BRIEFINGS

MATI AHARONI
COLLIN ANDERSON
NGUYEN ANH QUYNH
FERNANDO ARNABOLDI
AMIT ASHBEL
MICHAEL AUGER
LEONARD BAILEY
KEVIN BANKSTON
ANDREA BARISANI
MARK BASEGGIO
AVI BASHAN
OLEKSANDR BAZHANIUK
LAURA BELL
DANIELE BIANCO
HORMAZD BILLIMORIA
OHAD BOBROV
RODRIGO BRANCO
MIKE BROOKS
JONATHAN BROSSARD
REBEKAH BROWN
MATTHEW BRYANT
YURIY BULYGIN
NATE CARDOZO
COLIN CASSIDY
ERIC CASTRO
ALEX CHAPMAN
XIAOBO CHEN
JUN YOUNG CHOI

BRIEFINGS - AUGUST 5-6

WHITE PAPER

PRESENTATION

SOURCE

KEYNOTE

THE LIFECYCLE OF A REVOLUTION

PRESENTED BY

Jennifer Granick

In the early days of the public internet, we believed that we were helping build something totally new, a world that would leave behind the shackles of age, of race, of gender, of class, even of law. Twenty years on, "cyberspace" looks a lot less revolutionary than it once did. Hackers have become information security professionals. Racism and sexism have proven resiliant enough to thrive in the digital world. Big companies are getting even bigger, and the decisions corporationsnot just governmentsmake about security, privacy, and free speech affect hundreds of thousands, or millions, of people. The Four Horsemen of the Infocalypseterrorists, pedophiles, drug dealers, and money laundererare driving online policy as governments around the world are getting more deeply involved in the business of regulating the network. Meanwhile, the Next Billion Internet Users are going to connect from Asia and developing countries without a Bill of Rights. Centralization, Regulation, and Globalization are the key words, and over the next twenty years, we'll see these forces change digital networks and information security as we know it today. So where does that leave security, openness, innovation, and freedom?

The Digital Millennium Copyright Act is being used to weld the hood of cars shut to keep engine software safe from mechanics. Will we still have the Freedom to Tinker even in the oldest of technologies? What does it mean that the U.S. is a big player in the zero-day market even as international agreements seek to regulate exploit code and surveillance tools? Will we see liability for insecure software and what does that mean for open source? With advances in artificial intelligence that will decide who gets run over, who gets a loan, who gets a job, how far off can legal liability regimes for robots, drones, and even algorythms be? Is the global Internet headed for history's dustbin, and what does a balkanized network mean for security, for civil rights?

SEOKWOO CHOI
ANGELA ON-KIT CHOW
DAVID CINTZ
GREG CONTI
STEPHEN CRANE
TOM CROSS
ANG CUI
SOPHIA DANTOINE
DINO DAI ZOVI
JOSHUA DALMAN
HOANG-VU DANG
MICHAEL DAUGHERTY
ANDREW DAVIS
ANDY DAVIS
JAMES DENARO
ADRIEL DESAUTELS
ALBAN DIQUET
CHRISTOPHER DOMAS
JOSHUA DRAKE
BRIAN ENGLE
ERIC EVENCHICK
GADI EVRON
PETER FILLMORE
HALVAR FLAKE
ANDERS FOGH
TREY FORD
JAMES FORSHAW
AJIT GADDAM
ARTYOM GAVRICHENKOV
JOHANNES GILGER
GUANG GONG
SERGEY GORBATY
BRIAN GORENC
MIKHAIL GOROBETS
MATTHEW GRAEBER
JENNIFER GRANICK
MATTHEW GREEN
CLAUDIO GUARNIERI
MARK HAMMELL

In this talk, Granick will look forward at the forces that are shaping and will determine the next 20 years in the lifecycle of the revolutionary communications technology that we've had such high hopes for.

BRIEFINGS

ABUSING SILENT MITIGATIONS - UNDERSTANDING WEAKNESSES WITHIN INTERNET EXPLORERS ISOLATED HEAP AND MEMORYPROTECTION

PRESENTED BY

Brian Gorenc & Abdul-Aziz Hariri & Simon Zuckerbraun

In the Summer of 2014, Microsoft silently introduced two new exploit mitigations into Internet Explorer with the goal of disrupting the threat landscape. These mitigations increase the complexity of successfully exploiting a use-after-free vulnerability. June's patch (MS14-035) introduced a separate heap, called Isolated Heap, which handles most of the DOM and supporting objects. July's patch (MS14-037) introduced a new strategy called MemoryProtection for freeing memory on the heap.

This talk covers the evolution of the Isolated Heap and MemoryProtection mitigations, examines how they operate, and studies their weaknesses. It outlines techniques and steps an attacker must take to attack these mitigations to gain code execution on use-after-free vulnerabilities where possible. It describes how an attacker can use MemoryProtection as an oracle to determine the address at which a module will be loaded to bypass ASLR. Finally, additional recommended defenses are laid out to further harden Internet Explorer from these new attack vectors.

ABUSING WINDOWS MANAGEMENT INSTRUMENTATION (WMI) TO BUILD A PERSISTENT ASYNCHRONOUS AND FILELESS BACKDOOR

PRESENTED BY

Matthew Graeber

Imagine a technology that is built into every Windows operating system going back to Windows 95, runs as System, executes arbitrary code, persists across reboots, and does not drop a single file to disk. Such a thing does exist and it's called Windows Management Instrumentation (WMI).

With increased scrutiny from anti-virus and 'next-gen' host endpoints, advanced red teams and attackers already know that the introduction of binaries into a high-security environment is subject to increased scrutiny. WMI enables an attacker practicing a minimalist methodology to blend into their target environment without dropping a single utility to disk. WMI is also unlike other persistence techniques in that rather than executing a payload at a predetermined time, WMI conditionally executes code asynchronously in response to operating system events.

This talk will introduce WMI and demonstrate its offensive uses. We will cover what WMI is, how attackers are currently using it in the wild, how to build a full-featured backdoor, and how to detect and prevent these attacks from occurring.

ZACHARY HANIF
VALERIE HANTKE
ABDUL-AZIZ HARIRI
NISHAD HERATH
STEPHEN HILT
JENNIA HIZVER
ANDREI HOMESCU
CHUANMING HUANG
DAN HUBBARD
TRAMMELL HUDSON
ALEX IONESCU
JAMIL JAFFER
MARKUS JAKOBSSON
MARK JAYCOX
COREY KALLENBERG
THOMAS KEENAN
JAMES KETTLE
ROB KING
ENGIN KIRDA
BOB KLEIN
JOHANNES KLICK
JAKE KOUNS
XENO KOVAH
ADAM KOZY
MARINA KROTOFIL
CHRISTOPHER KRUEGEL
CHRISTINA KUBECKA
ARUN LAKHOTIA
JASON LARSEN
STEPHAN LAU
ROBERT LEE
TAMAS LENGYEL
EIREANN LEVERETT
HAIFEI LI
CHRISTOPHER LIEBCHEN
BO LIU
ALEX LONG
LEI LONG

ABUSING XSLT FOR PRACTICAL ATTACKS

PRESENTED BY

Fernando Arnaboldi

Over the years, XML has been a rich target for attackers due to flaws in its design as well as implementations. It is a tempting target because it is used by other programming languages to interconnect applications and is supported by web browsers. In this talk, I will demonstrate how to use XSLT to produce documents that are vulnerable to new exploits.

XSLT can be leveraged to affect the integrity of arithmetic operations, lead to code logic failure, or cause random values to use the same initialization vector. Error disclosure has always provided valuable information, but thanks to XSLT, it is possible to partially read system files that could disclose service or system's passwords. Finally, XSLT can be used to compromise end-user confidentiality by abusing the same-origin policy concept present in web browsers.

This presentation includes proof-of-concept attacks demonstrating XSLTs potential to affect production systems, along with recommendations for safe development.

ADVANCED IC REVERSE ENGINEERING TECHNIQUES: IN DEPTH ANALYSIS OF A MODERN SMART CARD

PRESENTED BY

Olivier Thomas

Hardware attacks are often overlooked since they are generally considered to be complex and resource intensive. However certain industries, such as pay TV, are plagued by piracy and hardware counterfeits. The threat of piracy was so great that pay TV manufacturers were forced to create extensive countermeasures to protect their smartcards in the field.

One of the most effective countermeasures is to implement parts or all of their proprietary algorithms in hardware. To analyze proprietary hardware implementations additional analysis techniques are necessary. It is no longer sufficient to follow individual signals on the chip. Instead, full extraction and analysis of the device's netlist is necessary.

This talk will focus on a case study of a widely-used pay TV smartcard. The card includes extensive custom hardware functions and has yet to be compromised after over 5 years in the field.

This talk will demonstrate the tools and techniques necessary for successfully performing the analysis of such a target. The research highlights the capabilities of advanced analysis techniques. Such techniques also make analysis significantly more efficient, reducing the time required for a study from many months to a few weeks.

ARTEM LOSEV
ADRIAN LUDWIG
JAN-OLE MALCHOW
MORGAN MARQUIS-BOIRE
MARION MARSCHALEK
DANIEL MARZIN
ALEXANDER MATROSOV
DANIEL MAYER
ALEJANDRO MAYORKAS
MICHAEL MCATEE
TERRELL MCSWEENY
HAROON MEER
ALEXANDREA MELLEN
SEAN METCALF
CHARLIE MILLER
COLBY MOORE
JOHN MOORE
SETH MOORE
JASON MORGAN
TIMOTHY MORGAN
LUCAS MORRIS
KATIE MOUSSOURIS
COLLIN MULLINER
AHAMED NAFEEZ
GABRIEL NEGREIRA BARBOSA
MATTHIAS NEUGSCHWANDTNER
VIVEK NOTANI
CHRISTOFOROS NTANTOGIAN
ALEXEY OSIPOV
MICHAEL OSSMANN
AIMIN PAN
SEAN PARK
YEONGUNG PARK
RYAN PETERS
ELLIOTT PETERSON
GREGORY PICKETT
ALEX PINTO
JOSHUA PITTS

ADVENTURES IN FEMTOLAND: 350 YUAN FOR INVALUABLE FUN

PRESENTED BY

Alexey Osipov & Alexander Zaitsev

GSM networks are compromised for over five years. Starting from passive sniffing of unencrypted traffic, moving to a fully compromised A5/1 encryption and then even to your own base station, we have different tools and opportunities. A Motorola phone retails for only $5 gives you the opportunity to peep into your girlfriend's calls. RTL-SDR retails for $20 which allows you to intercept all two-factor authentication in a medium-sized office building. Lastly, USRP retails for $700 and can intercept almost everything that you can see in 2G.

But who cares about 2G? Those who are concerned switched off of 2G. AT&T is preparing to switch off all its 2G networks by the end of 2016. Even GSMA (GSM Alliance) admitted that security through obscurity is a bad idea (referring to COMP128, A5/*, GEA algorithms and other things). 3G and LTE networks have mandatory cryptographical integrity checks for all communications, mutual authentication both for mobile devices and base station. The opportunity to analyze all protocols and cryptographical primitives due to their public availability is important.

However, the main problem is that we do not have calypso phones for 3G. We do not have cheap and ready to use devices to fuzz 3G devices over the air. Or do we? What about femtocells? Perhaps telecoms are to fast to take their guard down with security considerations embedded in 3G/4G? Users can connect to femocells. and have access the Internet on high speeds, make calls, ect.. Why don't we abuse it?

Yes, there is already research that allows you to gain control over femtocell. There is also research that allows sniffing calls and messages after gaining control. But all such solutions are not scalable. You are still bound to the telecom provider. You still have to connect to a VPN - to a core network. You have to bypass location binding and so on. Perhaps there is an easier solution? Perhaps we can create UMTS-in-a-box from readily available femtocell and have them available in large quantities without telecom-branding? We already know.

We will tell the whole story from unboxing to proof-of-concept data intercept and vulnerabilities in UMTS networks with all your favorite acronyms: HNB, SeGW, HMS, RANAP, SCTP, TR-069.

AH! UNIVERSAL ANDROID ROOTING IS BACK

PRESENTED BY

Wen Xu

In recent months, we focus on bug hunting to achieve root on android devices. Our kernel fuzzing, leaded by @wushi, generated a lot of crashes and among them, we found a kernel Use-After-Free bug which lies in all versions of Linux kernel and we successfully take advantage of it to root most android devices(version>=4.3) on the market nowadays, even for the 64-bit ones.

We leverage this bug to root whatever android devices(version>=4.3) of whatever brands. And also we are the first one in the world, as far as we are aware, rooting the 64-bit android device by taking advantage of a kernel memory corruption bug. The related kernel exploitation method is unique.

In this talk, we will explain the root cause of this UAF bug and also the methods used to exploit it. We will demonstrate how we can fill the kernel memory once occupied by the vulnerable freed kernel object with fully user-controlled data by spraying and finally achieved arbitrarily code execution in kernel mode to gain root. All our spraying methods and exploiting ways apply to the latest Android kernel, and we also bypass all the modern kernel mitigations on Android device like PXN

BRUCE POTTER
GIORGOS POULIOS
KYMBERLEE PRICE
MATTHEW PRINCE
DAVID RAYMOND
WIM REMES
EUGENE RODIONOV
VOLKER ROTH
AHMAD-REZA SADEGHI
MICHAEL SANDEE
RUNA A SANDVIK
JOSHUA SAXE
BARIS SAYDAG
CORY SCOTT
MARK SEABORN
DI SHEN
ITAMAR SHER
YAN SHOSHITAISHVILI
ALEXANDRE SIEIRA
NATALIE SILVANOVICH
MATY SIMAN
MARCO SLAVIERO
TRAVIS SMITH
ASHKAN SOLTANI
PAUL STONE
SEBASTIAN STROBL
BART STUMP
DREW SUAREZ
BING SUN
DEAN SYSMAN
SOFIANE TALMAT
OLIVIER THOMAS
ANDREE TOONK
CHRIS VALASEK
WILLIS VANDEVANTER
PAUL VIXIE
TIELEI WANG
XIAORAN WANG

and so on. Even introduced 64-bit address space fails to stop our rooting. And a very important thing is that the rooting is stable and reliable. Actually, we will present a common way to exploit android kernel Use-After-Free bug to gain root. We will also cover some new kernel security issue on the upcoming 64-bit android platform in the future.

ANDROID SECURITY STATE OF THE UNION

PRESENTED BY

Adrian Ludwig

The world of security is riddled with assumptions and guesses. Using data collected from hundreds of millions of Android devices, we'll establish a baseline for the major factors driving security in the Android ecosystem. This will help provide direction for the issues that we think will benefit the most from security community attention and research contributions.

API DEOBFUSCATOR: RESOLVING OBFUSCATED API FUNCTIONS IN MODERN PACKERS

PRESENTED BY

Seokwoo Choi

Modern packers use API obfuscation techniques to obstruct malware sandboxes and reverse engineers. In such packers, API call instructions are replaced with equivalent lengthy and complex code. API obfuscation techniques can be categorized into two according to the obfuscation time - static and dynamic. Static obfuscation embeds obfuscated instructions into the executable file. Dynamic obfuscation allocates a new memory block and copies obfuscated API function code into the newly allocated block.

For dynamic obfuscation, I suggest memory access analysis. Previous approaches use pattern matching of the obfuscating code or code optimization on instruction trace. Pattern matching and code optimization based approaches are fragile to pattern change along the version up of the packers. My approach utilizes the API function obfuscation process which is harder to change than obfuscation pattern. Embedded obfuscator in packed file obfuscates each API function during runtime by reading the original API function code and writing the obfuscated API code on a newly allocated memory block. Memory access analysis relates memory reads of each API function and its corresponding memory writes. Memory access analysis produces a map from the obfuscated API function addresses to the original API function. Obfuscated API calls are retrieved by obfuscated call pattern at OEP. Each obfuscated call instruction is replaced by the deobfuscated API calls of which the call target is resolved by the map from memory access analysis. This deobfuscation method is implemented with Intel Pin to record each memory read/write/execute of the packed binary.

For static obfuscation, I suggest iterative run-until-API method. Previous approaches used code emulators to identify obfuscated API calls. But most code emulators are not appropriate for deobfuscation because they are developed for emulating the whole operating system. Developing own emulators is time consuming because it requires implementing complex runtime behavior, such as exception based branches and multi-threads that modern packers use. I use a dynamic binary instrumentation tool - Intel Pin - by which the process can be monitored without being detected by protection mechanisms of the packers. After executing the packed binary until the original entry point, the tool changes the instruction pointer into an obfuscated API call address. The execution continues

ZHANYI WANG
PATRICK WARDLE
GEORGE WEBSTER
TAO WEI
RALF-PHILIPP WEINMANN
TILLMANN WERNER
KYLE WILHOIT
MATT WOLFF
SASHA WOOD
NEIL WYLER
CHRISTOS XENAKIS
PENG XIAO
HAO XU
WEN XU
MARK VINCENT YASON
TING-FANG YEN
YU YU
JOSEPH ZADEH
ALEXANDER ZAITSEV
KIM ZETTER
YULONG ZHANG
YUNHAI ZHANG
ZHUO ZHANG
TOBIAS ZILLNER
SIMON ZUCKERBRAUN

until the instruction pointer reaches the real API function. So the original API function is identified, but the function itself is not executed. In order to confirm the identified API function is correct, the integrity of stack pointer and stack data is also checked. This process is performed for each obfuscated API call instruction. In order to identify obfuscated API calls, the tool searches for all call instructions of which the target address is in the other section of the process.

With the two deobfuscation methods, obfuscated API calls of Themida 32/64 packed binaries can be deobfuscated. We can analyze the deobfuscated binary with common reversing tools, such as x64dbg, Ollydbg and IDA Pro.

ASSESSING AND EXPLOITING BIGNUM VULNERABILITIES

PRESENTED BY

Ralf-Philipp Weinmann

The majority of deployed asymmetric cryptography implementations (RSA, DH, ECDH/ECDSA with GF(p) curves) need to perform calculations on integers that are larger than a single machine word. Just like every software package, implementations of multi-precision integer arithmetic sometimes have bugs. This talk investigates the implications of these bugs and shows how they can be used by attackers to exploit asymmetric cryptographic primitives. Isolating bug patterns and understanding exploitation requirements allows us to develop strategies for automated bug hunting.

ATTACKING ECMASCRIPT ENGINES WITH REDEFINITION

PRESENTED BY

Natalie Silvanovich

The dynamic nature of ECMAScript allows for functions and properties to be redefined in a variety of ways - even functions that are vital for internal functionality of the ECMAScript engine. This presentation explores the problems that can arise from ECMAScript redefinition. It goes through the various ways that functions and properties can be redefined in different ECMAScript implementations and describes several vulnerabilities we found as a result of these methods. It also provides some strategies for finding these types of security issues in other targets.

ATTACKING HYPERVISORS USING FIRMWARE AND HARDWARE

PRESENTED BY

Yuriy Bulygin & Alexander Matrosov & Mikhail Gorobets & Oleksandr Bazhaniuk

In this presentation, we explore the attack surface of modern hypervisors from the perspective of vulnerabilities in system firmware, such as BIOS and in hardware emulation. We will demonstrate a number of new attacks on hypervisors based on system firmware vulnerabilities with impacts ranging from VMM DoS to hypervisor privilege escalation to SMM privilege escalation from within the virtual machines.

We will also show how a firmware rootkit based on these vulnerabilities could expose secrets within virtual machines and explain how firmware issues can be used for analysis of hypervisor-protected content such as VMCS structures, EPT tables, host physical addresses (HPA) map, IOMMU page tables etc. To enable further hypervisor security testing, we will also be releasing new modules in the open source CHIPSEC framework to test issues in hypervisors when virtualizing hardware.

ATTACKING INTEROPERABILITY - AN OLE EDITION

PRESENTED BY

Haifei Li & Bing Sun

Object Linking and Embedding (OLE) is a technology based on Component Object Model (COM) allowing an application to embed and link to other documents or objects, and its primarily used in Microsoft Office and WordPad. In the recent years, we have seen a number of vulnerabilities, especially some critical zero-day attacks, are involving OLE. The typical examples are the "Sandworm" attack (CVE-2014-4114) that was disclosed in October 2014, and the CVE-2012-0158 - a years-old vulnerability but is still being actively exploited in the real world.

However, the previous work usually focus on the vulnerability or malware but the internals of OLE are never examined. This paper intends to fill this gap. The another important part of this research is to explore the attack surface it exposes on Windows, and to explain how an attacker may possibly leverage OLE vulnerability to perform document-based exploitation. These areas are never being looked at from a security point of view. In the 0-day demo section of our presentation, we will disclose and demonstrate a previously-unknown OLE attack vector introduced by the nature of the OLE mechanism, which could lead to a series of similar vulnerabilities being discovered in future.

ATTACKING YOUR TRUSTED CORE: EXPLOITING TRUSTZONE ON ANDROID

PRESENTED BY

Di Shen

For years fingerprint scanning has been supported in many Android devices. Fingerprint scanning on ARM always needs an implementation of TrustZone. While we enjoy unlocking devices and paying by fingerprint, we also figure out these new features bring out some new attack surfaces. Attacking the kernel of Android or the secure world of TrustZone may be not impossible.

Theoretically, devices developed with TrustZone technology can support a full Trusted Execution Environment (TEE). TEE runs in a special CPU mode called secure mode, so memory for secure mode and security functions can be hidden to the normal world. In this way, Android vendors can provide many secure features such as fingerprint scanning, DRM, kernel protection, secure boot, and so on.

Even though TrustZone is designed for solving security problems, there may be some security issues inside when a developer implements a TEE for Android. The Huawei Hisilicon Kirin 925 processor is the new chip being used on the Huawei Ascend Mate 7, and Hisilicon implemented its own TEE software. There are few documents about it. I found some vulnerabilities both in a normal Android world and the secure world while analyzing Hisilicon's TEE OS.

In this talk, I'll show how to analyze the TEE architecture of Huawei Hisilicon and find some new vulnerabilities in such an undocumented black hole. Then, I'll talk about exploit development in TrustZone. I exploited two bugs, one for rooting Androids normal world and disabling the newest SE for Android, the other for running shellcode in secure world. With these exploits, we can get the fingerprint image or bypass some other security features.

AUTOMATED HUMAN VULNERABILITY SCANNING WITH AVA

PRESENTED BY

Laura Bell

It will not be a surprise to you that of all the elements within our organisations and systems, the people are most likely to expose us to risk. In short we are a mess of emotional unpredictablity that threaten us all (and security professionals are the worst of the bunch).

Many very clever people have spent a long time teaching us this. This is not news.

So if this is the case, why in 20 years of modern information security have we done so little to actively protect them?

Technical vulnerability scanning is now mature and commoditised, allowing us to repeatably test and adapt our systems in the face of a changing threat landscape. The time has come to apply the same logic to our people, actively understand human connectivity and behaviours when faced with threat and understand the effect of this behaviour with our organisations.

This talk will discuss why this is a difficult challenge and introduce AVA, the first automated human vulnerability scanner that allows us to map the connectivity of our people, test them with a range of security threats and measure their behaviour. A tool built to make human security risk (and the effectiveness of our countermeasures and training) measurable.

Let's change the way we approach human security risk. Let's protect our people.

BACK DOORS AND FRONT DOORS BREAKING THE UNBREAKABLE SYSTEM

PRESENTED BY

James Denaro & Matthew Green

Governments are demanding backdoor access to encrypted data - particularly on mobile devices and in the cloud - as strong encryption becomes commonplace. Governments fear going dark with encryption hindering criminal and national security investigations. Privacy advocates have opposed backdoors since the 1990s and the battle is heating up again, this time on a global scale. Backdoors have also been criticized as making systems inherently less secure. Current proposals, such as key escrow, split-key systems, and account mirroring, are complicated and difficult to implement securely. We provide a background on end-to-end encryption, a techno-political history of backdoors, and an update on the current state of affairs. We explore various options for working around end-to-end encryption, focusing on implementation details and potential weakness due to administrative failure in procedures to request and obtain access and technical attacks on the implementation. We conclude with proposals to answer the lingering question of whether there is a solution that does not weaken encryption systems or mandate technological designs while still enabling limited government access to secure communications.

BATTLE OF THE SKM AND IUM: HOW WINDOWS 10 REWRITES OS ARCHITECTURE

PRESENTED BY

Alex Ionescu

In Windows 10, Microsoft is introducing a radical new concept to the underlying OS architecture, and likely the biggest change to the NT design since the decision to move the GUI in kernel-mode.

In this new model, the Viridian Hypervisor Kernel now becomes a core part of the operating system and implements Virtual Secure Machines (VSMs) by loading a true microkernel - a compact (200kb) NT look-alike with its own drivers called the Secure Kernel Mode (SKM) environment, which then uses the Hypervisor to hook and intercept execution of the true NT kernel. This creates a new paradigm where the NT Kernel, executing in Ring 0, now runs below the Secure Kernel, at Ring ~0 (called Virtual Trust Level 1).

But it doesn't stop there - as the Ring 0 NT kernel now has the ability to not only create standard Ring 3 user-mode applications, but also Ring ~3 applications (or Virtual Trust Level 0) that run in Isolated User Mode (IUM). Because VTLs are all more privileged than Ring 0, this now creates a model where a user-mode application running inside a VSM now has data and rights that even the kernel itself cannot modify. Why go through all this trouble? Because it seems like the hottest thing these days is Pass-the-Hash, and attacks must seemingly be mitigated at all costs. And even in Windows 8.1, an attacker with the permissions to load a kernel driver can bypass the existing mitigations (and Mimikatz is signed!). With VTLs, now even the most privileged attacker is only as privileged as the hypervisor will allow it - never able to truly read the hash date that is stored in the secure partition.

How "secure" is this new model really? And what prevents a malicious application from running in such a secure mode to begin with?

BEHIND THE MASK: THE AGENDA TRICKS AND TACTICS OF THE FEDERAL TRADE COMMISSION AS THEY REGULATE CYBERSECURITY

PRESENTED BY

Michael Daugherty

While the FTC, FCC and Homeland Security joust over who is going to regulate the internet, Michael J. Daugherty will rivet you about his blood in the water battle with the Federal Trade Commission over their relentless investigation into LabMD's data security practices showing you what they do to those who dare not "go along to get along."

This is an insider's look at how agencies exploit their power by bullying the small and weak to control the private sector. You will hear about Mike's shrewd investigation of the investigator (FTC) which resulted in a House Oversight investigation, a stinging Congressional report about the FTC's behavior, and criminal immunity from the Justice Department for a whistleblower. The administrative case against LabMD, stayed in June 2014 when the whistleblower pled the 5th, started again May 5, 2015, after criminal immunity had been granted. Mike exposes the real time maneuvers of government lawyers and regulators who are accustomed to no one looking.

Because of his work, Mike has testified before the House of Representatives House Oversight Committee and regularly keynotes in front of healthcare, law, business and technology audiences educating them on what to expect when the Federal

Government investigates you.

BGP STREAM

PRESENTED BY

Dan Hubbard & Andree Toonk

BGP is the fabric of routing on the Internet today. There are approximately half a million routes on the Internet originated by about 50,000 unique Autonomous Systems. On a typical day there are thousands of changes and although the vast majority of these are simply planned routing changes, configuration updates, and network additions there are signals in the noise that can be detected as nefarious. Throughout the last couple years there have been several large scale BGP incidents, such as outages and hijacks of networks that have been done using BGP. These include government sponsored regimes taking entire countries offline and criminals routing traffic for profit.

BGPmon has been operating a network of BGP probes, classifiers, and associated alerts on these changes and has discovered and publicized several attacks that utilize BGP.

Today, we are announcing BGP Stream. This stream will be publishing on Twitter and open to everyone with a goal of announcing potentially malicious BGP/ASN data. By subscribing to the stream one can monitor and alert potentially damaging network changes that affect traffic flows.

BIG GAME HUNTING: THE PECULIARITIES OF NATION-STATE MALWARE RESEARCH

PRESENTED BY

Morgan Marquis-Boire & Marion Marschalek & Claudio Guarnieri

The security industry focus on state-sponsored espionage is a relatively recent phenomenon. Since the Aurora Incident brought nation-state hacking into the spotlight, there's been high profile reports on targeted hacking by China, Russia, U.S.A, Israel, to name a few. This has lead to the rise of a lucrative Threat intelligence business, propelling marketing and media campaigns and fueling political debate.

This talk will cover the idiosyncrasies of nation-state malware research using the experiences of presenters in the 'Threat Analyst Sweatshop.' Regin (aka WARRIORPRIDE, allegedly written by the Five Eyes) and Babar (aka SNOWGLOBE, allegedly written by France) will be used as case studies in examining attribution difficulties. Additionally, we'll examine attributing commercially written offensive software (implants and exploits) and the (mostly negative) vendor responses. We'll cover what happens when you find other players on the hunt, and address the public misconception that attribution is frequently done using open source information.

We will focus on the attribution problem and present a novel approach on creating credible links between binaries originating from the same group of authors. Our goal is to add to transparency in attribution and supply analysts with a tool to emphasize or deny vendor statements. The technique is based on features derived from different domains, such as implementation details, applied evasion techniques, classical malware traits or infrastructure attributes; which are then leveraged to compare the handwriting among binaries.

BREAKING ACCESS CONTROLS WITH BLEKEY

RFID access controls are broken. In this talk, we will demonstrate how to break into buildings using open-source hardware we are releasing.

Over the years, we have seen research pointing to deficiencies in every aspect of access control systems: the cards, the readers, and the backend. Yet, despite these revelations, there has been no meaningful change in their design or reduction in use around the world. Do these companies not care about physical security, or do they not understand the implications of these weaknesses?

We have improved upon previous research with an open-source hardware device that exploits the communication protocol used by the majority of access control systems today. Using a tiny device that can be easily embedded in an RFID reader, attendees will learn how to use Bluetooth LE and a cell phone (or PC) to circumvent access controls, log access information, and clone RFID cards.

Our goal is to use this device to help those relying on insecure devices understand the risks. We will also explain what can be done to lower the risk of access control attacks.

PRESENTED BY

Eric Evenchick & Mark Baseggio

BREAKING HONEYPOTS FOR FUN AND PROFIT

We will detect, bypass, and abuse honeypot technologies and solutions, turning them against the defender. We will also release a global map of honeypot deployments, honeypot detection vulnerabilities, and supporting code.

The concept of a honeypot is strong, but the way honeypots are implemented is inherently weak, enabling an attacker to easily detect and bypass them, as well as make use of them for his own purposes. Our methods are analyzing the network protocol completeness and operating system software implementation completeness, and vulnerable code.

As a case study, we will concentrate on platforms deployed in real organizational networks, mapping them globally, and demonstrating how it is possible to both bypass and use these honeypots to the attacker's advantage.

PRESENTED BY

Dean Sysman & Gadi Evron & Itamar Sher

BREAKING HTTPS WITH BGP HIJACKING

BGP hijacking is now a reality: it happens often (mostly in the form of route leak due to misconfiguration, though), there's no practical way to prevent it, we have to deal with it. Internet routing was designed to be a conversation between trusted parties, but now it isn't, though it still behaves like it is.

However, people are used to believe that BGP hijacking is not a huge issue. Yes, a denial of service can happen, and some plaintext data may be disclosed to an attacker, but there's nothing more to it, since all sensitive data transmitted over the

PRESENTED BY

Artyom Gavrichenkov

Internet should be encrypted already, and a man in the middle of the Internet cannot decrypt it or break into encrypted connection. So there's pretty much nothing to really worry about.

The problem is: the encryption is backed by SSL/TLS PKI, which itself trusts Internet routing. Now there's a way to exploit this trust, and we are going to show how, and to discuss how to prevent this from happening.

BREAKING PAYLOADS WITH RUNTIME CODE STRIPPING AND IMAGE FREEZING

PRESENTED BY

Collin Mulliner & Matthias Neugschwandtner

Fighting off attacks based on memory corruption vulnerabilities is hard and a lot of research was and is conducted in this area. In our recent work we take a different approach and looked into breaking the payload of an attack. Current attacks assume that they have access to every piece of code and the entire platform API. In this talk, we present a novel defensive strategy that targets this assumption. We built a system that removes unused code from an application process to prevent attacks from using code and APIs that would otherwise be present in the process memory but normally are not used by the actual application. Our system is only active during process creation time, and, therefore, incurs no runtime overhead and thus no performance degradation. Our system does not modify any executable files or shared libraries as all actions are executed in memory only. We implemented our system for Windows 8.1 and tested it on real world applications. Besides presenting our system we also show the results of our investigation into code overhead present in current applications.

BRING BACK THE HONEYPOTS

PRESENTED BY

Haroon Meer & Marco Slaviero

Honeypots were all the rage in the 90's - A raft of tools (and even a world-wide alliance) sprung up extolling their virtues but they never managed to live up to their hype. They were largely relegated to researchers and tinkerers on the fringes. At the same time, we have the Verizon DBIR telling us that most companies are first informed by 3rd parties that they are breached. This is a stupid situation to be in.

Well deployed honeypots can be invaluable tools in the defenders arsenal, and don't need to look anything like the honeypots of old. From application layer man-traps, to booby-trapped documents. From network-level deception, to cloud based honeypottery, we are bringing honeypots back!

During this talk, we will discuss and demonstrate the current state of the art regarding honeypots. We will explore the factors that limit adoption (and will discuss how to overcome them.) We will demonstrate new techniques to make your honeypots more "hacker-discoverable" & will share data from running actual honeypots in real organizations. We will also discuss (and release) OpenCanary, our new open source honeypot (along with supporting scripts and utilities).

Over the past few years, honeypots have gotten a bit of a bad rap. We will give you tools, techniques and takeaways, to move them from geeky time-wasters, to the most useful pieces of kit you will deploy.

BRINGING A CANNON TO A KNIFE FIGHT

PRESENTED BY

Adam Kozy & Johannes Gilger

Chinas Great Cannon (GC), the offensive standalone system that serves as a complement to its defensive Great Firewall (GFW), debuted with a bang in early 2015, carrying out massive attacks on anti-censorship site Greatfire.org and everyones favorite code-sharing resource, Github. Not cool, man...

This talk aims to examine Chinas destructive new toy and its methods for turning both Chinese users and global visitors to Chinese sites into the worlds largest botnet. We'll review the Great Cannons early construction, examine how it intercepts traffic as a Man-in-the-Middle proxy by doing live probe requests to the GC & GFW to determine the difference between their traffic, and show the relative ease with which it can further weaponize users to carry out attacks on sites deemed a threat to the Chinese Communist Party. Arguably as important as comprehending the methods by which the Great Cannon functions is understanding the WHY we intend to walk you through why the GC made an appearance at the time it did, the political underpinnings behind the decision to attack the Github repos, and how you can expect to see it change in the future as HTTPS and DNSSEC become more widely used.

Are you wondering how to protect your company's traffic even if you use Baidu Ads or communicate with Chinese servers? Yep, we'll cover that too.

Although the GC was wielded with all the subtlety of a sledgehammer during its debut, it is certainly capable of being a much more devious and dangerous tool to suppress perceived threats in a targeted and hard-to-detect fashion. Needless to say, it won't be going away anytime soon. Bulletproof yourself by attending this talk and learning all about Chinas Great Cannon.

BROADCASTING YOUR ATTACK: SECURITY TESTING DAB RADIO IN CARS

PRESENTED BY

Andy Davis

Digital Audio Broadcasting (DAB) radio receivers can be found in many new cars and are in most cases integrated into an IVI (In-Vehicle Infotainment) system, which is connected to other vehicle modules via the CAN bus. Therefore, any vulnerabilities discovered in the DAB radio stack code could potentially result in an attacker exploiting the IVI system and pivoting their attacks toward more cyber-physical modules such as those concerned with steering or braking. This talk will discuss the complex protocol capabilities of DAB and DAB+ and describe the potential areas where security vulnerabilities in different implementations may exist. I will discuss the use of Software Defined Radio in conjunction with open source DAB transmission software to develop our security testing tool (DABble). Finally, I will talk about some of our findings, the implications of exploiting DAB-based vulnerabilities via a broadcast radio medium, and what this could mean for the automotive world.

BYPASS CONTROL FLOW GUARD COMPREHENSIVELY

PRESENTED BY

Control Flow Guard (CFG) is an exploit mitigation technique that Microsoft enabled in Windows 8.1 Update 3 and Windows 10 technical preview. CFG checks the target of indirect call and raises an exception if the target is invalid, thus preventing a vital step of many exploit techniques.

This talk analyses the weak-point of CFG and presents a new technique that can be used to bypass CFG comprehensively and make the prevented exploit techniques exploitable again. Furthermore, this technique is based on a generic capability, thus more exploit techniques can be developed from that capability.

Yunhai Zhang

BYPASS SURGERY ABUSING CONTENT DELIVERY NETWORKS WITH SERVER-SIDE-REQUEST FORGERY (SSRF) FLASH AND DNS

PRESENTED BY

Mike Brooks & Matthew Bryant

It is unlikely when a bug affects almost every CDN and it becomes vulnerable, but when this happens the possibilities are endless and potentially disastrous.

Imagine – a Facebook worm giving an attacker full access to your bank account completely unbeknownst to you, until seven Bentleys, plane tickets for a herd of llamas, a mink coat once owned by P. Diddy, and a single monster cable all show up on your next statement. What a nightmare.

But in all seriousness, thousands of websites relying on the most popular CDNs are at risk. While some application requirements may need a security bypass in order to work, these intentional bypasses can become a valuable link in an exploit chain. Our research has unveiled a collection of general attack patterns that can be used against the infrastructure that supports high availability websites.

This is a story of exploit development with fascinating consequences.

CERTIFI-GATE: FRONT-DOOR ACCESS TO PWNING MILLIONS OF ANDROIDS

PRESENTED BY

Ohad Bobrov & Avi Bashan

Hundreds of millions of Android devices, including those running Lollipop, the latest and most secure version of Android OS, can be hijacked. A comprehensive study has revealed the existence of multiple instances of a fundamental flaw within the Android customisation chain that leave millions of devices (and users) vulnerable to attack.

These vulnerabilities allow an attacker to take advantage of unsecure apps certified by OEMs and carriers to gain unfettered access to any device, including screen scraping, key logging, private information exfiltration, back door app installation, and more. In this session, Lacoon researchers will walk through the technical root cause of these responsibly-disclosed vulnerabilities including hash collisions, IPC abuse and certificate forging which allow an attacker to grant their malware complete control of a victims device. We'll explain why these vulnerabilities are a serious problem that in some ways can't be completely eliminated, show how attackers exploit them, demonstrate an exploit against a live device, and provide remediation advice.

CLONING 3G/4G SIM CARDS WITH A PC AND AN OSCILLOSCOPE: LESSONS LEARNED IN PHYSICAL SECURITY

PRESENTED BY

Yu Yu

Recently, documents leaked from Edward Snowden alleged that NSA and GCHQ had stolen millions of SIM card encryption keys from one of the world's largest chip manufacturers. This incident draws the public attention to the longstanding concern for the mobile network security. Despite that various attacks against 2G (GSM) algorithms (COMP-128, A5) were found in literature, no practical attacks were known against 3G/4G (UMTS/LTE) SIM cards. 3G/4G SIM cards adopt a mutual authentication algorithm called MILENAGE, which is in turn based on AES-128, a mathematically secure block cipher standardized by NIST. In addition to the encryption key, MILENAGE also uses nearly a dozen of 128-bit secrets to further obfuscate the algorithm.

In this presentation, we show how to amount differential power analysis that recovers encryption key and other secrets in a divide-and-conquer manner within a few (10 to 40) minutes, allowing for SIM cards cloning. Our experiments succeeded on eight 3G/4G SIM cards from a variety of operators and manufacturers. The measurement setup of our experiment mainly consists of an oscilloscope (for power acquisition), an MP300-SC2 protocol analyzer (for interception of the messages), a self-made SIM card reader, and a PC (for signal processing and cryptanalysis). We finish the presentation by showing what happens to a 3G/4G SIM card and its duplicate when receiving texts/calls at the same time.

COMMERCIAL MOBILE SPYWARE - DETECTING THE UNDETECTABLE

PRESENTED BY

Joshua Dalman & Valerie Hantke

Research shows commercial spyware is becoming common place. These programs turn smartphones into effective spy tools and pose a threat to both smartphone users privacy and to corporate enterprises. Furthermore, the tools are sold and marketed as being completely undetectable to the users. We put that claim to the test.

CRACKLORD: MAXIMIZING PASSWORD CRACKING BOXES

PRESENTED BY

Lucas Morris & Michael McAtee

Over the past several years the world of password cracking has exploded with new tools and techniques. These new techniques have made it easier than ever to reverse captured password hashes. Based on our experience, within the past few years passwords have often become the first step into compromising the entire network. New techniques such as LLMNR/NetBIOS response have reduced the efficacy of pass the hash techniques, again increasing the necessity of actually cracking the hashes. With the addition of powerful techniques, from GPGPU cracking to rainbow tables, it is easier than ever to access the plaintext for fun and profit.

Heavy utilization of GPUs has increased the power of these tools exponentially. Many organizations and individuals have built massive GPU password cracking rigs and cloud based services, such as AWS GPU instances, have also placed high performance cracking into the realm of affordability. Although the current tools do an amazing job providing heavy utilization for individual hardware, they have not kept pace with the need for distributed cracking services. Additionally, these tools can often make the sharing of expensive hardware difficult, requiring manual job tracking, GNU screen, or scripts put together to queue cracking jobs.

CrackLord attempts to change this by providing a scalable, pluggable, and distributed password cracking system. Better said, CrackLord is a way to load balance the resources, such as GPUs and CPUs, from multiple hardware systems into a single queuing service. CrackLord uses two primary services: the Resource and Queue. The Resource is a service that runs on individual systems, providing access to their underlying hardware. Resources utilize various tools, such as Hashcat, John the Ripper, rcrack, or others, to run jobs and use the local CPU or GPU to crack hashes. The Queue is a service that runs on a single system, providing an interface for users to submit cracking jobs. These jobs are then processed and sent to available Resources to perform the actual crack. Users are able to create, pause, resume, and delete jobs in the Queue which will communicate with the Resource to handle the results. Finally, the system is designed to be extensible providing standard interfaces and libraries allowing new tools, resource types, and management interfaces to be written and added as necessary.

CRASH & PAY: HOW TO OWN AND CLONE CONTACTLESS PAYMENT DEVICES

PRESENTED BY

Peter Fillmore

With all this talk about NFC payments (Apple Pay, Google Wallet, etc.), are there claims on your card that can't be cloned? What security mechanisms can prevent this? How can they be subverted to make fraudulent transactions?

This talk answers these questions by taking you through how NFC payments work and how you can perform fraudulent transactions with just an off-the-shelf phone and a little bit of software. I'll take you through how you can clone common NFC payment cards; show you the attacks and explain why it is possible. Information will be provided on the inexpensive tools now available for testing NFC devices and how to put together your own testing lab to test for vulnerabilities over these interfaces.

DANCE LIKE NOBODYS WATCHING ENCRYPT LIKE EVERYONE IS: A PEEK INSIDE THE BLACK HAT NETWORK

PRESENTED BY

Neil Wyler & Bart Stump

Every year thousands of security professionals descend upon Las Vegas to learn the latest and greatest offensive and defensive infosec techniques. They check into a hotel, they pick up their badge, they get on the Black Hat network...and inevitably, they play. "Security professionals"? That's just corporate speak for "Hackers."

This presentation will explore the inner workings of what is, without a doubt, one of the most hostile network environments ever created. Oh!, we don't make it hostile. You do. We just try to keep it up and running.

So come see what goes into the planning, deployment, and maintenance of the Black Hat network infrastructure. We'll share as much as we can about the history of the network, the gear we're using today, and the traffic patterns that keep us sweating, and laughing, well into the night.

DATA-DRIVEN THREAT INTELLIGENCE: METRICS ON INDICATOR DISSEMINATION AND SHARING

PRESENTED BY

Alex Pinto & Alexandre Sieira

For the past 18 months, Niddel have been collecting threat intelligence indicator data from multiple sources in order to make sense of the ecosystem and try to find a measure of efficiency or quality in these feeds. This initiative culminated in the creation of Combine and TIQ-test, two of the open source projects from MLSec Project. These projects have been improved upon for the last year and are able to gather and compare data from multiple Threat Intelligence sources on the Internet.

We take this analysis a step further and extract insights form more than 12 months of collected threat intel data to verify the overlap and uniqueness of those sources. If we are able to find enough overlap, there could be a strategy that could put together to acquire an optimal number of feeds, but as Niddel demonstrated on the 2015 Verizon DBIR, that is not the case.

We also gathered aggregated usage information from intelligence sharing communities in order to determine if the added interest and "push" towards sharing is really being followed by the companies and if its adoption is putting us in the right track to close these gaps.

Join us in an data-driven analysis of over an year of collected Threat Intelligence indicators and their sharing communities!

DEEP LEARNING ON DISASSEMBLY

PRESENTED BY

Matt Wolff & Andrew Davis

Recently, the application of deep learning techniques to natural language processing has led to state-of-the-art results for speech recognition, language modeling, and language translation. To some degree, disassembly can be considered an extension or augmentation of natural language. As an loose example, many experienced reverse engineers can read through disassembled code and understand the meaning in one pass, similar to their skill in reading text in natural languages.

In this talk, we show the effectiveness of applying deep learning techniques to disassembly in an effort to generate models designed to identify malware. Starting with a brief explanation of deep learning, we then work through the different pieces of the pipeline to go from a collection of raw binaries, to extraction and transformation of disassembly data, and training of a deep learning model. We then conclude by providing data on the efficacy of these models, and follow up with a live demo where we will evaluate the models against active malware feeds.

DEFEATING MACHINE LEARNING: WHAT YOUR SECURITY VENDOR IS NOT TELLING YOU

PRESENTED BY

Bob Klein & Ryan Peters

Machine learning is rapidly gaining popularity in the security space. Many vendors and security professionals are touting this new technology as the ultimate malware defense. While evidence from both research and practice validates the improved efficacy of machine learning-based approaches, their drawbacks are rarely discussed.

In this talk, we will demonstrate, from an attacker's perspective, how commonly deployed machine learning defenses can be defeated. We then step back and examine how existing systemic issues in the network security industry allow this to occur, and begin the discussion with the community about these issues. Finally, we propose a solution that uses novel data sourcing techniques to address these problems.

DEFEATING PASS-THE-HASH: SEPARATION OF POWERS

PRESENTED BY

Seth Moore & Baris Saydag

The harvest and reuse of symmetric credentials has become a linchpin of system breaches. Under the guise of Pass-the-Hash, attackers are adept at reusing not only passwords, but derivatives such as hashes and keys. Windows 10 brings strong isolation of these artifacts, defeating Pass-the-Hash attacks originating from clients.

Legacy protocols such as Kerberos and NTLM are broadly deployed and will be vulnerable to attack for many years to come. Business needs dictate that Pass-the-Hash mitigations must work within the limitations of these protocols. In such an environment, how can Pass-the-Hash be stopped?

The answer is a new level of OS isolation, based on virtualization technology. Hashes, keys, and other secrets are sequestered within physical memory not even the kernel may read. If an attacker cannot read the secrets, the attacker cannot reuse them.

In this talk, we give an overview of the isolation technology. In addition, we answer questions such as: How does Windows 10 guarantee isolation of secrets? How does this go beyond simple client security? Can this even be achieved without major protocol revisions?

DISTRIBUTING THE RECONSTRUCTION OF HIGH-LEVEL INTERMEDIATE REPRESENTATION FOR LARGE SCALE MALWARE ANALYSIS

PRESENTED BY

Rodrigo Branco & Gabriel Negreira Barbosa & Eugene Rodionov & Alexander

Malware is acknowledged as an important threat and the number of new samples grows at an absurd pace. Additionally, targeted and so called advanced malware became the rule, not the exception. Analysts and companies use different degrees of automation to be able to handle the challenge, but there is always a gap. Reverse engineering is an even harder task due to the increased amount of work and the stricter time-frame to accomplish it. This has a direct impact on the investigative process and thus makes prevention of future threats more challenging.

Matrosov

In this work, the authors discuss distributed reverse engineering techniques, using intermediate representation (thanks Hex-Rays team for support us in this research) in a clustered environment. The results presented demonstrate different uses for this kind of approach, for example to find algorithmic commonalities between malware families.

A higher level abstraction of the malware code is constructed from the abstract syntax tree (ctree) provided by Hex-Rays Decompiler. That abstraction facilitates the extraction of characteristics such as domain generation algorithms (DGA), custom encryption and specific parsers for configuration data. In order to reduce the number of false positives in some C++ metadata identification, such as virtual function tables and RTTI, the authors created the object-oriented artifacts directly from the analyzed malware.

The extracted characteristics of 2 million malware samples are analyzed and the presented results provide a rich dataset to improve malware analysis efforts and threat intelligence initiatives. With that dataset, other researchers will be able to extract a ctree from new samples and compare to the millions we performed.

As an additional contribution, the gathered representation together with all the raw information from the samples will be available to other researchers after the presentation; together with additional ideas for future development. The developed Hex-Rays Decompiler plugin and analysis/automation tools used to extract the characteristics will also be made available to the audience on Github.

DOM FLOW - UNTANGLING THE DOM FOR MORE EASY-JUICY BUGS

PRESENTED BY

Ahamed Nafeez

Modern day web applications are quite JavaScript heavy and its only going to get worse for pen-testers and scanners alike, because of the complexity involved. Client side attacks like DOM XSS, insecure usage of WebSockets, unwanted use of Global variables, insecure user-defined functions, and many other similar patterns are quite hard to detect for the pen-tester manually or even by static JavaScript analysers.

How about we hook onto all the JavaScript actions dynamically and transparently? The results are very useful to conduct more advanced penetration tests on web apps. Existing JS dynamic analysis tools only work if its built within the code, such as performance analysis. Moreover, the JS files are minified in production. To solve this problem enter Hookish!

Hookish! is an open-source chrome-extension which overrides most of the DOM properties and brings out the interesting stuff to the pen-tester. For instance, imagine a single page web-app with some complex JS code and you would like to know whether all the content being dynamically updated to the DOM are clean. Do they use a safe filter / encoder before pushing it to the DOM? Well, Hookish! can solve this problem for you. It hooks into all XHR responses, and matches those strings with DOM mutation events like DOMNodeInserted, DOMSubtreeModified etc. and also tries relevant payloads to check whether there are possible DOM XSS vulnerabilities and other such shenanigans. This is just scratching the surface, things can become more intuitive when a pen-tester uses Dom Flow.

Dom Flow is a feature where one can drag and drop the sources and sinks as he wishes to understand how data flows between them in the given app. This is something which brings out more understanding of the app and reveals hidden DOM based bugs and also helps the pen-tester to conduct further attacks.

EMANATE LIKE A BOSS: GENERALIZED COVERT DATA EXFILTRATION WITH FUNTENNA

PRESENTED BY

Ang Cui

Funtenna is a software-only technique which causes intentional compromising emanation in a wide spectrum of modern computing hardware for the purpose of covert, reliable data exfiltration through secured and air-gapped networks. We present a generalized Funtenna technique that reliably encodes and emanates arbitrary data across wide portions of the electromagnetic spectrum, ranging from the sub-acoustic to RF and beyond.

The Funtenna technique is hardware agnostic, can operate within nearly all modern computer systems and embedded devices, and is specifically intended to operate within hardware not designed to to act as RF transmitters.

We believe that Funtenna is an advancement of current state-of-the-art covert wireless exfiltration technologies. Specifically, Funtenna offers comparable exfiltration capabilities to RF-based retro-reflectors, but can be realized without the need for physical implantation and illumination.

We first present a brief survey of the history of compromising emanation research, followed by a discussion of the theoretical mechanisms of Funtenna and intentionally induced compromising emanation in general. Lastly, we demonstrate implementations of Funtenna as small software implants within several ubiquitous embedded devices, such as VoIP phones and printers, and in common computer peripherals, such as hard disks, console ports, network interface cards and more.

EXPLOITING OUT-OF-ORDER EXECUTION FOR COVERT CROSS-VM COMMUNICATION

PRESENTED BY

Sophia D'Antoine

This presentation will demonstrate a novel side channel exploiting CPU out-of-order-execution to enable covert cross-VM communication in cloud computing environments. Live demonstrations will show several applications of this side channel, including cross process or VM eavesdropping, malware command & control and environmental keying. The presentation will conclude with a brief analysis of detection and mitigation techniques for this attack.

EXPLOITING THE DRAM ROWHAMMER BUG TO GAIN KERNEL PRIVILEGES

PRESENTED BY

Mark Seaborn & Halvar Flake

"Rowhammer" is a problem with DRAM in which repeatedly accessing a row of memory can cause bit flips in adjacent rows. While the industry has known about the problem for a while and has started mitigating the problem in newer hardware, it was rarely mentioned in public until the publication of Yoongu Kim et al's paper in the summer of 2014 which included hard data about the prevalence of the problem. In spite of the paper's speculations about the exploitability of the issue, most people still classified rowhammer as only a reliability issue - the probabilistic aspect of the problem seems to have made people think exploitability would be impractical.

We have shown that rowhammer is practically exploitable in real-world scenarios - both in-browser through NaCl, and outside of the browser to escalate to kernel privileges. The probabilistic aspect can be effectively tamed so that the problem can be reliably exploited.

Rowhammer, to our knowledge, represents the first public discussion of turning a widespread, real-world, physics-level hardware problem into a security issue.

We will discuss the details of our two exploits cause and use bit flips, and how the rowhammer problem can be mitigated. We will explore whether it is possible to cause row hammering using normal cached memory accesses.

EXPLOITING XXE VULNERABILITIES IN FILE PARSING FUNCTIONALITY

PRESENTED BY

Willis Vandevanter

In this 25-minute briefing, we will discuss techniques for exploiting XXE vulnerabilities in File Parsing/Upload functionality. Specifically, XML Entity Attacks are well known, but their exploitation inside XML supported file formats such as docx, xlsx, pptx, and others are not. Discussing the technically relevant points step by step, we will use real world examples from products and recent bug bounties. Finally, in our experience, creating 'XXE backdoored' files can be a very slow process. We will introduce our battle tested tool for infecting the file formats discussed.

FAUX DISK ENCRYPTION: REALITIES OF SECURE STORAGE ON MOBILE DEVICES

PRESENTED BY

Daniel Mayer & Drew Suarez

The number of mobile users has recently surpassed the number of desktop users, emphasizing the importance of mobile device security. In traditional browser-server applications, data tends to be stored on the server side where tight controls can be enforced. In contrast, many mobile applications cache data locally on the device thus exposing it to a number of new attack vectors. Moreover, locally stored data often includes authentication tokens that are, compared to browser applications, typically long-lived. One main concern is the loss or theft of a device which grants an attacker physical access which may be used to bypass security controls in order to gain access to application data. Depending on the application's data, this can result in a loss of privacy (e.g., healthcare data, personal pictures and messages) or loss of intellectual property in the case of sensitive corporate data.

In this talk, we discuss the challenges mobile app developers face in securing data stored on devices including mobility, accessibility, and usability requirements. Given these challenges, we first debunk common misconceptions about full-disk encryption and show why it is not sufficient for most attack scenarios. We then systematically introduce the more sophisticated secure storage techniques that are available for iOS and Android respectively. For each platform, we discuss in-depth which mechanisms are available, how they technically operate, and whether they fulfill the practical security and usability requirements. We conclude the talk with an analysis of what still can go wrong even when current best-practices are followed and what the security and mobile device community can do to address these shortcomings.

At the end of our talk, attendees will understand the significant challenges involved in storing data on an always-on and portable device, how to securely store data for different use cases, and how to uncover secure storage flaws in real-world applications.

FILECRY - THE NEW AGE OF XXE

PRESENTED BY

Xiaoran Wang & Sergey Gorbaty

Xml eXternal Entities (XXE) is one of the most deadly vulnerabilities on the Internet, and we will demonstrate how critical enterprise software packages are still vulnerable to these attacks today. In this action-packed presentation, we will demonstrate two 0-day vulnerabilities we identified in both popular server (Java) and client-side (Internet Explorer) technologies. The first vulnerability can be exploited with an attacker-controlled XML leading to arbitrary file ex-filtration on a target server even with all the Java protections enabled. The second vulnerability, allows an attacker to steal both arbitrary files on the local hard drive and secret information across origins with a malicious webpage. Therefore, effectively bypassing the Same Origin Policy and breaching the web-local separation. Both exploits are reliable and do not depend on memory corruptions.

Join us as we take you through an exciting journey of finding, exploiting these vulnerabilities, and preventing this class of attacks in the future.

FINGERPRINTS ON MOBILE DEVICES: ABUSING AND LEAKING

PRESENTED BY

Yulong Zhang & Tao Wei

Unlike passwords, fingerprints last a lifetime and are usually associated with critical identities. Thus, the leakage of fingerprints is irredeemable. It will be even a disaster if the attackers can remotely harvest fingerprints in a large scale.

In this talk, we will reveal some severe issues with the current Android fingerprint frameworks that have long been neglected by vendors and users. We will provide in-depth security analysis of the popular mobile fingerprint authentication/authorization frameworks, and discuss the security problems of existing designs, including (1) the confused authorization attack that enables malware to bypass pay authorizations protected by fingerprints, (2) TrustZone design flaws and fingerprint sensor spying attack to harvest fingerprints, (3) pre-embedded fingerprint backdoors, etc. We will show live demos, such as hijacking mobile payment protected by fingerprints, and collecting fingerprints from popular mobile devices. We will also provide suggestions for vendors and users to better secure the fingerprints.

FORGING THE USB ARMORY AN OPEN SOURCE SECURE FLASH-DRIVE-SIZED COMPUTER

PRESENTED BY

Andrea Barisani & Daniele Bianco

FROM FALSE POSITIVES TO ACTIONABLE ANALYSIS: BEHAVIORAL INTRUSION DETECTION MACHINE LEARNING AND THE SOC

PRESENTED BY

Joseph Zadeh

This talk outlines an approach to modeling human behavior in network traffic with the goal of automatically labeling events that have security context. Large-scale defensive programs now have the opportunity to invest resources in next generation distributed architectures and software stacks to build custom security solutions to augment existing SIEM and point solution driven escalations. We describe ways to create such a scalable framework of distributed forensic artificial intelligences to hunt for evil and to minimize time spent on repeatable remediation and evidence collection processes. This type of next-gen cybersecurity analytics engine can add immediate value through alarm reduction and attribution of attacks to threat actors and campaigns over time.

The goal of building such a framework is to reduce time to detection and to provide automated ways to help incident response and daily reporting and escalations. The amount of data present in corporate SIEM's and IT warehouses allows for security teams to build the central nervous system of the Security Operations Center (SOC). One of the more complex tasks in designing such a next generation defensive system to is leverage machine learning to build models that are dynamic and intelligent enough to adapt to changing threats (labels suffer from concept drift) and to catch threats that have never been observed before (no ground truth). We describe ways to roadmap such cybersecurity analytics and ways to calculate the best return on investment given existing coverage and needs mapped to the threat surface.

FUZZING ANDROID SYSTEM SERVICES BY BINDER CALL

PRESENTED BY

TO ESCALATE PRIVILEGE

Guang Gong

Binder is the IPC Mechanism in Android. It's used in Communication not only between processes with the same privilege but also between low privileged Apps and high privileged system services. The system services is a juicy attack surface to escalate privileges because parameters passed to it through binder call lack sanitization, but until now there are little disclosed vulnerabilities of this type.

In this presentation, I'll first introduce this attack surface and then demonstrate the first fuzzing tools to find this kind of vulnerabilities. The tool take the binder interfaces exported from system services as attacked targets. This tool is simple but efficient. Through this tool I've found 8 vulnerabilities with CVE-IDs got from Android Security Team and dozens of crashes of system services. At last, I'll detail how to exploit this type of vulnerability to get Android's system_server permission by an unpublicized vulnerability.

GAMEOVER ZEUS: BADGUYS AND BACKENDS

PRESENTED BY

Elliott Peterson & Michael Sandee & Tillmann Werner

This presentation will detail many of the individuals responsible for GameOver Zeus and Cryptolocker, summarize the law enforcement investigation, and highlight the novel legal processes used to wrest control of the botnet from its operators.

GameOver Zeus represents one of the most complex, and successful, law enforcement operations against cyber crime to date. The talk will highlight extensive industry and government partnerships, the many international agencies that played a part, and discuss some of the methods used by private industry and law enforcement personnel to track and identify those responsible for the malware. The investigation resulted in the highest ever reward offered for a cyber criminal: $3,000,000 for Evgeniy Bogachev.

GRAPHIC CONTENT AHEAD: TOWARDS AUTOMATED SCALABLE ANALYSIS OF GRAPHICAL IMAGES EMBEDDED IN MALWARE

PRESENTED BY

Alex Long

While automated approaches to static and dynamic malware analysis are key pieces of todays malware analysis pipeline, little attention has been focused on the automated analysis of the images commonly embedded in malware files, such as desktop icons and GUI button skins. This leaves a blind spot in current malware triage approaches because automated image analysis could help to quickly reveal how new malware tricks users and could inform the question of whether malware samples came from known adversaries (samples with near-duplicate rare images may have come from the same attacker). Therefore, to further the application of image analysis techniques to the automated analysis of malware images, in our presentation we will describe our efforts to solve two related problems: the problem of identifying malware samples with visually similar image sets in a scalable fashion, and the problem of quickly classifying malware images into topical categories (e.g. "video game related", "fake anti-virus", installer icon", etc.).

The first component of our research focuses on identifying malware samples with similar image sets. To identify these relationships we have taken inspiration from natural image scene comparison approaches: first we reduce images statically extracted from malware to low-dimensional binary vectors using a scale and contrast invariant approach. Then we index malware images from the target malware dataset using a randomized index designed to quickly approximate Hamming distance between stored vectors. Finally, we compute pairwise distances between malware samples image sets to identify malware samples that share visually similar images (even if these images contrasts, scales, or color schemes are different). Additionally, we have built a force-directed graph based visualization to display our results to end-users, which colleagues within our organization have found useful in practice. In our presentation, we will provide a detailed account of our approach and describe an evaluation we performed which demonstrates that our approach operates at deployable levels of speed and accuracy.

The second component of our research focuses on classifying malware images into topical categories. To perform classification in a scalable and automated fashion, the approach we have developed dynamically obtains labeled training examples using the Google Image Search API based on user defined queries (for example, a query for retrieving examples of anti-virus icons could be anti-virus desktop icon). Using the resulting labeled image data, we have trained and compared a number of image classifiers. To evaluate these classifiers we hand-labeled malware images with their correct class and computed confusion matrices for more than a dozen classes of malware images (for example, "fake anti-virus", "fake web browser", etc.), revealing that our classification techniques varied in accuracy, with some image category detectors (such as "fake word processor") providing deployable levels of accuracy and others generating misclassifications at an unacceptable rate. In conclusion, by presenting what we believe to be compelling early results vis-a-vis both malware image set similarity and malware image classification, we hope to inspire the malware research community to both adopt image analysis in practice and further research into this understudied research area.

HARNESSING INTELLIGENCE FROM MALWARE REPOSITORIES

PRESENTED BY

Arun Lakhotia & Vivek Notani

The number of unique malware has been doubling every year for over two decades. The majority of effort in malware analysis has focused on methods for preventing malware infection. We view the exponential growth of malware as an underutilized source of intelligence. Given that the number of malware authors are not doubling each year, the large volume of malware must contain evidence that connects them. The challenge is how to extract the connections.

Since a malware is a complex software, it's development necessarily follows software engineering principles, such as modular programming, using third-party libraries, etc. Thus, sharing of code between malware are viable indicators of connection between their creators. However, identifying such shared code is not straightforward. The task is made complicated since to survive in an environment hostile (to it) a malware uses a variety of deceptions, such as polymorphic packing, for the explicit purpose of making it difficult to infer such connections.

By using a combination of two orthogonal approaches - formal program analysis and data mining - we have developed a scalable method to search large scale malware repositories for forensic evidence. Program analyses aid in peeking through the deceptions employed by malware to extract fragments of evidence. Data mining aids in organizing this mass of fragments into a web of connections which can then be used to make a variety of queries, such as to determine whether two apparently disparate cyber attacks are related; to transfer knowledge gained in countering one malware to counter other similar malware; to get a holistic view of cyber threats and to understand and track trends, etc.

This talk will summarize our method, describe VirusBattle - a web service for cloud-based malware analysis - developed at UL Lafayette, and present empirical evidence of viability of mining large scale malware repositories to draw meaningful inferences.

HI THIS IS URGENT PLZ FIX ASAP: CRITICAL VULNERABILITIES AND BUG BOUNTY PROGRAMS

PRESENTED BY

Kymberlee Price

No More Free Bugs led to Bug Bounties, but some people believe that bug bounty hunters are low quality script kiddies and the most talented researchers aren't participating. The emergence of bug bounty programs is increasing the volume of vulnerability submissions, but how many of those can be found by running an automated scanning tool? Are any really critical bugs being found in the sea of clickjacking and weak password policy reports? How do you separate the signal from the noise, and more importantly, how do you shift the balance of bug reports to greater signal/less noise overall? In this presentation we will discuss several highly critical vulnerabilities that have been uncovered through a variety of bug bounty programs and their impact on the customers. With participation from researchers and vendors, attendees will not only see some sweet vulnerabilities broken down, but also why wading through another submission from @CluelessSec might be worth it.

HIDDEN RISKS OF BIOMETRIC IDENTIFIERS AND HOW TO AVOID THEM

PRESENTED BY

Thomas Keenan

Technology that identifies you by something you are is showing up in e-passports, laptop login screens, smart firearms and even consumer products, like the iPhone. Current generation systems generally use static biometric features, such as fingerprints, iris scans and facial recognition, either measured directly or mediated through a device, such as a smartphone.

We are on the cusp of a revolution that will usher in dynamic (e.g. gestural, heart rhythm, gait analysis) and chemical (e.g. DNA, body odor, perspiration) biometrics. There will also be hybrid technologies, such as the Nokias vibrating magnetic ink tattoos (US Patent 8, 766, 784) and the password pill from Proteus Digital Health. Biometrics will also play an increasingly significant role as one of the factors in multi-factor authentication. The author created one of the first typing rhythm recognition algorithms and one of the earliest DNA sequencing machines in the 1980s and has a long term perspective on this subject.

Like all new technologies, advances in biometrics will bring new advantages and also new risks. This presentation surveys cutting edge biometric technologies and provides a framework for evaluating them from the perspectives of security, reliability, privacy, potential for abuse and perceived creepiness. Learn what is coming down the biometrics road now, so you'll be ready to intelligently choose and implement these technologies as they come on the market in the near future.

HOW TO HACK GOVERNMENT: TECHNOLOGISTS AS POLICY MAKERS

PRESENTED BY

Ashkan Soltani & Terrell McSweeny

As the leading federal agency responsible for protecting your privacy rights online, technology is at the core of the Federal Trade Commissions work. You may be familiar with the agency's enforcement actions against some of the worlds biggest tech companies for privacy/data security violations, but you may not know how your research skills can inform its investigations and policy. Come hear about some of the Commissions recent tech-related actions, research and reports, plus how its work impacts both consumers and businesses. You'll also learn how you can directly or indirectly help the agency protect consumers, guide businesses to develop better/strong data security, and much more.

HOW TO IMPLEMENT IT SECURITY AFTER A CYBER MELTDOWN

PRESENTED BY

Christina Kubecka

The 2012 cyber attacks against Saudi Aramco and the Aramco family of affiliates was a major game changer in IT & ICS Security. The energy sector, relevant markets, and governments world wide shuddered. Although oil production wasn't directly affected, business operations were greatly interrupted and remain so.

This presentation is the story how I implemented the first IT Security unit for Aramco Overseas Company, a Saudi Aramco affiliate which provides all IT services for Saudi Aramco in South America and the EMEA region outside of Saudi Arabia.

HOW VULNERABLE ARE WE TO SCAMS?

PRESENTED BY

Markus Jakobsson & Ting-Fang Yen

The number of Internet scams has increased in recent years. According to a survey by the Federal Trade Commission, more than one out of every ten adult Americans fall victim to scams every year, where a third of these scams originated on the Internet. However, it is well understood that surveys of victimization and losses severely underestimate the problem, since victims are unwilling to come forward due to embarrassment or resignation. This paper attempts to gain a better understanding of the problem by directly quantifying the extent to which users are vulnerable to scams.

We design and carry out experiments to estimate the fraction of scam messages that bypass commercial spam lters (i.e., messages that land in the user's inbox); and to assess the probability that a delivered message will be considered harmless by its recipient. The latter experiment provides evidence that recent scams - many of which are targeted are substantially more credible to typical users than "traditional" scam.

INFORMATION ACCESS AND INFORMATION SHARING: WHERE WE ARE AND WHERE WE ARE GOING

PRESENTED BY

Alejandro Mayorkas

Deputy Secretary of the Department of Homeland Security, Alejandro Mayorkas, will discuss the challenges of information access in today's world. He will also describe the information sharing vision of DHS: is a future where cybersecurity information, such as indicators of specific cyber threats, is shared widely across the public and private sectors at machine-speed and in formats that can be immediately used for network defense. To achieve this goal, cyber threat indicators must be a public good, rather than a market differentiator between companies. When cyber threat indicators are a unique commodity, they are only shared among discrete communities - and we are all less secure. But when cyber threat indicators are not a profit driver for security firms and have zero marginal cost for network defenders, we can achieve information sharing that moves more quickly than our adversaries.

INTERNET PLUMBING FOR SECURITY PROFESSIONALS: THE STATE OF BGP SECURITY

PRESENTED BY

Wim Remes

The underbelly of the Internet has been in a precarious condition for a while now. Even with all the knowledge about it's weaknesses, we only make slow progress in implementing technology to secure it. We see BGP routing leaks on a regular basis. It almost feels like we take it for granted but at the same time it undermines our trust in the Internet. In this talk, we'll review the current situation for BGP, a foundational piece of the network we all rely on, and focus on the practical implementation of available countermeasures through live demos and examples. In and of itself, we launch a call to action for private organizations, government entities, and academia alike to roll up the sleeves and get cracking at fixing our Internet. If we want to keep trust in "The Internet of Things," we first have to build trust in the network that powers it.

INTERNET-FACING PLCS - A NEW BACK ORIFICE

PRESENTED BY

Johannes Klick & Stephan Lau & Daniel Marzin & Jan-Ole Malchow & Volker Roth

Pretty much everyone should have realized by now that our modern societies critically depend on industrial control systems (ICS) and that these systems are beginning to move into the focus of hacking attacks. A recent example that received comparatively little attention is a 2014 attack on a German steel production facility. The attack led to an uncontrolled shutdown of a blast furnace and caused damages in the millions. Reportedly, the attackers compromised the business IT first and worked their way to the actual control systems from there. Much simpler attack vectors frequently exist for those knowledgeable enough to use them. SHODAN is a case in point that a plethora of industrial control systems can be attacked directly.

In our talk, we will showcase novel tools and techniques to leverage one Internet-facing PLC, in order to explore and gain control over entire production networks.

We use Siemens PLCs as our example. Our tools differ from what has been made public before in that we implement and run them directly on PLCs in their native STL language. Specifically, we explain and demonstrate in detail the following attack process. We automatically locate PLCs and automatically instrument the STL code of a running PLC, so that it provides additional functions in parallel to its original ones. One function we implemented is that of a UDP/SNMP scanner. Another one is that of a SOCKS5 proxy. Using these functions, adversaries can easily map, instrument and control any remaining PLCs on the network using existing tools. We demonstrate attacks on Siemens PLCs through our proxy connection using an existing Metasploit S7-300 Stop module and an exploit for CVE-2015-2177 that we disclosed to Siemens. As part of our demonstration, we explain why implementing a TCP scanner is impractical on Siemens PLCs.

INTERNET-SCALE FILE ANALYSIS

PRESENTED BY

Zachary Hanif & Tamas Lengyel & George Webster

Malicious file analysis is well beyond the days when the humble PE32 file was all researchers needed to contend with. The use of malicious PDF, Office, and other files present a far more diverse threat than our defensive tools were originally designed to handle. To make matters worse, the sheer volume of files over time to analyze presents a meaningful logistical problem which becomes increasingly complex as analytical methods move from static to dynamic analysis. When the point in time problem is considered (the fact that historical discoveries can be viewed differently in the light of new analytical techniques or information), the problem seems all but intractable.

To this end, we have developed TOTEM, a system which is capable of coordinating, orchestrating, and scaling malware analytics across multiple cloud providers and thousands of running instances. It is easy to add new capabilities to and can intelligently segregate work based on features, such as filetype, analytic duration, and computational complexity. TOTEM supports dynamic analysis through DRAKVUF, a novel open-source dynamic malware analysis system which was designed specifically to achieve unparalleled scalability, while maintaining a high level of stealth and visibility into the executing sample. Building on the latest hardware virtualization extensions found in Intel processors and the Xen hypervisor, DRAKVUF remains completely hidden from the executing sample and requires no special software to be installed within the sandbox. Further addressing the problem of monitoring kernel-mode rootkits as well as user-space applications, DRAKVUF significantly raises the bar for evasive malware to remain undetected.

This talk will discuss the design, implementation, and practical deployment of TOTEM and DRAKVUF to analyze tremendous numbers of binary files.

IS THE NSA STILL LISTENING TO YOUR PHONE CALLS? A SURVEILLANCE DEBATE: CONGRESSIONAL SUCCESS OR EPIC FAIL

PRESENTED BY

Mark Jaycox & Jamil Jaffer

At BlackHat 2014, we debated the NSA's collection of Americans' phone calls, emails, address books, buddy lists, calling records, online video game chats, financial documents, browsing history, video chats, text messages, IP addresses, and calendar data. One section that's being used to collect calling records and other business records - Section 215 of the Patriot Act - expired in June. Within days, Congress passed a law to narrow the scope of the section and introduce much needed transparency. It was the first time since the 1970's that Congress reined in the NSA's surveillance practices.

This year we'll discuss Section 215 of the Patriot Act and debate what Congress did to reform the section. Did it fix the program? Did it do nothing? Does Congress ever do anything? Join us by hearing former Senior Counsel of the House Intelligence Committee Jamil Jaffer debate these issues with Mark Jaycox of the Electronic Frontier Foundation.

MOBILE POINT OF SCAM: ATTACKING THE SQUARE READER

PRESENTED BY

Alexandrea Mellen & John Moore & Artem Losev

We consider the security of Square, Inc.'s mobile card-reading device, the Square Reader, across multiple models, as well as the associated Square Register app where relevant. In doing so, we identify a number of vulnerabilities in the device that allow both malicious merchants and third parties to initiate fraudulent transactions and, with minor device modification, skim credit card information of unsuspecting customers. We highlight that since mobile card-reading devices like the Square Reader are necessarily compact, cheap, and compatible with a broad range of commodity smartphones, they pose new security challenges over traditional payment-processing hardware. In turn, these challenges expose an attack surface that is relatively new and unexplored given the infancy of mobile point-of-sale systems compared to their non-mobile counterparts. We investigate this attack surface and find a number of vulnerabilities that confirm that even current secure mobile point-of-sale systems suffer from software and hardware design flaws, leaving them vulnerable to both third parties and malicious merchants.

MOST RANSOMWARE ISNT AS COMPLEX AS YOU MIGHT THINK

PRESENTED BY

Engin Kirda

In this presentation, hear the findings of new academic research into ransomware in which we analyzed more than 1,300 samples captured in the wild from 2006 and 2014 from 15 malware families - including Calelk, Cryptolocker, CryptoWall, Gpcode, Filecoder, Kevtor, Reveton, Seftad, Urausy and Winlock. Our results indicate that (while ransomware authors have made some advancements in encryption, deletion and communication techniques over those eight years) the real impact on victims who don't pay is typically still both nondestructive and preventable. Even the very small set of truly destructive zero-day ransomware samples with sophisticated encryption capabilities we identified can be detected and stopped.

First, learn how ransomware appears to have changed - and stayed the same - from 2006 and 2014, including constants, commonalities and advancements across 15 ransomware families in that timeframe. For example, we verified the widely held belief that ransomware attacks have been increasing in volume in recent years. In fact, they grew by more than 500% from 2012-13. However, the majority have not been sufficiently increasing in sophistication in that timeframe to truly take victims data or hardware hostage. Discover previously undocumented aspects of ransomware attacks with a focus on distinctive and common behaviors among different families.

Second, see a comparison of the threatened impacts vs. the real impacts of the studied ransomware, demonstrating that the vast majority is essentially bluffing its own destructive capabilities in order to extract funds from the victim who is afraid of losing personal and/or valuable data or equipment. More than 94% of ransomware in our multi-year study simply attempted to lock the victims desktop and demand ransom, or used very similar and superficial approaches to encrypt or delete the victims files.

Third, delve into the inner workings of rare destructive ransomware to ascertain key attributes in the code and execution of its instructions that make it both effective and detectible. Hear about the API calls, file system activity and decoy files that consistently surface from different malware families in the wild. Take a look at the various charging methods adopted by different ransomware families including Bitcoin, Moneypak, Paysafecar and Ukash cards. More than 88% of ransomware samples used prepaid online payment systems.

Finally, understand why detecting and stopping advanced ransomware attacks is not as difficult as others have reported. In fact, by scanning for unusual behavior in file system activities, such as I/O requests you can detect even relatively sophisticated ransomware. By protecting the Master File Table (MFT) in the New Technology File System (NTFS) file system on Windows machines, you can prevent most zero-day ransomware attacks. These findings contradict some security community discussions that suggest the impossibility of detecting or stopping these types of attacks due to the use of sophisticated, destructive techniques.

MY BRO THE ELK: OBTAINING CONTEXT FROM SECURITY EVENTS

PRESENTED BY

Travis Smith

There are a number of powerful open source tools that empower us to collect, store and visualize data in our environments, as well as provide rich context using external threat intelligence. However, given the amount of data to sift through it can make us complacent and miss important indicators. Instead of having to sift through this data to identify important pieces of information, what if we could automate and orchestrate integrations across the various systems to help us identify and act on real threats?

At Black Hat, we will be releasing a tool that integrates several popular open source and commercial security frameworks to do just that. In this presentation we will highlight the use of ELK (ElasticSearch, Kibana, and LogStash), Bro IDS, and community threat intelligence feeds. By combining these frameworks with threat intelligence providers, security professionals can obtain the business and security context to the events flowing through their environment. We will also be releasing the open source framework that will automate the collection of evidence for incident response for quicker response times by security teams.

OPTIMIZED FUZZING IOKIT IN IOS

PRESENTED BY

Lei Long & Peng Xiao & Aimin Pan

Fuzzing is the most common way of exploiting vulnerabilities, and IOKit is an ideal target in kernel extensions for fuzzing. The interfaces in IOKit use specific structures, such as IOExternalMethod, IOExternalMethodDispatch, to check the input parameters in various ways. Purely random inputs when fuzzing IOKit can hardly pass the interfaces' parameter checking, so that most of fuzzing data cannot reach the kernel IOUserClient subclass at all. Thus, such kind of blindly fuzzing is inefficient. One way to improve it is to use the static information exported by sMethod symbols, which can be dumped by a static analysis tools such as IDA. However, it is not available since iOS 7 because of symbols hiding.

In this presentation, we will introduce an approach to resolve the symbols and parameter information dynamically based on a kernel patch to read and write memories. In this approach we can exploit quite a lot of useful information, including not only the standard parameters of IOKit interfaces, but also other supplementary data. We have also built a fuzzing framework, which uses the resolved information and generates the random inputs, which can pass the basic parameter checking by IOKit interfaces. Therefore, the fuzzing can be done efficiently. Finally, we also present the information of IOKit interfaces exported by our approach, and several typical vulnerabilities found by our fuzzing framework.

PANEL: GETTING IT RIGHT: STRAIGHT TALK ON THREAT & INFORMATION SHARING

PRESENTED BY

Trey Ford & Kevin Bankston & Rebekah Brown & Brian Engle & Mark Hammell

Sharing information isn't hard - getting past backroom deals, NDAs and approval from general counsel is *very hard*. This topic is not two-dimensional, even if we are quick to weigh data sharing in the face of data breaches, and the US has several pieces of legislation in play on this *right now*.

Conservatively there are over 300,00 open jobs available in information security-efficiency, prioritization and alignment with IT has never been more important. Information sharing and threat intelligence offers hope that we can better inform priorities to align with real threats, however these solutions come with a new set of questions:

- Can we collaborate outside our company *and* protect privacy?
- What information is worth sharing?
- Is there a level of minimum care in protecting civil liberties while enabling rapid information dissemination?

Clearly, we need to talk. If you've got thoughts, we want to hear them. Sharing isn't only the theme of this session, it is also the format. Attendees and panelists will discuss:

- What should you do with the information once you have it?
- What sharing models (hub-spoke vs. de-centralized) make sense?
- What are the privacy considerations in sharing information?
- What kinds of liability impact information sharing today?

- What corporate controls affect your ability to share information?
- What's the status of information-sharing legislation in Congress?

PANEL: HOW THE WASSENAAR ARRANGEMENTS EXPORT CONTROL OF INTRUSION SOFTWARE AFFECTS THE SECURITY INDUSTRY

In 2013, the group of countries that make up the Wassenaar Arrangement added "intrusion software" to the list of dual use controlled items. This rule has been implemented and enforced in different ways among participating countries since last year. The United States Government is currently working on how it will implement these rules. Much like the crypto wars of the 1990's, the ruling in its current form threatens to make some legitimate security work more difficult. This has the potential to raise the cost for defenders and lower the cost for attackers. Join us for a panel that brings together different members of our community to discuss their perspectives on these export regulations. The panel will include those involved in security research, bug bounty programs, and privacy.

PRESENTED BY

Kim Zetter & Collin Anderson & Nate Cardozo & Katie Moussouris & Dino Dai Zovi & Adriel Desautels

PEN TESTING A CITY

How would you take down a city? How would you prepare for and defend against such an attack? The information security community does a great job of identifying security vulnerabilities in individual technologies and penetration testing teams help secure companies. At the next level of scale, however, things tend to fall apart. The information security of cities, the backbone of modern civilization, often receives little to no holistic attention, unless you count the constant probing of nation state aggressors. The information technology infrastructure of cities is different from other entities. Cities feature complex interdependencies between agencies and infrastructure that is a combination of federal, state and local government organizations and private industry, all working closely together in an attempt to keep the city as a whole functioning properly. Preparedness varies widely. Some cities have their act together, but others are a snarl of individual fiefdoms built upon homegrown technological houses of cards. If you can untangle the policy and politics and overcome the bureaucratic infighting to create workable leadership, authorities, and funding, you are still faced with an astronomically complex system and an attack surface the size of, well, a city. Our talk identifies these necessary precursor steps and provide a broadly applicable set of tools to start taming and securing, such an attack surface.

In this talk, we first explore a notional city, deconstruct it layer by layer, and use these insights to suggest a comprehensive methodology for reverse engineering any city and deriving its attack surface. We complement these insights with a broad analysis of proven capabilities demonstrated by hacker and information security researchers as well as known capabilities of criminal and nation-state actors applicable to city-level attacks. Next, we develop a coherent strategy for penetration testing as an approach to highlight and then mitigate city-level vulnerabilities. Finally, we conclude with a wide-ranging set of approaches to complement pen testing efforts, including exercises and collective training, metrics and a maturity model for measuring progress, and specialized city-level attack/defend ranges. You'll leave this talk fearing for the survival of your respective country, but also possessing a toolkit of techniques to help improve the situation. By better securing cities we have a glimmer of hope in securing nations.

PRESENTED BY

Greg Conti & Tom Cross & David Raymond

RED VS BLUE: MODERN ACTIVE DIRECTORY ATTACKS DETECTION AND PROTECTION

PRESENTED BY

Sean Metcalf

Kerberos "Golden Tickets" were unveiled by Alva "Skip" Duckwall & Benjamin Delpy in 2014 during their Black Hat USA presentation. Around this time, Active Directory (AD) admins all over the world felt a great disturbance in the Force. Golden Tickets are the ultimate method for persistent, forever AD admin rights to a network since they are valid Kerberos tickets and can't be detected, right?

The news is filled with reports of breached companies and government agencies with little detail on the attack vectors and mitigation. This briefing discusses in detail the latest attack methods for gaining and maintaining administrative access in Active Directory. Also covered are traditional defensive security measures that work (and ones that don't) as well as the mitigation strategies that can keep your company's name off the front page. Prepare to go beyond "Pass-the-Hash" and down the rabbit hole.

This talk explores the latest Active Directory attack vectors and describes how Golden Ticket usage can be detected. When forged Kerberos tickets are used in AD, there are some interesting artifacts that can be identified. Yes, despite what you may have read on the internet, there are ways to detect Golden & Silver Ticket usage!

Some of the topics covered:

- How attackers go from zero to (Domain) Admin
- MS14-068: the vulnerability, the exploit, and the danger.
- "SPN Scanning" with PowerShell to identify potential targets without network scans (SQL, Exchange, FIM, webservers, etc.).
- Exploiting weak service account passwords as a regular AD user.
- Mimikatz, the attacker's multi-tool.
- Using Silver Tickets for stealthy persistence that won't be detected (until now).
- Identifying forged Kerberos tickets (Golden & Silver Tickets) on your network.
- Detecting offensive PowerShell tools like Invoke-Mimikatz.
- PowerShell v5 security enhancements
- Active Directory attack mitigation.

Kerberos expertise is not required since the presentation covers how Active Directory leverages Kerberos for authentication identifying the areas useful for attack. Information presented is useful for both Red Team & Blue Team members.

REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE

PRESENTED BY

Charlie Miller & Chris Valasek

Although the hacking of automobiles is a topic often discussed, details regarding successful attacks, if ever made public, are non-comprehensive at best. The ambiguous nature of automotive security leads to narratives that are polar opposites: either we're all going to die or our cars are perfectly safe. In this talk, we will show the reality of car hacking by demonstrating exactly how a remote attack works against an unaltered, factory vehicle. Starting with remote exploitation, we will show how to pivot through different pieces of the vehicle's hardware in order to be able to send messages on the CAN bus to critical electronic control units. We will conclude by showing several CAN messages that affect physical systems of the vehicle. By chaining these elements together, we will demonstrate the reality and limitations of remote car attacks.

REMOTE PHYSICAL DAMAGE 101 - BREAD AND BUTTER ATTACKS

PRESENTED BY

Jason Larsen

It is possible to physically damage equipment through purely cyber means. Most of the time the attacker takes advantage of something specific to the CyberPhysical System (CPS) thats being targeted. As an example mixing in a cleaning agent during a production cycle can cause an unwanted chemical reaction. Attacking software has been described as "unexpected computation". Attacking a process is all about "unexpected physics."

Finding and exploiting process-specific flaws generally takes subject matter expertise in the victim process. However, there are some generic attacks that can be applied in a wide range of scenarios. I call these bread and butter attacks. They take advantage of common configurations of valves, pumps, pipe, etc. to achieve damage to the process. These scenarios can be used as a basis for a first look in a process audit. During a full audit, a subject matter expert will still need to be consulted.

Nearly the entire budget for security processes from cyber attack is spent attempting to keep an attacker from gaining code execution in the process control network. This is roughly equivalent to the early 2000s where the industry attempted to find every possible buffer overflow in code. In 2015 were still finding them regularly. It wasn't until ALSR and DEP were introduced that defenders started making attacker work harder. In process control networks, defending the network is still key, but adding a few physical controls can greatly reduce the effectiveness of an attacker. It is hoped that this presentation can help stimulate discussion on how attacker can be mitigated after code execution is already achieved.

REPURPOSING ONIONDUKE: A SINGLE CASE STUDY AROUND REUSING NATION STATE MALWARE

PRESENTED BY

Joshua Pitts

The news media is awash with nation-states and criminals reusing malware. Why should they have all the fun? This is a case study about reversing the suspected Russian government made OnionDuke MitM patching system, discovered by the speaker in October 2014. During this talk we will seek to understand its inner workings, selecting desirable features, and repurposing it for use in other tools. This is pure malware plagiarism.

RETURN TO WHERE? YOU CANT EXPLOIT WHAT YOU CANT FIND

Detecting and preventing exploitation of memory corruption vulnerabilities is highly challenging. Until now, no countermeasure has been able to fully prevent sophisticated exploitation techniques, such as return-oriented programming (ROP). Recent control-flow integrity (CFI) defenses from Google and Microsoft can be bypassed by constructing a ROP payload that adheres to the control-flow constraints or by exploiting implementation flaws. Microsoft's EMET has less overhead than full CFI, but offers less protection in return, and can be bypassed. Probabilistic countermeasures based on memory layout randomization (such as ASLR) are already in widespread use. However, the Pwn2own competitions have repeatedly demonstrated that attackers can bypass code randomization using memory leaks in browsers.

To reduce the impact of memory disclosure, recent defenses utilize execute-only memory. In this work we show that execute-only memory is insufficient and that these solutions can still be bypassed. In particular, we show how to determine the code layout by analyzing pointers in the heap and on the stack without ever reading the code.

On the defensive side, we build a comprehensive yet practical defense called Readactor that counters both direct reading of code and indirect layout disclosure through analysis of code pointers. We employ a thin hypervisor and a kernel patch to utilize true hardware execute-only memory, and prevent direct reading of code in Linux processes. We hide all code pointers in readable memory using a patched version of the LLVM compiler. We deploy a number of techniques to break ROP gadget chains and disorient the adversary. Specifically, we hide code pointers by converting them into direct jumps stored in execute-only memory to prevent indirect layout disclosure.

Our solution is efficient, because it activates previously unused hardware capabilities in modern x86 processors and is often faster than industry CFI implementations. Our solution is also highly practical; we were able to automatically apply our defense to the Chromium web browser. Finally, our solution is comprehensive; we also protect the dynamically generated code emitted by the V8 JavaScript JIT compiler.

PRESENTED BY

Christopher Liebchen & Ahmad-Reza Sadeghi & Andrei Homescu & Stephen Crane

REVIEW AND EXPLOIT NEGLECTED ATTACK SURFACES IN IOS 8

The security design of iOS significantly reduces the attack surfaces for iOS. Since iOS has gained increasing attention due to its rising popularity, most major attack surfaces in iOS such as mobile safari and IOKit kernel extensions have been well studied and tested. This talk will first review some previously known attacks against these surfaces, and then focus on analyzing and pointing out those neglected attack surfaces. Furthermore, this talk will explore how to apply fuzzing testing and whitebox code auditing to the neglected attack surfaces and share interesting findings. In particular, this talk will disclose POCs for a number of crashes and memory corruption errors in system daemons, which are even triggerable through XPC (a lightweight inter-process communication mechanism) by any app running in the container sandbox, and analyze and share the POC for an out-of-boundary memory access 0day in the latest iOS kernel.

PRESENTED BY

Tielei Wang & HAO XU & Xiaobo Chen

ROCKING THE POCKET BOOK: HACKING CHEMICAL PLANT FOR COMPETITION AND EXTORTION

PRESENTED BY

Marina Krotofil

The appeal of hacking a physical process is dreaming about physical damage attacks lighting up the sky in a shower of goodness. Lets face it, after such elite hacking action nobody is going to let you present it at a conference like Black Hat. As a poor substitute, this presentation will get as close as using a simulated plant for Vinyl Acetate production for demonstrating a complete attack, from start to end, directed at persistent economic damage to a production site while avoiding attribution of production loss to a cyber-event. Such an attack scenario could be useful to a manufacturer aiming at putting competitors out of business or as a strong argument in an extortion attack.

Picking up a paper these days its easy to find an article on all the SCADA insecurity out there associated with an unstoppable attacker with unsophisticated goal of kicking up another apocalypse. Sorry to disappoint excited crowd but formula Your wish is my command does not work for control systems. The target plant may not have been designed in a hacker friendly way. Hopefully by the end of the presentation, the audience will understand the difference between breaking into the system and breaking the system, obtaining control and being in control. An attacker targeting a remote process is not immediately gifted with complete knowledge of the process and the means to manipulate it. In general, an attacker follows a series of stages before getting to the final attack. Designing an attack scenario is a matter of art as much as economic consideration. The cost of attack can quickly exceed damage worth. Also, the attacker has to find the way to compare between competing attack scenarios.

In traditional IT hacking, a goal is to go undetected. In OT (operational technologies) hacking this is not an option. An attack will change things in the real world that cannot be removed by simply erasing the log files. If a piece of equipment is damaged or if a plant suddenly becomes less profitable, it will be investigated. The attacker has to create forensic footprint for investigators by manipulating the process and the logs in such a way that the analysts draw the wrong conclusions.

Exploiting physical process is an exotic and hard to develop skill which have so far kept a high barrier to entry. Therefore, real-world control system exploitation has remained in the hands of a few. To help the community mastering new skills we have developed 'Damn Vulnerable Chemical Process" - first open source framework for cyber-physical experimentation based on two realistic models of chemical plants. Come to the session and take your first master class on complex physical hacking.

ROPINJECTOR: USING RETURN ORIENTED PROGRAMMING FOR POLYMORPHISM AND ANTIVIRUS EVASION

PRESENTED BY

Giorgos Poulios & Christoforos Ntantogian & Christos Xenakis

The downside of current polymorphism techniques lies to the fact that they require a writeable code section, either marked as such in the corresponding Portable

Executable (PE) section header, or by changing permissions during runtime. Both approaches are identified by AV software as alarming characteristics and/or behavior, since they are rarely found in benign PEs unless they are packed. In this paper we propose the use of Return-Oriented Programming (ROP) as a new way to achieve polymorphism and evade AV software. To this end, we have developed a tool named ROPInjector which, given any piece of shellcode and any non-packed 32-bit Portable Executable (PE) file, it transforms the shellcode to its ROP equivalent and patches it into (i.e. infects) the PE file. After trying various combinations of evasion techniques, the results show that ROPInjector can evade nearly and completely all antivirus software employed in the online VirusTotal service. The main outcome of this research is: A) the developed algorithms for analysis and manipulation of assembly code on the x86 instruction set, and B) the release and demonstration of the ROPInjector tool.

SECURING YOUR BIG DATA ENVIRONMENT

PRESENTED BY

Ajit Gaddam

Hadoop and big data are no longer buzz words in large enterprises. Whether for the correct reasons or not, enterprise data warehouses are moving to Hadoop and along with it come petabytes of data. How do you ensure big data in Hadoop does not become a big problem or a big target. Vendors pitch their technologies as the magical silver bullet. However, did you realize that some controls are dependent on how many maps are available in the production cluster. What about the structure of the data being loaded? How much overhead does decryption operation add? If tokenizing data, how do you distinguish between in and original production data? However, in certain ways, Hadoop and big data represent a greenfield opportunity for security practitioners. It provides a chance to get ahead of the curve, test and deploy your tools, processes, patterns, and techniques before big data becomes a big problem.

Come join this session, where we walk through control frameworks we built and what we discovered, reinvented, polished, and developed to support data security, compliance, cryptographic protection, and effective risk management for sensitive data.

SERVER-SIDE TEMPLATE INJECTION: RCE FOR THE MODERN WEB APP

PRESENTED BY

James Kettle

Simple inputs can conceal an {expansive} attack surface. Feature-rich web applications often embed user input in web templates in an attempt to offer flexible functionality and developer shortcuts, creating a vulnerability easily mistaken for XSS. In this presentation, I'll discuss techniques to recognize template injection, then show how to take template engines on a journey deeply orthogonal to their intended purpose and ultimately gain arbitrary code execution. I'll show this technique being applied to craft exploits that hijack four popular template engines, then demonstrate RCE zero-days on two corporate web applications.

This presentation will also cover techniques for automated detection of template injection, and exploiting subtle, application-specific vulnerabilities that can arise in otherwise secure template systems.

SMBV2: SHARING MORE THAN JUST YOUR FILES

PRESENTED BY

Jonathan Brossard & Hormazd Billimoria

In this presentation, we detail a new attack vector against SMBv2, affecting all versions of IE, including the Spartan version shipped with Windows10. While attacks involving SMB have long time been common in LANs, our attack allows complete user compromise from the internet. By leveraging a series of bugs and malfunctions, we'll see how remote credentials theft or user impersonation can be performed without user interaction, extremely reliably, and from the Internet.

SOCIAL ENGINEERING THE WINDOWS KERNEL: FINDING AND EXPLOITING TOKEN HANDLING VULNERABILITIES

PRESENTED BY

James Forshaw

One successful technique in social engineering is pretending to be someone or something you're not and hoping the security guard who's forgotten their reading glasses doesn't look too closely at your fake ID. Of course there's no hyperopic guard in the Windows OS, but we do have an ID card, the Access Token which proves our identity to the system and let's us access secured resources. The Windows kernel provides simple capabilities to identify fake Access Tokens, but sometimes the kernel or other kernel-mode drivers are too busy to use them correctly. If a fake token isn't spotted during a privileged operation local elevation of privilege or information disclosure vulnerabilities can be the result. This could allow an attacker to break out of an application sandbox, elevate to administrator privileges, or even compromise the kernel itself. This presentation is about finding and then exploiting the incorrect handling of tokens in the Windows kernel as well as first and third party drivers. Examples of serious vulnerabilities, such as CVE-2015-0002 and CVE-2015-0062 will be presented. It will provide clear exploitable patterns so that you can do your own security reviews for these issues. Finally, I'll discuss some of the ways of exploiting these types of vulnerabilities to elevate local privileges.

SPREAD SPECTRUM SATCOM HACKING: ATTACKING THE GLOBALSTAR SIMPLEX DATA SERVICE

PRESENTED BY

Colby Moore

Recently, there have been several highly publicized talks about satellite hacking. However, most only touch on the theoretical rather than demonstrate actual vulnerabilities and real world attack scenarios. This talk will demystify some of the technologies behind satellite communications and do what no one has done before - take the audience step-by-step from reverse engineering to exploitation of the GlobalStar simplex satcom protocol and demonstrate a full blown signals intelligence collection and spoofing capability. I will also demonstrate how an attacker might simulate critical conditions in satellite connected SCADA systems.

In recent years, Globalstar has gained popularity with the introduction of its consumer focused SPOT asset-tracking solutions. During the session, I'll deconstruct the transmitters used in these (and commercial) solutions and reveal design and implementation flaws that result in the ability to intercept, spoof, falsify, and intelligently jam communications. Due to design tradeoffs these vulnerabilities are realistically unpatchable and put millions of devices, critical infrastructure, emergency services, and high value assets at risk.

STAGEFRIGHT: SCARY CODE IN THE HEART OF ANDROID

PRESENTED BY

Joshua Drake

With over a billion activated devices, Android holds strong as the market leading smartphone operating system. Underneath the hood, it is primarily built on the tens of gigabytes of source code from the Android Open Source Project (AOSP). Thoroughly reviewing a code base of this size is arduous at best - arguably impossible. Several approaches exist to combat this problem. One such approach is identifying and focusing on a particularly dangerous area of code.

This presentation centers around the speaker's experience researching a particularly scary area of Android, the Stagefright multimedia framework. By limiting his focus to a relatively small area of code that's critically exposed on 95% of devices, Joshua discovered a multitude of implementation issues with impacts ranging from unassisted remote code execution down to simple denial of service. Apart from a full explanation of these vulnerabilities, this presentation also discusses; techniques used for discovery, Android OS internals, and the disclosure process. Finally, proof-of-concept code will be demonstrated.

After attending this presentation, you will understand how to discover vulnerabilities in Android more effectively. Joshua will show you why this particular code is so scary, what has been done to help improve the overall security of the Android operating system, and what challenges lie ahead.

STAYING PERSISTENT IN SOFTWARE DEFINED NETWORKS

PRESENTED BY

Gregory Pickett

The Open Network Install Environment, or ONIE, makes commodity or WhiteBox Ethernet possible. By placing a common, Linux-based, install environment onto the firmware of the switch, customers can deploy the Network Operating Systems of their choice onto the switch and do so whenever they like without replacing the hardware. The problem is, if this gets compromised, it also makes it possible for hackers to install malware onto the switch. Malware that can manipulate it and your network, and keep doing it long after a Network Operating System reinstall.

With no secure boot, no encryption, no authentication, predictable HTTP/TFTP waterfalls, and exposed post-installation partition, ONIE is very susceptible to compromise. And with Network Operating Systems such as Switch Light, Cumulus Linux, and Mellanox-OS via their agents Indigo and eSwitchd not exactly putting up a fight with problems like no authentication, no encryption, poor encryption, and insufficient isolation, this is a real possibility.

In this session, we'll cover the weaknesses in ONIE, ways to reach the platform through these Network Operating Systems, and what can happen if we don't properly protect the Control Plane these switches run on. I'll even demonstrate with a drive-by web-attack that is able to pivot through a Windows management station to reach the isolated control plane network, and infect one of these ONIE-based switches with malware, malware that's there even after a refresh. You'll even get the source code to take home with you to see how easily it's done. Finally, we'll talk about how to compensate for these issues so that your network doesn't become infected with and manipulated by this sort of persistent firmware-level malware.

STRANGER DANGER! WHAT IS THE RISK FROM 3RD PARTY LIBRARIES?

PRESENTED BY

Jake Kouns

Since Heartbleed, the (in)security of third party libraries has taken center stage in infosec thanks to the follow up releases of Shellshock, POODLE, and FREAK, each causing vendors to scramble to investigate and remediate flaws in third party libraries. Clearly, vulnerability counts and patch frequency are just the beginning of evaluating product and library security. Days of Risk (DoR) analysis starts at public disclosure of a vulnerability, but doesn't account for the time from initial discovery through fix availability which could be months. We analyze the risks that are created by the extended Time of Exposure that DoR does not address. Learn how metrics can assist in the evaluation of vendors and products, and provide a scorecard for organizations to understand their effectiveness in managing vulnerabilities.

This presentation will will also share case studies of companies who took action in 2014 to get ahead of 3rd party patch whack-a-mole, and provide concrete actions security practitioners can take to mitigate risk in their environments.

SUBVERTING SATELLITE RECEIVERS FOR BOTNET AND PROFIT

PRESENTED BY

Sofiane Talmat

New generation Set Top Boxes (Satellite receivers) are embedded linux boxes offering all the features of any linux based machine, including wireless and network connectivities, this allowed hackers to crack most satellite DVB-CA encryption schemes promoting the apparition of a parallel black market for pay tv subscription at very low cost.

In this engaging session, we will present a practical attack that will exploit human weakness, Satellite receivers design, used protocols and subscription mechanisms that mainly relay on custom plugins on satellite receivers for channel decryption.

We will also describe technically a similar attack that was already conducted some years ago using a backdoor within CCCAM protocol provider.

This attack could be exploited to build a massive botnet of linux based satellite receivers or even computers used for satellite decryption and accessing end users local area networks that will be used as an edge for any other kind of attacks. There are millions of unaware end users downloading and installing any kind of plugins seeking cheap or even free satellite television, then the attack could be difficult to mitigate, and could easily lead to a hacker controlling millions of devices on the internet.

SWITCHES GET STITCHES

PRESENTED BY

Colin Cassidy & Robert Lee & Eireann Leverett

This talk will introduce you to Industrial Ethernet Switches and their vulnerabilities. These are switches used in industrial environments, like substations, factories, refineries, ports, or other homes of industrial automation. In other words: DCS, PCS, ICS & SCADA switches. The researchers focus on attacking the management plane of these switches, because we all know that industrial system protocols lack authentication or cryptographic integrity. Thus, compromising any switch allows the creation of malicious firmwares for further MITM manipulation of a live process. Such MITM manipulation can lead to the plant or process shutting down (think: nuclear reactor SCRAM) or getting into a unknown and hazardous state (think: damaging a blast furnace at a steel mill). Not only will vulnerabilities be disclosed for the first time (exclusively at Black Hat), but the methods of finding those vulnerabilities will be shared. All vulnerabilities disclosed will be in the default configuration state of the devices. While these vulnerabilities have been responsibly disclosed to the vendors, SCADA/ICS patching in live environments tends to take 1-3 years. Because of this patching lag, the researchers will also be providing live mitigations that owner/operators can use immediately to protect themselves. At least four vendors switches will be examined: Siemens, GE, Garrettcom, and Opengear.

TAKE A HACKER TO WORK DAY - HOW FEDERAL PROSECUTORS USE THE CFAA

PRESENTED BY

Leonard Bailey

What would happen if Black Hat invited the Department of Justice (DOJ) to give us a better understanding of the Computer Fraud and Abuse Act (or "CFAA") and explain how federal prosecutors use it and the DOJ actually showed up?

Attendees will hear directly from a Department of Justice's Computer Crime & Intellectual Property Section Prosecutor explaining the CFAA in plain English and breaking down the process for deciding whether to bring charges in federal hacking cases.

This session will cover data about how the CFAA has been used and pointers on how practitioners and researchers can stay out of hot water. You'll also gain insight into how prosecutors think about the intersection between their mission to protect computer networks and data from criminals, and the efforts of the computer security community to ferret out critical system vulnerabilities.

Seating will be limited for this rare briefing to our community. Bring your most thoughtful and meaningful questions, and be on your best behavior- our communities must work closely together to make security research safer while enabling law enforcement to pursue truly criminal behavior.

TAKING EVENT CORRELATION WITH YOU

PRESENTED BY

Rob King

Event correlation problems appear everywhere in information security and forensics: log analysis ("I'm seeing a lot of 404 errors from one range of IP addresses"), behavior detection ("That account may be compromised, he logged in twice from two different locations"), record linkage ("Is Jones, Robert the same as Bob Jones?"), and expert systems ("I have a system running Windows 7 Japanese Locale, with these hotfixes, what's my biggest security risk?", or from the other side, "What attacks should I try first?").

Despite the usefulness of event correlation, many security practitioners either ignore it or use ad hoc tools. This talk presents Giles, a compiler that creates event correlation engines. Its most interesting feature is that the output of Giles is a schema for a normal SQL database, and databases created using this schema are fully-fledged event correlation engines. This allows users to put an event correlation engine anywhere they could put a database (which is everywhere), and access it using any programming language that can access databases (which is all of them).

TARGETED TAKEDOWNS: MINIMIZING COLLATERAL DAMAGE USING PASSIVE DNS

PRESENTED BY

Paul Vixie

When civil investigators and law enforcement officers aggressively pursue and takedown cyber criminal enterprises, that undertaking should be subject to an important limitation: their online operations must be narrowly and precisely targeted so as to avoid harming innocent third parties.

For example, when evaluating an abused domain name for seizure, investigators need to ensure that innocent third parties are not also using that domain.

In his presentation, I will provide an overview of Passive DNS and how it can help investigators to reduce or eliminate collateral damage during takedowns, thereby avoiding negative publicity and potentially costly settlements.

TAXONOMIC MODELING OF SECURITY THREATS IN SOFTWARE DEFINED NETWORKING

PRESENTED BY

Jennia Hizver

Recent advances in software defined networking (SDN) provide an opportunity to create flexible and secure next-generation networks. Many companies have expressed the interest in SDN utilization. Much has been said about the ability of SDN to solve persistent network security problems. By contrast, our current knowledge on SDN vulnerabilities, threats, and attacks is very limited.

This study seeks to fill the knowledge gap through development of a novel taxonomic model of SDN threats. To better characterize the SDN threats, I classify them using the following three dimensions: the source triggering a vulnerability, the SDN component where the vulnerability arises, and the threat event by which a SDN attack is carried out. The model accounts for many-to-many relationships between the threat sources and threat events as well as threat events and vulnerability sources. From these relationships, various paths attackers could pursue to exploit SDN networks may be derived. Some of the paths are merely conceptual and are unlikely to materialize into actual attacks whereas some paths may represent real-life attack scenarios posing realistic dangers. I demonstrate the applications of the abstract taxonomic model by constructing concrete SDN attack examples to achieve unauthorized access, unauthorized disclosure of information, unauthorized modification, misuse, and disruption of service.

By exposing potential attack paths on SDN, the proposed taxonomic model will help companies to better understand SDN threat scenarios and to narrow down a set of threats most relevant for their environments. Based on the analysis of the attacks, I also provide a set of security recommendations to help security practitioners to choose the appropriate controls and countermeasures to combat the attacks.

THE APPLICATIONS OF DEEP LEARNING ON TRAFFIC IDENTIFICATION

PRESENTED BY

Zhanyi Wang & Chuanming Huang & Zhuo Zhang & Bo Liu

Generally speaking, most systems of network traffic identification are based on features. The features may be port numbers, static signatures, statistic characteristics, and so on. The difficulty of the traffic identification is to find the features in the flow data. The process is very time-consuming. Also, these approaches are invalid to unknown protocol. To solve these problems, we propose a method that is based on neural network and deep learning a hotspot of research in machine learning. The results show that our approach works very well on the applications of feature learning, protocol identification, and anomalous protocol detection.

THE BATTLE FOR FREE SPEECH ON THE INTERNET

PRESENTED BY

Matthew Prince

Google, Facebook, and Twitter all started out with admirable, lofty goals about preserving freedom of speech online saying that they wouldn't arbitrarily remove "distasteful" content. Yet one-by-one they all changed their position. Now countries, like Turkey are holding YouTube for ransom and bullying them to remove anything that they consider offensive or even inconvenient.

By protecting lawful content, no matter the source or how distasteful, you're protecting freedom of speech. So what does this mean for these companies on the front-line of the Internet? Matthew Prince, co-founder and CEO of CloudFlare, will explain what the cost of mob rule trumping the rule of law will be in the fight to keep the Internet free and open. He will share the real world impact that censorship has had on the Internet and the hidden cost born by the enterprises ultimately forced to censor themselves.

Protecting a free Internet can be a difficult and lonely road with pitfalls and traps that, once triggered, leads to a dead end of total censorship. Matthew will conclude with strategies for managing high-risk content, and suggested strategies for the future. We, as an industry, can work together to ensure that illegal content is effectively targeted and lawful content is protected.

THE KALI LINUX DOJO WORKSHOP #1: ROLLING YOUR OWN - GENERATING CUSTOM KALI LINUX 20 ISOS

PRESENTED BY

Mati Aharoni

Pre-Registration Required: This workshop is completely full. There are no more seats available.

THE KALI LINUX DOJO WORKSHOP #2: KALI USB SETUPS WITH PERSISTENT STORES AND LUKS NUKE SUPPORT

Pre-Registration Required: This workshop is completely full. There are no more seats available.

THE LITTLE PUMP GAUGE THAT COULD: ATTACKS AGAINST GAS PUMP MONITORING SYSTEMS

PRESENTED BY

Kyle Wilhoit & Stephen Hilt

Over a period of months, several Guardian AST gas pump monitoring systems were attacked. These attacks occurred on real pump monitoring systems, but also on systems that we controlled, created, and deployed. We watched these attackers, what they did, and performed intelligence gathering on the nefarious actors.

Details and intelligence on whom the attackers were, possible motivations behind the attacks, and detailed indicators of compromise will be shared in this. At the end of the talk, a script- named Gaspot will be released, allowing for anyone to deploy these virtual monitoring systems themselves.

THE MEMORY SINKHOLE - UNLEASHING AN X86 DESIGN FLAW ALLOWING UNIVERSAL PRIVILEGE ESCALATION

PRESENTED BY

Christopher Domas

In x86, beyond ring 0 lie the more privileged realms of execution, where our code is invisible to AV, we have unfettered access to hardware, and can trivially preempt and modify the OS. The architecture has heaped layers upon layers of protections on these negative rings, but 40 years of x86 evolution have left a labyrinth of forgotten backdoors into the ultra-privileged modes. Lost in this byzantine maze of decades-old architecture improvements and patches, there lies a design flaw that's gone unnoticed for 20 years. In one of the most bizarre and complex vulnerabilities we've ever seen, we'll release proof-of-concept code exploiting the vast, unexplored wasteland of forgotten x86 features, to demonstrate how to jump malicious code from the paltry ring 0 into the deepest, darkest realms of the processor. Best of all, we'll do it with an architectural 0-day built into the silicon itself, directed against a uniquely vulnerable string of code running on every single system.

THE NODEJS HIGHWAY: ATTACKS ARE AT FULL THROTTLE

PRESENTED BY

Maty Siman & Amit Ashbel

The popularity of the Node.js coding language is soaring. Just five years after its debut, the language's framework now boasts more 2 million downloads a month. It's easy to understand why. This event-driven language kept the simplicity of existing Web concepts and trashed the complexities; applications built on Node.js do not require a dedicated Web server to run; and Google is even pushing the language with its enhanced V8 engine for the Google Chrome Web browser. In fact, just consider Node.js as the drive-and-go language.

But before accelerating too quickly, it is important to understand the power and corresponding mishaps of this language. This talk is not intended to put the brakes on Node.js. On the contrary, this talk aims to raise awareness to its security issues during application development.

As such, our talk ends with effective security measures that enterprises can adopt in order to drive their business forward and securely.

THE NSA PLAYSET: A YEAR OF TOYS AND TOOLS

PRESENTED BY

Michael Ossmann

Inspired by the contents of the leaked NSA ANT catalog, the NSA Playset project has produced an array of gadgets with capabilities similar to those employed by the spooks. I will review the entire collection since the start of the project. This includes new tools for USB, PCI Express, I2C, GSM, Bluetooth, and a family of RF retroreflectors for eavesdropping on a wide variety of electronic devices. Now you can play along with the NSA!

THE TACTICAL APPLICATION SECURITY PROGRAM: GETTING STUFF DONE

PRESENTED BY

Cory Scott & David Cintz

How many times have we heard the following pieces of wisdom from CISOs or other security talking heads? Be strategic, not tactical. Build security in - forget about break-fix.

Like a siren song, these words have caused a great many professionals to crash upon the rocks, and the strategy-first camp is simply doing a disservice to your users. Maybe that is why the average CISO only lasts a couple of years.

In our talk, we're going to tackle this conventional wisdom in the name of Getting Shit Done and propose a new path: The Tactical Security Program. We've established a lightweight, heavy hitting team thats performed over 400 assessments, handled over 900 bugs, and established a private bug bounty program all in one year, and we'd like to share some of our practices. If you are managing a program, you will come out of our talk with some actionable advice. If you are a worker bee, we will teach you how to subvert the system from within.

And while we're at it, we will tell you why following some of the newer trends of security wisdom, including embracing public bug bounty programs, is also a bad idea. Yeah, we said it.

THESE ARE NOT YOUR GRAND DADDYS CPU PERFORMANCE COUNTERS - CPU HARDWARE PERFORMANCE COUNTERS FOR SECURITY

PRESENTED BY

Nishad Herath & Anders Fogh

CPU hardware performance counters allow us to do low latency performance measuring, without special runtime or compile time software instrumentation. It is said "advanced users often rely on those counters to conduct low-level performance analysis or tuning" according to Wikipedia. But is this all we can do? Maybe it is all that they were meant for, faster debugging and profiling. But these days, the performance counters you find in your CPUs are not exactly your grand daddy's CPU performance counters! They can do bigger and better things - even defending against RowHammer! Yes, they can be used to to make platforms more secure!

Okay, so on Intel x86/x64 compatible CPUs, the MSR_DEBUGCTLA MSR (Model Specific Register) can be used for LBR (Last Branch Recording). BTF CPU flag can facilitate "single stepping" on branching rather than just single stepping on every instruction. Clearly many uses. Some of it security related, like the potential for ROP mitigation. These are reasonably well explored. Perhaps not widely discussed though.

Anyway, in this talk, we will be talking about very interesting features that we find today on Intel x86/x64 compatible CPUs that can be leveraged to achieve platform security relevant outcomes that were simply impractical using software only means, or your grandaddy's CPU performance counters. Some of the use cases might surprise you! We will be demonstrating these techniques against real world exploit code, with performance impact numbers to boot!

We might even share our code with those who ask us nicely.

THIS IS DEEPERENT: TRACKING APP BEHAVIORS WITH (NOTHING CHANGED) PHONE FOR EVASIVE ANDROID MALWARE

PRESENTED BY

Yeongung Park & Jun Young Choi

Malwares on Android platform are increasing every year by explosive growth over the years and it is a serious threat on Android platform. Many tools have been released in order to quickly analyze these malicious code. Depending on the appearance of analysis tools, Android Malwares have been applied to the anti-analysis techniques, such as packing, environment detection, cryptography, and anti-debugging. These technique can hide the malicious behaviors, as well as prevent the analysis. Various obfuscation techniques is also applied to Android applications and malwares. For this reason, we take a long time to analyze the app. In addition, it makes difficult to find a vulnerability and to carck through analysis of the app in attacker's perspective.

To analyze the Android application and evasive malware, we need to overcome following challenges:

- Fast code analysis (It's always challenge)
- Environment detection (Emulator detection, Device detection and Rooting detection)
- Obfuscation
- Dynamic code loading(in file/on memory)
- Anti-analysis techniques (anti-ptrace, anti-disassembly, self-modification check, etc)
- Behaviors in native level

In this talk, we will introduce new powerful tool tracking method to monitor behaviors of evasive Android malware without OS modification. We used a different concept to analyze the Android application fast and deeply. The tools can track all methods you want to monitor, such as User-defined classes/methods, 3rd-Party libraries, and Java/Android APIs. Furthermore, the tool can monitor functions in native level like JNI(Java Natvie Interface), Functions in libc and Binder on nothing-changed phone. We are going to present base techniques for implementation and demonstrate on how to analyze very complicated evasive and advanced Android malware.

THUNDERSTRIKE 2: SITH STRIKE

PRESENTED BY

Trammell Hudson & Xeno Kovah & Corey Kallenberg

The number of vulnerabilities in firmware disclosed as affecting Wintel PC vendors has been rising over the past few years. Although several attacks have been presented against Mac firmware, unlike their PC counterparts, all of them required physical presence to perform. Interestingly, when contacted with the details of previously disclosed PC firmware attacks, Apple systematically declared themselves not vulnerable.

This talk will provide conclusive evidence that Mac's are in fact vulnerable to many of the software only firmware attacks that also affect PC systems. In addition, to emphasize the consequences of successful exploitation of these attack vectors, we will demonstrate the power of the dark side by showing what Mac firmware malware is capable of.

TRUSTKIT: CODE INJECTION ON IOS 8 FOR THE GREATER GOOD

PRESENTED BY

Alban Diquet & Eric Castro & Angela On-kit Chow

With the release of iOS 8, Apple has relaxed the rules regarding how code can be packaged within an iOS App when submitting to the App Store. While in the pre-iOS 8 world, all code had to be statically linked into the Apps binary, Apple is now allowing third-party frameworks and libraries to be embedded in an Apps package and be dynamically loaded at runtime, as needed by the App.

We will describe what has changed exactly and why, and the new opportunities it provides to mobile and security engineers. While doing so, we will also provide a quick overview of the library loading mechanism on iOS as well as how to perform function hooking in a non-jailbroken environment, and how developers can take advantage of this functionality.

We will then present a new open-source library for iOS that leverages these mechanisms: TrustKit.

TrustKit provides universal SSL public key pinning (NSURLSession, NSURLConnection, UIWebView, Cordova, etc.) and can be deployed within an App in a matter of minutes, without having to modify the Apps source code. This work is a collaboration between Data Theorem and Yahoo's mobile engineers, and offers a novel and easy-to-use implementation; we call it drag & drop SSL pinning.

Throughout the presentation, attendees will have the opportunity to understand how the rules regarding dynamic linking have changed in iOS 8 and how this change can be leveraged to solve security issues in a novel way. Additionally, as TrustKit will be released as an open-source library, attendees will also be able to discover and deploy this library in their own iOS Apps.

UNDERSTANDING AND MANAGING ENTROPY USAGE

PRESENTED BY

Bruce Potter & Sasha Wood

As security and privacy concerns become an above the fold concern for the public at large and enterprises continue to grapple with targeted intrusions, cryptography is becoming a ubiquitous and necessary characteristic of modern IT systems. While the primitives and core algorithms are well understood, there are still numerous concerns regarding properly encrypting data that transcend decisions such as public vs. private key or key length. Underlying nearly every modern cryptosystem is the need to have cryptographically strong random numbers. Key generation and inclusion of nonces to prevent replay are two areas where lack of quality random numbers can completely destroy the security provided by the underlying cryptosystem.

For decades, we have used Pseudo Random Number Generators (PRNGs) as a surrogate for truly random numbers. While these PRNGs have been generally sufficient for historic cryptographic usage, they are only as good as their underlying entropy source. With advances, such as Perfect Forward Secrecy in TLS (and its wide scale deployment), entropy usage has skyrocketed. Unfortunately, enterprises dont have any understanding of their entropy requirements and entropy usage in the systems we use every day. How much entropy does an OpenSSL PFS transaction actually use? What are the sources of entropy used in your front line webservers? How does entropy creation vary in different versions of Linux? These are all important questions with no clear answer.

This talk aims to shine light on the core concerns of entropy creation and entropy utilization. We have analyzed a wide variety of systems, including different versions of the Linux and FreeBSD kernel, OpenSSL, OpenSSH, OpenVPN, and other crypto systems and documented their requirements for random numbers and required amount of entropy to function correctly. The team will also present findings entropy consumption for a variety of TLS modes including the impact of PFS. We will also present analysis of the quality and quantity of entropy sources available on common desktop, laptop, server, and mobile hardware. Finally, the team will also release the first version of our open source software, libentropy, that provides a unified interface for OpenSSL to manage sources of entropy and report status of entropy creation and utilization.

UNDERSTANDING THE ATTACK SURFACE AND ATTACK RESILIENCE OF PROJECT SPARTANS NEW EDGEHTML RENDERING ENGINE

PRESENTED BY

Mark Vincent Yason

EdgeHTML is the new rendering engine that will power the next generation web browser (codenamed Spartan) to be introduced in Windows 10. Because EdgeHTML will be widely deployed - from Windows 10 mobile devices to PCs, it is important that we have understanding of its attack surface and its stance against exploitation.

In this presentation, I'll discuss EdgeHTML's attack surface and the different methods for enumerating it. Then, I'll describe the process of comparing EdgeHTML and MSHTML to identify and understand what had changed from the forking process, and more importantly identify new features and added internal functionalities that can contribute to its attack surface. Finally, I'll discuss the exploit mitigations in place, how they help against certain classes of vulnerabilities, and discuss known bypass techniques that are still applicable.

UNICORN: NEXT GENERATION CPU EMULATOR FRAMEWORK

PRESENTED BY

Nguyen Anh Quynh & Hoang-Vu Dang

CPU emulator is a program emulating the internal operation of a physical CPU in software. CPU emulator plays a vital role and has a lot of applications in computer security area, such as reversing obfuscated malware or verifying code semantics.

Unfortunately, such a fundamental component does not get the attention it absolutely deserves. At the moment, all the existing CPU emulators suffer from some major issues:

- Do not get updated with latest hardware. Example: PyEmu for X86 was released in 2009, but no longer developed since then.
- Mostly available only for Python, but support for other programming languages is not existent.
- Often restricted to some environments, thus cannot be used to build independent tools. Example: IDA-x86emu is for IDA Pro only.
- No single tool supports Intel X86_64, which is the dominant architecture at the moment.
- Solely focus on X86, but support for other important architectures are horribly missing: Arm, Arm64, Mips, PPC, Sparc, etc.

It is unbelievable that the lack of such a fundamental component as CPU emulator has happened forever without a proper fix. We decided to step up and took the problem in our own hands to solve it once and for all. As a result, Unicorn emulator was born and succesfully handles all the outstanding problems.

Unicorn offers some unparalleled features, as highlighted below:

- Provide an independent framework to develop independent security tools on top of it. Building plugins for other environment, such as IDA is also well supported.

- Multi-architectures: Unicorn can emulate all the popular architectures, such as X86 (including X86_64), ARM, ARMv8, M68K, Mips, PowerPC, and Sparc, etc.
- Multi-platforms: Natively available for Windows, Mac OSX, Linux & *BSD.
- Implemented in pure C, with bindings for Python available. Support for other languages are also in pipeline.
- Clean/simple/lightweight/intuitive architecture-neutral API.
- Thread-safe by design.
- Open source.

This talk introduces some existing emulators, then goes into details of their design/implementation and explains their current issues. Next, we will present the architecture of Unicorn and the challenges of designing and implementing it. The audience will understand the advantages of our framework and see why the future is assured, so that Unicorn will keep getting better, stronger and become the emulator engine of choice for the security community.

Unicorn aims to lay the ground for innovative works. To conclude the talk, some new advanced tools built on top of Unicorn will be introduced to demonstrate its power, so the audience can see how our framework can open up many opportunities for future of security research & development.

USING STATIC BINARY ANALYSIS TO FIND VULNERABILITIES AND BACKDOORS IN FIRMWARE

PRESENTED BY

Christopher Kruegel & Yan Shoshitaishvili

Over the last few years, as the world has moved closer to realizing the idea of the Internet of Things, an increasing amount of the things with which we interact every day have been replaced with embedded devices. These include previously non-electronic devices, such as locks, light switches, and utility meters (such as electric meters and water meters), as well as increasingly more complex and ubiquitous devices, such as network routers and printers. Other devices are becoming increasingly intelligent as well. Modern printers and cameras include complex social media functionality, smart televisions are increasingly including Internet-based entertainment options, and even previously-simple devices, such as watches and glasses are being augmented with complex embedded components.

The increasingly-complex systems that drive these devices have one thing in common: they must all communicate to carry out their intended functionality. Smart TVs communicate with (and accept communication from) online media services, smart locks allow themselves to be unlocked by phones or keypads, digital cameras contact social media services, and smart meters communicate with the users utility company. Such communication, along with other functionalities of the device, is handled by software (termed firmware) embedded in the device. Because these devices often receive privacy-sensitive information from their sensors (such as what a user is watching, or how much electricity they are using), or carry out a safety-critical function (such as actuators that lock the front door), errors in the devices firmware, whether present due to an accidental mistake or purposeful malice, can have serious and varying implications in both the digital and physical world.

Firmware, like any piece of software, is susceptible to a wide range of software errors. These include memory corruption flaws, command injection vulnerabilities and application logic flaws. Another common error seen in firmware is a logic flaw called an authentication bypass or less formally, a backdoor. An authentication bypass occurs when an error in the authentication routine of a device allows a user to perform actions for which they would otherwise need to know a set of credentials. In other cases, backdoors are deliberately inserted by the manufacturer to get access to deployed devices for maintenance and upgrade.

Detecting vulnerabilities and backdoors in firmware is challenging for several reasons. To begin with, the devices in question are usually proprietary, and therefore the source code of the firmware is not available. While this is a problem common to analyzing binary software in general, firmware takes it one step further: firmware often takes the form of a single binary image that runs directly on the hardware of the device, without an underlying operating system. Because of this, OS and library abstractions do not exist in some cases, and are non-standard or undocumented in others, and it is frequently unknown how to properly initialize the runtime environment of the firmware sample (or even, at what offset to load the binary and at what address to begin execution). We term such firmware as binary blob firmware. These blobs can be very large, and therefore any analysis tool must be able to handle such complex firmware. Additionally, embedded devices frequently require their firmware to be cryptographically signed by the manufacturer, making modification of the firmware on the device for analysis purposes infeasible.

In this presentation, we will talk about the challenges of performing automated vulnerability analysis and backdoor finding in firmware. Then, we report on a binary static analysis system, called Angr, that automates most of the process of searching firmware binaries for the presence of flaws. To the best of our knowledge, Angr is the first firmware analysis system working at the binary level, in a scalable manner, and with no requirement to instrument code on the original device. To this end, Angr utilizes advanced program analysis techniques to analyze binary code in complex firmware of diverse hardware platforms, and it automates much of the process of identifying occurrences of buffer overflow and authentication bypass vulnerabilities. The tool uses novel techniques to improve the scalability of the analysis, which we will explain during the presentation. This includes a combination of more traditional static program analysis, value set analysis (VSA), and symbolic execution. The presentation will conclude with a few examples of vulnerabilities that our tool has discovered in firmware samples. We also plan to run a live demo that highlights the capabilities of our system.

WEB TIMING ATTACKS MADE PRACTICAL

PRESENTED BY

Timothy Morgan & Jason Morgan

Timing side-channel attacks are a well-known class of flaw in cryptographic systems and applications in general. While these issues have been researched for decades, the complexities involved in obtaining accurate timing measurements and performing accurate statistical analysis has prevented the average pentester from identifying and exploiting these issues on a day-to-day basis.

In this paper, we build on past research to make remote timing attacks practical against modern web applications. We scrutinize both methods of data collection and statistical analysis used by previous researchers, significantly improving results in both areas. We implement an adaptive Kalman filter, which provides greater accuracy in classifying timing differences, making timing attacks more practical in congested networks and speeding up attacks in ideal conditions. As part of this research, a new open source timing attack tool suite is being released to the community.

WHEN IOT ATTACKS: HACKING A LINUX-POWERED RIFLE

PRESENTED BY

Runa A. Sandvik & Michael Auger

TrackingPoint is an Austin startup known for making precision-guided firearms. These firearms ship with a tightly integrated system coupling a rifle, an ARM-powered scope running a modified version of Linux, and a linked trigger mechanism. The scope can follow targets, calculate ballistics and drastically increase its user's first shot accuracy. The scope can also record video and audio, as well as stream video to other devices using its own wireless network and mobile applications.

In this talk, we will demonstrate how the TrackingPoint long range tactical rifle works. We will discuss how we reverse engineered the scope, the firmware, and three of TrackingPoint's mobile applications. We will discuss different use cases and attack surfaces. We will also discuss the security and privacy implications of network-connected firearms.

WHY SECURITY DATA SCIENCE MATTERS AND HOW ITS DIFFERENT: PITFALLS AND PROMISES OF DATA SCIENCE BASED BREACH DETECTION AND THREAT INTELLIGENCE

PRESENTED BY

Joshua Saxe

As our networks generate an ever-larger deluge of security-relevant data, data science (machine learning, data visualization, and scalable storage technologies) has become necessary if we are to succeed in both stopping advanced attackers and gaining intelligence about their tactics. Unfortunately, there is still a gap between the security and data science communities: security professionals often have limited knowledge of data science, and security data scientists often come from non-security backgrounds and may not understand why security data science is different than the solutions taught in traditional machine learning and visualization programs.

In my talk, I will bridge this gap, speaking to both audiences, discussing the challenges and opportunities posed by applying data science to security, demonstrating exciting results achieved by my research group, and empowering attendees to apply security data science in new and powerful ways. The first part of the talk will provide a non-mathematical overview of security data science, introducing state of the art data visualization and the big three machine learning tasks (classification, clustering and regression). For each of the topics, I will give examples of how my colleagues and I have successfully applied the topic to problems like attack detection, threat intelligence, malware analysis and scalable malware analytics.

The second part of the talk will cover both major security-specific data science challenges and solutions to these challenges. One challenge is that malicious activity exists as a needle in the haystack of terabytes of benign data, causing textbook data science methods, which are often not designed for such scenarios, to generate reams of false positives. Another challenge is the inevitable lack of access to 0-day attack data with which to train machine-learning approaches. I will go over multiple mitigations for both of these problems, including statistical methods designed to generalize to new attacks and minimize false positives, and will show

how these methods have performed impressively in detecting 0-day malware in my groups work.

The third part of my talk will address security data visualization, discussing my groups ongoing and past log visualization, malware analysis visualization, and threat intelligence visualization work [4][5]. In discussing this work I will describe how we use machine-learning approaches to address a challenge unique to security data visualization: the semantic gap between low-level security data and the high-level activity we actually care about. In summary, my talk will explore the emerging and exciting world of security data science, discussing opportunities, challenges and effective approaches. My goal is that attendees leave the talk excited about the possibilities of applying data science to their own security related work, newly aware of the pitfalls of this area, and more knowledgeable about solutions to these pitfalls.

WINNING THE ONLINE BANKING WAR

PRESENTED BY

Sean Park

Currently, most security products and financial institutions defending against banking malware rely on online banking page integrity check to detect the presence of financial malware. This technique works due to the inherent mechanics of financial malware injecting into the browser's DOM space. However, this purely web-based page integrity check can be subverted in many ways. This presentation will talk about evasion techniques such as replay attack, polymorphism, inject randomisation, and DOM stealth rootkit as well as countermeasures for those in clientless way.

The presentation also includes a novel method derived from Zero Knowledge Protocol that prevents banking malware from reverse engineering secrets transmitted between an online banking client and its server by eaves dropping HTTPS traffic.

WRITING BAD @$$ MALWARE FOR OS X

PRESENTED BY

Patrick Wardle

In comparison to Windows malware, known OS X threats are really quite lame. As an Apple user that has drank the 'Apple Juice,' I didn't think that was fair!

From novel persistence techniques, to native OS X components that can be abused to thwart analysis, this talk will detail exactly how to create elegant, bad@ss OS X malware. And since detection is often a death knell for malware, the talk will also show how OS X's native malware mitigations and 3rd-party security tools were bypassed. For example I'll detail how Gatekeeper was remotely bypassed to allow unsigned download code to be executed, how Apple's 'rootpipe' patch was side-stepped to gain root on a fully patched system, and how all popular 3rd-party AV and personal firewall products were generically bypassed by my simple proof-of-concept malware.

However, don't throw out your Macs just yet! The talk will conclude by presenting several free security tools that can generically detect or even prevent advanced OS X threats. Armed with such tools, we'll ensure that our computers are better protected against both current and future OS X malware.

So unless you work for Apple, come learn how to take your OS X malware skills to the next level and better secure your Mac at the same time!

WSUSPECT - COMPROMISING THE WINDOWS ENTERPRISE VIA WINDOWS UPDATE

PRESENTED BY

Paul Stone & Alex Chapman

Ever wondered what really happens when you plug in a USB device and Windows begins 'searching for Drivers'? Who doesn't have that Windows Update reboot dialog sitting in the corner of their desktop? Our talk will take an exciting look at one of the dullest corners of the Windows OS.

WSUS (Windows Server Update Services) allows admins to co-ordinate software updates to servers and desktops throughout their organisation. Whilst all updates must be signed by Microsoft, we find other routes to deliver malicious updates to Windows systems using WSUS. We will demonstrate how a default WSUS deployment can be leveraged to gain SYSTEM level access to machines on the local network.

We also take a look at exactly what happens when you plug in a new USB device into a Windows desktop. There are thousands Microsoft-signed updates for 3rd party drivers available through Windows Update. We show how driver installs can be triggered by low privileged users and look at the insecurities that can be introduced by these Microsoft-blessed drivers.

In addition to some exciting demos we will also describe how to lock down enterprise WSUS configurations to avoid these "on by default" vulnerabilities.

You have 1 malicious update ready to install...

ZIGBEE EXPLOITED THE GOOD THE BAD AND THE UGLY

PRESENTED BY

Tobias Zillner & Sebastian Strobl

ZigBee is one of the most widespread communication standards used in the Internet of Things and especially in the area of smart homes. If you have, for example, a smart light bulb at home, the chance is very high that you are actually using ZigBee. Popular lighting applications, such as Philips Hue or Osram Lightify are based on this standard. Usually, IoT devices have very limited processing and energy resources, and therefore not capable of implementing well-known communication standards, such as Wifi. ZigBee is, however, an open, publicly available alternative that enables wireless communication for such devices.

ZigBee also provides security services for key establishment, key transport, frame protection, and device management that are based on established cryptographic algorithms.

So, is a ZigBee home automation network with applied security and smart home communication protected? No, absolutely not. Due to interoperability and compatibility requirements, as well as the application of legacy security concepts, it is possible to compromise ZigBee networks and take over control of all connected devices. For example, it is entirely possible for an external party to gain control over every smart light bulb that supports the ZigBee Light Link profile. This is made possible because the initial key transport is done in an unsecured way, and support of this weak key transport is, in fact, even required by the standard itself.

Due to these shortfalls and limitations created by the manufacturers themselves, the security risk in this last tier communication standard can be considered as very high.

This talk will provide an overview of the actual applied security measures in ZigBee, highlight the included weaknesses, and show practical exploitations of actual product vulnerabilities, as well as our recently developed ZigBee security-testing framework tool.

Technology Group

Black Hat
Content Marketing Institute
Content Marketing World
Dark Reading

Enterprise Connect
Fusion
GDC
Gamasutra

HDI
ICMI
InformationWeek
Interop ITX

Network Computing
No Jitter
VRDC

COMMUNITIES SERVED

Content Marketing
Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing Solutions
Contact Us
Licensing

Terms of Service | Privacy Statement | Copyright © 2021 UBM, All rights reserved.