BLACK HAT DC 2011 //BRIEFINGS

HYATT REGENCY CRYSTAL CITY

TRAINING: JAN.16 - 17 | BRIEFINGS: JAN.18 - 19

(MEDIA LEGEND)

 WHITE PAPER DOCUMENT  PRESENTATION

SOURCE MATERIAL

KEYNOTE SPEAKER // FRANKLIN D. KRAMER

Day 1 Keynote - Cyber Conflicts: Challenging the Future

ABSTRACT TBA

//BIO: Franklin D. Kramer

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).

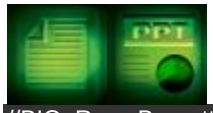
//BIO: Itzhak Avraham

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.



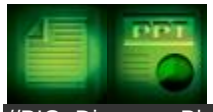
//BIO: Ryan Barnett

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.



//BIO: Dionysus Blazakis

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.

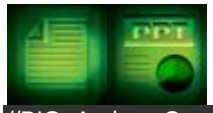
//BIO: Tom Brennan

//BIO: Ryan Barnett

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.



//BIO: Andrew Case

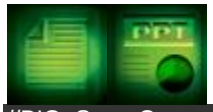
SEAN COYNE

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.

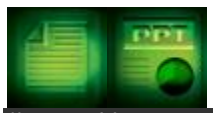


//BIO: Sean Coyne

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.



//BIO: Adrian Crenshaw

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.

//BIO: Neil Daswani

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.

//BIO: Mariano Nunez Di Croce

MARIANO NUNEZ DI CROCE, JORDAN SANTARSIERI

WORKSHOP - 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!

//BIO: Mariano Nunez Di Croce

//BIO: Jordan Santarsieri

MICHAEL EDDINGTON

WORKSHOP - 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.

//BIO: Michael Eddington

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.

//BIO: Marc Eisenbarth

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.

//BIO: Chris Gates

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).

//BIO: Cassio Goldschmidt

JOE GRAND

WORKSHOP - 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.

//BIO: Joe Grand

CHRIS HADNAGY

WORKSHOP: How to Hack Large Companies and Make Millions

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.

//BIO: Chris Hadnagy

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.

//BIO: Rob Havelt

//BIO: Bruno Goncalves de Oliveira

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.

//BIO: Vincenzo Iozzo

//BIO: Giovanni Gola

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.

//BIO: Jon Larimer

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.

//BIO: Tarjei Mandt

LAURENT OUDOT

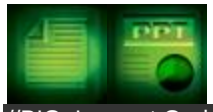
Inglourious Hackerds: Targeting Web Clients

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.



//BIO: Laurent Oudot

TOM PARKER

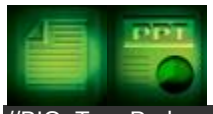
Stuxnet Redux: Malware Attribution & Lessons Learned

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.



//BIO: Tom Parker

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.

//BIO: David Perez

//BIO: Jose Pico

THOMAS ROTH

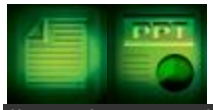
Breaking encryption in the cloud: GPU accelerated supercomputing for everyone

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.



//BIO: Thomas Roth

JAMIE SCHWETTMANN, ERIC MICHAUD

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.

//BIO: Jamie Schwettmann

//BIO: Eric Michaud

VAL SMITH, ALEXANDER POLYAKOV

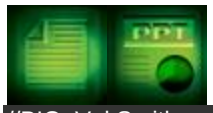
Forgotten World: Corporate Business Application Systems

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 companies 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.



//BIO: Val Smith

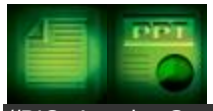
//BIO: Alexander Polyakov

ANGELOS STAVROU, ZHAOHUI WANG

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.

Angelos Stavrou is an Assistant Professor at George Mason University.



//BIO: Angelos Stavrou

//BIO: Zhaohui Wang

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.

//BIO: Matthieu Suiche

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.

//BIO: Bryan Sullivan

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.

//BIO: Matthew Weeks

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.

//BIO: Ralf-Philipp Weinmann

DINO DAI ZOVI, VINCENZO IOZZO

WORKSHOP: 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.

//BIO: Dino Dai Zovi

//BIO: Vincenzo Iozzo