



SCHEDULE / WED, JULY 25

Time	Track 1	Track 2	Track 3	Track 4
Track	Defining the Scope	Upper Layers	Lower Layers	Mobile <i>Track Chair: Vincenzo Iozzo</i>
ROOM	Augustus III + IV	Augustus I + II	Augustus V + VI	Palace I
08:00-12:00	REGISTRATION: Emperors Ballroom			
08:00-08:50	BREAKFAST: Octavius Ballroom —Sponsored by 			
08:50-09:00	Jeff Moss: Welcome & Introduction to Black Hat USA 2012: Augustus Ballroom			
09:00-10:00	Keynote Speaker: Shawn Henry: Augustus Ballroom			
10:00-10:15	Break			
10:15-11:15	Smashing the Future for Fun and Profit <i>with Jeff Moss, Adam Shostack, Marcus Ranum, Bruce Schneier</i> <i>Moderated by Jennifer Granick</i>			Advanced ARM Exploitation <i>by Stephen Ridley + Stephen Lawler</i>
11:15-11:45	Coffee Service —Sponsored by 			
11:45-12:45	Black Ops <i>by Dan Kaminsky</i>	Google Native Client: Analysis Of A Secure Browser Plugin Sandbox <i>by Chris Rohlf</i>	How The Analysis of Electrical Current Consumption of Embedded Systems Could Lead to Code Reversing? <i>by Yann Allain + Julien Moïnard</i>	Scaling Up Baseband Attacks: More (unexpected) Attack Surface <i>by Ralf-Philipp Weinmann</i>
12:45-14:15	Lunch: Forum Ballroom —Sponsored by 			
14:15-15:15	CuteCats.exe and The Arab Spring <i>by Morgan Marquis-Boire</i> The Last Gasp of the Industrial Air-Gap... <i>by Eireann Leverett</i> STIX: The Structured Threat Information eXpression <i>by Sean Barnum</i>	ModSecurity as Universal Cross-platform Web Protection Tool <i>by Greg Wroblewski + Ryan Barnett</i> HTExploit bypassing htaccess restrictions <i>by Maximiliano Soler + Matias Katz</i> libinjection: A C library for SQLi detection and generation through lexical analysis of real world attacksTurbo <i>by Nick Galbreath</i>	Looking Into the Eye of The Meter <i>by Don C. Weber</i>	Don't Stand So Close To Me: An Analysis of the NFC Attack Surface <i>by Charlie Miller</i>
15:15-15:30	Break / Booksigning with the authors of "iOS Hacker's Handbook": Palace Pre-Function			
15:30-16:30	Errata Hits Puberty: 13 Years of Chagrin <i>by Jericho</i>	PRNG: Pwning Random Number Generators (in PHP applications) <i>by George Argyros + Aggelos Kiaylas</i>	Windows 8 Heap Intervals <i>by Chris Valasek + Tarjei Mandt</i>	Probing Mobile Operator Networks <i>by Collin Mulliner</i>
16:30-17:00	Coffee Service —Sponsored by 			
17:00-18:00	The Myth of Twelve More Bytes: Security on the Post-Scarcity Internet <i>by Alex Stamos + Tom Ritter</i>	Owning Bad Guys {and Mafia} with Javascript Botnets <i>by Chema Alonso</i>	Ghost is in the Air(traffic) <i>by Andrei Costin</i>	Adventures in Bouncer Land <i>by Nicholas Percoco + Sean Schulte</i>
18:00-19:30	Reception: Octavius Ballroom —Sponsored by our Diamond, Platinum, Gold Sponsors			
18:15-19:30	PWNIE awards: Augustus III + IV			

Track 5	Track 6	Track 7	Track 8	Track 9
Defense <i>Track Chair: Shawn Moyer</i>	Breaking Things <i>Track Chair: Chris Rohlf</i>	Gnarly Problems	Applied Workshop I	Applied Workshop II
Palace II	Palace III	Romans I-IV	Florentine	Pompeian
SexyDefense: Maximizing the Home-Field Advantage <i>by Iftach Ian Amit</i>	A Stitch in Time Saves Nine: A Case of Multiple Operating System Vulnerability <i>by Rafal Wojtczuk</i>	File Disinfection Framework: Striking Back at Polymorphic Viruses <i>by Mario Vuksan + Tomislav Pericin</i>	<GHZ or Bust: Black Hat <i>by Atlas</i>	Advanced Chrome Extension Exploitation: Leveraging API Powers for The Better Evil <i>by Kyle Osborn + Krzysztof Kotowicz</i>
The Defense RESTs: Automation and APIs for Improving Security <i>by David Mortmon</i>	Exploiting The Jemalloc Memory Allocator: Owning Firefox's Heap <i>by Patroklos Argyroudis + Chariton Karamitas</i>	Confessions of a WAF Developer: Protocol-Level Evasion of Web Application Firewalls <i>by Ivan Ristic</i>	<GHZ or Bust: Black Hat <i>cont.</i>	Advanced Chrome Extension Exploitation: Leveraging API Powers for The Better Evil <i>cont.</i>
Control-Alt-Hack(TM): White Hat Hacking for Fun & Profit (A Computer Security Card Game) <i>by Tadayoshi Kohno + Tamara Denning + Adam Shostack</i>	The Info Leak Era on Software Exploitation <i>by Fermin J. Serna</i>	Torturing OpenSSL <i>by Valeria Bertacco</i>	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) <i>by Abraham Kang</i>	Linux Interactive Exploit Development with GDB and PEDAs <i>by Long Le</i>
Intrusion Detection Along the Kill Chain: Why your Detection System Sucks and What to Do About it <i>by John Flynn</i>	Are You My Type?-Breaking.net Sandboxes Through Serialization <i>by James Forshaw</i>	WebTracking For You <i>by Gregory Fleischer</i>	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) <i>cont.</i>	Linux Interactive Exploit Development with GDB and PEDAs <i>cont.</i>
Exploit Mitigation Improvements in Windows 8 <i>by Matt Miller + Ken Johnson</i>	PinPadPwn <i>by Nils + Rafael Dominguez Vega</i>	Here Be Backdoors: A Journey Into the Secrets of Industrial Firmware <i>by Ruben Santamarta</i>	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) <i>cont.</i>	From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems <i>by Javier Galbally</i>

SCHEDULE / THU, JULY 26

Time	Track 1	Track 2	Track 3	Track 4
Track	Big Picture	Web Apps <i>Track Chair: Nathan Hamiel</i>	Malware <i>Track Chair: Stefano Zanero</i>	Enterprise Intrigue
ROOM	Augustus III + IV	Augustus I + II	Augustus V + VI	Palace I
08:00-11:00	REGISTRATION: Emperors Ballroom			
08:00-08:50	BREAKFAST: Octavius Ballroom —Sponsored by 			
09:00-10:00	Keynote Speaker: Neal Stephenson: Augustus Ballroom			
10:00-10:15	Break / Booksigning with Neal Stephenson: Palace Pre-Function			
10:15-11:15	Trust, Security, and Society <i>by Bruce Schneier</i>	HTML5 Top 10 Threats: Stealth Attacks and Silent Exploits <i>by Shreeraj Shah</i>	A Scientific (but not academic) Study of Malware Employs Anti-Debugging, Anti-disassembly, and Anti-virtualization Technologies <i>by Rodrigo Branco</i>	Catching Insider Data Theft With Stochastic Forensics <i>by Jonathan Grier</i>
11:15-11:45	Coffee Service —Sponsored by  / Booksigning with Bruce Schneier: Palace Pre-Function			
11:45-12:45	The Christopher Columbus Rule and DHS <i>by Mark Weatherford</i>	AMF Testing Made Easy <i>by Luca Caretoni</i>	De Mysteriis Dom Jobsivs: Mac Efi Rootkits <i>by Loukas K</i>	Find Me in Your Database: An Examination of Index Security <i>by David Litchfield</i>
12:45-14:15	Lunch: Forum Ballroom —Sponsored by Microsoft			
14:15-15:15	Legal Aspects of Cyberspace Operations <i>by Robert Clark</i>	Hacking with WebSockets <i>by Sergey Shekyan + Vaagan Toukharian</i>	Dex Education: Practicing Safe Dex <i>by Timothy Strazzere</i>	Passive Bluetooth Monitoring in Scapy <i>by Ryan Holeman</i> SYNful Deceit, Stateful Subterfuge <i>by Tom Steele + Chris Patten</i> Stamp Out Hash Corruption, Crack All The Things <i>by Ryan Reynolds + Jonathan Claudius</i>
15:15-15:30	Break			
15:30-16:30	Targeted Intrusion Remediation: Lessons From The Front Lines <i>by Jim Aldridge</i>	Blended Threats and JavaScript: A Plan for Permanent Network Compromise <i>by Phil Purviance + Joshua Brashars</i>	Hardware Backdooring is Practical <i>by Jonathan Brossard</i>	Clonewise: Automated Package Clone Detection <i>by Silvio Cesare</i>
16:30-17:00	Coffee Service —Sponsored by 			
17:00-18:00	Hacking the Corporate Mind: Using Social Engineering Tactics to Improve Organizational Security Acceptance <i>by James Philput</i>	State of Web Exploit Toolkits <i>by Jason Jones</i>	Flowers for Automated Malware Analysis <i>by Chengyu Song + Paul Royal</i>	SSRF VS. Business Critical Applications <i>by Alexander Polyakov + Dmitry Chastuhin</i>

Track 5	Track 6	Track 7	Track 8	Track 9
92.2% Market Share	Over the Air and In the Device	Mass Effect	Applied Workshop I	Applied Workshop II
Palace II	Palace III	Romans I-IV	Florentine	Pompeian
Exploitation of Windows 8 Metro Style Apps <i>by Sung-ting Tsai + Ming-chieh Pan</i>	iOS Security <i>by Dallas De Atley</i>	Still Passing the Hash 15 Years Later? Using the Keys to the Kingdom to Access all Your Data <i>by Alva Duckwall + Christopher Campbell</i>	Lessons of Binary Analysis <i>by Christien Rioux</i>	The Dark Art of iOS Application Hacking <i>by Jonathan Zdziarski</i>
We have you by the Gadgets <i>by Mickey Shkatov + Toby Kohlenberg</i>	iOS Kernel Heap Armageddon Revisited <i>by Stefan Esser</i>	Recent Java Exploitation Trends and Malware <i>by Jeong Wook Oh</i>	Lessons of Binary Analysis <i>cont.</i>	The Dark Art of iOS Application Hacking <i>cont.</i>
Exchanging Demands <i>by Peter Hannay</i>	When Security Gets in the Way: Tools for PenTesting Mobile Apps That Use Certificate Pinning <i>by Alban Diquet + Justine Osborne</i>	Digging Deep Into The Flash Sandboxes <i>by Paul Sabanal + Mark Vincent Yason</i>	SNSCat: What You Don't Know About Sometimes Hurts the Most <i>by Dan Gunter + Solomon Sonya</i>	Ruby for Pentesters: The Workshop <i>by Cory Scott + Michael Tracy + Timur Duehr</i>
	Embedded Device Firmware Vulnerability Hunting Using FRAK <i>by Ang Cui</i>			
	Mapping and Evolution of Android Permissions <i>by Andrew Reiter + Zach Lanier</i>			
Windows Phone 7 Internals and Exploitability <i>by Tsukasa Oi</i>	iOS Application Security Assessment and Automation: Introducing SIRA <i>by Justin Engler + Seth Law + Joshua Dubik + David Vo</i>	SQL Injection to MIPS Overflows: Rooting SOHO Routers <i>by Zachary Cutlip</i>	Mobile Network Forensics <i>with Eric Fulton</i>	Ruby for Pentesters: The Workshop <i>cont.</i>
Easy Local Windows Kernel Exploitations <i>by Cesar Cerrudo</i>	How Many Bricks does it take to crack a microcell? <i>by Mathew Rowley</i>	Hookin' Ain't Easy: BeEF Injection with MITM <i>by Steve Ocepek + Ryan Linn</i>	Mobile Network Forensics <i>cont.</i>	Ruby for Pentesters: The Workshop <i>cont.</i>