



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 1 (Disc 2)

- 004 Perspectives in Cybersecurity and Cyberwarfare**
Max Kelly
- 009 Meet the Feds - CSI:TCP/IP** (Video Only)
Panel
- 014 DNS Systemic Vulnerabilities and Risk Management: A Discussion** (Video Only)
Panel
- 020 Meet the Feds - Policy, Privacy, Deterrence and Cyber War** (Video Only)
Panel
- 026 Enough Cyber Talk Already! Help Get this Collaboration Engine Running!**
Riley Repko
- 032 Open Letter - Call to Action** (Video Only)
Panel
- 038 Of Bytes and Bullets** (Video Only)
Panel
- 039 Exploiting WebSphere Application Server's JSP Engine**
Ed Schaller
- 044 Mastering the Nmap Scripting Engine**
Fyodor, David Fifield
- 050 Meet the EFF** (Video Only)
Kevin Bankston, Eva Galperin, Jennifer Granick, Marcia Hofmann, Kurt Opsahl
- 056 Black Ops Of Fundamental Defense: Web Edition**
Dan Kaminsky
- 065 Legal Developments in Hardware Hacking**
Jennifer Granick, Matt Zimmerman
- 070 App Attack: Surviving the Mobile Application Explosion**
Kevin Mahaffey, John Hering
- 075 This is Not the Droid You're Looking For...**
Nicholas J. Percoco, Christian Papathanasiou
- 080 Practical Cellphone Spying**
Chris Paget
- 085 HD Voice - The Overdue Revolution**
Doug Mohny
- 090 These Aren't the Permissions You're Looking For**
Anthony Lineberry, David Luke Richardson, Tim Wyatt



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 1 (Disc 2)

- 095 Mobile Privacy: Tor on the iPhone and Other Unusual Devices**
Marco Bonetti
- 100 Resilient Botnet Command and Control with Tor**
Dennis Brown
- 105 Ripping Media Off Of the Wire**
HONEY
- 110 You're Stealing It Wrong! 30 Years of Inter-Pirate Battles**
Jason Scott
- 116 The Search for Perfect Handcuffs... and the Perfect Handcuff Key**
Deviant Ollam, Dave, Dr. Tran, Ray
- 121 Attack the Key, Own the Lock**
Schuyler Towne, datagram
- 126 PCI, Compromising Controls and Compromising Security**
Jack Daniel, Panel
- 131 How I Met Your Girlfriend**
Samy Kamkar
- 136 Decoding reCAPTCHA**
Chad Houck, Jason Lee
- 141 So Many Ways to Slap A Yo-Ho:: Xploiting Yoville and Facebook for Fun and Profit**
Tom Stracener "Strace", Sean Barnum, Chris Peterson
- 146 Social Networking Special Ops: Extending Data Visualization Tools for Faster Pwnage**
The Suggmeister
- 151 Getting Social with the Smart Grid**
Justin Morehouse, Tony Flick



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 2 (Disc 3)

- 005 Passive DNS Hardening**
Robert Edmonds, Paul Vixie
- 010 Cloud Computing, a Weapon of Mass Destruction?**
David "VideoMan" M. N. Bryan, Michael Anderson
- 015 How Unique Is Your Browser?**
Peter Eckersley
- 021 Token Kidnapping's Revenge**
Cesar Cerrudo
- 027 Lord of the Bing: Taking Back Search Engine Hacking from Google and Bing**
Rob Ragan, Francis Brown
- 033 Tales from the Crypto**
G. Mark Hardy
- 045 Hacking Oracle From Web Apps**
Sumit Siddharth
- 051 Drivesploit: Circumventing Both Automated AND Manual Drive-By-Download Detection**
Wayne Huang
- 057 Hacking and Protecting Oracle Database Vault**
Esteban Martínez Fayó
- 066 Exploiting SCADA Systems**
Jeremy Brown
- 071 Kim Jong-il and Me: How to Build a Cyber Army to Defeat the U.S.**
Charlie Miller
- 076 Cyber[CrimelWar] Charting Dangerous Waters**
Iftach Ian Amit
- 081 The Power of Chinese Security**
Anthony Lai, Jake Appelbaum, Jon Oberheide
- 086 Wardriving the Smart Grid: Practical Approaches to Attacking Utility Packet Radios**
Shawn Moyer, Nathan Keltner
- 091 SCADA and ICS for Security Experts: How to Avoid Cyberdouchery**
James Arlen
- 096 The Night The Lights Went Out In Vegas: Demystifying Smartmeter Networks**
Barrett Weisshaar, Garret Picchioni
- 101 Cyberterrorism and the Security of the National Drinking Water Infrastructure**
John McNabb



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 2 (Disc 3)

- 106 NoSQL, No Injection !?**
Wayne Huang, Kuon Ding
- 111 An Examination of the Adequacy of the Laws Related to Cyber Warfare**
Dondi West
- 115 Industrial Cyber Security**
Wade Polk, Paul Malkewicz, J. Novak
- 117 Multiplayer Metasploit: Tag-Team Penetration and Information Gathering**
Ryan Linn
- 122 Balancing the Pwn Trade Deficit**
Val Smith, Colin Ames, Anthony Lai
- 127 Powershell...omfg**
David Kennedy (ReL1K), Josh Kelley
- 132 Build Your Own Security Operations Center for Little or No Money**
Josh Pyorre, Chris McKenney
- 137 Seccubus - Analyzing Vulnerability Assessment Data the Easy Way...**
Frank Breedijk
- 142 Toolsmithing an IDA Bridge, Case Study for Building a Reverse Engineering Tool**
Adam Pridgen, Matt Wollenweber
- 147 You Spent All That Money and You Still Got Owned...**
Joseph McCray
- 152 SHODAN for Penetration Testers**
Michael Schearer



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 3 (Disc 4)

- 006 How To Get Your FBI File (and Other Information You Want from the Federal Government)**
Marcia Hofmann
- 011 Our Instrumented Lives: Sensors, Sensors, Everywhere...**
Greg Conti
- 016 Your ISP and the Government: Best Friends Forever**
Christopher Soghoian
- 022 The Law of Laptop Search and Seizure (Video Only)**
Jennifer Granick, Kevin Bankston, Marcia Hofmann, Kurt Opsahl
- 028 Search & Seizure & Golfballs**
Jim Rennie, Eric Rachner
- 034 Exploiting Internet Surveillance Systems**
Decius
- 040 Hacking Facebook Privacy**
Chris Conley
- 046 An Observatory for the SSLiverse**
Peter Eckersley, Jesse Burns
- 052 Bad Memories**
Elie Bursztein, Baptiste Gourdin, Gustav Rydstedt, Dan Boneh
- 058 FOCA2: The FOCA Strikes Back**
Chema Alonso, José Palazón "Palako"
- 062 Big Brother on the Big Screen: Fact/Fiction?**
Nicole Ozer, Kevin Bankston
- 067 Changing Threats To Privacy: From TIA to Google**
Moxie Marlinspike
- 072 masSEXploitation**
Michael Brooks "The Rook"
- 077 This Needs to be Fixed, and Other Jokes in Commit Statements**
Bruce Potter, Logan Lodge
- 082 Trolling Reverse-Engineers with Math: Ness... It hurts...**
frank^2
- 087 pyREtic - In-memory Reverse Engineering for Obfuscated Python Bytecode**
Rich Smith
- 092 WPA Too!**
Md Sohail Ahmad



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 3 (Disc 4)

- 097 How to Hack Millions of Routers**
Craig Heffner
- 102 Hacking DOCSIS For Fun and Profit**
Blake Self, bitemytaco
- 107 Advanced Format String Attacks**
Paul Haas
- 112 Connection String Parameter Attacks**
Chema Alonso, José Palazón "Palako"
- 118 Browser Based Defenses**
James Shewmaker
- 123 Constricting the Web: Offensive Python for Web Hackers**
Nathan Hamiel, Marcin Wielgoszewski
- 128 Repelling the Wily Insider**
Matias Madou, Jacob West
- 133 The Anatomy of Drug Testing**
Jimi Fiekert
- 138 A New Approach to Forensic Methodology - !!BUSTED!! Case Studies**
David C. Smith, Samuel Petreski
- 143 Open Source Framework for Advanced Intrusion Detection Solutions**
Patrick Mullen, Ryan Pentney
- 153 Obox Analyzer: AfterDark Runtime Forensics for Automated Malware Analysis and Clustering**
Wayne Huang, Jeremy Chiu, Benson Wu



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 4 (Disc 5)

- 007 Welcome and Making the DEF CON 18 Badge**
Dark Tangent, Joe Grand
- 017 Build a Lie Detector/Beat a Lie Detector**
Rain, urbanmonkey
- 023 How Hackers Won the Zombie Apocalypse**
Dennis Brown
- 029 Build your own UAV 2.0 - Wireless Mayhem from the Heavens!**
Michael Weigand, Renderman, Mike Kershaw
- 035 Exploiting Digital Cameras**
Oren Isacson, Alfredo Ortega
- 041 VirGraffiti101: An Introduction to Virtual Graffiti**
Tottenkoph
- 047 DCFluX in: Moon-Bouncer**
Matt Krick
- 053 Weaponizing Lady GaGa, Psychosonic Attacks**
Brad Smith
- 059 Getting Root: Remote Viewing, Non-Local Consciousness, Big Picture Hacking, and Knowing Who You Are (Video Only)**
Richard Thieme
- 063 Live Fire Exercise: Baltic Cyber Shield 2010**
Kenneth Geers
- 068 Extreme-Range RFID Tracking**
Chris Paget
- 073 Jackpotting Automated Teller Machines Redux**
Barnaby Jack
- RE3 Jackpotting Automated Teller Machines Redux**
Barnaby Jack
- 078 Insecurity Engineering of Physical Security Systems: Locks, Lies, and Videotape**
Marc Weber Tobias, Tobias Bluzmanis, Matt Fiddler
- 083 Bypassing Smart-Card Authentication and Blocking Debiting: Vulnerabilities in Atmel Cryptomemory-Based Stored-Value Systems**
Jonathan Lee, Neil Pahl
- 088 We Don't Need No Stinkin' Badges: Hacking Electronic Door Access Controllers**
Shawn Merdinger



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 4 (Disc 5)

- 093 Physical Security : You're Doing It Wrong!**
A.P. Delchi
- 098 Deceiving the Heavens to Cross the Sea: Using the 36 Stratagems for Social Engineering**
Jayson E. Street
- 103 Physical Computing, Virtual Security: Adding the Arduino Microcontroller Development Environment to Your Security Toolbox**
Leigh Honeywell, follower
- 108 Hacking with Hardware: Introducing the Universal RF Usb Keyboard Emulation Device - URFUKED**
Monta Elkins
- 113 Programmable HID USB Keystroke Dongle: Using the Teensy as a Pen Testing Device**
Adrian Crenshaw
- 119 Web Services We Just Don't Need**
Mike "mckt" Bailey
- 124 IPv6: No Longer Optional**
John Curran
- 129 Exploitation on ARM - Technique and Bypassing Defense Mechanisms**
Itzhak "zuk" Avraham
- 134 Implementing IPv6 at ARIN**
Matt Ryanczak
- 139 Breaking Bluetooth by Being Bored**
JP Dunning
- 144 SMART Project: Applying Reliability Metrics to Security Vulnerabilities**
Blake Self, Wayne Zage, Dolores Zage
- 149 ExploitSpotting: Locating Vulnerabilities Out of Vendor Patches Automatically**
Jeongwook Oh
- 154 Function Hooking for Mac OSX and Linux**
Joe Damato



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 5 (Disc 6)

- 008 oCTF: 5 years in 50 minutes**
Panel
- 012 Open Public Sensors and Trend Monitoring**
Daniel Burroughs
- 013 FOE, The Release of Feed Over Email, a Solution to Feed Controversial News to Censored Countries**
Sho Ho
- 018 Google Toolbar: The NARC Within**
Jeff Bryner
- 019 Crawling BitTorrent DHTs for Fun**
Scott Wolchok
- 024 Who Cares About IPv6?**
Sam Bowne
- 025 Operating System Fingerprinting for Virtual Machines (Video Only)**
Nguyen Anh Quynh
- 030 Web Application Fingerprinting with Static Files**
Patrick Thomas
- 036 Air Traffic Control Insecurity 2.0**
Righter Kunkel
- 042 Like a Boss: Attacking JBoss**
Tyler Krpata
- 043 Letting the Air Out of Tire Pressure Monitoring Systems**
Mike Metzger
- 048 Evilgrade, You Still Have Pending Upgrades?**
Francisco Amato, Federico Kirschbaum
- 049 Training the Next Generation of Hardware Hackers -- Teaching Computer Organization and Assembly Language Hands-On with Embedded Systems**
Andrew Kongs, Dr. Gerald Kane
- 054 Be a Mentor!**
Marisa Fagan
- 055 Your Boss is a Douchebag... How About You?**
Luiz "effffn" Eduardo
- 060 Antique Exploitation (aka Terminator 3.1.1 for Workgroups)**
Jon Oberheide



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 5 (Disc 6)

- 061 Pwned By The Owner: What Happens When You Steal a Hacker's Computer**
Zoz
- 069 Facial Recognition: Facts, Fiction; and Fcsk-Ups!**
Joshua Marpet
- 074 Searching for Malware: A Review of Attackers' Use of Search Engines to Lure Victims**
David Maynor, Paul Judge, PhD
- 079 Katana: Portable Multi-Boot Security Suite**
JP Dunning
- 084 From "No Way" to 0-day: Weaponizing the Unweaponizable**
Joshua Wise
- 089 Malware Migrating to Gaming Consoles: Embedded Devices, an Antivirus-Free Safe Hideout For Malware**
Ahn Ki-Chan, Ha Dong-Joo
- 094 My Life as a Spyware Developer**
Garry Pejski
- 099 Malware Freak Show 2: The Client-Side Boogaloo**
Nicholas J. Percoco, Jibran Ilyas
- 104 Hacking .Net Applications: A Dynamic Attack**
Jon McCoy
- 109 Blitzableiter - the Release**
Felix "FX" Lindner
- 114 Defcon Security Jam III: Now in 3-D?**
Panel
- 120 WiMAX Hacking 2010**
Pierce, Goldy, aSmig, sanitybit
- 125 Hardware Hacking for Software Guys**
Dave King
- 130 Electronic Weaponry or How to Rule the World While Shopping at Radio Shack**
Mage2
- 135 ChaosVPN for Playing CTFs**
mc.fly, ryd, vyrus, no_maam
- 140 The Games We Play**
Brandon Nesbit



Riviera Hotel & Casino • Las Vegas, NV
July 30th - August 1, 2010

Track 5 (Disc 6)

- 145 Kartograph : Finding a Needle in a Haystack or How to Apply Reverse Engineering Techniques to Cheat at Video Games**
Elie Bursztein, Jocelyn Lagarenne
- 150 Gaming in the Glass Safe - Games, DRM and Privacy**
Ferdinand Schober
- 155 Securing MMOs: A Security Professional's View from the Inside**
metr0