

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 1 part A

Disc 2

- T101** **Making of the DEFCON 15 Badge**
Joe Grand
- T102** **Q&A with Bruce**
Bruce Schneier
- T103** **Turn-Key Pen Test Labs**
Thomas Wilhelm
- T104** **How I Learned to Stop Fuzzing and Find More Bugs**
Jacob West
- T105** **Covert Debugging: Circumventing Software Armoring Techniques**
Danny Quist & Val Smith
- T106** **Functional Fuzzing with Funk**
Benjamin Kurtz
- T107** **Tactical Exploitation**
H.D. Moore & Val Smith
- T108** **Intelligent Debugging for vuln-dev**
Damien Gomez
- T109** **Fingerprinting and Cracking Java Obfuscated Code**
Subere
- T110** **Comparing Application Security Tools**
Edward Lee
- T111** **Meet the Feds**
Panel
- T112** **No-Tech Hacking**
Johnny Long
- T131** **The SOA/XML Threat Model and New XML/SOA/Web 2.0 Attacks & Threats**
Steve Orrin
- T133** **Pen-testing Wi-Fi**
Aaron Peterson
- T134** **Hacking EVDO**
King Tuna

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 1 part B

Disc 3

- T135** **Multipot: A More Potent Variant of Evil Twin**
K.N. Gopinath
- T136** **The Next Wireless Frontier - TV White Spaces**
Doug Mohny
- T137** **Creating Unreliable Systems, Attacking the Systems that Attack You**
Sysmin & Marklar
- T138** **GeoLocation of Wireless Access Points and "Wireless GeoCaching"**
Ricky Hill
- T139** **Being in the Know... Listening to and Understanding Modern Radio Systems**
Brett Neilson
- T140** **The Emperor Has No Cloak - WEP Cloaking Exposed**
Vivek Ramachandran
- T141** **Hardware Hacking for Software Geeks**
nosequitor & Ab3nd
- T142** **The Church of WiFi Presents: Hacking Iraq**
Michael Schearer
- T161** **HoneyJax (AKA Web Security Monitoring and Intelligence 2.0)**
Dan Hubbard
- T162** **Hacking Social Lives: MySpace.com**
Rick Deacon
- T163** **The Inherent Insecurity of Widgets and Gadget**
Aviv Raff & Iftach Ian Amit
- T164** **Greater than 1: Defeating "Strong" Authentication in Web Applications**
Brendan O'Connor
- T165** **Intranet Invasion With Anti-DNS Pinning**
David Byrne
- T166** **Biting the Hand that Feeds You - Storing and Serving Malicious Content
From Well Known Web Servers**
Billy Rios & Nathan McFeters

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 2 part A

Disc 4

- T201** **Church Of WiFi's Wireless Extravaganza**
Church Of WiFi's
- T202** **SQL Injection and Out-of-Band Channeling**
Patrik Karlsson
- T203** **Z-Phone**
Philip Zimmermann
- T204** **OpenBSD Remote Exploit and Another IPv6 Vulnerabilities**
Alfredo Ortega
- T205** **MQ Jumping**
Martyn Ruks
- T206** **Virtual World, Real Hacking**
Greg Hoglund
- T207** **It's All About the Timing**
Haroon Meer & Marco Slaviero
- T208** **Revolutionizing the Field of Grey-box Attack Surface Testing with Evolutionary Fuzzing**
Jared DeMott, Dr. Richard Enbody & Dr. Bill Punch
- T209** **How Smart is Intelligent Fuzzing - or - How Stupid is Dumb Fuzzing?**
Charlie Miller
- T210** **INTERSTATE: A Stateful Protocol Fuzzer for SIP**
Ian G. Harris
- T211** **One Token to Rule Them All**
Luke Jennings
- T212** **Trojans: A Reality Check**
Toralv Dirro & Dirk Kollberg
- T231** **Multiplatform Malware Within the .NET-Framework**
Paul Ziegler
- T232** **Malware Secrets**
Valsmith & Delchi
- T233** **44 Lines About 22 Things That Keep Me Up at Night**
Agent X
- T234** **Click Fraud Detection with Practical Memetics**
Broward Horne

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 2 part B

Disc 5

- T235** **Fighting Malware on your Own**
Vitaliy Kamlyuk
- T236** **Virtualization: Enough Holes to Work Vegas**
D.J.Capelis
- T237** **Homeless Vikings, (Short-Lived bgp Prefix Hijacking and the Spamwars)**
Dave Josephsen
- T238** **Webserver Botnets**
Gadi Evron
- T239** **The Commercial Malware Industry**
Peter Gutmann
- T240** **CaffeineMonkey: Automated Collection, Detection and Analysis of Malicious JavaScript**
Daniel Peck & Ben Feinstein
- T241** **Greetz from Room 101**
Kenneth Geers
- T242** **Estonia and Information Warfare**
Gadi Evron
- T261** **The Completion Backward Principle**
geoffrey
- T262** **Boomstick Fu: The Fundamentals of Physical Security at its Most Basic Level**
Deviant Ollam, Noid, Thorn, Jur1st
- T263** **Locksport: An Emerging Subculture**
Schuyler Towne
- T264** **Satellite Imagery Analysis**
Greg Conti
- T265** **High Insecurity: Locks, Lies, and Liability**
Marc Weber Tobias & Matt Fiddler

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 3 part A

Disc 6

- T301** **Analyzing Intrusions & Intruders**
Sean Bodmer
- T302** **Aliens Cloned My Sheep**
Major Malfunction
- T303** **Breaking Forensics Software**
Chris Palmer & Alex Stamos
- T304** **Re-Animating Drives & Advanced Data Recovery**
Scott Moulton
- T305** **Cool Stuff Learned from Competing in the DC3 Digital Forensic Challenge**
David C. Smith
- T306** **Windows Vista Log Forensics**
Rich Murphey
- T307** **When Tapes Go Missing**
Robert Stoudt
- T308** **CiscoGate**
The Dark Tangent
- T309** **Hacking UFOlogy: Thirty Years in the Wilderness of Mirrors**
Richard Thieme
- T311** **Hack Your Car for Boost and Power!**
Aaron Higbee
- T312** **The Executable Image Exploit**
Michael Schrenk
- T331** **A Crazy Toaster: Can Home Devices Turn Against Us?**
Dror Shalev
- T332** **IPv6 is Bad for Your Privacy**
Janne Lindqvist
- T333** **Injecting RDS-TMC Traffic Information Signals a.k.a. How to freak out your Satellite Navigation**
Andrea Barisani

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 3 part B

Disc 7

- T335** **Unraveling SCADA Protocols: Using Sulley Fuzzer**
Ganesh Devarajan
- T336** **Hacking the Extensible Firmware Interface**
John Heasman
- T337** **Hacking your Access Control Reader**
Zac Franken
- T338** **Security by Politics - Why it Will Never Work**
Lukas Grunwald
- T339** **Kernel Wars**
Joel Eriksson, Karl Janmar, Claes Nyberg, Christer Öberg
- T340** **(un)Smashing the Stack: Overflows, Counter-Measures, and the Real World**
Shawn Moyer
- T341** **Remedial Heap Overflows: dmalloc styl**
atlas
- T342** **Thinking Outside the Console (box)**
Squidly1
- T361** **Hacking the EULA: Reverse Benchmarking Web Application Security Scanners**
Tom Stracener & Marce Luck
- T362** **Network Mathematics: Why is it a Small World?**
Oskar Sandberg
- T363** **Beyond Vulnerability Scanning - Extrusion and Exploitability Scanning**
Matt Richard
- T364** **LAN Protocol Attacks Part 1 - Arp Reloaded**
Jesse D'Aguanno
- T365** **Entropy-Based Data Organization Tricks for Log and Packet Capture Browsing**
Sergey Bratus
- T366** **Securing Linux Applications With AppArmor**
Crispin Cowan

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 4 part A

Disc 8

- T401** **Disclosure and Intellectual Property Law: Case Studies**
Jennifer Granick
- T402** **Computer and Internet Security Law - A Year in Review 2006 - 2007**
Robert Clark
- T403** **Picking up the Zero Day; An Everyones Guide to Unexpected Disclosures**
Dead Addict
- T404** **Everything you ever wanted to know about Police Procedure in 50 Minutes.**
Steve Dunker
- T405** **Bridging the Gap Between Technology and the Law**
John Benson
- T406** **Protecting Your IT Infrastructure From Legal Attacks- Subpoenas, Warrants and Transitive Trust**
Alexander Muentz
- T407** **Digital Rights Worldwide: Or How to Build a Global Hacker Conspiracy**
Danny O'Brien
- T408** **A Journalist's Perspective on Security Research**
Peter Berghammer
- T409** **Teaching Hacking at College**
Sam Bowne
- T410** **Faster PwninG Assured: New adventures with FPGAs**
David Hulton
- T411** **Ask the EFF**
Panel
- T431** **The Market for Malware**
Thomas Holt
- T433** **Routing in The Dark: Pitch Black**
Nathan Evans & Christian Grothoff

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 4 part B

Disc 9

- T434** **Technical Changes Since You Last Heard About Tor**
Nick Mathewson
- T435** **Social Attacks on Anonymity Networks**
Nick Mathewson
- T436** **Tor and Blocking- Resistance**
Roger Dingledine
- T438** **Saving The Internet With Hate**
Zed Shaw
- T439** **Securing the Tor Network**
Mike Perry
- T441** **Portable Privacy**
Steve Topletz
- T442** **Real-time Steganography with RTP**
}}ruid

DEFCON15

August 3-5, 2007 | The Riviera | Las Vegas, NV

[Track 1](#) | [Track 2](#) | [Track 3](#) | [Track 4](#) | [Track 5](#)

Track 5

Disc 10

- T501** **Vulnerabilities and The Information Assurance Directorate**
Tony Sager
- T502** **Meet The VCs**
Panel
- T503** **Anti Spyware Coalition**
Panel
- T504** **Disclosure Panel**
Panel
- T505** **Dirty Secrets of the Security Industry**
Bruce Potter
- T506** **Self Publishing in the Underground**
Myles Long, Rob "Flack" O'Hara, & Christian "RaDMan" Wirth
- T507** **The Hacker Society Around the (Corporate) World**
Luiz Eduardo
- T508** **Creating and Managing Your Security Career**
Mike Murray & Lee Kushner
- T509** **kNAC!**
Ofir Arkin
- T531** **Hack Your Brain with Video Games**
NeOnRa1n & Joe Grant
- T532** **How to be a WiFi Ninja**
Pilgrim
- T534** **The Science of Social Engineering: NLP, Hypnosis and the Science of Persuasion**
Mike Murray & Anton Chuvakin
- T535** **Black Ops 2007: Design Reviewing The Web**
Dan Kaminsky
- T536** **The Edge of Forever - Making Computer History**
Jason Scott
- T538** **Stealing Identity Management Systems**
Plet
- T539** **Internet Wars 2007**
Panel