UBM
TechWeb

MASTER OFFENSE

// PROGRAM GUIDE

// january 16-19, 2011

// WWW.BLACKHAT.COM

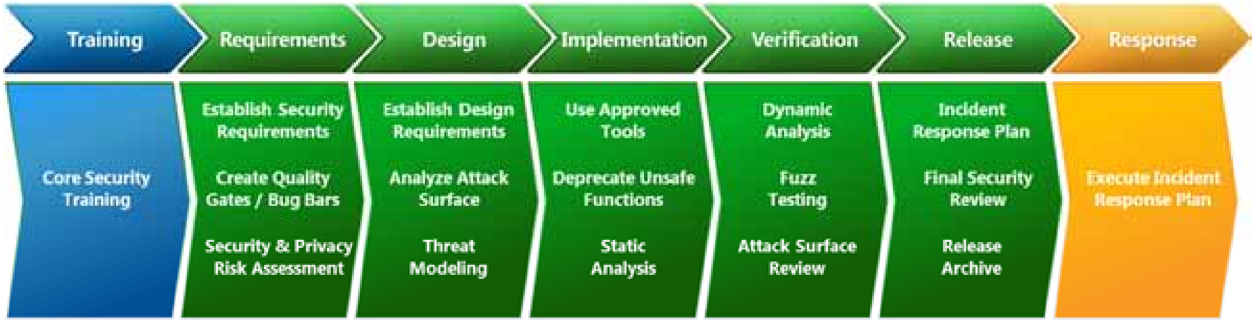
// SUSTAINING SPONSORS

CORE SECURITY TECHNOLOGIES · IBM · IOActive™ COMPREHENSIVE COMPUTER SECURITY SERVICES · Microsoft® · NETWITNESS · QUALYS® · Trustwave® Information Security & Compliance

Microsoft | Security Development Lifecycle

What is the Microsoft Security Development Lifecycle (SDL)?

The Microsoft SDL is the industry leading software security assurance process. Combining a holistic and practical approach, the Microsoft SDL embeds security and privacy throughout the development process. A Microsoft-wide initiative and a mandatory policy at Microsoft since 2004, the SDL has played a critical role in improving the security and privacy of Microsoft's software and services.



Leverage the Microsoft SDL in your organization

The adoption of a comprehensive software security process, such as the Microsoft SDL, will help your organization improve its software security, reduce customer risk, and reduce your total cost of development. Visit the www.microsoft.com/sdl website and download the *Simplified Implementation of the Microsoft SDL* whitepaper to learn about the security activities your organization will need to perform in order to follow the SDL process.

Connect with the Pros

The SDL Pro Network is a group of security consultants, training companies, and tool providers that specialize in application security and have substantial experience and expertise with the methodology and technologies of the SDL. Visit the Microsoft SDL booth and meet SDL Pro Network member companies to understand how they can help you implement the Microsoft SDL at your company.

www.microsoft.com/sdl

Welcome to Black Hat DC 2011

I have decided to begin shifting the focus of this event to be more oriented towards offensive technologies and less on defensive and policy. This is not to say they have no place at Black Hat D.C., just that the primary focus going forward will be more attack-oriented.

I have always worried that Black Hat DC suffered from the “Black Hat lite” syndrome—perceived as a smaller, but essentially same, conference to its big brother in Las Vegas. The more time I spend around DC, the more I realize that here, more than any other place, there is a legitimate and urgent need to focus on offensive technologies.

Expect to see this trend continue over the coming years as I reshape the focus of the DC event to be solely oriented towards offensive technologies, research, strategies and policies.

We are moving into a world where politicians have entered the fray, cyber legislation is being considered and everyone expects something to happen this year or next. Will a national breech notification law be instituted? A kill switch? An expanded role of ISPs in the defense of the net?

There seems to be an acknowledgement that absolute defense is not possible, therefore recovery is even more important. If an infrastructure attack would cause a week of outage, how could we reduce it to a day? If a resilient site could mitigate a DDoS attack in matter of hours instead of days then the calculus of whether an attack is worth the energy and law enforcement attention would have an increased deterrent effect.

Just like the term ‘cloud’ having different meanings to different people, ‘resiliency’ too will become a buzzword that points to a different way of thinking about response.

A strong offense can have a deterrent effect. A highly resilient infrastructure can have a deterrent effect. The clearly articulated policies of what would be considered cybercrime vs. cyberwar would help guide norms of behavior.

This is the second year that we have been able to present you with an expanded lineup of content, including the addition of a workshop track. New this year, the workshops are two or three-hour sessions that really delve into a topic area.

I would like to thank our event sponsors and speakers. We’ve assembled more than 20 of the most influential companies in IT security and over 35 speakers to help you plot your security plans for 2011. Please join us for the reception, hosted by Microsoft, following the first day of Briefings.

It’s going to be a terrific week. Thank you for joining us.

Jeff Moss

Jeff Moss
Director, Black Hat

// table of contents

// upcoming events

black hat europe 2011
hotel rey juan carlos
barcelona, spain
march 15-18, 2011

black hat usa 2011
caesars palace hotel
and casino
las vegas, nevada
july 30 - august 4, 2011

black hat abu dhabi 2011
abu dhabi,
united arab emirates
date to be announced

// stay connected

twitter:
twitter.com/BlackHatEvents
Tweet about DC: #BlackHatDC

facebook:
facebook.com/blackhat

linked.in:
search for “Black Hat”
on Linked.In Groups

rss:
www.blackhat.com/
BlackHatRSS.xml

//day one: schedule

08:00 - 12:00	REGISTRATION // *INDEPENDENCE LEVEL, INDEPENDENCE FOYER*			
08:00 - 09:00	BREAKFAST // INDEPENDENCE CENTER A // SPONSORED BY IBM			
08:00 - 19:30	SPONSOR EXHIBIT HALL OPEN // *INDEPENDENCE CENTER A*			
09:00 - 09:50	OPENING ADDRESS: *Jeff Moss* // KEYNOTE: *Franklin D. Kramer "Cyber Conflicts: Challenging the Future" // REGENCY BALLROOM E+F*			
TRACK	TRACK 1 OFFENSIVE: IRREGULAR TACTICS	TRACK 2 OFFENSIVE: WEB SKIRMISHES	TRACK 3 DEFENSIVE: FORTIFICATIONS	TRACK 4 WORKSHOPS: APPLIED KNOWLEDGE
LOCATION	REGENCY BALLROOM E	REGENCY BALLROOM F	REGENCY BALLROOM C+D	LINCOLN // LEVEL 3
09:50 - 10:00	BREAK			
10:00 - 11:15	TOM PARKER *Stuxnet Redux: Malware Attribution & Lessons Learned*	LAURENT OUDOT *Inglourious Hackers: Targeting Web Clients*	MARC EISENBARTH *Active Exploitation Detection*	MARIANO NUNEZ DI CROCE, JORDAN SANTARSIERI *Cyber-attacks to SAP Platforms: The Insider Threat*
11:15 - 11:30	COFFEE SERVICE			
11:30 - 12:45	JAMIE SCHWETTMANN *How to Steal Nuclear Warheads Without Voiding Your Xbox Warranty*	CHRIS GATES *Attacking Oracle Web Applications With Metasploit*	CASSIO GOLDSCHMIDT *Responsibility for the Harm and Risk of Software Security Flaws*	MARIANO NUNEZ DI CROCE, JORDAN SANTARSIERI *Cyber-attacks to SAP Platforms: The Insider Threat (Continued)*
12:45 - 13:45	LUNCH // INDEPENDENCE CENTER B // SPONSORED BY Trustwave			
14:15 - 15:15	MATTHEW WEEKS *Counterattack: Turning the Tables on Exploitation Attempts from Tools Like Metasploit*	NEIL DASWANI *Malware Distribution via Widgetization of the Web*	RYAN BARNETT *XSS Street-Fight: The Only Rule Is There Are No Rules*	DINO DAI ZOVI, VINCENZO IOZZO *The Mac Exploit Kitchen*
15:00 - 15:15	BREAK			
15:15 - 16:30	ADRIAN CRENSHAW *Identifying the True IP/Network Identity of I2P Service*	MARIANO NUNEZ DI CROCE *Your Crown Jewels Online: Attacks to SAP Web Applications*	SEAN COYNE *The Getaway: Methods and Defenses for Data Exfiltration*	DINO DAI ZOVI, VINCENZO IOZZO *The Mac Exploit Kitchen (Continued)*
16:30 - 16:45	COFFEE SERVICE			
16:45 - 18:00	VAL SMITH *Forgotten World: Corporate Business Application Systems*	TOM BRENNAN, RYAN BARNETT *Checkmate with Denial of Service*	ANDREW CASE *De-Anonymizing Live CDs through Physical Memory Analysis*	DINO DAI ZOVI, VINCENZO IOZZO *The Mac Exploit Kitchen (Continued)*
18:00 - 19:30	RECEPTION // INDEPENDENCE CENTER A // SPONSORED BY Microsoft | Security Development Lifecycle			

//day two: schedule

08:00 - 12:00	REGISTRATION // *INDEPENDENCE LEVEL, INDEPENDENCE FOYER*			
08:00 - 09:00	BREAKFAST // INDEPENDENCE CENTER A // SPONSORED BY IBM			
08:00 - 14:00	SPONSOR EXHIBIT HALL OPEN // *INDEPENDENCE CENTER A*			
TRACK	TRACK 1 OFFENSIVE: AIRBORNE OPERATIONS	TRACK 2 OFFENSIVE: TRENCH WARFARE	TRACK 3 WORKSHOPS: APPLIED KNOWLEDGE	TRACK 4 WORKSHOPS: APPLIED KNOWLEDGE
LOCATION	REGENCY BALLROOM E	REGENCY BALLROOM F	REGENCY BALLROOM C+D	LINCOLN // LEVEL 3
09:00 - 9:50	BRYAN SULLIVAN *Hey You, Get Off Of My Cloud: Denial of Service in the *aaS Era*	JON LARIMER *Beyond AutoRun: Exploiting Software Vulnerabilities with Removable Storage*		MICHAEL EDDINGTON *Peach Fuzzing Workshop*
9:50 - 10:00	BREAK			
10:00 - 11:15	RALF-PHILIPP WEINMANN *The Baseband Apocalypse*	VINCENZO IOZZO, GIOVANNI GOLA *Stale Pointers are the New Black*	CHRIS HADNAGY *How to Hack Large Companies and Make Millions by Offensive Security*	MICHAEL EDDINGTON *Peach Fuzzing Workshop (Continued)*
11:15 - 11:30	COFFEE SERVICE			
11:30 - 12:45	DAVID PEREZ, JOSE PICO *A Practical Attack Against GPRS/EDGE/UMTS/HSPA Mobile Data Communications*	DIONYSUS BLAZAKIS *The Apple Sand Box*	CHRIS HADNAGY *How to Hack Large Companies and Make Millions by Offensive Security (Continued)*	MICHAEL EDDINGTON *Peach Fuzzing Workshop (Continued)*
12:45 - 13:45	LUNCH // INDEPENDENCE CENTER B // SPONSORED BY TENABLE Network Security			
13:45 - 15:00	THOMAS ROTH *Breaking Encryption in the Cloud: GPU Accelerated Supercomputing for Everyone*	ITZHAK AVRAHAM *Popping Shell on A(ndroid)RM Device*		JOE GRAND *Hardware Reverse Engineering: Access, Analyze, and Defeat*
15:00 - 15:15	BREAK			
15:15 - 16:30	MATTHIEU SUICHE *Your Cloud in My Pocket*	ANGELOS STAVROU *Exploiting Smart-Phone USB Connectivity For Fun And Profit*		JOE GRAND *Hardware Reverse Engineering: Access, Analyze, and Defeat (Continued)*
16:30 - 16:45	COFFEE SERVICE			
16:45 - 18:00	ROB HAVELT *Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE*	TARJEI MANDT *Kernel Pool Exploitation on Windows 7*		JOE GRAND *Hardware Reverse Engineering: Access, Analyze, and Defeat (Continued)*

FRANKLIN D. KRAMER
Keynote Presentation – Cyber Conflicts: Challenging the Future

Franklin Kramer will present a compelling discourse on how the future will be challenged by cyber conflicts.

ITZHAK AVRAHAM
Popping Shell on A(ndroid)RM Devices

The attendees will gain knowledge on how to exploit ARM buffer overflows, use Ret2ZP attack and will demo a vulnerable application that is in current Android and can be used for remote attacks(!).

Also, We'll cover the problems with native/mixed code debugging, issues with current implementations of Androids and how ARM exploits can be used if better security prevention techniques is being implied (like XN bit—same as NX bit on X86).

RYAN BARNETT
XSS Street-Fight: The Only Rule Is There Are No Rules

Defending web applications from Cross-Site Scripting (XSS) attacks is extremely challenging, especially when the application's code can not be updated to fix the issue. This presentation will provide a walk-through of various XSS attack/defense/evasion lessons learned by Trustwave's SpiderLabs Research Team while working with commercial WAF customers, as well as, by receiving thousands of attacks against our public ModSecurity demonstration page. We will highlight cutting-edge XSS protection methods that are external to the web application's code such as Defensive Javascript Content Injection.

DIONYSUS BLAZAKIS
The Apple Sandbox

Despite the never ending proclamations of the end of memory corruption vulnerabilities, modern software still falls to exploits that target these bugs. Current operating systems incorporate a battery of exploit mitigations making life significantly more complex for attackers. Additionally, developers are becoming increasingly aware of the security implications of previously idiomatic code. Leading software publishers are teaching defensive coding techniques and have adopted an offensive mindset for product testing. Unfortunately, a single vulnerability can still provide the attacker the leverage needed to gain entry. Security researchers have disclosed multiple ways to render the mitigations ineffective (under the right circumstances)—imagine what techniques are not public. One bug can still "ruin your day".

In this presentation, I describe the architecture and implementation of the Apple XNU Sandbox framework (previously codenamed "Seatbelt"). This framework is used to contain App Store applications on iOS and some server applications on OS X. I will give you a complete tour of the Sandbox internals, most of which are in closed source modules (kernel extensions and dynamic libraries). This information is useful for auditors or exploit developers attempting to escape the sandbox and for developers or defenders attempting to secure their applications. I will also release an automated profile decompiler to extract a human readable policy definition from a compiled profile inside the kernel (iOS kernelcache or OS X). By the end of the presentation, you will have a working understanding of the entire access control system from policy definition to sandbox initialization to the kernel's policy enforcement.

TOM BRENNAN, RYAN BARNETT
Checkmate with Denial of Service

Denial-Of-Service is an attempt to make a computer resource unavailable to its intended users and is not new. In recent history April 2009, government and financial sites in the U.S. and South Korea were attacked by DDOS and were brought offline for days. This incident followed the Georgian DDOS attacks in 2008 and Estonian DDOS attacks in 2007.

Common attack methods include systems infected with malware that are controlled and all connect to the target host at the same time using Layer 4 (Transport) which are already addressed by anti-DDOS solutions when employed.

In 2009 a lethal form of Layer 7 (Application) attack techniques were being examined by Wong Onn Chee of OWASP Foundation Singapore and in 2010 together with Tom Brennan of OWASP Foundation presented the findings publicly for the first time with code samples.

Tom Brennan will walk through the history and details of how this lethal HTTP POST DOS technique works, interesting findings in the protocol and the challenges in defending critical infrastructure against targeted attacks and demonstrate and release his open-source tool that can be used to test your own production systems—or render others useless with the touch of a button from a single laptop.

ANDREW CASE
De-Anonymizing Live CDs through Physical Memory Analysis

Traditional digital forensics encompasses the examination of data from an offline or "dead" source such as a disk image. Since the filesystem is intact on these images, a number of forensics techniques are available for analysis such as file and metadata examination, timelining, deleted file recovery, indexing, and searching. Live CDs present a large problem for this forensics model though as they run solely in RAM and do not interact with the local disk. This removes the ability to perform an orderly examination since the filesystem is no longer readily available and putting random pages of data into context can be very difficult for in-depth investigations. In order to solve this problem, we present a number of techniques that allow for complete recovery of a live CD's in-memory filesystem and partial recovery of its previously deleted contents. We also present memory analysis of the popular Tor application as it is used by a number of live CDs in an attempt to keep network communications encrypted and anonymous.

SEAN COYNE
The Getaway: Methods and Defenses for Data Exfiltration

There are several stages to a successful cyber attack. The most crucial of which is also the least discussed: data theft. Cyber criminals, insider threats, advanced persistent threats; every attacker has ways to get into your network and find what they want. While there are several tools, methods and strategies to combat intruders, once they've made off with your data there is no getting it back, the game is over.

MANDIANT's consultants regularly respond to incidents where data, intellectual property even money is being stolen from victim organizations. During this presentation we will take a look at some of the advanced methods of stealing data that we have recently encountered in the field, including: preparing and cleaning staging areas, avoiding DLP/traffic scanning products and how attackers use a victim's own infrastructure and architecture against them. We will discuss why these tricks work and what, if anything, can be done to stop them.

Whether it be financial information, intellectual property, or personally identifiable information; the most valuable thing on your network is the data. Intruders may get in, but until they get out with what they came for the game's not over.

ADRIAN CRENSHAW
Identifying the True IP/Network Identity of I2P Service Hosts

This paper will present research into services hosted internally on the I2P anonymity network, especially I2P hosted websites known as eepSites, and how the true identity of the Internet host providing the service may be identified via information leaks on the application layer. By knowing the identity of the Internet host providing the service, the anonymity set of the person or group that administrates the service can be greatly reduced. The core aim of this paper will be to test the anonymity provided by I2P for hosting eepSites, focusing primarily on the application layer and mistakes administrators and developers may make that could expose a service provider's identity or reduce the anonymity set they are part of. We will show attacks based on the intersection of I2P users hosting eepSites on public IPs with virtual hosting, the use of common web application vulnerabilities to reveal the IP of an eepSite, as well as general information that can be collected concerning the nodes participating in the I2P anonymity network.

NEIL DASWANI
Malware Distribution via Widgetization of the Web

The Web 2.0 transformation has in part involved many sites using third-party widgets. We present the "widgetized web graph" showing the structure of high traffic web sites from the standpoint of widgets, show how web-based malware and scareware is propagated via such widgets, and provide data on how a mass web-based malware attack can take place against the Quantcast 1000 web sites via widgets.

MARIANO NUNEZ DI CROCE
Your Crown Jewels Online: Attacks to SAP Web Applications

"SAP platforms are only accessible internally". You may have heard that several times. While that was true in many organizations more than a decade ago, the current situation is completely different: driven by modern business requirements, SAP systems are getting more and more connected to the Internet. This scenario drastically increases the universe of possible attackers, as remote malicious parties can try to compromise the organization's SAP platform in order to perform espionage, sabotage and fraud attacks.

SAP provides different Web interfaces, such as the Enterprise Portal, the Internet Communication Manager (ICM) and the Internet Transaction Server (ITS). These components feature their own security models and technical infrastructures, which may be prone to specific security vulnerabilities. If exploited, your business crown jewels can end up in the hands of cyber criminals.

Through many live demos, this talk will explain how remote attackers may compromise the security of different SAP Web components and what you can do to avoid it. In particular, an authentication-bypass vulnerability affecting "hardened" SAP Enterprise Portal implementations will be detailed.

MARC EISENBARTH
Active Exploitation Detection

Security professionals have a massive number of acronyms at their disposal: IPS, VA, VM, SIEM, NBAD, and more. This talk is about a tool that resists classification by these acronyms. The goal of Active Exploitation Detection (AED) is to actively monitor and identify compromise of arbitrary, remote systems with the express intent to discover novel exploitation methods, track down elusive zero-day details, compile a list of known-compromised hosts, and most importantly get into the mind of today's cyber criminals. Simplistically, AED correlates changes visible to the remote monitoring system with external stimuli such as software patch schedules and security media sources in order to gain unique insight into the security threat landscape on an Internet scale. AED is a framework which is driven by arbitrary pluggable modules that must provide four high level implementations, namely port scanning, application identification via static and dynamic methods, and a data mining engine. The primary goal of this talk is to both present findings that trend the threat landscape of the Internet as a whole, and the tool itself, which is a means to introduce the audience to a number of best-of-breed open-source tools which have been integrated into this project.

CHRIS GATES
Attacking Oracle Web Applications with Metasploit

In 2009, Metasploit released a suite of auxiliary modules targeting oracle databases and attacking them via the TNS listener. This year lets beat up on... errr security test Oracle but do it over HTTP/HTTPS. Rather than relying on developers to write bad code lets see what we can do with default content and various unpatched Oracle middleware servers that you'll commonly run into on penetration tests. We'll also re-implement the TNS attack against the isqlplus web portal with Metasploit auxiliary modules.

CASSIO GOLDSCHMIDT
Responsibility for the Harm and Risk of Software Security Flaws

Who is responsible for the harm and risk of security flaws? The advent of worldwide networks such as the internet made software security (or the lack of software security) became a problem of international proportions. There are no mathematical/statistical risk models available today to assess networked systems with interdependent failures. Without this tool, decision-makers are bound to overinvest in activities that don't generate the desired return on investment or under invest on mitigations, risking dreadful consequences. Experience suggests that no party is solely responsible for the harm and risk of software security flaws but a model of partial responsibility can only emerge once the duties and motivations of all parties are examine and understood.

State of the art practices in software development won't guarantee products free of flaws. The infinite principles of mathematics are not properly implemented in modern computer hardware without having to truncate numbers and calculations. Many of the most common operating systems, network protocols and programming languages used today were first conceived without the basic principles of security in mind. Compromises are made to maintain compatibility of newer versions of these systems with previous versions. Evolving software inherits all flaws and risks that are present in this layered and interdependent solution. Lastly, there are no formal ways to prove software correctness using neither mathematics nor definitive authority to assert the absence of vulnerabilities. The slightest coding error can lead to a fatal flaw. Without a doubt, vulnerabilities in software applications will continue to be part of our daily lives for years to come.

Decisions made by adopters such as whether to install a patch, upgrade a system or employed insecure configurations create externalities that have implications on the security of other systems. Proper cyber hygiene and education are vital to stop the proliferation of computer worms, viruses and botnets. Furthermore, end users, corporations and large governments directly influence software vendors' decisions to invest on security by voting with their money every time software is purchased or pirated.

Security researchers largely influence the overall state of software security depending on the approach taken to disclose findings. While many believe full disclosure practices helped the software industry to advance security in the past, several of the most devastating computer worms were created by borrowing from information detailed by researcher's full disclosure. Both incentives and penalties were created for security researchers: a number of stories of vendors suing security researchers are available in the press. Some countries enacted laws banning the use and development of "hacking tools". At the same time, companies such as iDefense promoted the creation of a market for security vulnerabilities providing rewards that are larger than a year's worth of salary for a software practitioner in countries such as China and India.

Effective policy and standards can serve as leverage to fix the problem either by providing incentives or penalties. Attempts such PCI created a perverse incentive that diverted decision makers' goals to compliance instead of security. Stiff mandates and ineffective laws have been observed internationally. Given the fast pace of the industry, laws to combat software vulnerabilities may become obsolete before they are enacted. Alternatively, the government can use its own buying power to encourage adoption of good security standards. One example of this is the Federal Desktop Core Configuration (FDCC).

The proposed presentation is based on the research done by Cassio Goldschmidt, Sr. Manager at Symantec Corporation; Melissa J. Dark, Professor & Assistant Dean Department of Computer and Information Technology Purdue University and Hina Chaudhry, PhD. Candidate at Purdue University and is reflection of the role of each player involved in the software lifecycle and the incentives (and disincentives) they have to perform the task, the network effects of their actions and the results on the state of software security. The full text is available as a chapter of Information Assurance & Security Ethics (ISBN: 978-1-61692-245-0, hardcover. ISBN: 978-1-61692-246-7, ebook).

ROB HAVELT, BRUNO GONCALVES DE OLIVEIRA

Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE

The new 802.11p standard aims to provide reliable wireless communication for vehicular environments. The P802.11p specification defines functions and services required by Wireless Access in Vehicular Environments (WAVE) conformant stations to operate in varying environments and exchange messages either without having to join a BSS or within a BSS, and defines the WAVE signaling technique and interface functions that are controlled by the 802.11 MAC.

Wireless telecommunications and information exchange between roadside and vehicle systems present some interesting security implications. This talk will present an analysis of the 802.11p 5.9 GHz band Wireless Access in Vehicular Environments (WAVE) / Dedicated Short Range Communications (DSRC), Medium Access Control (MAC), and Physical Layer (PHY) Specifications of this protocol. We will present methods of analyzing network communications (GNU Radio/USRP, firmware modifications, etc.), and potential security issues in the implementation of the protocol in practical environments such as in toll road implementations, telematics systems, and other implementations.

VINCENZO IOZZO, GIOVANNI GOLA

Stale Pointers are the New Black

Memory corruption bugs such as dangling pointers, double frees and uninitialized memory are some of the open issues in application security.

Finding dangling pointers and similar vulnerabilities in large code bases it's arguably more difficult than overflows because of the complexity and heterogeneity of applications memory management. Fuzzing has been proved to be an effective method for finding such bugs in browsers and other similar COTS applications, nonetheless it's not uncommon to see bugs found by fuzzers burned after a short period of time because of multiple rediscovery of the same vulnerabilities.

In this talk the challenges of finding such bugs with static analysis and the results we got will be discussed, specifically we will explore the algorithms and techniques borrowed from program analysis and graph theory that can be employed to achieve our goal. We will also discuss what improvements can be made in order to increase precision and reduce the number of false positives.

JON LARIMER

Beyond AutoRun: Exploiting Software Vulnerabilities with Removable Storage

Malware has been using the AutoRun functionality in Windows for years to spread through removable storage devices. That feature is easy to disable, but the Stuxnet worm was able to spread through USB drives by exploiting a vulnerability in Windows. In this talk, I'll examine different ways that attackers can abuse operating system functionality to execute malicious payloads from USB mass storage devices without relying on AutoRun. There's a lot of code that runs between the USB drivers themselves and the desktop software that renders icons and thumbnails for documents, providing security researchers and hackers with a rich set of targets to exploit. Since the normal exploit payloads of remote shells aren't totally useful when performing an attack locally from a USB drive, we'll look at alternative payloads that can give attackers immediate access to the system. To show that these vulnerabilities aren't just limited Windows systems, I'll provide a demonstration showing how I can unlock a locked Linux desktop system just by inserting a USB thumb drive into the PC.

TARJEI MANDT

Kernel Pool Exploitation on Windows 7

In Windows 7, Microsoft introduced safe unlinking to the kernel pool to address the growing number of vulnerabilities affecting the Windows kernel. Prior to removing an entry from a doubly-linked list, safe unlinking aims to detect memory corruption by validating the pointers to adjacent list entries. Hence, an attacker cannot easily leverage generic "write 4" techniques in exploiting pool overflows or other pool corruption vulnerabilities. In this talk, we show that in spite of the efforts made to remove generic exploit vectors, Windows 7 is still susceptible to generic kernel pool attacks. In particular, we show that the pool allocator may under certain conditions fail to safely unlink free list entries, thus allowing an attacker to corrupt arbitrary memory. In order to thwart the presented attacks, we conclusively propose ways to further harden and enhance the security of the kernel pool.

LAURENT OUDOT

Inglourious Hackerds: Targeting Web Clients

This talk will propose to look at technical security issues related to multiple Internet Web Clients.

While such tools are used to crawl the Net and retrieve information, there might exist many scenarios where evil attackers can abuse them.

By studying the protocols (HTTP, etc), and by doing some kind of fuzzing operations, we will show how TEHTRI-Security was able to find multiple security issues on many handled devices and workstations.

The offensive concepts explained during this talk, will show many different tricks, like how evil attackers can become anonymous and create cover channels based on web clients, or like how to own or crash most famous current web clients and devices.

TOM PARKER

Stuxnet Redux: Malware Attribution & Lessons Learned

Recent incidents commonly thought to be linked to state sponsored activities have given rise to much discussion over the reliability of technical analysis as a source for adversary attribution - specifically in regards to what is commonly termed as the Advanced Persistent Threat (or APT). We now live in a world where the reverse engineering of a malicious binary, or analysis of a compromised host may very well play into a world-changing decision, such as whether a country should declare war on another—or indeed, whether it is no longer viable for a large, multinational corporation to continue doing business in a given part of the globe.

Of perhaps most note—stuxnet has dominated much of the information security media since it's public acknowledgment in June 2010. Multiple schools of thought have emerged, casting speculation over the identities of those responsible for the authorship and operalization of what some suggest is the most advanced piece of malware observed in the public domain. Nation state? Organized crime? Disgruntled vendor employee? This talk will take a close look at what we really know about this mysterious culmination of bits, closely analyzing some of the popular hypothesis, and identify others which have perhaps not drawn as much momentum.

As a basis for our analysis, we will discuss in depth the merits and demerits of technical analysis; demonstrating ways in which various techniques including static binary analysis and memory forensics may be utilized to build a granular profile of the adversary, and where the same techniques may fall short. The presentation will discuss detailed characterization matrix that can be leveraged to assess and even automate assessment of multiple aspects of the adversary (such as motive, technical skill, technological research resources) that may all play into the way in which we respond to an incident, or reposition ourselves to handle a specific threat over in long term.

Finally, we will review what lessons we can learn from stuxnet—to further attribution related research efforts, and ways in which we might adjust our security posture when it comes to protecting our nations most critical assets.

DAVID PEREZ, JOSE PICO

A Practical Attack against GPRS/EDGE/UMTS/ HSPA Mobile Data Communications

In this presentation we will show a practical attack against GPRS, EDGE, UMTS and HSPA (2G/3G) mobile data communications. We will demonstrate that an attacker with a budget of less than $10,000 can set up a rogue BTS, make the victim devices connect to such BTS, and gain full control over the victim's data communications. Two vulnerabilities make the attack possible: first, the absence of mutual authentication in GPRS and EDGE (2G), which makes GPRS and EDGE devices completely vulnerable to this attack, and second, the mechanism implemented on most UMTS and HSPA (3G) devices that makes them fall back to GPRS and EDGE when UMTS or HSPA are not available, which makes it possible to extend the attack to these 3G devices.

THOMAS ROTH

Breaking Encryption in the Cloud: Cheap, GPU Accelerated Supercomputing for Everyone

It has been known since some time now that the massive parallel architecture of modern GPUs provide enormous acceleration when trying to break encryption—or hashalgorithms: GPUs are (depending on the algorithm and the implementation) some hundred times faster compared to standard quad core CPUs when it comes to brute forcing SHA1 and MD5. The enormous potential can also be seen in the supercomputing business: The Tianhe-1A, leader of the top 500 list of supercomputers, is not only equipped with 14.336 CPUs but also with 7.168 NVIDIA Tesla "Fermi" M2050 GPUs—each of which has 448 cores and 3GB RAM. Until recently, one needed to spend a lot of money to get a small cluster of GPU assisted servers, but Amazon now provides an instance type in it's EC2 cloud that sports two of the GPUs that are also used in the Tianhe-1A, resulting in a cheap way to boot up a cluster of GPU accelerated servers that can be used for own purposes.

The first part of the talk will be about the design and the implementation of a massive parallel and GPU assisted environment for breaking encryptions: From generation, the storing and the use of rainbow tables to brute forcing in the cloud. In the second part of the talk the "Cloud Cracking Suite" is introduced: An open source suite designed to demonstrate the performance of breaking several algorithms in the cloud.

The 'Cloud Cracking Suite' is splitted in two parts: The server side and the client. The server side consists of especially for the Fermi-architecture optimized, high performance implementations of SHA1 and MD5 with an interface to use them for rainbow table generation or brute forcing as well as a self-configuring Pyrit for WPA database generation. The client side provides an easy to use CLI which allows one to spawn and control a cluster for a specific task.

As the server side will be available as a hosted AMI, everyone participating can simply download the client, create an account at the AWS and try it out himself.

JAMIE SCHWETTMANN

How to Steal Nuclear Warheads Without Voiding Your Xbox Warranty

We will present the common elements and basic mechanisms of modern tamper-evident seals, tags, and labels, with emphasis on attack and circumvention. Adhesive seals, crimp seals, wire wraps, fiber optic seals, electronic, chemical, biological, and make-shift seals will be dissected, examined, and explained, with emphasis on their shortcomings and circumvention techniques. We will also present an overview of typical applications for tags, seals, and labels, including covert traps and uses ranging from consumer goods to loss reduction to government secrets.

VAL SMITH, ALEXANDER POLYAKOV

Forgotten World: Corporate Business Application Systems

Do you know where are all critical company data is stored? Do you know how easily you can be attacked by cybercriminals targeting this data? How can attacker sabotage or commit espionage against your company just having access to one system?

Amidst SCADA, Win 7, and the Cloud there is a type of critical system no one is talking about. Enterprise Resource Planning (ERP). All that is needed is to gain access to the corporate business application infrastructure, specifically systems such as ERP, Customer Relationship Management (CRM), and Supplier Relationship Management (SRM). If an attacker seeks to gather critical financial, personnel, or other sensitive data, these are the types of systems where it is stored. These systems are often also trusted and connected to other secure systems such as banking client workstations as well as SCADA systems.

These days most companies have strong security policies and patch management as it applies to standard networks and operating systems, but these rarely exist or are in place for ERP type systems. An attacker can bypass all of a company's investments in security by attacking an ERP system.

We will show examples of different custom business applications including custom as well as the more popular ones and previously unknown vulnerabilities that can be exploited to gain unauthorized access to critical business data. Many of these type vulnerabilities cannot be easily patched because they are design flaws or business logic problems requiring a redesign of the system.

ANGELOS STAVROU

Exploiting Smart-Phone USB Connectivity for Fun And Profit

The Universal Serial Bus (USB) connection has become the de-facto standard for both charging and data transfers for smart phone devices including Google's Android and Apple's iPhone. To further enhance their functionality, smart phones are equipped with programmable USB hardware and open source operating systems that empower them to alter the default behavior of the end-to-end USB communications. Unfortunately, these new capabilities coupled with the inherent trust that users place on the USB physical connectivity and the lack of any protection mechanisms render USB a insecure link, prone to exploitation. To demonstrate this new avenue of exploitation, we introduce novel attack strategies that exploit the functional capabilities of the USB physical link. In addition, we detail how a sophisticated adversary who has under his control one of the connected devices can subvert the other. This includes attacks where a compromised smart phone poses as a Human Interface Device (HID) and sends keystrokes in order to control the victim host. Moreover, we explain how to boot a smart phone device into USB host mode and take over another phone using a specially crafted cable. Finally, we point out the underlying reasons behind USB exploits and propose potential defense mechanisms that would limit or even prevent such USB borne attacks.

MATTHIEU SUICHE

Your Cloud in My Pocket

LiveCloudKd makes possible to debug live Microsoft Hyper-V and VMWare Workstation virtual machines without having to enable the debug mode. With read+write access on the memory.

BRYAN SULLIVAN

*Hey You, Get Off Of My Cloud: Denial of Service in the *aaS Era*

Why care about denial-of-service attacks when there are so many privilege elevation and information disclosure threats we should be worried about? For one reason, DoS costs you money: in *aaS environments, there's not only the indirect cost of disrupting your legitimate users' access to the service, but also the more immediate and measurable cost of the bandwidth, storage, and processing power that the attack consumes (and that the platform provider will happily bill you for). We should all care about DoS for another, darker, reason too: a foreign power may someday use a DoS attack as an act of cyberwarfare or cyberterrorism against US critical infrastructure systems.

This talk will examine six DoS attack techniques used against cloud services.

These attacks all target the application layer of the service, cannot be stopped with firewalls or IPS, do not require distributed attacks or botnets, and are highly efficient and asymmetric. In some cases, a single HTTP request of less than 50 bytes is sufficient to knock out a server until reboot. In addition to describing the attacks, we will also investigate the application design issues that lead to vulnerability, and demonstrate coding fixes and free testing tools that can be used to solve the problem.

MATTHEW WEEKS
Counterattack: Turning the Tables on Exploitation Attempts from Tools like Metasploit

In hostile networks, most people hope their con kung-fu is good enough to avoid getting owned. But for everyone who has ever wanted to reverse the attack, not getting owned is not enough. We will see how it is often possible for the intended victim to not only confuse and frustrate the attacker, but actually trade places and own the attacker. This talk will detail vulnerabilities in security tools, how these vulnerabilities were discovered, factors increasing the number of vulnerable systems, how the exploits work, creating cross-platform payloads, and how to defend yourself whether attacking or counterattacking. The audience will be invited to participate as complete exploit code will be released and demonstrated against the Metasploit Framework itself.

RALF-PHILIPP WEINMANN
The Baseband Apocalypse

Attack scenarios against smartphones have concentrated on vulnerable software executed on the application processor. The operating systems running on these processors are getting hardened by vendors as can best be seen in the case of Apple's iOS, which both uses uses data execution prevention and code signing to make exploitation of memory corruptions and running malicious software harder. In contrast, the GSM/3GPP stack running on the baseband processor has been neglected. The advent of open-source solutions for running GSM base stations is a game-changer: Malicious base stations are not considered in the attack model assumed by the GSMA and the ETSI; similarly vendors of baseband stacks seem to not have taken malicious input from the network side into account. This paper explores the viability of attacks against baseband processors of GSM cellular phones, the focus being on smartphones.

We demonstrate the first over-the-air exploitations of memory corruption in GSM/3GPP stacks that result in malicious code being executed on the baseband processors.

workshops

DINO DAI ZOVI AND VINCENZO IOZZO
The Mac Exploit Kitchen

Learn Mac vulnerability exploitation from master exploit chefs Dino Dai Zovi and Vincenzo Iozzo, who will cook up several exploits in front of a live conference audience. The master chefs will demonstrate all the stages in the preparation of a gourmet exploit, from how to find and choose the right ingredients (vulnerabilities) to various preparation methods (exploitation techniques) that you may use in your own home kitchen. The recipes demonstrated will include both local privilege escalation and remote browser-based client-side vulnerabilities.

Attendees are invited to "play along" on their own laptops. All that will be required is a laptop running the latest version of Snow Leopard and IDA Pro. The demonstrations will use IDA Pro 6.0 for Mac OS X, but attendees will also be able to follow along somewhat using IDA Pro 5.0 Freeware in Wine or a Windows VM. No network access will be required and demonstration materials will be available via CD/USB.

MARIANO NUNEZ DI CROCE AND JORDAN SANTARSIERI
Cyber-attacks to SAP Platforms: The Insider Threat

How would a malicious insider exploit vulnerabilities in your SAP environment to get hold of your most sensitive business data? Which are the chances of him being successful? What can you do to stop him? If you are looking for answers to these questions, you should consider attending this workshop.

By joining us in this session, you will:

- Learn how to detect some of the existing threats *yourself* using Bizploit, the first opensource ERP Penetration Testing framework.
- Watch several *live* demos to understand how successful exploitations can result in espionage, sabotage and fraud attacks to your organization.
- Find out how you can *protect yourself from the detected risks*, improving the security of your platform.
- Discover the *latest outcome* from the Onapsis Research Labs, focused on the hot "ERP security" topic.

You do not require any previous SAP knowledge to attend this event. Take-aways: Copy of Bizploit, presentation slides and new knowledge!

MICHAEL EDDINGTON
Peach Fuzzing

Join us for look at fuzzing with Peach and the Peach extension HotFuzz. Peach is the most widely used fuzzer across a wide range of security professionals including: security researchers, consultants, and corporate security teams.

This workshop will provide a solid look at Peach, how it works and a jump-start on its usage. Additionally, we will demonstrate the usage of HotFuzz an extension of Peach that is able to "automatically" fuzz known network protocols by acting as a "fuzzing proxy."

Attendees with laptops and correct software can follow along with the demonstrations to get a more "hands on" feel to how Peach and HotFuzz work.

JOE GRAND
Hardware Reverse Engineering: Access, Analyze, and Defeat

Electronics are embedded into nearly everything we use. Hardware products are being relied on for security-related applications and are inherently trusted, though many are completely susceptible to compromise. In this workshop, Joe will discuss the hardware hacking and reverse engineering processes, and then provide an open lab environment for you to probe, analyze, and hack.

Joe will bring a variety of products to tinker with, though attendees are heavily encouraged to bring their own pieces of hardware to explore. Basic tools and electronics test/measurement equipment will be provided.

You'll leave the workshop with new skills, ideas for further attacks, and maybe even some defeated hardware.

CHRIS HADNAGY
How to Hack Large Companies and Make Millions by Offensive Security

Offensive Security wants to take you on a non-stop thrill ride through an actual hack. From Information Gathering, Social Engineering and Client Side Exploitation we will show you complete and total domination of the target.

This session will showcase the skills that are taught in Offensive Security's world-renowned Pentesting With BackTrack course as well as our Penetration Testing services. Our goal is raise awareness of the real world threats that exist in corporate business today.

speaker bios

Franklin D. Kramer

KEYNOTE SPEAKER – CYBER CONFLICTS: CHALLENGING THE FUTURE

The Honorable Franklin D. Kramer is a national security and international affairs expert. Mr. Kramer has been a senior political appointee in two administrations, including as Assistant Secretary of Defense for International Security Affairs for President Clinton, Secretary Perry and Secretary Cohen; and, previously, as Principal Deputy Assistant Secretary of Defense for International Security Affairs.

Among his current activities, Mr. Kramer is the author of *Cyber Security: An Integrated Governmental Strategy for Success*, as well as the principal editor and chapter author for the book *Cyberpower and National Security*. Mr. Kramer is also the principal editor for, and co-author of the policy chapter of, the book *Civil Power in Irregular Conflict*. He is the co-author and was co-project director of *Transatlantic Cooperation for Sustainable Energy Security*, and of *Central Europe and the Geopolitics of Energy*. At George Washington University, he teaches a course on "The Department of Defense and Winning Modern War." He has written numerous additional articles on international affairs, including in the cyber arena on "Cyber Influence and International Security," "I-Power: The Information Revolution and Stability Operations," and "Sweden's Use of Commercial Information Technology for Military Applications."

At the Department of Defense, Mr. Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO, the Middle East, Asia, Africa and Latin America. He has been responsible for activities in Iraq, the Balkans and other areas involving the use of force as well as reconstruction efforts and humanitarian and disaster relief activities throughout the world. He has chaired numerous bilateral and multilateral groups including with many of the central and eastern European states; Israel, Jordan and Saudi Arabia in the Middle East; Pakistan and India in South Asia; and Japan and South Korea in East Asia; and led delegations to NATO, China, Singapore, Egypt, Nigeria and numerous others. He was the primary interface with U.S. Combatant Commanders, and in addition to leading the International Security Affairs Office, supervised the Defense Security Cooperation Agency, including the foreign military sales and foreign military assistance budgets; the NATO Defense Advisor's Office; and the DOD POW-MIA.

In the non-profit world, Mr. Kramer is Vice Chairman of the Atlantic Council, a Distinguished Fellow at CNA which operates the Center for Naval Analysis and the Institute for Public Research, is chairman of International Advisory Committee and has been chairman of the board of the World Affairs Council of Washington, D.C; and is a Capstone Professor at the Elliott School of International Affairs, George Washington University, and has been a Distinguished Research Fellow at the Center for Technology and National Security Policy of the National Defense University. In the private sector, Mr. Kramer is a director and consultant and has been a partner at the law firm of Shea and Gardner.

Mr. Kramer received a BA cum laude from Yale University and a JD magna cum laude from Harvard Law School.

Itzhak Avraham

Itzhak Avraham (zuk) is a Computer & Network Security Expert who has done a wide variety of vulnerability assessments. Itzhak worked at the IDF as a Security Researcher and later as Security Researcher Training Specialist. Itzhak has worked at top penetration testing companies in Israel. He is a Senior Engineer at Samsung R&D (Israel) and he's the proud owner of zImperium.com where he does freelance work for special pentesting/hacking/research/reverse engineering projects. He's interested in all hacking related topics and really dislikes writing about himself in the third person. Itzhak can be found on Twitter :@ihackbanme and on his personal hacking related blog at http://imthezuk.blogspot.com

Ryan Barnett

TRUSTWAVE'S SPIDERLABS RESEARCH TEAM

Ryan Barnett is a Senior Security Researcher at Trustwave. He is a member of Trustwave's SpiderLabs—the advanced security team focused on penetration testing, incident response, and application security where he focuses on web application defensive research and serves as the ModSecurity web application firewall project lead. In addition to his work at Trustwave, Ryan is also a SANS Institute certified instructor and a member of both the Top 20 Vulnerabilities and CWE/SANS Top 25 Most Dangerous Programming Errors teams. He is also a Web Application Security Consortium (WASC) Member where he leads the Web Hacking Incidents Database (WHID) and Distributed Web Honeypots Projects, as well as, the OWASP ModSecurity Core Rule Set (CRS) project leader. Mr. Barnett has also authored a Web security book for Addison/Wesley Publishing entitled *Preventing Web Attacks with Apache* and is a frequent speaker at industry conferences such as Blackhat and OWASP.

Dionysus Blazakis

INDEPENDENT SECURITY EVALUATORS (ISE)

Dion has been breaking software since 1994, playing with debug.com and Ralf Brown's Interrupt List. Somewhere along the way, he took a more respectable path and ended up a software developer. After years working on embedded devices, he left development to write long reports that no one reads (i.e. he's a consultant). As an analyst for Independent Security Evaluators, Dion "audits" the DRM systems used for small consumer devices. He spends the rest of his time reversing, bug hunting, and thinking about model checking. His relevant interests include compilers, operating systems, programming languages, and Minecraft.

Tom Brennan

PROACTIVERISK

Tom Brennan started with technology as a COSYSOP for a underground 8-bit BBS and writing code for fun when Pascal and CP/M was cool -"xyzzy". Builds enterprise networks like legos... and molds custom web applications like clay to meet defined project requirements.

Today, Tom is a team member at proactiveRISK (www.proactiverisk.com) and volunteers his time to the Open Web Application Security Project (www.owasp.org) as Global Board Director.

Andrew Case

DIGITAL FORENSICS SOLUTIONS

Andrew Case is a security researcher at Digital Forensics Solutions where he is responsible for source code audits, penetration testing, and other computer security related tasks. He is also a GIAC-certified digital forensics investigator and has conducted numerous large scale investigations. Andrew's primary research focus is physical memory analysis, and he has published a number of peer-reviewed papers in the field.

Sean Coyne

MANDIANT

Sean Coyne is a security consultant for MANDIANT, where he conducts penetration tests of networks and webapps, teaches cyber investigation to federal agents, and performs forensics investigations for government and commercial clients. Prior to this he has worked for an elite handful of security and consulting firms serving intelligence & defense clients here and overseas. Sean was one of the first graduates of Penn State's Information Assurance program and is currently studying Intelligence Analysis at Mercyhurst College.

Adrian Crenshaw

TENACITY SOLUTIONS INC

Adrian Crenshaw has worked in the IT industry for the last twelve years. He runs the information security website Irongeek.com, which specializes in videos and articles that illustrate how to use various pen-testing and security tools. He did the cert chase for awhile (MCSE NT 4, CNE, A+, Network+. i-Net+) but stopped once he had to start paying for the tests himself. He's currently working on a Masters in Security Informatics, and is interested in obtaining a network security/research/teaching job in academia.

Dino Dai Zovi

TRAIL OF BITS

Dino Dai Zovi is an independent security consultant at Trail of Bits LLC. As an independent security researcher, Mr. Dai Zovi has been discovering and exploiting security vulnerabilities in commercial software and presenting his research at conferences such as DEF CON and Black Hat for over a decade. He is a co-author of both *The Mac Hacker's Handbook* and *The Art of Software Security Testing*, as well as the winner of the first PWN2OWN contest at CanSecWest 2007.

Neil Daswani

DASIENT

Neil Daswani is a co-founder of Dasient, Inc., a security company backed by some of the most influential investors in Silicon Valley and New York. In the past, Neil has served in a variety of research, development, teaching, and managerial roles at Google, Stanford University, DoCoMo USA Labs, Yodlee, and

Bellcore (now Telcordia Technologies). While at Stanford, Neil co-founded the Stanford Center Professional Development (SCPD) Security Certification Program (http://scpd.stanford.edu/computerSecurity/courses/softwareSecurityFoundations.htm). He has published extensively, frequently gives talks at industry and academic conferences, and has been granted several U.S. patents. He received a Ph.D. and a master's in computer science from Stanford University, and earned a bachelor's in computer science with honors with distinction from Columbia University. Neil is also the lead author of *Foundations of Security: What Every Programmer Needs To Know* (published by Apress; ISBN 1590597842; http://tinyurl.com/33xs6g). More information about Neil is available at http://www.neildaswani.com

Bruno Goncalves de Oliveira

TRUSTWAVE, SPIDERLABS

Bruno Goncalves de Oliveira is a Security Consultant at Trustwave's Spiderlabs in the Network Penetration Test Team. He is a member of Trustwave's SpiderLabs—the advanced security team focused on penetration testing, incident response, and application security where conducts penetration tests in the premier clients, holds some certs and a title of computer engineer by Universidade Norte do Paraná. Over 10 years working / studying / having fun with security always focused on offensive tasks, the main focus of his works is based on network security and penetration tests, trying to figure out different/other/more beautiful ways to attack systems, part of these studies/works became talks at some security conferences like SOURCE Barcelona (Spain), DEF CON 18 -Skytalks (USA), HITBSecConf 2009 (Malaysia), Toorcon X (USA), YSTS 2.0/3.0 and H2HC IV/VI (Brazil & Mexico).

Mariano Nunez di Croce

ONAPSIS

Mariano Nunez Di Croce is the Director of Research and Development at ONAPSIS. Mariano has a long experience as a Senior Security Consultant, mainly involved in security assessments and vulnerability research. He has discovered critical vulnerabilities in SAP, Microsoft, Oracle and IBM applications.

Mariano leads the SAP Security Team at Onapsis, where he works hardening and assessing the security of critical SAP implementations in world-wide organizations. He is the author and developer of the first open-source SAP Penetration Testing Framework and has discovered more than 40 vulnerabilities in SAP applications. Mariano is also the lead author of the "SAP Security In-Depth" publication.

Mariano has been invited to hold presentations and trainings in many international security conferences such as Blackhat USA/EU, DeepSec, Sec-T, Hack.lu, Seacure.it, Ekoparty, CIBSI as well as to host private trainings for Fortune-100 companies and defense contractors. Mariano has a degree in Computer Science Engineering from the UTN.

Michael Eddington

DÉJÀ VU SECURITY

Michael Eddington is a senior security consultant with over ten years providing security services to Fortune 500 companies in the United States. Michael has extensive expertise in many areas of computer security, including application security, network security, threat modeling, and fuzz testing. Michael is an industry expert who routinely speaks and provides training at the top industry technical conferences including Blackhat and RSA.

Michael has worked for some of the leading security companies, including Leviathan Security Group and ISAG. Michael also founded the security services practice for IOActive, Inc. and co-founded the Security Services Center for Hewlett-Packard's services division.

Michael is an accomplished software architect and developer. Michael has worked on shipping products, from trading applications to designing and building numerous commercial web applications. Michael has also participated in a number of open-source security development projects ranging from threat modeling (such as the Trike threat modeling conceptual framework) to fuzzing (e.g. The Peach Fuzzer Framework).

Michael's research is currently heavily focused on fuzzing (fuzz testing), in which he is considered one of the foremost experts, having developed the industry leading open source fuzzing platform Peach. Peach is used by many top technology companies and most security consultancies to perform fuzzing. Michael is currently engaged in pushing fuzzing to the next level with new tools and techniques.

Marc Eisenbarth

HP TIPPINGPOINT DVLABS

Marc Eisenbarth recently noticed the word "Architect" has been appended to his business cards, and while not entirely sure what that means, he has continued to just do what he has been doing for the last five years, namely improving the HP TippingPoint Intrusion Prevention System (IPS) as a member of DVLabs' Advanced Security Intelligence team. Prior to this, he managed "cyber liability" at a US defense contractor for five years and completed a graduate program at Columbia University in Computer Science. Off the clock, he is a "hardware guy" who enjoys releasing various do-it-yourself projects to the general public.

Chris Gates

METASPLOIT PROJECT

Chris Gates (CG/carnal0wnage) is a member of the Metasploit Project and Attack Research. He enjoys business logic flaws, misconfigured databases and the occasional client-side attack. He has spoken at various other security conferences including BlackHat USA, Defcon, CSI 2009, Brucon, SOURCE Boston, Toorcon, Notacon, and Chicagocon.

Giovanni Gola

Giovanni Gola is a student at Politecnico di Milano in computer engineering. He used to spend his spare time doing math olympics in his youth. Nowadays he does networking consultancies for various Italian companies and in his spare time he likes playing the sax and studying network security.

Cassio Goldschmidt

SYMANTEC

Cassio Goldschmidt is senior manager of the product security team under the Office of the CTO at Symantec Corporation. In this role he leads efforts across the company to ensure the secure development of software products. His responsibilities include managing Symantec's internal secure software development process, training, threat modeling and penetration testing. Cassio's background includes over 13 years of technical and managerial experience in the software industry. During the seven years he has been with Symantec, he has helped to architect, design and develop several top selling product releases, conducted numerous security classes, and coordinated various penetration tests. Cassio is also known for leading the Open Web Application Security Project (OWASP) chapter in Los Angeles.

Cassio represents Symantec on the SAFECode technical committee and (ISC)2 in the development of the CSSLP certification. He holds a bachelor degree in computer science from Pontificia Universidade Catolica do Rio Grande Do Sul, a masters degree in software engineering from Santa Clara University, and a masters of business administration from the University of Southern California.

Joe Grand

GRAND IDEA STUDIO, INC.

Joe Grand is an electrical engineer, hardware hacker, and president of Grand Idea Studio (www.grandideastudio.com) where he specializes in the invention, design, and licensing of consumer products and modules for electronics hobbyists. He is a former member of the legendary hacker collective L0pht Heavy Industries and has spent over a decade finding security flaws in hardware devices and educating engineers on how to increase the security of their designs. Joe holds a Bachelor of Science degree in Computer Engineering from Boston University and a Doctorate of Science in Technology (Honorary) degree from the University of Advancing Technology.

Chris Hadnagy

OFFENSIVE SECURITY & SOCIAL-ENGINEER.ORG

Chris Hadnagy, aka loganWHD, has been involved with computers and technology for over 13 years. Presently his focus is on the human aspect of technology such as social engineering and physical security. Chris has spent time in providing training in many topics and also has had many articles published in local, national and international magazines and journals.

He is presently the operations manager of Offensive Security and is Offensive Security's PWB Trainer and the lead developer of Social-Engineer.Org. He is the author of the book *Social Engineering: The Art of Human Hacking*. Chris can be found online at www.offsec.com and www.social-engineer.org or on twitter as @humanhacker.

Rob Havelt

TRUSTWAVE, SPIDERLABS

Rob Havelt is the director of penetration testing at Trustwave's SpiderLabs, the advanced security team within Trustwave focused on forensics, ethical hacking, and application security testing for premier clients. Rob has worked with offensive security seemingly forever, and from running a start-up ISP, to working as a TSCM specialist, he's held just about every job possible in the realm of system administration and information security.

Formerly a bourbon-fueled absurdist, raconteur, and man about town, currently a sardonic workaholic occasionally seeking meaning in the finer things in life—Rob is, and will always be, a career hacker.

Vincenzo Iozzo

ZYNAMICS GMBH

Vincenzo Iozzo is a student and a reverse engineer. At zynamics he does research on topics like vulnerability development, reverse engineering techniques and tools. Vincenzo is also a regular speaker at various international security conferences including Black Hat, EuSecWest and DeepSec on various topics reverse engineering related. He is probably best known for having won the PWN2OWN contest together with Ralf-Philipp Weinmann with an exploit for iPhoneOS.

Jon Larimer
IBM

Jon Larimer is a senior researcher on IBM's X-Force Advanced Research team. Jon has been working in the security industry for over 12 years at companies including Internet Security Systems, nCircle Network Security, and now IBM. He has been involved in an array of security fields such as penetration testing, vulnerability research, security software development, and malware analysis.

Tarjei Mandt
NORMAN

Tarjei Mandt is a security researcher with Norman. He specializes in vulnerability research, operating systems security, and exploit mitigations. Recently, he has been doing extensive work on the Windows kernel and has reported several vulnerabilities.

Laurent Oudot
TEHTRI-SECURITY

Laurent is a French senior IT Security consultant, who founded TEHTRI-Security in 2010. Last 15 years, he has been hired as a security expert to protect and pentest networks and systems of highly sensitive places like the French Nuclear Warhead Program, the French Ministry of Defense, the United Nations, etc.

He has been doing research on defensive technologies and underground activities with numerous security projects handled, and he was a member of team RstAck and of the Steering Committee of the Honeynet Research Alliance. Laurent has been a frequent presenter or instructor at computer security and academic conferences like Cansecwest, Pacsec, Black Hat, Hack In The Box, DEF CON, US DoD/DoE, Hope, Honeynet, PH-Neutral, Hack.LU, as well as a contributor to several research papers for SecurityFocus, *MISC Magazine*, IEEE, etc.

Tom Parker
SECURICON

Tom Parker is the Director of Security Consulting Services at Securicon. Tom is a recognized throughout the security industry for his research in multiple areas including adversary profiling and software vulnerability research & analysis. Tom has published over four books on the topic of information security including *Cyber Adversary Characterization—Auditing the Hacker Mind* and a contributor to the popular *Stealing the Network* series. Tom is a frequent speaker at conferences including a past speaker at Black Hat. Tom often lends his time to guest lecturing at Universities, involvement in community research initiatives, and is often called to provide his expert opinion to mass media organizations, including BBC News, CNN, and online/print outlets such as *The Register*, *Reuters News*, *Wired* and *Business Week*.

David Perez
TADDONG

David Perez is a senior security analyst with Taddong, a security research & consulting company he co-founded in 2010. He has more than 10 years of experience delivering advanced security services to domestic and multinational clients, including several Fortune Global 500 companies. He is deeply involved in Taddong's research activities in security areas like GSM/UMTS mobile communications or Windows security. He is also co-author and instructor of Taddong's training course "Security in GSM/GPRS/UMTS Mobile Communications."

Jose Pico
TADDONG

Jose Pico has 12 years of experience working for multinational companies, touching nearly every aspect of IT technologies, from operating systems support to leading the IT systems infrastructure of a telco company. In the latter years, he has focused his activity in the security field, and in 2010 he co-founded Taddong, a security research and consulting company. He delivers security services and training, and performs research activities. He has co-authored the Wireshark SMB export plugin and the "Security in GSM/GPRS/UMTS mobile communications" course.

Alexander Polyakov
DIGITAL SECURITY RESEARCH GROUP

Alexander Polyakov is the CTO at Digital Security Research Group (department of Alexander Polyakov is the CTO at Digital Security Research Group (department of Digital Security company). His expertise covers enterprise business-critical software like ERP, CRM, SRM, RDBMS, SCADA, banking and processing software. He found a lot of vulnerabilities in the products of such vendors as SAP and Oracle, and has made a lot of projects focused on special applications security in oil and gas, retail and banking sphere. He is the author of a book titled *Oracle Security from the Eye of the Auditor: Attack and Defense* (in Russian).

He is also lead a OWASP-EAS, architect of ERPSCAN Security scanner for SAP, Expert Council member of PCIDSS.RU, QSA and PA-QSA auditor and one of the contributors to Oracle with Metasploit project. Speaker at HITB, Source, DeepSec, Confidence, Troopers and many Russian conferences.

Thomas Roth
LANWORKS AG

Thomas Roth is a consultant for security and software engineering from Germany whose main interests are exploiting techniques, low-level programming languages and cryptographic algorithms. Recently he started implementing and optimizing hash algorithms like MD5 and SHA1 on GPUs, using the CUDA and the OpenCL framework. Some of his private work can be found on his Blog (http://stacksmashing.net/) or on Twitter (@stacksmashing).

Jordan Santarsieri
ONAPSIS

Jordan Santasieri is a senior Onapsis security consultant and researcher. Being also a member of the Onapsis Research Labs, he is engaged in a daily effort to identify, analyze, exploit and mitigate vulnerabilities affecting business-critical applications. Jordan has discovered critical vulnerabilities in SAP software and produced white papers on the subject. Through his work, he has contributed to the security of Fortune-100 companies and defense contractors. His interests include penetration testing, exploit writing, forensics, data mining, psychology applied to information technology and playing with the toys lying around at the Onapsis playroom.

Val Smith
ATTACK RESEARCH

Val Smith has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on a variety of problems in the security community. He specializes in penetration testing (over 40,000 machines assessed), reverse engineering and malware research. He works on the Metasploit Project development team as well as other vulnerability development efforts. Most recently Valsmith founded Attack Research which is devoted to deep understanding of the mechanics of computer attack. Previously Valsmith founded Offensive Computing, a public, open source malware research project.

Angelos Stavrou
GEORGE MASON UNIVERSITY

Angelos Stavrou is an Assistant Professor at George Mason University.

Matthieu Suiche
MOONSOLS

Matthieu Suiche is a security researcher who focuses on reverse code engineering and volatile memory analysis. His previous researches/utilities include Windows hibernation file, Windows physical memory acquisition (Win32dd/Win64dd) and Mac OS X Physical Memory Analysis.

Matthieu has been a speaker during various security conferences such as PacSec, BlackHat USA, EUROPOL High Tech Crime Meeting, Shakacon etc. Prior to starting in 2010 MoonSols, a computer security and kernel code consulting and software company based in France, Matthieu worked for companies such as E.A.D.S. (European Aeronautic Defence and Space Company) and the Netherlands Forensics Institute of the Dutch Ministry of Justice.

Bryan Sullivan
ADOBE

Bryan Sullivan is a Senior Security Researcher with Adobe Systems, where he focuses on cloud security issues. Prior to Adobe, he was a program manager on Microsoft's Security Development Lifecycle team, and a development manager at HP, where he helped to design HP's vulnerability scanning tools WebInspect and DevInspect.

Bryan has spoken at security industry conferences such as Black Hat, RSA Conference, BlueHat and TechEd on topics such as RIA architecture, REST, cryptography, denial-of-service defense, URL rewriting, and applying secure development processes to Agile projects. He was the author of the *MSDN Magazine* column Security Briefs, and is also the coauthor of the book *Ajax Security*.

Matthew Weeks
SECURITY RESEARCHER

Matthew Weeks is a recent graduate of Cedarville University. He has performed research in mathematics in chaos and cryptology, and focuses on information security. He enjoys finding ways to break application security, writing shellcode, and creating post-exploitation techniques. Also known as scriptjunkie, he is a frequent contributor to the Metasploit framework. His interest in infosec led him to join the Air Force and he is currently an officer.

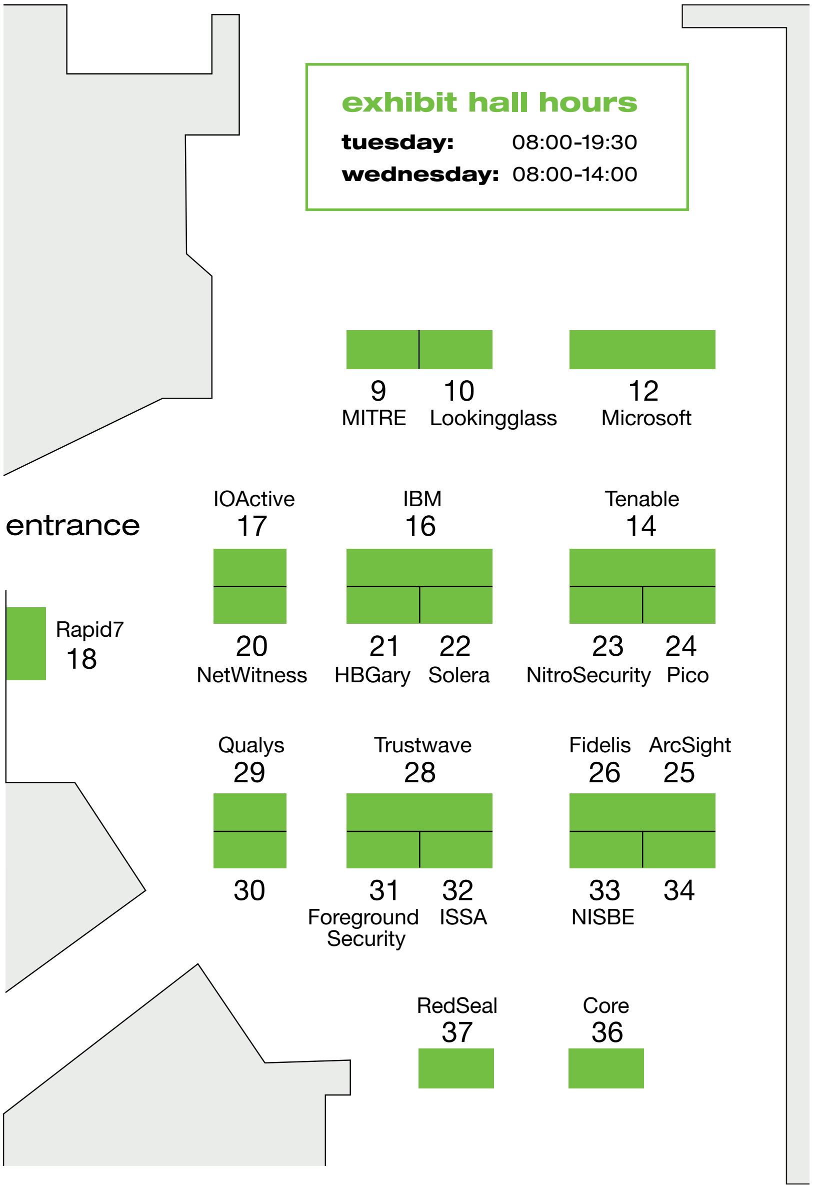
Ralf-Philipp Weinmann
UNIVERSITY OF LUXEMBOURG

Ralf-Philipp Weinmann is a cryptologist at day, and a reverse-engineer at night. He has studied and obtained his Ph.D. at the Technical University of Darmstadt and is currently researching as a post-doc at the LACS laboratory of the University of Luxembourg.

Sponsor Exhibit Hall: Independence Center A

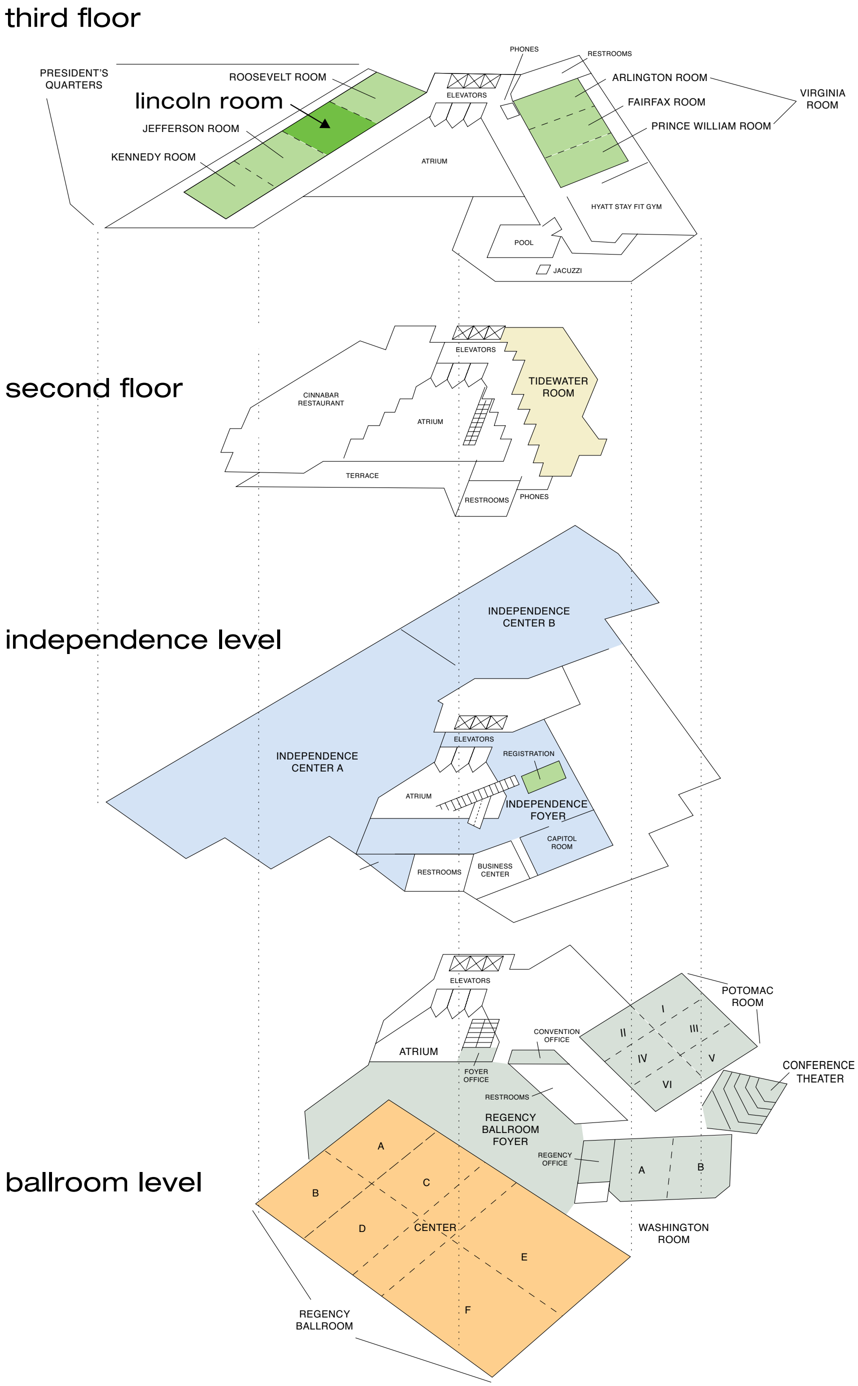
exhibit hall hours

tuesday:	08:00-19:30
wednesday:	08:00-14:00



sponsor	table
ArcSight an HP Company	25
Core Security Technologies	36
Fidelis Security Systems	26
Foreground Security	31
HBGary, Inc.	21
IBM Corporation	16
IOActive	17
ISSA	32
Lookingglass Cyber Solutions	10
Microsoft I Security Development Lifecycle	12
MITRE - CVE/OVAL	9
NetWitness	20
NISBE	33
NitroSecurity	23
Pico Computing	24
Qualys	29
Rapid7	18
RedSeal Systems, Inc.	37
Solera Networks	22
Tenable Network Security, Inc.	14
Trustwave	28

//floor plan



third floor
PRESIDENT'S QUARTERS
ROOSEVELT ROOM
lincoln room
JEFFERSON ROOM
KENNEDY ROOM
ELEVATORS
ATRIUM
PHONES
RESTROOMS
ARLINGTON ROOM
FAIRFAX ROOM
PRINCE WILLIAM ROOM
VIRGINIA ROOM
HYATT STAY FIT GYM
POOL
JACUZZI
second floor
CINNABAR RESTAURANT
ELEVATORS
ATRIUM
TIDEWATER ROOM
TERRACE
RESTROOMS
PHONES
independence level
INDEPENDENCE CENTER B
INDEPENDENCE CENTER A
ELEVATORS
REGISTRATION
ATRIUM
INDEPENDENCE FOYER
CAPITOL ROOM
RESTROOMS
BUSINESS CENTER
ballroom level
ELEVATORS
ATRIUM
CONVENTION OFFICE
FOYER OFFICE
RESTROOMS
POTOMAC ROOM
I
II
III
IV
V
VI
CONFERENCE THEATER
REGENCY BALLROOM FOYER
REGENCY OFFICE
A
B
WASHINGTON ROOM
A
B
C
D
CENTER
E
F
REGENCY BALLROOM

MASTER OFFENSE

//sponsors

diamond sponsor: Microsoft®

platinum sponsors: IBM® TENABLE Network Security® Trustwave® Information Security & Compliance

gold sponsors:
ArcSight BlackBerry® CORE SECURITY TECHNOLOGIES FIDELIS SECURITY SYSTEMS
FOREGROUND SECURITY™ Superior Security. Visible Results. GENERAL DYNAMICS Advanced Information Systems HBGary DETECT. DIAGNOSE. RESPOND. IOActive™ COMPREHENSIVE COMPUTER SECURITY SERVICES
Lookingglass MITRE NETWITNESS nitrosecurity PICO tiny mighty machines
QUALYS® RAPID7 RedSeal™ SOLERA NETWORKS™

www.blackhat.com