

## SynchVue® DVD-ROM

View slides and demos "synched" with speaker video of all recorded sessions

	On-Site	Post-Con
<input type="checkbox"/> <b>Black Hat USA 2013/ DEF CON 21 Combo</b>	<b>\$499</b> (+ s/h)	<b>\$899</b> (+ s/h)
<input type="checkbox"/> <b>Black Hat USA 2013 Only</b>	<b>\$399</b> (+ s/h)	<b>\$499</b> (+ s/h)



## SelectVue DVD® Set

Features recorded sessions on Individual DVD Videos with Multiple Viewing angles:  
**Slides Only, Speaker Only, or Slides And Speaker**

	On-Site	Post-Con
<input type="checkbox"/> <b>Black Hat USA 2013/ DEF CON 21 Combo</b>	<b>\$1999</b> (+ s/h)	<b>\$2499</b> (+ s/h)
<input type="checkbox"/> <b>Black Hat USA 2013 Only</b>	<b>\$1299</b> (+ s/h)	<b>\$1699</b> (+ s/h)



**Enterprise License** **Add \$200\***

Provide access and/or post the SynchVue® media files within your organization

\*Black Hat USA 2013 Only. Other Restrictions May Apply. Request copy for details.



**FREE DOMESTIC SHIPPING**  
On-Site Cash Orders Only

**Please visit our Sales Desk located in Palace Pre-Function 1**

### HOW TO ORDER

**ON-SITE** Bring this form with payment and shipping information to the Sales Desk  
**EMAIL** sales@sok-media.com  
**PHONE** (858) 635-5969 7am-4pm (PST) Mon-Fri  
**FAX** (858) 635-5974 24 hours; 7 days/week

**WEB** www.tsok.net/BHB13/index.html  
**MAIL** Send completed form and payment to Source of Knowledge  
7636 Miramar Road, Suite 1400  
San Diego, CA 92126 USA  
**QR-CODE** Scan with a QR-Code Reader

Scan & Order Online



### SHIPPING AND HANDLING COSTS

All U.S. orders shipped priority mail  
Orders outside the U.S. shipped via trackable carrier  
**\$10 PER ORDER** WITHIN U.S. and U.S. TERRITORIES  
**\$25 PER ORDER** MEXICO or CANADA  
**\$60 PER ORDER** ALL OTHER COUNTRIES

### PLEASE PROVIDE BUSINESS CARD OR COMPLETE FORM

NAME: \_\_\_\_\_  
COMPANY: \_\_\_\_\_  
STREET (NO INT'L PO BOX): \_\_\_\_\_  
CITY: \_\_\_\_\_ ST: \_\_\_\_\_ ZIP: \_\_\_\_\_  
COUNTRY: \_\_\_\_\_  
TEL: (\_\_\_\_\_) \_\_\_\_\_  
EMAIL: \_\_\_\_\_  
 Yes! I would like to receive emails about available industry related recordings

VISA  MASTERCARD  AMEX  DISCOVER

Signature: \_\_\_\_\_

--	--

EXP. DATE \_\_\_\_\_ CREDIT CARD OR P.O. NUMBER \_\_\_\_\_

CV CODE \_\_\_\_\_ AMOUNT FOR DVD-ROM \$ \_\_\_\_\_

SALES TAX (8.0%) CALIFORNIA DELIVERED ONLY \$ \_\_\_\_\_

SHIPPING & HANDLING (\*SEE COSTS ABOVE) \$ \_\_\_\_\_

**ALL SALES ARE FINAL!** TOTAL AMOUNT \$ \_\_\_\_\_

The sessions are being recorded at Black Hat USA 2013. The recordings are professional, unedited, live recordings that are guaranteed for life.  
**PLEASE NOTE: Recording options may change. Some sessions may be omitted due to speaker or program revisions.**

# BLACK HAT USA 2013 RECORDED SESSIONS

## AWARDS

A01 **PWNIE AWARDS**

## KEYNOTES

K01 **Welcome & Introduction to Black Hat USA 2013 / Keynote Speaker: General Keith B. Alexander**  
General Keith B. Alexander

K02 **KEYNOTE SPEAKER: BRIAN MUIRHEAD**  
Brian Muirhead

## TRACK 1

- T101 **Mainframes: The Past Will Come to Haunt You**  
Philip Young
- T102 **Black-box Assessment of Pseudorandom Algorithms**  
Derek Soeder + Christopher Abad + Gabriel Acevedo
- T103 **End-to-end Analysis of Domain Generating Algorithm Malware Family**  
Jason Geffner
- T104 **Javascript Static Security Analysis Made Easy with JSPrime**  
Nishant Das Patnaik + Sarathi Sabyasachi Sahoo
- T105 **The Web IS Vulnerable: XSS Defense on the BattleFront**  
Greg Wroblewski + Ryan Barnett
- T106 **Malicious File for Exploiting Forensic Software**  
Takahiro Haruyama + Hiroshi Suzuki
- T107 **CMX: IEEE Clean File Metadata Exchange**  
Mark Kennedy + Igor Muttik
- T108 **Mobile Malware: Why the Traditional AV Paradigm is Doomed**  
Guy Stewart
- T109 **Bochspwn: Identifying 0-Days via System-Wide Memory Access Pattern Analysis**  
Mateusz 'j00ru' Jurczyk + Gynvael Coldwind
- T110 **Using Online Activity as Digital DNA to Create a Better Spear Phisher**  
Joaquim Espinhara + Ulisses Albuquerque
- T111 **CreepyDOL: Cheap, Distributed Stalking**  
Brendan O'Connor
- T112 **OptiROP: The Art of Hunting ROP Gadgets**  
Nguyen Anh Quynh + Eric Forner

## TRACK 2

- T201 **BlackberryOS 10 From a Security Perspective**  
Ralf-Philipp Weinmann
- T202 **Shattering Illusions in Lock-Free Worlds: Compiler/Hardware Behaviors in OSeS and VMs**  
Marc Blanchou
- T203 **Password Hashing: The Future is Now**  
Jean-Philippe Aumasson
- T204 **Pass the Hash and other credential theft and reuse: Preventing Lateral Movement and Privilege Escalation**  
Mark Simos + Patrick Jungles
- T205 **How to grow a TREE (Taint-Enabled Reverse Engineering Environment) from a CBASS (Cross-platform Binary Automated Symbolic-execution System)**  
Nathan Li + Loc Nguyen + Xing Li + James Just
- T206 **Predicting Susceptibility to Socialbots on Twitter**  
Chris Sumner + Randall Wald
- T207 **Pass-the-Hash 2: The Admin's Revenge**  
Chris Campbell + Skip Duckwall
- T208 **Energy Fraud and Orchestrated Blackouts: Issues with Wireless Metering Protocols (wM-Bus)**  
Cyrill Brunschwiler
- T209 **Hot Knives Through Butter: Bypassing Automated Analysis Systems**  
Abhishek Singh + Zheng Bu
- T210 **Post Exploitation Operations with Cloud Synchronization**  
Jake Williams
- T211 **Defending Networks With Incomplete Information: A Machine Learning Approach**  
Alexandre Pinto

## TRACK 3

- T301 **With BIGDATA comes BIG responsibility: Practical exploiting of MDX injections**  
Dmitry Chastuhin + Alexander Bolshev
- T302 **Power Analysis Attacks for CheapSkates**  
Colin O'Flynn
- T303 **Fact and Fiction: Defending Medical Devices**  
Jay Radcliffe
- T304 **Maltego Tungsten As a Collaborative Attack Platform**  
Roelof Temmingh + Andrew MacPherson
- T305 **BinaryPig - Scalable Malware Analytics in Hadoop**  
Zachary Hanif + Telvis Calhoun + Jason Trost
- T306 **Abusing Web APIs Through Scripted Android Applications**  
Daniel Peck
- T307 **Big Data for Web Application Security**  
Mike Arpaia + Kyle Barry
- T308 **Dissecting CSRF Attacks and Countermeasures**  
Mike Shema + Sergey Shekhan + Vaagn Toukharian
- T309 **Above My Pay Grade: Cyber Response at the National Level**  
Jason Healey
- T310 **Virtual Deobfuscator - A DARPA Cyber Fast Track Funded Effort**  
Jason Raber
- T311 **Teridian SoC Exploitation: Exploration of Harvard Architecture Smart Grid Systems**  
Josh 'm0nk' Thomas + Nathan Keltner

## TRACK 4

- T401 **New Trends in FastFlux Networks**  
Wei Xu + Xinran Wang
- T402 **CrowdSource: An Open Source, Crowd Trained Machine Learning Model for Malware Detection**  
Joshua Saxe
- T403 **Denying Service to DDoS Protection Services**  
Allison Nixon
- T404 **Denial of Service as a Service - Asymmetrical Warfare at its Finest**  
Robert Masse
- T405 **Universal DDoS Mitigation Bypass**  
Tony Miu + Albert Hui + Wai Leng Lee
- T406 **Untwining Twine**  
Jon Chittenden + Anson Gomes
- T407 **LTE Booms with Vulnerabilities**  
Ankit Gupta
- T408 **Smashing the Font Scaler Engine in Windows Kernel**  
Ling Chuan Lee + Lee Yee Chan
- T409 **The SCADA That Didn't Cry Wolf - Who's Really Attacking Your ICS Devices - Part Deux!**  
Kyle Wilhoit
- T410 **Hunting the Shadows: In-Depth Analysis of Escalated APT Attacks**  
Fyodor Yarochki + Jeremy 'Birdman' Chiu + Tsung Pei Kan + Benson Wu
- T411 **' ) UNION SELECT `This\_Talk` AS ('New Optimization and Obfuscation Techniques')%00**  
Roberto Salgado
- T412 **Is that a Government in Your Network or are you Just Happy to See Me?**  
Eric Fiterman
- T413 **Bugalyze.com - Detecting bugs using decompilation and data flow analysis**  
Silvio Cesare

# BLACK HAT USA 2013 RECORDED SESSIONS (continued)

## TRACK 5

- T501 Lessons from Surviving a 300Gbps Denial of Service Attack**  
Matthew Prince
- T502 What Security Researchers Need to Know About Anti-Hacking Law**  
Marcia Hofmann
- T503 Legal Aspects of Full-spectrum Computer Network (Active) Defense**  
Robert Clark
- T504 A Practical Attack Against MDM Solutions**  
Daniel Brodie + Michael Shaulov
- T505 Pixel-Perfect Timing Attacks with HTML5**  
Paul Stone
- T506 Mobile Rootkits: Exploiting and Rootkitting ARM TrustZone**  
Thomas Roth
- T507 The Outer Limits: Hacking The Samsung Smart TV**  
Aaron Grattafiori + Josh Yavor
- T508 Out of Control: Demonstrating SCADA Device Exploitation**  
Brian Meixell
- T509 Compromising Industrial Facilities from 40 Miles Away**  
Lucas Apa + Carlos Panagos
- T510 Hacking Like in the Movies: Visualizing Page Tables for Local Exploitation**  
Georg 'Oxiff' Wicherski + Alexandru Radocea

## TRACK 6

- T601 Combating the Insider Threat at the FBI: Real-world Lessons Learned**  
Patrick Reidy
- T602 Just-In-Time Code Reuse: The More Things Change, the More They Stay the Same**  
Kevin Snow + Lucas Davi
- T603 BIOS Security**  
John Butterworth + Corey Kallenberg + Xeno Kovah
- T604 TOR... ALL-THE-THINGS!**  
Jason Geffner
- T605 Truncating TLS Connections to Violate Beliefs in Web Applications**  
Ben Smyth + Alfredo Pironti
- T606 Rooting SIM Cards**  
Karsten Nohl
- T607 Fully Arbitrary 802.3 Packet Injection: Maximizing Ethernet Attack Surface**  
Andrea Barisani + Daniele Bianco
- T608 Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions**  
Andy Davis
- T609 Funderbolt: Adventures in Thunderbolt DMA Attacks**  
Russ Sevinsky
- T610 RFID Hacking: Live Free or RFID Hard**  
Fran Brown
- T611 Home Invasion v2.0 - Attacking Network-Controlled Hardware**  
Daniel Crowley + David Bryan + Jennifer Savage

## TRACK 7

- T701 Beyond the Application: Cellular Privacy Regulatory Space**  
Christie Dudley
- T702 Legal Considerations for Cellular Research**  
Marcia Hofmann
- T703 A Tale of One Software Bypass of Windows 8 Secure Boot**  
Yuriy Bulygin + Oleksandr Bazhaniuk + Andrew Furtak
- T704 I Can Hear You Now: Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell**  
Tom Ritter + Doug DePerry + Andrew Rahimi
- T705 Buying into the Bias: Why Vulnerability Statistics Suck**  
Jericho + Steve Christey
- T706 How CVSS is DOSSing Your Patching Policy (and wasting your money)**  
Luca Allodi + Fabio Massacci

## TRACK 7 continued

- T707 Bluetooth Smart: The Good, the Bad, the Ugly, and the Fix!**  
Mike Ryan
- T708 UART THOU MAD?**  
Toby Kohlenberg + Mickey Shkatov
- T709 Press ROOT to Continue: Detecting OSX and Windows Bootkits with RDFU**  
Mario Vuksan + Tomislav Pericin
- T710 SSL, Gone in 30 Seconds - A BREACH beyond CRIME**  
Angelo Prado + Neal Harris + Yoel Gluck
- T711 Multiplexed Wired Attack Surfaces**  
Michael Ossmann + Kyle 'Kos' Osborn

## TRACK 8

- T801 Java Every-Days: Exploiting Software Running on Three Billion Devices**  
Brian Gorenc + Jasiel Spelman
- T802 TLS 'SECRETS'**  
Florent 'NextGen\$' Daigniere
- T803 Lawful Access Panel**  
TBA
- T804 Clickjacking Revisted: A Perceptual View of UI Security**  
Devdatta Akhawe
- T805 OPSEC Failures of Spies**  
Matthew Cole
- T806 Hiding @ Depth - Exploring, Subverting, and Breaking NAND Flash Memory**  
Josh 'm0nk' Thomas
- T807 Honey, I'm Home!! - Hacking Z-Wave Home Automation Systems**  
Behrang Fouladi + Sahand Ghanoun
- T808 Android: One Root to Own them All**  
Jeff Forristal
- T809 What's on the Wire? - Physical Layer Tapping with Project Daisho**  
Dominic Spill + Michael Ossmann + Michael 'Dragon' Kershaw
- T810 Exploiting Network Surveillance Cameras Like a Hollywood Hacker**  
Craig Heffner
- T811 Owning the Routing Table - Part II**  
Gabi Nakibly

## TRACK 9

- T901 How to Build a SpyPhone**  
Kevin McNamee
- T902 Million Browser Botnet**  
Jeremiah Grossman + Matt Johansen
- T903 Evading Deep Inspection for Fun and Shell**  
Opi Niemi + Antti Levomäki
- T904 Let's Get Physical: Breaking Home Security Systems and Bypassing Building Controls**  
Drew Porter + Stephen Smith
- T905 Mactans: Injecting Malware Into iOS Devices via Malicious Chargers**  
Billy Lau + Yeongjin Jang + Chengyu Song
- T906 The Factoring Dead: Preparing for Cyptopocalypse**  
Alex Stamos + Thomas Ptacek + Tom Ritter + Javed Samuel
- T907 Stepping p3wns: Adventures in Full Spectrum Embedded Exploitation**  
Ang Cui + Michael Costello + Salvatore Stolfo
- T908 Implantable Medical Devices: Hacking Humans**  
Barnaby Jack
- T909 Hacking, Surveiling, and Deceiving Victims on Smart TV**  
SeungJin 'Beist' Lee
- T910 Spy-jacking the Booters**  
Brian Krebs + Lance James