BREAKPOINT 2014: STEPPING THROUGH SECURITY

BREAKPOINT RUXCON

8th and 9th October, 2014
InterContinental Rialto, Melbourne, Australia
www.ruxconbreakpoint.com

ABOUT BREAKPOINT

www.ruxconbreakpoint.com

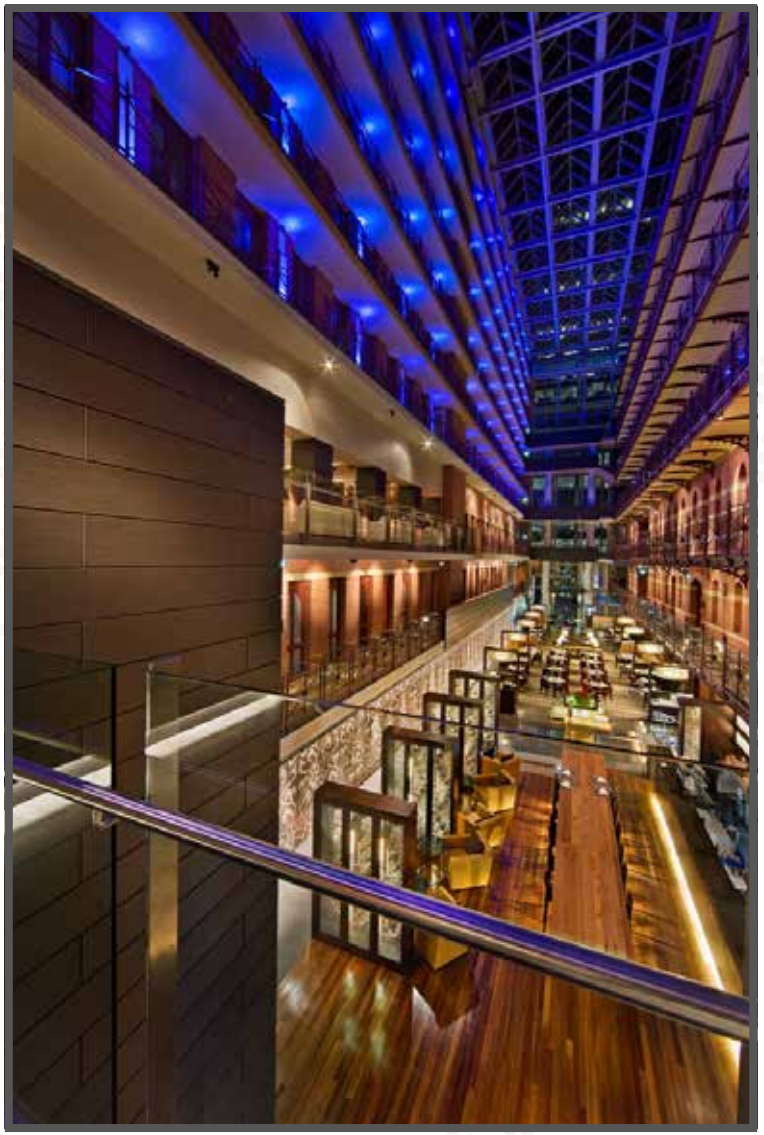
Breakpoint is Australia's leading technical IT security event.

The conference brings two days of seminars delivered by world-leading experts, along with high quality training courses not usually available in Australia. Industry leaders will provide participants with an over-the-horizon view on a full range of emerging threats facing business and government.

Breakpoint also provides a platform to engage and collaborate with a broad spectrum of like-minded industry professionals and an opportunity to gain valuable face-time with international speakers.

Breakpoint is the only security event in Australia with a large number of high calibre international speakers. Don't miss out on this unique opportunity to catch world-class experts right at your doorstep.

If you specialise in this industry then you cannot afford to miss this event.



Breakpoint is a world-class con where attendees can actually get access to the speakers. If you want to stay at the cutting edge of information security, you need to go.
Patrick Gray, Risky.biz

Visiting Breakpoint kills two birds with one stone: you can meet star presenters of overseas conferences who will talk about relevant, interesting and important (no fluff!) new research and at the same time show your boss you're being frugal by not demanding a week in Vegas for Blackhat. I will attend again this year.
Vitaly Osipov, Security Engineering Team Lead, Atlassian

WHY ATTEND?

www.ruxconbreakpoint.com

ONE

TWO

THREE

FOUR

FIVE

SIX

Learn from world class security researchers who have been carefully selected as the best and brightest in their respective fields.

Expand upon your skills and knowledge and increase your professional development. Be among the first to learn about cutting edge security techniques.

Network with a broad spectrum of delegates, develop new business opportunities, or find people to exchange ideas and experiences.

Gain exposure to new concepts which will help you to discover and deliver solutions for real-world security problems.

Engage and socialise with the speakers and delegates during discussion sessions and the networking cocktail party event.

Save on your company travel and airfare budget by attending a local conference with international quality.

The inaugural Breakpoint conference was an overall highly valuable conference that managed to fill a void in the Australasian conference agenda. The number of high calibre speakers that presented was something that had not been seen before in this area, and the organisers managed to arrange speakers across a wide range of topics. If you specialise in this industry then you cannot afford to miss the next one.

Brett Moore, Director, Insomnia Security

Topics covered at Breakpoint

- Threat Intelligence
- Mobile and Telecommunications Security
- Banking and Payment Security
- Hardware and Embedded Device Security
- Exploitation Technologies Mitigation
- Malware and Vulnerability Analysis
- Reverse Engineering and Forensics
- Data Breakches and Stolen Data Markets
- Social Engineering

Neel Mehta

Neel Mehta is a world-renowned vulnerability researcher and reverse engineer. He has discovered many high-impact bugs, including Heartbleed. Neel works at Google, where he studies state-sponsored attacks and malware. Neel is the co-author of the 'The Shellcoder's Handbook: Discovering and Exploiting Security Holes'.

TLS UNDER SIEGE - A BUG HUNTER'S PERSPECTIVE

At first glance, SSL / TLS stacks have taken a beating in 2014, some more than others. TLS stacks are evolving rapidly. Public demand for encryption is at a historical high, and understandably so. To use TLS at this scale required protocol extensions and changes, with more on the way. New features means new code, and sometimes new bugs, including Heartbleed.

From a bug hunter's perspective, I'll dissect and compare TLS stacks, with an emphasis on implementation errors (both historical and modern). I'll also examine their relative structure, feature set, and coding styles, highlighting the attack surfaces and details that matter most.

Is the discovery of implementation flaws really accelerating? Are some TLS stacks riskier than others, and why? Where are the rest of the bugs buried?

More

Stefan Esser

Stefan Esser is best known in the security community as the PHP security guy. Since he became a PHP core developer in 2002 he devoted a lot of time to PHP and PHP application vulnerability research. However in his early days he released lots of advisories about vulnerabilities in software like CVS, Samba, OpenBSD or Internet Explorer. In 2003 he was the first to boot Linux directly from the hard disk of an unmodified XBOX through a buffer overflow in the XBOX font loader. In 2004 he founded the Hardened-PHP Project to develop a more secure version of PHP, known as Hardened-PHP, which evolved into the Suhosin PHP Security System in 2006. Since 2007 he works as head of research and development for the German web application company SektionEins GmbH that he co-founded.

In 2010 and 2011 he got a lot of attention for presenting about iPhone security topics and supplying the jailbreaking scene with an exploit that survived multiple updates by Apple.

More

CONFIRMED SPEAKERS

www.ruxconbreakpoint.com/speakers

Mathew Solnik and Marc Blanchou

Mathew Solnik works in consulting and research with Accuvant LABS. Mathew's primary focus is in the mobile, M2M, and embedded space specializing in cellular network, hardware level, and OS level security. Prior to joining LABS, Mathew helped design and build an automated mobile threat and malware analysis platform for use in the Enterprise and Defense space.

CELLULAR EXPLOITATION ON A GLOBAL SCALE: THE RISE & FALL OF THE CONTROL PROTOCOL

Since the introduction of the smart phone, the issue of control has entered a new paradigm. Manufacturers and Enterprises have claimed control over not just how your phone operates, but the software that is allowed to run on it. However, few people know that Service Providers have a hidden and pervasive level of control over your device. Someone with knowledge of these controls and the right techniques could potentially leverage them for cellular exploitation on a global scale.

In this presentation, we will discuss and disclose how Over-the-Air code execution can be obtained on the major cellular platforms and networks (GSM/CDMA/LTE). Including but not limited to Android, iOS, Blackberry, and Embedded M2M Devices. You will come away from this talk armed with detailed insight into these hidden control mechanisms. We will also release open source tools to help assess and protect from the new threats this hidden attack surface presents. These tools will include the ability to dynamically test proprietary system applications and simulate different aspects of a cellular environment.

More

Brian Gorenc and Jasiel Spelman

Brian Gorenc is the Manager of Vulnerability Research in HP's Security Research organization where his primary responsibility is running the world's largest vendor-agnostic bug bounty program, the Zero Day Initiative (ZDI). He's analyzed and performed root cause analysis on hundreds of zero-day vulnerabilities submitted by ZDI researchers from around the world.

THINKING OUTSIDE THE SANDBOX - VIOLATING TRUST BOUNDARIES IN UNCOMMON WAYS

Attacking the modern browser and its plugins is becoming harder. Vendors are employing numerous mitigation technologies to increase the cost of exploit development. An attacker is now forced to uncover multiple vulnerabilities to gain privileged-level code execution on his targets. Our journey begins at the sandbox and investigates some of the more obscure techniques used to violate this trust boundary.

Our presentation will examine four bypass techniques successfully used in winning entries at this year's Pwn2Own contest. We will analyze the attack vector used, root causes, and possible fixes for each technique. These uncommon, yet highly effective, approaches have been used to bypass the most advanced application sandboxes in use today, and understanding them will provide a unique perspective for those working to find and verify such bypasses.

More

CONFIRMED SPEAKERS

www.ruxconbreakpoint.com/speakers

Joe Fitzpatrick

Joe is an Instructor, Consultant, and Researcher at SecuringHardware.com. Joe specializes in low-cost attacks, hardware tools, and hardware design for security. Previously, he spent 8 years doing test/debug and hardware pen-testing of desktop and server microprocessors, as well as conducting security validation training for hardware validators worldwide.

NSA PLAYSET: PCIE

Hardware hacks tend to focus on low-speed (jtag, uart) and external (network, usb) interfaces, and PCI Express is typically neither. After a crash course in PCIe Architecture, we'll demonstrate a handful of hacks showing how pull PCIe outside of your system case and add PCIe slots to systems without them, including embedded platforms. We'll top it off with a demonstration of SLOTSCREAMER, an inexpensive device we've configured to access memory and IO, cross-platform and transparent to the OS - all by design with no 0-day needed. The open hardware and software framework that we will release will expand your NSA Playset with the ability to tinker with DMA attacks to read memory, bypass software and hardware security measures, and directly attack other hardware devices in the system. Anyone who has installed a graphics card has all the hardware experience necessary to enjoy this talk and start playing NSA at home!

More

Mike Bond

Mike Bond is a visiting researcher at University of Cambridge where he did a PhD in computer security, specialising in the security of Hardware Security Modules and banking systems. He currently works full time in industry for Cryptomathic Ltd, a supplier of authentication and security software for banks, including for EMV card issuance and authorisation.

EMV SECURITY: CLONING, SKIMMING & SHIMMING - A PRACTICAL GUIDE TO ATTACK & DEFENCE

EMV is the world's most widely deployed payment framework, and is a growing target for fraud. The speaker reviews the important attacks on EMV found in the last ten years, describes his own research on skimming cards with the pre-play attack, and using chip cards without PINs. The talk discusses the economic and technical reasons for the failures and discusses how to go about detecting and fixing them in real banking systems.

More

CONFIRMED SPEAKERS

www.ruxconbreakpoint.com/speakers

Corey Kallenberg

Corey Kallenberg is a Security Researcher for The MITRE Corporation who has spent several years investigating operating system and firmware security on Intel computers. In 2013, he helped discover critical problems with current implementations of the Trusted Computing Group's "Static Root of Trust for Measurement" and co-presented this work at NoSuchCon and Black Hat USA.

EXTREME PRIVILEGE ESCALATION ON WINDOWS 8/UEFI SYSTEMS

The UEFI specification has more tightly coupled the bonds of the operating system and the platform firmware by providing the well-defined "runtime services" interface between the operating system and the firmware.

This interface is more expansive than the interface that existed in the days of conventional BIOS, which has inadvertently increased the attack surface against the platform firmware. Furthermore, Windows 8 has introduced APIs that allow accessing this UEFI interface from a userland process. Vulnerabilities in this interface can potentially allow a userland process to escalate its privileges from "ring 3" all the way up to that of the platform firmware, which includes permanently attaining control of the very-powerful System Management Mode (SMM).

This talk will disclose two of these vulnerabilities that were discovered in the Intel provided UEFI reference implementation, and detail the unusual techniques needed to successfully exploit them.

More

Dr. Thomas Holt

Dr. Thomas Holt is an Associate Professor in the School of Criminal Justice at Michigan State University specializing in cybercrime, policing, and policy. He received his Ph. D. in Criminology and Criminal Justice from the University of Missouri-Saint Louis in 2005. He has published extensively on cybercrime and cyberterror with over 35 peer-reviewed article.

STOLEN DATA MARKETS: AN ECONOMIC AND ORGANIZATIONAL ASSESSMENT

Since the TJX corporation revealed a massive data breach in 2007, incidents of mass data compromise have grabbed media attention. The substantial loss of customer data and resulting fraud have seemingly become more common, including the announcement of the Target and Neiman Marcus compromises in 2013. As a result, the social and technical sciences are increasingly examining the market for data resale which is driven in part by these data breaches.

This presentation will explore the economy and organizational composition of stolen data markets through qualitative and quantitative analyses of a sample of threads from 13 Russian and English language forums involved in the sale of stolen data. We present estimates for the costs of various forms of data, and examine the relationship between various social and market conditions and the advertised price for dumps and other financial data. The policy implications of this study for consumers, law enforcement, and security analysts will be discussed in depth.

More

HOW TO REGISTER

www.ruxconbreakpoint.com/register

Online

To register online, please visit the registration page at: www.ruxconbreakpoint.com/register

Email/Phone/Fax

Please call us on +61-407-848-737 or email us at bpx@ruxconbreakpoint.com to arrange registration.

Accepted payment methods include Visa, Mastercard, Amex and Electronic Funds Transfer.

Registration Includes

- Attendance to Breakpoint conference
- Breakpoint branded bag including program and sponsor inserts
- Breakpoint branded polo shirt
- Morning tea, lunch, and afternoon tea on Wednesday and Thursday
- Breakpoint delegate and speaker cocktail party

Fees Per Delegate All prices include GST.	Early Bird Rate (Ends July 15)	Standard Rate (Ends September 15)	Late Rate (Ends October 7)
Delegate	$1,760	$1,980	$2,310
Group Rate (6-11 delegates)	$1,584 (10% discount)	$1,782 (10% discount)	$2,079 (10% discount)
Group Rate (12 or more)	$1,496 (15% discount)	$1,683 (15% discount)	$1,963.50 (15% discount)

* Delegates must be from same organisation and registrations must be submitted together.

VENUE

The InterContinental (The Rialto)

495 Collins Street
Melbourne, Australia

Located on legendary Collins Street in the heart of the Central Business District, InterContinental Melbourne The Rialto is one of the city's leading world-class hotels. Steps away is the vibrant Southbank, the Yarra River, the ever changing Docklands, leading tourist attractions, exclusive shops and boutiques and some of the best restaurants this cosmopolitan city has to offer.

Completed in 1891 when Melbourne was the richest city in the world, the Rialto is as grand today as it was back then. The hotel's elegant rooms blend style with comfort. Beyond your guestroom, discover the outstanding Alluvial Restaurant, Rialto Bluestone Bar and Market Lane Bar.

11th – 12th October
CQ Function Centre, Melbourne

Ruxcon is a larger and more casual conference run over a weekend and can be likened to an Australian version of Defcon.

Established in 2003, Ruxcon is a conference organised by and for the Australian computer security community. It is an attempt to bring together the individual talents of the Australian scene, through live presentations, activities, and demonstrations. Ruxcon has grown to become one of the largest security get-togethers running in the southern hemisphere.

The conference is held over two days in a relaxed and informal atmosphere, allowing delegates to enjoy themselves whilst expanding their knowledge on security. More than 25 Australian and New Zealand speakers are expected to join the conference along with an attendance of 600-650 delegates.

Presentations will include in-depth talks on varying subject matter. Delegates will have the opportunity to meet new people, both socially and through some friendly rivalry, during many of the activities and competitions. These activities will allow novices to improve their basic skills, while experts can test their skills against their peers, with everyone having the opportunity of winning prizes.