

ToorCon Final Lineup Announcement

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2007-09/msg00141.html>

- *From:* "David Hulton" <h1kari@xxxxxxxxxxx>
 - *Date:* Thu, 20 Sep 2007 16:07:31 -0700
-

Hey guys,

Just thought I'd shoot out a quick shameless plug for ToorCon and mention that we've published our full speaker lineup and have finalized our Seminars and Workshops schedule. We will be increasing the registration prices on Sunday, September 23rd so if you're interested in coming out, make sure you register before then or you'll be stuck paying extra later. More information about ToorCon this year can be found at <http://www.toorcon.org>.

WORKSHOPS – Thu, Oct 18th – \$900

NEW – Penetrating the Epoxy Curtain: Hands-On Silicon Hacking
Instructors: Bunnie & Christopher Tarnovsky
Availability: 9 seats left

I'm really excited about this workshop. It'll involve dissecting a stored value smart card die and reverse engineering the transistors to determine what the different parts of the chip do and by the end of the course be able to circumvent some of the card's hardware access controls. We're gearing this workshop towards software reverse engineers that want to learn more about how the hardware ticks and get a better understanding for how things are implemented at the even lower levels. People attending this course will receive decaped parts, large format prints of the die, flash drives with high-resolution pictures of the die, and hands-on access to chip reverse engineering equipment.

Building/Hacking Open Source Embedded Wireless Routers
Instructor: Ken Caruso & Matt Westervelt
Availability: 9 seats left

This workshop is setup to teach people how to deploy real-world large scale wireless networks using open source hardware and software. People attending this class will receive a free Soekris access point setup and will get all of the software pre-packaged to readily boot it up and run any of the standard mesh-networking protocols. This workshop is run by the guys that run the Seattle Wireless community

ToorCon Final Lineup Announcement

network and have extensive experience with setting up wireless networks all around the world.

Crash Course in Penetration Testing

Instructor: Joseph McCray

Availability: 5 seats left

This workshop has received a lot of attention recently and is filling up quick. The premise behind this workshop is that the first half of the class teaches the basics of penetration testing and the second half involves running wild on a rootwars network setup in the classroom and learning techniques with hands-on exercises. People attending this workshop will leave with a 250GB 2.5" harddrive filled with vmware images of challenge VMs and an attack VM pre-loaded with all of the basic hacking tools needed to start playing. The goal is that after people leave the class they'll be able to continue developing their skills by completing further challenge levels in the rootwars VMs.

All of these workshops are taking place at the Hotel Solamar in Downtown San Diego on Thursday, October 18th. Workshop admission is currently \$900 which includes entrance to the general ToorCon conference and we're offering a discount for people who wish to also attend our Seminars on Friday, October 19th for only \$1100, a \$300 savings!

SEMINARS – Fri, Oct 19th – \$500

- Gabriel Lawrence, Linux Kernel Rootkit Detection and Analysis during Incident Response
- Andre Gironda, Continuous Prevention Testing
- Rodney Thayer, Crypto Boot Camp: You have to become an enterprise crypto expert and you only have time to attend a 2 hour seminar
- Crispin Cowan, AppArmor Profile Sharing Portal
- Charles Miller, Real World Fuzzing

CONFERENCE – Fri, Oct 19th to Sun, Oct 21st – \$70

- Dan Kaminsky, Black Ops 2007: Design Reviewing the Web
- Charles Miller, Fuzzing with Code Coverage by Example
- Remorse, Textella: An Alternative Application of Peer to Peer Structured Networks
- Matt Miller, Cthulhu: A software analysis framework built on Phoenix
- Scott Moulton, Advanced Hacking Flash/Hard Drive Recoveries
- Jerome Athias, Speeding up the exploits' development process
- Richard Johnson, AutoHacking with Phoenix Enabled Data Flow Analysis
- Travis Goodspeed, Exploiting Wireless Sensor Networks over 802.15.4
- Brandon Enright, Exposing Stormworm

ToorCon Final Lineup Announcement

- Jason Medeiros, The Last Stand: 100% Automatic Oday, Achieved, Explained, and Demonstrated.
- Alexander Lash, CDMA Unlocking and Modification
- Kevin Bauer, Damon McCoy, BitBlender: Providing Lightweight Anonymity for BitTorrent
- Jason Ostrom, John Kindervag, VoIP Penetration Testing: Lessons Learned, Tools and Techniques
- Deviant Ollam, Beating Back the Physical Security Boogeyman: How to Stop Fearing Things That Go Bump in the Night
- Nathan Rittenhouse, Byakugan: Automating Exploitation
- Richard Rushing, Hotspot Analysis: Looking at Hotspots with a Magnifying Glass
- Paul Battista, Matt Fisher, New SQL Injection Tricks
- datagram, Live Memory Forensics
- Sachin Joglekar, Nick Kezhaya, Attacking VoIP to gain control of a laptop
- Sam Bowne, Teaching Hacking at College
- Druid, Context-keyed Payload Encoding
- asm, Social Data Mining Through Telephony Vulnerabilities
- Brenda Larcom, Privilege-Centric Security Analysis
- Zax, Using Type Systems to Reduce your Security Risks
- Billy Rios, Nathan McFeters, Rob Carter, URI Use and Abuse
- Tom Stracener, Hacking the EULA: Reverse Benchmarking Web Applications
- Vivek Ramachandran, Md Sohail Ahmad, Cafe Latte with a Free Topping of Cracked WEP: Retrieving WEP Keys From Road-Warriors
- Robert Bird, Techniques for Exploiting Anomaly Detection Systems
- Dan Griffin, Hacking Windows Vista Security
- Christopher Abad, Post-Scarcity
- Blake Hartstein, Matt Richard, Extrusion and Exploitability Scanning
- Rodney Thayer, Does the security press suck? Panel
- Zane Lackey, vnak (VoIP Network Attack Kit): a grand unified VoIP attack tool for H.323, IAX, and SIP

Thanks,
–h1kari

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution FREE today!

<http://www.cenzic.com/downloads>
