DEFCON 21 - August 02-04, 2013 - Las Vegas, NV

Steve Holden, sholden@pobox.com (personal) or technewsradio@gmail.com (tech podcasting), 619-631-4433

NOTE: These are my own personal notes taken during the conference for TechNewsRadio.com [@technewsradio]. I have reviewed them but not for 100% accuracy and not for 100% correct spelling. Presentations that had "No slides" are marked accordingly. All the other presentations had slides on the DEFCON RED DISC (DATA) and I can email or share those with you if there is something of interest. Also if the slides were available via Blackhat I put a link to them if I found them. Presentation titles that start with a * are ones I attended in person. All the shortened URLs from (goo.gl) were done by me.

FRIDAY - AUGUST 2, 2013

Ambassador Joseph R. DeTrani: Proliferation
- No slides

The DEF CON 21 Badge with 1o57 & The Dark Tangent
- No slides
- http://www.wired.com/threatlevel/2013/08/defcon-badges-revealed/

I Can Hear You Now: Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell with Doug Deperry & Tom Ritter
- No slides
- http://www.reuters.com/article/2013/07/15/us-verizon-hacking-idUSBRE96E06X20130715

*Adventures in Automotive Networks and Control Units with Charlie Miller & Chris Valasek
- No slides
- Research started in 2010-2011 (including work at UCSD)
- [Original R&D] Data packets attacks were hidden and not released
- Open this up generalize / example code / etc
- Hacking software vs. hardware in a car is much different [about 8+ funny slides]
- cars: 2010 Ford Escape, 2010 Toyota Prius
- Really want park assist
- Details on ECU (different architectures, cabling, components, chips, etc)
- CAN network: ID, data length, broadcast in nature
- Some standards ISO-TP/ISO 15765-2; ISO 14229/14230
- Main interface: Ecom > ODB-II connector (reader/writer) + CarDaq-Plus
- Software: EcomCat, Ecomcat_api, PyEcom
- Demos: change speed displays, braking, steering, acceleration, diagnostics
- Demos: stop car, lights, horn, hank the seat belt, etc
- Keys: all easily unencrypted (included in software release)
- Advanced persistence demo (run stuff after unhooked - reflash the 'firmware')
- Some thoughts on how to protect: diagnostics packets while driving (no no), etc
- Paper will be releases 101 (@0xcharlie, @nudehaberdasher)

All Your RFz Are Belong to Me - Hacking the Wireless World with Software Defined Radio with Balint Seeber
- Previous recording of this talk: http://www.youtube.com/watch?v=pbgeLRvjirI
- @spenchdotnet

Torturing Open Government Systems for Fun, Profit and Time Travel with Tom Keenan
- http://goo.gl/n8gwiE

The Growing Irrelevance of US Government Cyber Security Intelligence Information with Mark Weatherford
- No slides

*The Secret Life of SIM Cards with Karl Koscher & Eric Butler
- Started by wanting to run a cell phone network for toorcamp in Pacific Northwest
- Background on SIM (suppose to be secure, smart card, used for GSM/LTE)
- SIM is also suppose to provide clone protection
- SIM Apps? - applications can live on the SIM / plus data moves with them
- What can a SIM applet do: AT commands, meta data, access data, mobile payments

- Not very common in the US
- That tech is there: SmartCards, Java Card, SIM Toolkit (STK) API, GlobalPlatform
- You can build Java solution using Oracle software, and Eclipse
- https://github.com/simhacks // simhacks.github.io
- SIMAlliance Loader (app from industry - very slow software)
- GlobalPlatform
- More info from Karsten Nohl
- Loaded/writing to SIM via SMS msg (sent locally)
- SIM Cards can be tested using the Android Emulator
- Other interactions with SIM: SingleWireProtocol (SWP)
- NFC payments with going through the OS
- NFC payment company example: ISIS
- SIM also uses Secure Element chips/cards that is used by Google Wallet (NFC)
- TWITTER: @supersat @codebutler

Hacking Driverless Vehicles with Zoz
- http://www.kcsr.org/showthread.php?p=2088626

Backdoors, Government Hacking and The Next Crypto Wars with Christopher Soghoian
- https://twitter.com/csoghoian
- No slides

*The Dirty South ñ Getting Justified with Technology with David Kennedy & Nick Hitchcock
- No slides
- from TRUSTEDSEC
- history of 'security' (build, break, fix, repeat)
- Demo: Social Engineering Toolkit (new version, setup a dummy website, client goes to site)
- Demo: Target runs Java, target goes back to bad guy system, metasploit loads the bad payload
- Demo: all over HTTPS (hidden from IDS/Firewalls/Etc).
- Demo using Facebook as a way of controlling a man-in-the-middle attack (also a future release for SET)
- Other threat options: Application Whitelisting / Behavioral Analysis / Anit-Virus / Content Filtering
- Kevin Mitnick social engineering demo that used a new PowerShell exploit via SET/Metasploit
- 12 step program for fixing security: understand the users/business; isolate to least priviledge
- 12 step (cont.): education; be helper; focus 1 year just on security; keep it basic;
- 12 step (cont.): stay away from complexity); penetration testing; do a 1 week off; read REWORK book

DragonLady: An Investigation of SMS Fraud Operations in Russia with Ryan W. Smith & Tim Strazzere
- No slides
- Speaker: http://www.linkedin.com/in/ryanwsmith & http://www.linkedin.com/in/timstrazzere

10000 Yen into the Sea with Flipper
- About underwater glider
- nickflipper@gmail.com

ACL Steganography - Permissions to Hide Your Porn with Michael Perklin
- Online slides: http://www.perklin.ca/~defcon21/aclsteganography.pdf

Prowling Peer-to-Peer Botnets After Dark with Tillmann Werner
- No slides

*Offensive Forensics: CSI for the Bad Guy with Benjamin Caudill
- No slides
- Detailed look at Windows
- Registry
- Disk/Registry (encrypted files get listed differently)
- Memory
- Browser Files / Even those used "private" mode
- Backup/Recovery
- Crash Dump
- Metasploit has a growing number of modules (IE Cookies, Network History, Firefox details)

- @rhinosecurity
- http://www.rhinosecuritylabs.com/blog/

*Pwn'ing You(r) Cyber Offenders with Piotr Duszynski
- twitter: @drk1wi
- Works at @trustwave
- Focus on active defense in practice / slow down your attackers / get them off sooner
- nmap -sv -O portspoof.org (used by bad guy for reconnaiassee)
- worst case is 65,535 ports with ~120 MB data center --- 8.h hours
- spice up the data going back - data hidding
- make different devices look different or the same
- when bad guy is doing webscanning send them XSS exploit /Javascript / Beef
- video of the demo will be posted (portspoof.org)

Business Logic Flaws In Mobile Operators Services with Bogdan Alecu
- https://twitter.com/msecnet

Protecting Data with Short-Lived Encryption Keys and Hardware Root of Trust with Dan Griffin
- Toorcon presentation: http://goo.gl/MqP75f
- jwsecure.com post: http://goo.gl/PJ9c8h
- https://twitter.com/JWSdan

Evil DoS Attacks and Strong Defenses with Sam Bowne & Matthew Prince
- http://samsclass.info/seminars/defcon21-cfp.htm

*Man In The Middle (MITM) All The IPv6 Things with Scott Behrens & Brent Bandelgar
- NEOHAPSIS on gethub.com
- Follow-on to SLAAC Attack from Alec Waters
- Windows VISTA and higher always listen for IPv6
- Background/History/Basic Architecture Slide (need evil router and evil DNS on the network]
- Works on Vista/Win7 but not exactly working on Win8
- Their research: single bash script uses Ubuntu and Kali to create a MITM
- You do need IPv4 address and the interface (same subnet) // highly recommend you do testing
- Defeat this: turn off IPv6, if you do RFC6105 you can stop this (cisco has a product)
- Another issue is DNS race conditions (much more an issue for mobile computing)
- Future plans: IPv6 tunneling, look at more IPv6 tools, mobile devices

*HTTP Time Bandit with Vaagn Toukharian & Tigran Gevorgyan
- slow down web servers / attacking memory hags
- future: stages of testing, understanding load balancers, SQL wild card impacts
- consider mod_security
- presenters: @tukharian
- http://www.youtube.com/watch?v=aSh3_0t6wmM&list=UUUHW9oR4Ti3nxIgVwln2KuA

Google TV or: How I Learned to Stop Worrying and Exploit Secure Boot with Amir Etemadieh & Panel
- accuvant.com PR: http://goo.gl/b7SJ21
- https://twitter.com/Zenofex

Kill 'em All ñ DDoS Protection Total Annihilation! with Tony Miu & Wai-Leng Lee
- https://media.blackhat.com/us-13/US-13-Lee-Universal-DDoS-Mitigation-Bypass-Slides.pdf

*How to use CSP to Stop XSS with Kenneth Lee
- No Slides
- Content Security Policy (CSP) -- only execute in the browser what is allowed
- CSP should help to stop Cross Site Scripting attacks
- There is a way to do report-uri to see the CSP violations (dry run / does not block)
- This is still version 1.0
- There is some issues with JavaScript and CSP
- Approaches for deploying this: Twitter's CSP is website specific
- You can get also get started with splunk for tracking

- CSP is easy to find mix content (which is probably going to create some issues)
- Outlined CST Tools (3): proxy, browser, parser [with demo] [see code on Github]
- @kennysan / link with slides on twitter

*So You Think Your Domain Controller is Secure? with Justin Hendricks
- focus of this talk: SCOM, HP ILO, and Hyper-V
- no exploits, only using the standard tools and looks at misconfiguration opportunities
- if you can get access to credentials, you can do pretty much anything
- System Center Operations Manager (SCOM)
- SDK published
- Users ports 5723/5724 becomes open via many firewalls (has high priviledges)
- If you can own SCOM then you can run any script you want on any system being monitored
- Microsoft recommends a 2 x SCOM server: 1 for AD servers & 1 for managing everything else
- Demo via videos
- Recommendations: limit access to admin role; others should be read only;
- Recommendations: read the SCOM security guide; block access from the internet
- Audit: Review logs of SCOM to make sure all tasks run are approved
- Out-of-bound Mgmt: Lights Out (ILO), SSH, HTTPS, being on he console, default passwords
- Rapid7 has new exploits related to ILO
- https://twitter.com/Script_Happens

A Password is Not Enough: Why Disk Encryption is Broken and How We Might Fix It with Daniel Selifonov
- Go get the code: https://github.com/thyth/phalanx
- Web: http://thyth.com/
- Email: ds@thyth.com

VoIP Wars: Return of the SIP with Fatih Ozavci
- author's previous presenation slides http://www.slideshare.net/fozavci

*Getting The Goods With smbexec with Eric Milam
- Business Wire Story: http://goo.gl/y0qELl
- http://www.linkedin.com/pub/eric-milam/0/229/281
- http://sourceforge.net/projects/smbexec/
- looks like normal windows traffic over the network
- collection of scripts and code from previous one off examples
- commands are run as system (dump hash, volume shadow copy, disable UAC, etc)
- pretty easy to use tool for doing security assessments
- good tool to run to see what can be done if you don't mitigate
- need local account with some priviledges / ettercap [MITM http://ettercap.github.io/ettercap/]
- This will get caught in a forensic analysis
- there is a version 2.0 in Ruby in the works

*Abusing NoSQL Databases with Ming Chow
- http://www.cs.tufts.edu/News/chow-returns-to-defcon.html
- https://twitter.com/tufts_cs_mchow
- Mongo example: collection, find routine, JSON [CBS database of financial news on twitter]
- Where is the security for NOSQL DBs? It is all over the board ...
- So we are currently at a point were the NOSQL DB is being secured by developer
- Very few encryption options standard, full admin features for admins is considered standard practice
- Shoodan has 1000s of these servers accessible via the Internet
- These have three types of injections: schema, query, javascript
- These injections may expose information not expected to be released
- JavaScript injection can also create DDOS/System Resources (RAM, Processor, Storage)

The Government and UFOs: A Historical Analysis with Richard Thieme
- http://www.thiemeworks.com/

Decapping Chips the Easy Hard Way with with Adam "Major Malfunction" Laurie & Zac Franken
- No slides
- https://twitter.com/rfidiot

- http://zacsblog.aperturelabs.com/

*Unexpected Stories - From a Hacker Who Made It Inside the Government with Peiter "Mudge" Zatko
- No slides
- https://twitter.com/dotMudge

Examining the Bitsquatting Attack Surface with Jason Schultz
- No slides but whitepaper available

Please Insert Inject More Coins with Nicolas Oberli
- https://github.com/Baldanos/ccTools
ñ http://www.balda.ch
- @Baldanos

How my Botnet Purchased Millions of Dollars in Cars and Defeated the Russian Hackers with Michael Schrenk
- mgschrenk@gmail.com
- www.schrenk.com

SATURDAY - AUGUST 3, 2013

*Proactive Defense and Mission Assurance with Lt. Gen. Robert Elder USAF (Retired)
- No slides
- Nuclear weapons was global, so cyber was considered global
- Nuclear was a deterrence
- Cyber is not really a deterrence
- alternative view for defense/assurance -- ecosystem model?
- culture: hierarchical to cyber (distributed, connected (more is better), contribution)
- http://sysarch.gmu.edu/main/people/current/dr-robert-elder/

Dude, WTF in my car? with Alberto Garcia Illera & Javier Vasquez Vidal
- No slides
- twitter: https://twitter.com/algillera
- http://www.newscientist.com/article/mg21929266.500-25-gadget-lets-hackers-seize-control-of-a-car.html

Do-It-Yourself Cellular IDS with Sherri Davidoff & Panel
- No slides
- http://lmgsecurity.com/blog/2013/07/26/diy-cellula [with link to whitepaper]
- twitter: https://twitter.com/SherriDavidoff

Predicting Susceptibility to Social Bots on Twitter with Chris Sumner & Randall Wald
- https://www.blackhat.com/us-13/speakers/Randall-Wald.html
- https://www.blackhat.com/us-13/speakers/Chris-Sumner.html
- BLACK HAT SLIDES: https://www.blackhat.com/us-13/briefings.html#Sumner

Insecurity - A Failure of Imagination with Marc Weber Tobias & Tobias Bluzmanis
- About lockpicking
- https://twitter.com/Marcwebertobias
- http://en.wikipedia.org/wiki/Marc_Tobias
- http://www.wired.com/techbiz/people/magazine/17-06/ff_keymaster?currentPage=all

The Politics of Privacy and Technology: Fighting an Uphill Battle with Eric Fulton & Daniel Zolnikov
- http://www.blackhat.com/usa/speakers/Eric-Fulton.html
- https://www.facebook.com/permalink.php?id=352517808109574&story_fbid=634172319944120

The Road Less Surreptitiously Traveled with Pukingmonkey
- https://twitter.com/pukingmonkey
- Details on how your car is being tracked: licensed plates, picture cameras, future RFID

Fear the Evil FOCA: IPv6 attacks in Internet Connections with Chema Alonso
- No slides

- https://twitter.com/chemaalonso

*Key Decoding and Duplication Attacks for the Schlage Primus High-Security Lock with David Lawrence & Panel
- Forbes.com: http://goo.gl/zjy33p
- These have a top and a side "key" (standard pin-tumbler on the top but a side key that has a side bar)
- There are people who can pick these but it is very hard (requires a good deal of talent)
- So how to get into the copy mode? - read the patent and vendor docs/manual
- Lockwiki has pictures
- Demo of building 3D models for keys using OPENSCAD [~eleven key numbers]
- Building: cut by hand (dremel, calipers, blank); CCM (very costly); micromill (~$1000)
- Best solution was 3D Printing (plastic [cheap]/titanium [expensive])
- 3D Printing Solution: http://www.shapeways.com/
- FUTURE: Making models from pictures of keys (University research, others)

Defeating Internet Censorship with Dust, the Polymorphic Protocol Engine with Brandon Wiley
- No slides
- CODE: https://github.com/blanu/Dust

Home Invasion 2.0 - Attacking Network-Controlled Consumer Devices with Daniel "UnicornFurnace" Crowley, Jennifer "SavageJen" Savage, & David "Videoman" Bryan
- BLACKHAT SLIDES: https://media.blackhat.com/us-13/US-13-Crowley-Home-Invasion-2-0-Slides.pdf
- GOOGLE PLUS for Crowley: https://plus.google.com/116693824563032601688/posts
- TWITTER: https://twitter.com/savagejen
- These folks are from: TrustWave/SpiderLabs, Tabbedout
- What gets hacked once it is hooked to the Internet (not the standard stuff)
- "Smart" devices / science fiction becomes science fact
- Race to release = poor product security
- NOT COVERING: Android devices, Smart TV, Video surveillance
- South Korea is building a digital city: Songdo
- Review: Karotz Smart Rabbit (usb port, wifi, video, sound, microphone, RFID, etc)
- Major issues with rabit: no wifi encryption, python code was hijacked, no API encryption
- Rabit demo - iphone app connection not over SSL
- Review: Belkin WeMo Switch (fixed all the problems that were reported)
- Belkin does have t a free hardware for hackers program (link?)
- Belkin: [uses uPMP] {basically a small linux box - can be used forsniffing, launch attacks, etc]
- Note: there is an NMAP scan that will give you back all the UPMP devices on a network segment scan
- Review: SONOS Bridge (very chatty exposing more information than needed)
- Review: LIXIL Satis Smart Toilet (Japanese - Android app that uses bluetooth to control functions)
- LIXIL Android app: zero security features
- Review: INSTEON Hub (home network control device for home automation)
- INSTEON has no encryption, no authentication by default
- INSTEON new version has authentication but default admin account and password set to last 3 of MAC
- REVIEW: MiCasaVerde VeraLite (home network control for home automation) {TONS of issues)

BoutiqueKit: Playing WarGames with Expensive Rootkits and Malware with Josh 'Monk" Thomas
- TWITTER: https://twitter.com/m0nk_dot

Legal Aspects of Full Spectrum Computer Network (Active) Defense with Robert Clark
- http://www.blackhat.com/usa/speakers/Robert-Clark.html
- http://www.linkedin.com/pub/robert-clark/b/76b/7a

Privacy In DSRC Connected Vehicles with Christie Dudley
- https://twitter.com/longobord

RFID Hacking: Live Free or RFID Hard with Francis Brown
- No slides
- Speaker annoucement on personal blog: http://goo.gl/c8g5wK
- BLACKHAT: https://media.blackhat.com/us-13/US-13-Brown-RFID-Hacking-Live-Free-or-RFID-Hard-Slides.pdf

Android WebLogin: Google's Skeleton Key with Craig Young

- https://twitter.com/craigtweets

Building an Android IDS on Network Level with Jaime Sanchez
- https://twitter.com/segofensiva

*We are Legion: Pentesting with an Army of Low-power Low-cost Devices with Dr. Philip Polstra
- Need move your code to ARM / cross compile
- Recommends LittleBeagle (ARM processor) with Ubuntu
- 802.15.4 networking (Xbee) - creates a true mesh network / radio / ~250kbps max
- Program the modems via USB adapter to interoperate
- EXAMPLE: Drone with "lunch bunch" controller
- https://twitter.com/ppolstra
- Example Code: Python script (polstra.org)
- Power via battery or PoE (power over ethernet)
- DRONES: can be updated to use better battery technology
- FUTURE: XB Gateway to Internet, SND/REC files, Pentest capes
- DEMOS: ~8 examples of what you can do: NMAP, password capture, password crack, etc.

*Phantom Network Surveillance UAV / Drone with Ricky Hill
- http://www.linkedin.com/in/rickyhill
- DC area, SCADA, previous talks (WarRocketing, WarBallooning, etc)
- not dry cleaning but more about surveillance, can lift about 2-pounds
- uses a 'cotton candy computer' (android or Ubuntu) and you can add a wireless capture
- other attempts: UAVForge by DARPA (perch and stare - turn off the engines), WASP spy drone
- in UAVForge test (2011) the average time to crash was 3 minutes
- REVIEW: Phantom from DJI Innovations (released in Jan'13)
    - $679, 400 grams payload
    - GPS
    - Auto "Return To Home"
    - Two stick
- PAYLOAD: #1.) CottonCandy; #2.) Hak5 Pineapple + GSM 3G/46 (with custom power supply)
- Recommends the CottonCandy (Demo)
- DEMO FLIGHTS (3-4 examples) -- roof landing

*Stalking a City for Fun and Frivolity with Brendan O'Connor
- Cameras, surveillance
- Review some hardware options: F-Bomb v.1, v.2
- Code review: Portal Smach, Command&Control,
- CreepyDOL
- DARPA / Visualization / Unity Game Engine
- www.maliceafterthought.com
- https://twitter.com/USSJoin

Defeating SEAndroid with Pau Oliva Fora
- ComputerWorld: http://goo.gl/pzU3Mt
- http://pof.eslack.org/
- @pof

Doing Bad Things to 'Good' Security Appliances with Phorkus (Mark Carey) & Evilrob (Rob Bathurst)
- No slides
- https://plus.google.com/106510726760297485386/posts
- http://www.blackhat.com/us-13/speakers/Rob-Bathurst.html

*Pwn The Pwn Plug: Analyzing and Counter-Attacking Attacker-Implanted Devices with Wesley McGrew
- How to respond? Seizure vs. Counter-Attack
- You have physical control
- you can do forensics analysis on the device
- most of these devices have accessible interface: web, other ports
- there OS and apps are as vulnerable as any other
- demo

- https://twitter.com/McGrewSecurity

*Safety of the Tor Network: a Look at Network Diversity, Relay Operators, and Malicious Relays with Runa A. Sandvik
- goal: free speech, free access, journalists, activism, domestic abuse
- lots of growing questions
- History of TOR
- Since 2002 it has been open source and not government funded
- How to setup a relay - how to run the client?
- The # of hops through relays does reduce from the 4000 total replays down to 1000
- Note: clients take 2 hops before leaving TOR exit node (3 all together)
- TOR protects your location not that you are communicating
- Does the threat model for TOR need to get updated?
- TOR R&D effort at NPS: looking at what can be pulled from exit node analysis
- % of relay 1, relay 2, and exit by country [heavy on US and Germany]
- Who are the relays? Analysis of IP address - nothing significant points to gov running relays
- Review of couple of TOR relays that were "interesting" - one in China, one in the Baltics (botnet?)
- TOR can turn off "bad" relays?
- torservers.net (German non-profit - looking for more diversity - exit relay funding) [other examples]
- They are doing analysis all relays via consensus tracker / Snakes on a Tor (SOAT) tool
- Recommendations: use TOR, fund/run relay, exit scanner

Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks with Hunter Scott
- https://twitter.com/hunterscott

How to Hack Your Mini Cooper: Reverse Engineering Controller Area Network (CAN) Messages on Passenger Automobiles with Jason Staggs
- Research from The University of Tulsa iSEC (isec.utulsa.edu)

An Open Letter - The White Hat's Dilemma: Professional Ethics in the Age of Swartz, PRISM and Stuxnet with Alex Stamos
- https://twitter.com/alexstamos
- No slides

De-Anonymizing Alt.Anonymous.Messages with Tom Ritter
- No slides

BYO-Disaster and Why Corporate Wireless Security Still Sucks with James Snodgrass (PuNk1nPo0p) & Josh Hoover (wishbone)
- No slides

*Electromechanical "Automated" PIN Cracking with Robotic Reconfigurable Button Basher (and C3BO) with Justin Engler & Paul Vines
- iSECpartners
- Mechanical PIN cracking / robots [note there are 10,000 guesses]
- countermeasures: time delay for dev / users pick longer passwords
- why do you need brute force -- when code and other hardware attacks don't work
- built a "delta" robot (3D movement X-Y-Z) -- fast but not a "lifter"
- capacity overlay concept isn't working ... they don't know why?
- PIN choice not sequential: danielamitay.com
- They find most passwords between 25-50% less than expected with brute force
- Android is 80% successful by default in 20 hours / iOS is 20% successful after 20 hours
- PINs in apps are significantly easier

Data Evaporation from SSDs with Sam Bowne
- http://samsclass.info/121/proj/ssd-evaporation.htm

*PowerPreter: Post Exploitation Like a Boss with Nikhil Mittal
- https://twitter.com/nikhil_mitt
- Tool review / based on PowerShell / see Nishang

- best used for remote sessions
- things it can do: persist, pivot, admin system, help other efforts, tamper with logs, etc.
- several deployment options: software, USB, user download, etc.
- demo
- issues: needs more testing, no keylogger, can be detected by network traffic analysis

Noise Floor: Exploring the World of Unintentional Radio Emissions with Melissa Elliott
- No slides

GoPro or GTFO: A Tale of Reversing an Embedded System with Todd Manning & Zach Lanier
- Presentation annoucement: http://goo.gl/c345Kw

JTAGulator: Assisted Discovery Of On-Chip Debug Interfaces with Joe Grand aka Kingpin
- http://www.grandideastudio.com/
- http://www.grandideastudio.com/wp-content/uploads/jtagulator_slides.pdf

*DNS May Be Hazardous to Your Health with Robert Stucke
- DNS needs constant monitoring to see what normal is that you tell what not normal is
- dinaburg.org has good references
- what is bit-squatting (1 goes to 0, 0 goes to 1)
- a single bit-squat error can cause issues google.com becomes goofle.com
- gstatic.com / CSS, image, javascript, xml [got 29 bit-squating domains]
- got a lot of requests / may refers (50,000 unique queries)
- is this just random noise? / Google.gif they got Occupy.gif [pattern matching]
- Logs showed Feedfetcher xml (iGoogle) > in Beligum
- Turned out to be a widget asking his servers for - so he gave them what they asked
- Need to look at bit flip domains especially for short them
- www.google.com, google.com, google.com. are all handled differently (Suffix Search Path)
- XP changed the DNS Devolution: www.phx.ad.foo.com > www.ad.foo.com > www.foo.com [stop]
- This caused problems with for example x.x.x.co.uk
- set-proxy.com is his domain, and because of the search path issue is getting proxy traffic directly
- Looking at help desk support docs on setting up devices he then registered sites based on support docs
- EXAMPLE: quanta.com >> rsquanta.com [customer assets at remote customer sites]
- monitor: pastebin, bleeping computer
- looking at domains for old botnets (expired domains, aka microsoft-windows-security.com)
- This site still has #268 machines still reporting
- MORE INFORMATION: www.bro.org, passive DNS code, DNS sinkholes

OTP, It won't save you from free rides! with bughardy & Eagle1753
- bughardy@cryptolab.net & eagle1753@onenetbeyond.org
- Near Field Communications (NFC) hacks

How to Disclose or Sell an Exploit Without Getting in Trouble with James Denaro
- @CipherLaw

SUNDAY - AUGUST 4, 2013

The Cavalry Isn't Coming: Starting the Revolution to Fsck it All! with Nicholas J. Percoco & Joshua Corman
- No slides
- https://twitter.com/joshcorman
- https://twitter.com/c7five

gitDigger: Creating useful wordlists from public GitHub repositories with Jamie Filson (WiK) & Rob Fuller (Mubix)
- https://twitter.com/mubix
- https://twitter.com/jaimefilson
- https://github.com/wick2o/gitDigger

Made Open: Hacking Capitalism with Todd Bonnewell
- No slides
- https://twitter.com/MadeOpen

Exploiting Music Streaming with JavaScript with Franz Payer
- https://twitter.com/Franz780
- http://cyberexplo.it/

*Defense by numbers: Making Problems for Script Kiddies and Scanner Monkeys with Chris John Riley
- @ChrisJohnRiley
- HTTP Status Codes (All requests get these)
- RFC 2616 (HTTP/1.1) with five main classes - 1XX, 2XX, 3XX, 4XX, 5XX (with 7XX proposed RFC)
- NOTE: Apache doesn't support all the RF2616 reporting mechanism
- 2XX: working stuff, OK, created, Accepted, no content, etc
- 3XX: redirection / action required
- 4XX: Client error: long list
- 5XX: Server error: long list
- Increase attacker costs/time / be more active in defense
- Some prior error: slideshare.net/sensepost/strikeback, www.technicalinfo.net/paper
- examples: proxy returning all 2XX, example PHP file,
- SLIDES will be released later
- Analysis on how browsers respond: Firefox, Chrome, IE [differences/similarities]
- If you send a 1XX code to a Android Chrome browser ...
- ... it will continue to try to download unit the device is rebooted or process killed
- Review of how to use this as browser fingerprinting >
- > This helps with sending stuff back that is not expected
- Review of script kiddy tools and how they responded
- Review of what worked and what doesn't - good idea to send them semi-random stuff
- Data on how the codes cause reports: good analysis (best one was sending back 5XX)
- Lots of false positives in a random way is great
- HTTP Tarpit does slow things down and give your attacker some bad info
- Implementation: PHP script (auto-prepend-file), MITMProxy, nginx (recommended) [reverse proxity]
- Move to modsecurity effort

*The Dark Arts of OSINT with Noah Schiffman & Skydog
- No slides
- http://www.layerone.org/speakers/#schiffman
- https://twitter.com/SkyDogCon
- background on top: what is OSINT, acquisition, etc.
- enough data collection = intelligence (actionable)
- Example: maltego (drill into a target); FOCA (meta data tool)
- More Examples: Search Diggity, Recorded Future (temporal analysis)
- Continued Examples: Google Hacking Database / Social Networking (public data)
- Stop with the examples: SessionID (confidential) / governmental(institution)
- These $$$ databases: Gov, Edu, Com [paid - gives you analysis options, trends, etc]
- Example: freebase, powerset, etc
- Big Data - really a big thing?
- Can this data be really anonymization?

The Dawn of Web 3.0: Website Mapping and Vulnerability Scanning in 3D, Just Like You Saw in the Movies with Teal Rogers & Alejandro Caceres
- Using Apache Nutch with some custom plugins
- Also have a cluster based Hadoop and a distributed web spider architecture (PunkSPIDER)
- Have a lot of data

Java Every-Days: Exploiting Software Running on 3 Billion Devices with Brian Gorenc & Jasiel Spelman
- BLACKHAT SLIDES: http://goo.gl/eNcmMs
- @MaliciousInput, @thezdi, @WanderingGlitch

Resting on Your Laurels Will Get You Pwned: Effectively Code Reviewing REST Applications to Avoid Getting Pwned with Abraham Kang & Dinis Cruz
- https://twitter.com/DinisCruz
- Links to several apps, demos, etc in the presentation slides

EMET 4.0 PKI Mitigation with Neil Sikka
- https://twitter.com/neilsikka

*Combating Mac OSX/iOS Malware with Data Visualization with Remy Baumgarten
- http://www.linkedin.com/pub/remy-baumgarten/3/87a/26a
- https://twitter.com/anrctraining
- tool to look at mach-o files / most tools are not web-based
- build snort signatures based on found files
- there are tools to look at mach-o (http://en.wikipedia.org/wiki/Mach-O)
- Review of new beta tool that is web-based (Mac focused) with open source utilities [MachOViz]
- White Paper also released with how to use
- Good demo / slides are posted online

*A Thorny Piece Of Malware (And Me): The Nastiness of SEH, VFTables & Multi-Threading with Marion Marschalek
- http://prezi.com/dqlj_vqimbbt/defcon21-thorny-malware/
- https://twitter.com/pinkflawd
- Review of a specific piece of malware: file-infecting spy-bot
- FEATURES: screen capture, file transfer, run commands, etc
- Review of how exception handling process (changed, Win32, multithreaded)
- Catching the inter-tread comms lead to the most information to point to other key pieces of info
- When analyzing binary that comes from C++, look for virtual classes as hints of trying to hide

HiveMind: Distributed File Storage Using JavaScript Botnets with Sean Malone
- IRONGEEK.com: http://goo.gl/Fv5NcS
- http://www.seantmalone.com/
- No slides

This Presentation Will Self-Destruct in 45 Minutes: A Forensic Deep Dive into Self-Destructing Message Apps with Drea London & Kyle O'Meara
- No slides
- @strozfriedberg (company that both presenters work at)
- http://www.linkedin.com/in/dreagrrl

Stepping P3wns: Adventures in Full Spectrum Embedded Exploitation (and defense!) with Ang Cui & Michael Costello
- No slides
- http://ids.cs.columbia.edu/users/ang.html
- https://plus.google.com/108242664911923835822/posts

Transcending Cloud Limitations by Obtaining Inner Piece with Zak Blacher
- http://ca.linkedin.com/in/zakblacher

Utilizing Popular Websites for Malicious Purposes Using RDI with Daniel Chechick & Anat (Fox) Davidi
- http://il.linkedin.com/in/foxdavidi
- @afoxdavidi, @danielchechik

*Defending Networks with Incomplete Information: A Machine Learning Approach with Alexandre Pinto
- BLACKHAT SLIDES: http://goo.gl/bT3fP6
- https://twitter.com/alexcpsec
- SIEM tools have issues; rules are hard to maintain; alerts need to be very tailored
- Even the behavioural searches aren't working
- We are getting into really Big Data; SIEM
- Need an army of robot looking through all this data -> MACHINE LEARNING
- Some areas where ML is accepted: sales, trading, image recognition, voice recognition
- Security uses: fraud detection, spam filtering but not so much in network anomaly detection
- Types of learning: supervised vs. unsupervised (scikit-learn.github.io/scikit-learn-tutorial)
- The people who build these models do not think how people will mess with the model (bad data, etc)
- Worked with SANS DShield (started bulk mining - blocked summarized block data)
- This analysis pointed to: group by netblock (/16, /24) -- group by ASN

- Models need to be sync with day rankings (blacklist vs. whitelist?
- more like training data by BAD vs. GOOD)
- Support Vector Machines (SVM) is some serious math
- Accuracy improves over time > use the prediction for tomorrows to then train for the next
- The model then tells you something is worth looking at: the recommendation is 20% more likely bad
- You could then take those predictions and either block them or send them to a honeypot
- www.mlsecproject.org

Fast Forensics Using Simple Statistics and Cool Tools with John Ortiz
- very detailed presentation on the topic of Steganography
- more info: stego@satx.rr.com

* EDS: Exploitation Detection System with Amr Thabet
- No slides
- @amr_thabet
- attacks are focused on clients, and then they attack the clients
- using HTTP/HTTPS
- perimeter defenses are being
- many of the new malware is not able to be detected
- need to move to full client protection (EDS is the next wave)
- goals: stop attacks; stop memory corruptions (www.corelan.be)
- architecture: shellcode & ROP chain directors with HEAP and STACK Mitigations
- issues are categorized in EDS by a scoring system (payload, attack vector, processes)

Open Public Sensors, Trend Monitoring and Data Fusion with Daniel Burroughs
- No slides

*Collaborative Penetration Testing With Lair with Tom Steele & Dan Kottmann
- @_tomsteele, @djkottmann
- pentesters / lots of files / lots of windows / fix duplication of work
- Lair (new tool, released): browser based / architecture review [web, db, realtime]
- Key tech used: meteor web server/JavaScript/Mongo
- Lair interfaces with tools/command line [aka drone] - nesus, nmap, burp, etc.
- drones are written in python
- Tracks: hosts, services, vulnerabilities, notes, credentials, contributors, files, logs
- Demo: IP data from NMAP + NESUS are additive
- There are color coding categorization to separate work and filter work by categories
- Source code is on github.com

Blucat: Netcat For Bluetooth with Joseph Paul Cohen
- No slides

Forensic Fails - Shift + Delete Won't Help You Here with Eric Robi & Michael Perklin
- No slides

Conducting Massive Attacks with Open Source Distributed Computing with Alejandro Caceres
- @dotslashpunk
- author of punkspider
- used Hadoop
- more info at www.hyperiongray.com

*PowerPwning: Post-Exploiting By Overpowering PowerShell with Joe Bialek
- @joesphbialek
- PowerShell is Win32 API
- never touches disk (PowerShell.exe or WsmProvHost.exe)
- if powershell is whitelisted then your code will be whitelisted
- load PE (EXE/DLL) is that topic he is discussing (as he doesn't want to rewrite tools in powershell)
- example: how to load a PE (DLL output isn't going to stdout so you can't get it from remote execution)
- note: there are some issues with EXE loaded in Powershell because exit will actually kill powershell
- workaround: load in thread and then end thread

- Demos (Remote PowerShell running a hacker tool to Domain Controller to pull all passwords in clear)
- NTFS Parser (open source) -- turned into Powershell tool in about 2 hours
- Can this detected/protected? Still need admin access
- Recommend: limit powershell access, use pipeline logging,
- More recommends: cmds in powershell can be restricted by users
- Also: some machine specific profiles could capture this but admin can turn this off
- SOURCE CODE: clymb3r on github.com

Evolving Exploits Through Genetic Algorithms with Soen
- Attack surface: SQL Injection, command injection, HTTP/HTTPS, GET parameters
- Tools: Acunetix, Burp, ZAP, SQLMAP, Forced Evolution
- Pros & Cons
- Demo
- CODE: forced-evolution @ github.com
- @soen_vanned

BYOD PEAP Show with Josh Yavor
- No slides
- http://www.blackhat.com/us-13/speakers/Josh-Yavor.html

Let's Screw with Nmap with Gregory Pickett
- gregory.pickett@hellfiresecurity.com
- Development environment: Debian, VMs, rcp100, IDGuard

Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions with Andy Davis
- From nccgroup

The Bluetooth Device Database with Ryan Holeman
- @hackgnar
- Opensouce: bnapbnap, hackfromacave, bluetoothdatabase.com
- https://github.com/OpenSecurityResearch/bnapbnap
- http://ubertooth.sourceforge.net/

C.R.E.A.M. Cache Rules Evidently Ambiguous, Misunderstood with Jacob Thompson
- jthompson@securityevaluators.com
- Find cached sensitive data from browsers: SSN, bank info, etc
- Solution: cache-control, pragma