - THROWBACK tool (beacon backdoor with a DLL & EXE) - silentbreaksecurity.io [supports proxy, payloads, encrypted comms, dll injection, etc]
- DEMO of Throwback + METASPLOIT + Shell (also Throwback can control multiple payloads via single interface)

Old Skewl Hacking: Porn Free!
- No slides
- https://twitter.com/rfidiot

== DAY 3 ==

Burner Phone DDOS 2 dollars a day : 70 Calls a Minute [Weston Hecker]
- Slides are on the CDROM

Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog [Gene Bransfield]
- Slides are on the CDROM

+ I am a legend: Hacking Hearthstone with machine learning [Elie Bursztein & Celine Bursztein]
- http://www.elie.net/hs @elie @cealtea
- Slides are not on CDROM
- World of Warcraft (WoW) related game Heartstone research (very complicated application)
- Complexity = exploit
- Goals: find undervalued cards, predicting opponent deck, predict outcome
- You play 1on1 against someone, decks (30 cards), get the opponent health to zero, you can play a card if you have a mana (1-10) -- card can be a weapon or a creature (up to 7) [minions] {like Magic but simplier)
- Everything is based on a card (Yeti - Mana to play the card attack, and health) … some cards have special abilities and then applying them together
- How do we find undervalue cards: build a model, mana cost is proportional to card power - card power increases linearly - card effects have constant price - having a care has some intrinsic value - there is no hidden balancing value (card attribute sum will be validate)
- mana = attack + health + intrinsic value | 4 = 4a + 5h + i
- orge = 6 = 6a +7h + i vs. yeti (baseline to 1 mana)
- Fireball (4 mana = 4 damage), 1 mana = 1.5 dmg
- Pyroblast (10 = 10 damage), 1 mana = 1 dmg
- There is imbalance between Fireball & Pyoblast (mismatch)
- Model cards = reverse coefficients => real value of the card => look for value
- Published research and got some feedback related to applying budget and characterization of characters => new model with a good list of undervalued cards
- What do you do next? Game replays -- learn how people are actually playing (strategy)
- For instance what about something that give +1 to all your cards in play. There is a right time to play it 3, 4, 5 cards? 1-4 is overpriced, 5-6 fair, 7-9 undervalued
- Tool Demo - Dashboard on advantage / Game data from: SNIFF packets, OCR, Debug Log (make a conf change) - need a real log in the future - you also get a hand by hand play by play to learn from your mistake. There is a GITHUG code: heartstone-dashboard
- There are new Naxx cards that have not yet be modeling
- Details on many replay analysis to determine when prediction starts to work. Around 3rd turn you get much better prediction that matches replay analysis.

"Around the world in 80 cons" - A Perspective [Jayson E. Stree]

- No slides
- POC: https://twitter.com/jaysonstreet

NSA Playset: DIY WAGONBED Hardware Implant over I2C [Josh Datko & Terry Reed]
- Slides are available on CDROM (does not appear to have any publically released classified slides in the briefing material)

Optical Surgery; Implanting a DropCam [Patrick Wardle & Colby Moore]
- Slides are available on CDROM

+ The Simple Route to Backbone Routers [Luca "kaeso" Bruno & Mariano "emdel" Graziano]
- www.s3.eurecom.fr/lg
- Slides are available on CDROM
- Interesting motivation for doing this research: no skills but big impact/havoc (Internet -> BGP Router]
- LOOKING-GLASS (not a straight attack on Cisco/Juniper) = aka network troubleshooting architecture and capabilities
- Review the IPv4/v6 network of networks (autonomous systems = AS) using BGP
- Each AS has their own routing table, configurations (local vs. worldwide)
- Start looking at how troubleshooting is done by current NOC's with AS (RIPE Logs, NLNOG, etc) that will more than likely have some web-access to AS infrastructure (probes
- Most LOOKING GLASS (LG) software is PHP or Perl based, very simple website, usually allow for SSH/telnet to router console, cleartext config files + easy to get to credentials
- These private LOOKING GLASS services (NOC VLAN, not exposed directly) usually have a remote access option to support offsite troubeshooting
- Very basic interfaces: ping, trace, bgp (advertised-routes, summary, etc) but allow for full set of all "your" routers
- Tools examined: Cougar LG, Cistron LG, MRLG, and MRLG4PHP [all open source]
- Review issues & examples/demos: exposed credentials (via Google searches [inurl:lg.conf] + SSH private keys; reading the source code also points out additional areas of information exposure; cookie stealing; attack using LG to AS via automated tools; most of these also have XSS problems; one of PHP LG tools you can do router command injection;
- There are also issues with LG plugins (source code available) which can be used to actually get root on the LG.
- Countermeasures: Code reviews and apply better software engineering best practices (aka no hard coded credentials); deployment (read-only LG access with mirrored data, lock down LGs web servers); and networking ACL (plus strong passwords, private VLANs, harden all out-of-band communications)

You're Leaking Trade Secrets [Michael Schrenk]
- Slides are not on CDROM
- POC: https://twitter.com/mgschrenk

NSA Playset : GSM Sniffing [Pierce & Loki]
- Slides are available on CDROM and do not appear to have any classified information in them.

Open Source Fairy Dust [John Menerick]
- Slides are available on CDROM

+ Catching Malware En Masse: DNS and IP Style [Dhia Mahjoub, Thibault Reuille, & Andree Toonk]
- Slides are available on CDROM (but the new visualization code demos not in the slides)
- POCS: @dhialite @thibaultreuille @attonk
- All from OpenDNS.org with overview of their architecture (22 data centers)
- Malware is using Fast Flux Proxy Networks for Command and Control (CnC)
- Detecting currently CnCs by using a Hadoop periodic data pulls and analysis (IP, DNS requests, etc) [source, convert, etc.]
- Visualization using a SemanticNet Library (release to open source) {3D visualization} [playback over time]

- Results: see urls and links to CnC domains > links to DDOS services, and where the malware is being hosted (names, binaries, etc)
- Review of Pony malware (PHP based, probably written in Moscow time zone) [clients (US) > CnC (Eastern Europe)]
- IP analysis shows how things move around and how many days the IPs stay operational (they put on bad stuff then move to good stuff). Register > Use > then die
- They also work on fingerprinting the types of servers/OS/services (these create a good pattern)
- The bad guys constantly change their methodologies for domains, IPs, who they abuse
- Internet is an Autonomous System (AS) - OpenDNS, Google, etc (ID'd by an ASN - unique number) using BGP
- The visualization of ASN shows where countries have issues related to DDoS

Dropping Docs on Darknets: How People Got Caught [Adrian Crenshaw]
- Slides are available on CDROM

Blowing up the Celly - Building Your Own SMS/MMS Fuzzer [Brian Gorenc & Matt Molinyawe]
- Slides are available on CDROM

Deconstructing the Circuit Board Sandwich: Effective Techniques for PCB Reverse Engineering [Joe "Kingpin" Grand]
- Slides are available on CDROM

+Weird-Machine Motivated Practical Page Table Shellcode & Finding Out What's Running on Your System [Shane Macaulay]
- Slides are available on CDROM (but different in many ways from what was presented)
- New tool released to attack and detect the Rootkit on 64-bit OSes
- POC: http://www.linkedin.com/in/shanemacaulay
- Hypervisors need the same protection pillars: structure; memory; and integrity
- Page Table Shellcode: harder to do post Win7, X64 Kernal space is much improved (8.1 Update 1 especially)
- For instance VirtualAlloc() from user space has kernel code executiion options (Win7 and lower)
- Let's solve the process hiding attack vector/catch a rootkit in Hypervisor
- Recommend moving to latest versions, latest OS, and 64-bit to get to the best base to know you have the recommended protections
- Review of Tool: Valid PFN will be bounded by system memory physical capabilities (so Self Mapping will be detected) [code is available]
- The Memory Cruncher (tool demo - freely available)

Home Alone with localhost: Automating Home Defense [Chris Littlebury]
- Slides are available on CDROM

Playing with Car Firmware or How to Brick your Car [Paul Such 0x222 & Agix]
- Slides are available on CDROM

NSA Playset: PCIe [Joe FitzPatrick & Miles Crabill]
- Slides are available on CDROM (and do not appear to include classified data that has been released previously to the Internet)
- POC: https://twitter.com/milescrabill
- https://securinghardware.com/blog/

+ Generating ROP payloads from numbers [Alexandre Moneger]
- Slides are available on CDROM
- Why ROP? Shellcode in memory execution has gotten hard. Need to get target to run the code for you.
- ROP = Return-Oriented Programming
- Uses Stack Pivoting
- More info on ROP http://resources.infosecinstitute.com/return-oriented-programming-rop-attacks/
- It does require the target to have large number of mov gadgets but in large applications this is usually not an issue.

- This should work on RELRO, X^W, and ASLR protections
- Good example in slides about how "Hello World" is built and how this technique could use that.
- This research was done using gcc 4.4.5 (cc -Q -v ⇒ lists the options) and can give you some gadgets that enable control a function, stack pivot, write to mem, write to reg [but you need eax to actually run]
- Details: shellcode to # (good examples in the slides)
- Review of new tool Ropnum / www.github.com/alexmgr/numstitch

Android Hacker Protection Level 0 [Tim Strazzere & Jon Sawyer]
- Slides are not on CDROM
- POC: https://twitter.com/timstrazz

+Elevator Hacking - From the Pit to the Penthouse [Deviant Ollam & Howard Payne]
- Slides are on CDROM
- POC: https://twitter.com/deviantollam http://enterthecore.net
- Very safe systems, overview of hardware, standard configurations, there is a series sensors in the system, and a main processor unit
- If you get the elevator into non standard mode you can do stuff like hide in an elevator, go up from 1 to top without stopping, etc.

Shellcodes for ARM: Your Pills Don't Work on Me, x86 [Svetlana Gaivoronski & Ivan Petrov]
- Slides are on CDROM

Is This Your Pipe? Hijacking the Build Pipeline [Kyle Kelley & Greg Anderson]
- Slides are on CDROM

MORE INFO

If you are still reading then you might be interested in my DEFCON reports for 18, 19, 20, & 21. Send me email at: technewsradio@gmail.com if you are interested in them.