black hat® dc+2010

DIGITAL SELF DEFENSE

ARLINGTON, VA
HYATT REGENCY CRYSTAL CITY

welcome

Welcome to Black Hat Briefings DC. As Black Hat heads into its 13th year, I see this as a pivotal time for the entire industry. In my short time as a participating member on the Department of Homeland Security Advisory Committee, it has become apparent the need for talented security professionals such as yourselves—in both the public and private sectors.

The DHS announced it will be adding up to 1,000 people in security, intelligence analysts, computer and electronic engineers, computer scientists, investigators and analysts, criminal investigators and IT specialists before the end of 2012 at the GS 9 to 15 levels. The U.S. Cyber Command is hiring. NSA is hiring. We are at the beginning of a wider acknowledgement through government that 'Cyber' matters. Every government or private project of note relies on the stability and security of its computer systems. It's a good time to be alive!

I am excited for this year's conference because it has grown from two tracks to three, a long-time personal goal of mine. I think the only way Black Hat DC will grow is by staying focused on technical security content and research and by adding more of it. This third track is the first major step in that direction.

This year's three tracks will feature over 25 speakers discussing their latest research. In addition we have selected a wider range of topics, instead of being forced to only have one presenter on a given topic there are now more topics that complement and build on each other.

In 2010 you will see Black Hat in more places, as we try to expand the reach of Black Hat speakers and trainers. In late 2009 we held a successful joint Virtual Event with Dark Readings, a great lead in to our own stand alone Virtual Black Hat Briefings in Q4 of this year. Think of it as a regular Briefings with a Call for Papers, keynote address and multiple tracks. Same great content delivered at Black Hat, just all on-line.

Black Hat Europe will be hosted in Barcelona, Spain at the Hotel Rey Juan Carlos. Black Hat has out grown the available appropriate venues in Amsterdam. As much as it pains me to leave the Netherlands I am looking forward to Spain. This new venue will give us the much needed space to deliver a three-track Briefings and expanded trainings. Once again, a positive step in delivering more content. The CFP is now open, so if you wanted to present and help kick-off our new European venue, now is your opportunity.

Also of note for 2010 is that we will be hosting the first Middle East Black Hat event in Abu Dhabi, bringing the Black Hat way of thinking about security to a different region of the world. With three tracks and training it will be the full Black Hat experience! I hope it inspires the security experts in the region to participate. I'm really interested to learn what's going on in their security community.

Take advantage of the wonderful networking opportunities with your peers and our sponsoring companies during the breaks and this evening's reception. Enjoy the show!

Jeff Moss

Jeff Moss
Director, Black Hat

contents

SUSTAINING sponsors

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

WWW.BLACKHAT.COM

presentations

CONNECTION STRING PARAMETER POLLUTION ATTACKS

Chema Alonso & Jose Palazon

This session is about Parameter Pollution in Connection Strings Attack. Today, a lot of tools and web applications allow users to configure dinamicly a connection agains a Database server. This session will demonstrate the high risk in doing this unsecurely. This session will show how to steal, in Microsoft Internet Information Services, the user account credential, how to get access to this web applications impersonating the conneciton and taking adavance of the web server credentials and how to connect against internal databases servers in the DMZ without credentials. The impact of these techniques are specialy dangerous in hosting companies which allow customers to connect against control panels to configure databases.

INTERNET EXPLORER TURNS YOUR PERSONAL COMPUTER INTO A PUBLIC FILE SERVER

Jorge Luis Alvarez Medina

In this presentation we will show how an attacker can read every file of your filesystem if you are using Internet Explorer. This attack leverages different design features of Internet Explorer entailing security risks that, while low if considered isolated, lead to interesting attack vectors when combined altogether. We will also disclose and demonstrate proof of concept code developed for the scenarios proposed.

NEUROSURGERY WITH METERPRETER

Colin Ames & David Kerb

A crucial step in post-exploitation technology is memory manipulation. Metasploit's Meterpreter provides a robust platform and API on which to build memory exploitation tools to assist the attacker in post-exploitation tasks. This talk will cover several examples of memory manipulation using meterpreter and introduce an extension to aid post-exploitation activities.

We will demonstrate the extraction of unique process memory to analyze for valuable information such as passwords. We will also demonstrate the injection of utilities into a processes memory in order to alter execution flow to provide new "features" like Putty Hijack. Another example that will be covered is interacting with the lsass process memory in order to steal windows session hashes required for pass the hash. Finally we will discuss the use of meterpreter to patch process memory in order to introduce vulnerabilities which can be leveraged for things such as persistence.

Another form of "memory" is the knowledge a host has about its network environment. This presentation will discuss the utilization of a meterpreter extension to automate and facilitate passive network reconnaissance over time, allowing for smart network data acquisition and analysis.

ADVANCED COMMAND INJECTION EXPLOITATION: CMD.EXE IN THE 00's

Bannedit

Command injection vulnerabilities have always been a neglected vulnerability class when it comes to exploitation. Many researchers simply view command injection bugs as a direct interface with a shell. While this is true, much more complex tasks can be acheived rather than just executing commands. The purpose of this talk is to discuss the advanced techniques to exploit command injection bugs to leverage more out of these types of vulnerabilities than just a shell. The techniques covered in this talk will show examples of taking a command injection bug and turning it into full native payload execution.

NEAT, NEW, AND RIDICULOUS FLASH HACKS

Mike Bailey

Flash is scary stuff. It's installed on just about everybody's web browser, used everywhere, and has a poor security track record. Even within the web application security community, its quirks are poorly understood. Known and intentional behavior can have serious consequences which merit exploration.

This talk is a discussion of new flash-based attacks, repurposing of old attacks, and demonstrations of working (and sometimes ridiculously complex) attacks on Gmail, Twitter, and other major websites.

INTERPRETER EXPLOITATION: POINTER INFERENCE AND JIT SPRAYING

Dionysus Blazakis

As remote exploits have dwindled and perimeter defenses have become the standard, remote client-side attacks are the next best choice for an attacker. Modern Windows operating systems have quelled the explosion of client-side vulnerabilities using mitigation techniques such as data execution prevention (DEP) and address space layout randomization (ASLR). This work will illustrate two novel techniques to bypass DEP and ASLR mitigations. These techniques leverage the attack surface exposed by the advanced script interpreters or virtual machines commonly accessible within the browser. The first technique, pointer inference, is used to find the memory address of a string of shellcode within the ActionScript interpreter despite ASLR. The second technique, JIT spraying, is used to write shellcode to executable memory by leveraging predictable behaviors of the ActionScript JIT compiler bypassing DEP. Future research directions and countermeasures for interpreter implementers are discussed.

AN UNINVITED GUEST (WHO WON'T GO HOME)

Bill Blunden

While there are a multitude of battle-tested forensic tools that focus on disk storage, the domain of memory analysis is still emerging. In fact, even the engineers who work at companies that sell memory-related tools have been known to admit that the percentage of investigators who perform an in-depth examination of memory is relatively small. In light of this, staying memory resident is a viable strategy for rootkit deployment. The problem then becomes a matter of remaining inconspicuous and finding novel ways to survive a system restart. In this presentation I'll look at rootkit technology that tackles both of these issues on the Windows platform.

REVERSING DPAPI AND STEALING WINDOWS SECRETS OFFLINE

Elie Bursztein & Jean-Michel Picod

The Data Protection API (DPAPI) plays a key role in Windows security: This API is meant to be the standard way on Windows OS to store encrypted data on the disk. DPAPI is used by many popular applications including Internet Explorer, Google Talk, Google Chrome, Skype, MSN (6.5-7) to encrypt their passwords. It is also used by Windows itself to store sensitive information such as EFS certificates and and Wifi (WEP and WPA) keys.

DPAPI use very opaque structures to store these encrypted data on disk and the available documentation is very sparse. Therefore prior to our work it was impossible to extract and analyze these secrets offline for forensic purpose. This is a particular huge issue for files encrypted using EFS because unless the EFS certificate protected by DPAPI is recovered these files can't be decrypted and analyzed.

To address these issues, we did reverse the DPAPI and in this presentation will provide a complete walkthrough DPAPI and its structures. Afterward armed with this knowledge, anyone interested in windows forensic will be able to deal with data stored with DPAPI. We will cover the change made by Microsoft from Windows XP up to Windows Seven. Finally we will demonstrate and release DPAPick (www.dpapick.com) which we believe, is the first tool that allows to decrypt offline data encrypted with DPAPI.

BEWARE OF SERIALIZED GUI OBJECTS BEARING DATA

David Byrne & Rohini Sulatycki

This presentation will highlight 0-days in Apache MyFaces and Sun Mojarra that allow an attacker to access all server-side session data, as well as some globally-scoped application variables. This presentation will provide a live demonstration of the flaws. The tool used to exploit the vulnerability will also be released.

A similar vulnerability is present in Microsoft's ASP.Net view state. This may not technically be an 0-day, but it is a poorly known flaw that has been present since the beginning days of .Net. A live demonstration of this will also be performed.

EXPLOITING LAWFUL INTERCEPT TO WIRETAP THE INTERNET

Tom Cross

Many goverments require telecommunications companies to provide interfaces that law enforcement can use to monitor their customer's communications. If these interfaces are poorly designed, implemented, or managed they can provide a backdoor for attackers to perform surveillance without lawful authorization. Most lawful intercept technology is proprietary and difficult to peer review. Fortunately, Cisco has published the core architecture of it's lawful intercept technology in an Internet Draft and a number of public configuration guides.

This talk will review Cisco's architecture for lawful intercept from a security perspective. The talk will explain how a number of different weaknesses in its design coupled with publicly disclosed security vulnerabilities could enable a malicious person to access the interface and spy on communications without leaving a trace.

The talk will explain what steps network operators need to take to protect this interface. The talk will also provide a set of recommendations for the redesign of the interface as well as SNMP authentication in general to better mitigate the security risks.

UNMANNED AERIAL VEHICLES: EXPLOIT AUTOMATION WITH THE METASPLOIT FRAMEWORK

Egypt

Sometimes you need to choose your exploits precisely and be careful about the packets you write to the wire. Sometimes you just want to type a command, go get some coffee, and come back to a pile of shells.

CONTINUED »

This talk will cover the means that the Metasploit Framework provides for accomplishing both of these goals, including many advancements from my talk at Black Hat USA in the realm of client-side exploitation.

WHOSE INTERNET IS IT, ANYWAY?
Andrew Fried, Ben Butler & Richard Cox

Malware injecting emails and websites have reached epidemic proportions on the Internet. Virtually all spam originates from bot-infected systems, which have the capacity to send out millions of emails per hour. The sites hosting malware are often part of large fast flux botnets that are geographically dispersed and change with great frequency. The threats have gotten larger; they hit victims faster and have been causing unprecedented losses.

Historically, the primary defense against these attacks has been the anti-virus program. Today, however, antivirus products no longer provide adequate protection – detection rates of less than 20% are commonly seen on newly discovered malware.

The detection, suppression and mitigation of these threats require timely and coordinated efforts between security researchers, anti-virus/content filter vendors, realtime blackhole list maintainers and domain registrars/registries.

This presentation will provide a rare glimpse "behind the curtain" of the efforts undertaken by security researchers (represented by Internet Systems Consortium), domain registrars (represented by GoDaddy) and realtime blackhole providers (represented by The Spamhaus Project and SURBL).

HARDWARE IS THE NEW SOFTWARE
Joe Grand

Society thrives on an ever increasing use of technology. Electronics are embedded into nearly everything we touch. Hardware products are being relied on for security-related applications and are inherently trusted, though many are completely susceptible to compromise with simple classes of attacks that have been known for decades.

Bolstered by the flourishing hobbyist electronics/do-it-yourself movement, easy access to equipment, and realtime information sharing courtesy of the internet, hardware is an area of computer security that can no longer be overlooked. In this session, Joe will explore the hardware hacking process and share some of his favorite attacks against electronic devices.

ENHANCING ZFS
Christian Kendi

ZFS is a revolutionary Open Source file system with many capabilities. Snapshots and Storage pools open new ways on how to store data. Attacking the most valuable assets of a company, their data.

This Talk will focus on how to enhance ZFS and the Solaris Kernel by hijacking ZFS kernel symbols. Furthermore, a demo will be given a new 0day technique will be revealed on how to hide file systems and entire store pools from forensics.

WIRELESS SECURITY ISN'T DEAD: ATTACKING CLIENTS WITH MSF
Mike Kershaw

We've figured out how to defend wireless access points, but clients remain exposed. A look at new attacks against clients using old methods we'd all forgotten about and new methods leveraging Metasploit. This talk will include pre-owning clients before vpn authentication, new ways of using gifars, crossdomain.xml attacks and more.

0-KNOWLEDGE FUZZING
Vincenzo Iozzo

Nowadays fuzzing is a pretty common technique used both by attackers and software developers. Currently known techniques usually involve knowing the protocol/format that needs to be fuzzed and having a basic understanding of how the user input is processed inside the binary.

In the past since fuzzing was little-used obtaining good results with a small amount of effort was possible. Today finding bugs requires digging a lot inside the code and the user-input as common vulnerabilities are already identified and fixed by developers.

This talk will present an idea on how to effectively fuzz with no knowledge of the user-input and the binary. Specifically the talk will demonstrate how techniques like code coverage, data tainting and in-memory fuzzing allow to build a smart fuzzer with no need to instrument it.

HACKING ORACLE 11G
David Litchfield

Sometimes you need to choose your exploits precisely and be careful about the packets you write to the wire. Sometimes you just want to type a command, go get some coffee, and come back to a pile of shells. This talk will cover the means that the Metasploit Framework provides for accomplishing both of these goals, including many advancements from my talk at Black Hat USA in the realm of client-side exploitation.

PHYSICAL SECURITY IN A NETWORKED WORLD: VIDEO ANALYTICS, VIDEO SURVEILLANCE, AND YOU
Joshua Marpet

Video Analytics is a component of many advanced video surveillance systems. It includes such well known features as License Plate Recognition and Facial Recognition. Does it actually work? How well does it work? How can you hack it? How can you access it?

Video surveillance is becoming more and more prevalent in our world, with some estimates showing that walking down Bourbon Street in New Orleans gets you photographed or videoed 3 times for every step you take. Are these systems legal? Who can see that video, or publish it? Is there a way to take advantage of the huge amount of video cameras? You'll find out.

HACKING RUSSIA: INSIDE AN UNPRECEDENTED PROSECUTION OF ORGANIZED CYBERCRIME
Joseph Menn

Almost all of the talk from Western law enforcement agencies of signs of cooperation by Russian authorities in the pursuit of master cybercriminals is an expression of hope, not experience. There is one major documented exception: the 2006 prosecution, conviction and imprisonment of three members of a criminal ring that organized and carried out dozens of denial-of-service attacks on business websites worldwide as part of an extensive extortion racket. Why that case succeeded where all others failed--and why its success has never been replicated, has never been explained. Based on years of research including the only interviews with Russian authorities and the British police detective sent to work with the MVD, author and Financial Times correspondent Joseph Menn gives the highlights of the account in his just-published book, FATAL SYSTEM ERROR: The Hunt for the New Crime Lords Who Are Bringing Down the Internet.

METASPLOIT AND MONEY
HD Moore

In 2008 Metasploit expanded from a community-run project to a corporate product managed by Rapid7. This talk focuses on the transition, the lessons learned during the acquisition process, the challenges of maintaining a community, and the latest improvements to the Metasploit Framework. The points covered in this talk are valuable for anyone building an open-source product, contemplating the purchase of one, or considering using an open source product to build a commercial application.

PLAYING IN A SATELLITE ENVIRONMENT 1.2
Leonardo Nve

This presentation is a warning call to those responsible for the companies that use or provide data connection (especially the Internet) via satellite, proving some of the attacks that are possible in this environment.

THE FOUR TYPES OF LOCK
Deviant Ollam

Physical security is an oft-overlooked component of data and system security in the technology world. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a console keyboard or, worse yet, march your hardware right out the door. While numerous ratings and standards exist in order classify specific security hardware, many of these standards are ill-defined and poorly-understood. Do you know what makes a "hardened" or "contractor grade" lock special? What does the phrase "high security" signify on hardware packaging? As it turns out, many of these terms are just for show... but Deviant will walk you step-by-step through some distinct and easy-to-follow examples of how low-grade locks can fail as well as how to clearly identify quality equipment. Additionally, we will cover the more difficult matter of hardware purchase decisions at the highest levels... fine distinctions such as which locks belong on the CEO's office versus which ones to use on your server rooms. Every situation calls for something a bit different, and those differences add up when you're spending $100 or more per lock. Make your money count and keep your budget, and your data, secure.

GLOBAL SECURITY REPORT 2010
Nicholas J. Percoco

From January 1, 2009 to December 31, 2009, we performed approximately 2000* penetration tests (network, application, wireless, and physical) for organizations ranging from the largest companies on the planet to nimble start-ups. In addition, we also performed around 200* security incident and compromise investigations

CONTINUED »

for organizations located in nearly 20 different countries around the world.

The data we have gathered from these engagements is substantial and comprehensive. This presentation will be the first viewing of the results of the analysis of the data gathered during 2009.

The results will be presented both technical and business impact analysis with an emphasis on technical for the Black Hat audience.

This presentation will coincide with the release of the paper with the same title. The paper will be released after the conclusion of the talk.

** Trending numbers as of November 5, 2009.*

CYBER EFFECTS PREDICTION

Shane Powell

Once the sole domain of military planners, public sector organizations must begin to understand the extent to which cyber attacks may affect their ability to conduct mission essential operations. Various information security regulations and standards aid organizations with configuring information systems securely. Common processes are used to assess system vulnerabilities and assign risk. However, vulnerability and risk assessments can easily mislead system owners into a false sense of security. While vulnerabilities can be patched and risks may be mitigated, the end result is inevitable that someone must accept responsibility should their organization fall prey to cyber attack through exposures that remain.

The approach to Cyber Effects Prediction proposed in this paper harnesses traditional and emerging analytic methods to provide a deep understanding of the actual security state of an organization's information system. Cyber Effects Prediction harnesses detailed knowledge of how an organization's information systems are configured, business operations, continuity of operations planning, and external relationships. Determination can be made from this information of how information systems will likely be attacked, allowing for prediction of the cascading effects that result from successful cyber attack.

MALWARE ANALYSIS FOR THE ENTERPRISE

Jason Ross

Your organization has Anti-Virus deployed and is logging virus activity to a central location. Your IDS is watching the perimeter, and you have your systems on a regular patch cycle. Malware doesn't affect you, right? Wrong.

This presentation shows where these technologies are falling short and why malware analysis is quickly becoming a need for companies other than Anti Virus vendors. We'll discuss the pros and cons to virtual machines and bare metal as they apply to the purpose of analyzing malicious software.

After talking about the "why," we'll move on to the "how" and walk through setting up a sandnet, or "virtual internet", comprised of a victim host and a server running multiple services so that you can observe Operating System changes made by malware, capture network traffic being sent by the compromised host, intercept DNS calls and redirect them to services you control, and set up netcat to interact with unknown protocols.

Using these methods, an organization can determine exactly what has been compromised on a host, and more importantly, determine where their data is going.

Armed with accurate information as a result of analyzing the malware an effective response to the incident can be formed.

IPHONE PRIVACY

Nicolas Seriot

The iPhone business model relies on consumers' trust in a closed ecosystem.

According to Apple: "Applications on the device are sandboxed so they cannot access data stored by other applications. In addition, system files, resources, and the kernel are shielded from the user's application space."

This presentation will discuss iPhone privacy issues and challenge Apple's stance and assertions regarding iPhone security.

The presentation will also show how a rogue application can access substantial quantities of personal data on an unmodified device and expose how it could go unnoticed in spite of AppStore tight reviews.

WHY BLACK HATS ALWAYS WIN

Val Smith & Chris

From the origins of hacking and black hat hackers a new industry called penetration testing has evolved. Penetration testing is intended to emulate a real attacker in order to uncover what vulnerabilities an organization may have that could put them at risk so they can be fixed. This has led to the term "White Hat Hacker" being used to describe those who perform these tests. However the goals of a White Hat differ greatly from the goals of a Black Hat, as do the mindsets. This presentation will describe these differences as well as some of the things black hats have to consider that white hats may not even be aware of. This paper will explain why black hats have the advantage over white hats and why the penetration industry has to change. The take away from this presentation is that current common penetration methodologies are ineffective in demonstrating the actual risk and threats that exist and hopefully provide some insight into how real attacks actually work from the point of view of a black hat.

THE UNDERGROUND ECONOMY OF THE PAY-PER-INSTALL (PPI) BUSINESS

Kevin Stevens

This presentation shows how hackers are recruiting hundreds of affiliates to join their Pay Per Install Affiliate Programs. While purporting to be programs that merely install adware, they are actually scams to install some of the most malicious malware and spyware out on the market today.

I will present different PPI programs as well as the forums where there are guides posted and tips on how to be successful in this business. I will also uncover some of the details of the people running these sites and some stats on how much money is being made.

ADVANCED MAC OSX PHYSICAL MEMORY ANALYSIS

Matthieu Suiche

In 2008 and 2009, companies and governments interests for Microsoft Windows physical memory growed significantly. Now it is time to talk about Mac OS X. This talk will describe basis of Mac OS X Kernel Internals (and not a XNU kernel creation timeline) and how to retrieve various information like machine information, mounted file systems, processes listing and extraction and threads, kernel extensions listing and extraction and Rootkit detection.

AGILE SECURITY; OR, HOW TO DEFEND APPLICATIONS WITH FIVE-DAY-LONG RELEASE CYCLES

Bryan Sullivan

Some security experts would have you believe that it is "impossible" to implement secure development practices in organizations using Agile development methodologies. Admittedly, the use of Agile does pose some challenges to traditional Security Development Lifecycle (SDL) processes—challenges such as meteorically short release cycles, infinitely long product lifetimes (as in the case of cloud applications), and a general You-Ain't-Gonna-Need-It aversion to planning mentality. However, despite these challenges, securing Agile projects is not impossible. SDL and Agile can be made to work well together, and in many ways they can actually work better together than they can separately.

This session will detail the process changes that the Microsoft SDL team has made to improve the applicability of the SDL to Agile development methodologies. We will discuss key challenges faced in adapting secure development practices to Agile and how they were overcome, and we will discuss inherent strengths of Agile that work exceptionally well with the SDL and can potentially lead to a best-of-both-worlds scenario.

HACKING THE SMARTCARD CHIP

Christopher Tarnovsky

From start to finish, we will walk through how a current generation smartcard was successfully compromised. The talk will discuss everything that was required in the order the events took place. We will cram several months into an hour!

PS- The talk will be very technical mixed hardware and software (60% hardware, 40% software).

MS OFFICE DOCUMENT WAR: PARSE DEEPLY, FUZZ WIDELY, SHOOT PRECISELY AND MEASURED SCIENTIFICALLY

Qing Wang

The concepts of "Sample based," "Logic oriented" and "Data type oriented" will bring us a lot of benefits if we use them in our security testing (fuzzing). Besides reducing thousands of useless cases with smart, accurate and efficient case generation strategies, they will also offer us a scientific measurement to evaluate our testing work. To demonstrate these concepts, a fuzzer with advanced fuzzing concepts, called Megatron (Yes, it is the name in the movie transformer A.K NBE1), will be shown up. Microsoft office document will be also used as a file format example to illustrate the file fuzzing concept.

With the tool we will release on the conference, you can generate malformed office documents smartly and easily. Programming is not necessary at all for it. Smart fuzzing won't be the special skill which is only owned by security expert. The ease of use and the intelligence are the key points for the design of Megatron. All the QA engineers, even the middle school students, could generate complex fuzzing cases and crash the application if they have this tool.

premier sponsors

PLATINUM SPONSORS

Novell

Palantir Technologies

GOLD SPONSORS

ArcSight

Microsoft

Rsignia The X Factor in Cyber Warfare

Berico Technologies Be Smarter. Be Faster.

netForensics

SAINT

CORE Security Technologies

NETWITNESS

SecureWorks

FORTIFY Software

nitrosecurity

SOLERA Networks

HARRIS

Pico tiny mighty machines

splunk>

intel

SRA International, Inc.

IOActive Comprehensive Computer Security Services

QUALYS

JOHNS HOPKINS UNIVERSITY

RedSeal

StillSecure

loglogic

BlackBerry

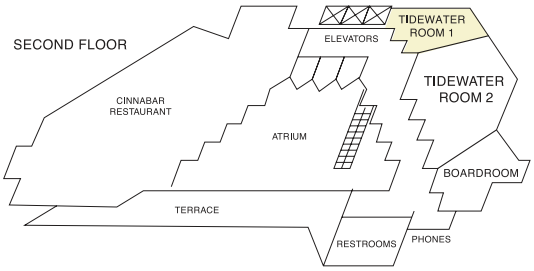
TippingPoint a division of 3Com

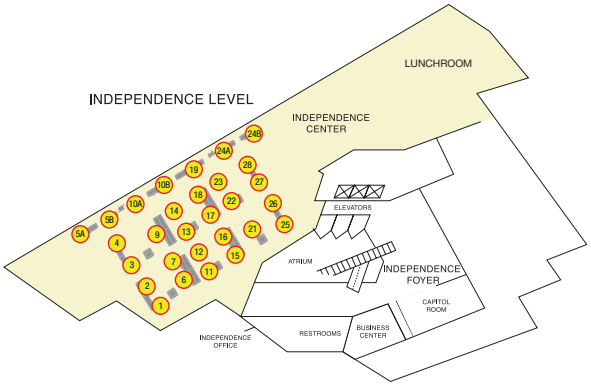
Lookingglass

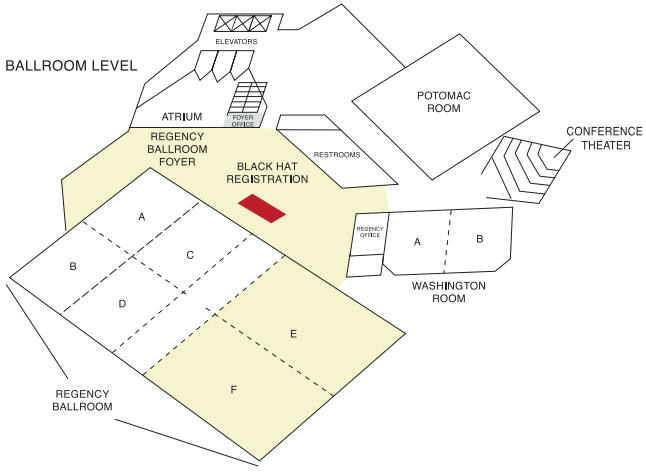
rovi

Trustwave Information Security & Compliance

briefings floorplan







DAY 1 & 2

PRESS ROOM	Second Floor, Tidewater 1
LUNCH	Independence Level, Independence Center

DAY 1 ONLY

APPLICATION SECURITY	Regency Ballroom C+D
THE BIG PICTURE	Regency Ballroom E
HARDWARE KEYNOTE	Regency Ballroom F
RECEPTION	Independence Level, Independence Center
SPONSORS	Independence Level, Independence Center
BREAKFAST	Independence Level, Independence Center
COFFEE SERVICE	Independence Level, Independence Center

DAY 2 ONLY

APPLICATION SECURITY	Regency Ballroom C+D
FORENSICS AND PRIVACY	Regency Ballroom E
METASPLOIT	Regency Ballroom F
BREAKFAST	Ballroom Level, Regency Foyer E+F
COFFEE SERVICE	Ballroom Level, Regency Foyer E+F

SPONSOR TABLE LOCATIONS

1	Johns Hopkins
2	Core
3	Berico
4	Rovi
5A	SRA
5B	Intel
6	Splunk
7	SecureWorks
9	Palantir Technologies
10A	Rsignia
10B	ArcSight
11	Qualys
12	Lookingglass
13	Trustwave
14	Harris
15	IO Active
16	RedSeal
17	StillSecure
18	LogLogic
19	Microsoft
21	Novell
22	Saint
23	Fortify
24A	Solera
24B	TippingPoint
25	NetWitness
26	NitroSecurity
27	NetForensics
28	Pico Computing

black hat world tour 2010

black hat DIGITAL SELF DEFENSE europe+2010

briefings & training: **europe**

HOTEL REY JUAN CARLOS BARCELONA, SPAIN

Apr 12 - 15, 2010

black hat DIGITAL SELF DEFENSE abu dhabi+2010

briefings & training: **abu dhabi**

UNITED ARAB EMIRATES

May 30 - Jun 2, 2010

black hat DIGITAL SELF DEFENSE usa+2010

briefings & training: **las vegas**

CAESARS PALACE LAS VEGAS, NEVADA

July 24 - 29, 2010

black hat dc+2011

HYATT REGENCY CRYSTAL CITY

Jan 16 - Jan 19, 2011

UPCOMING EVENTS //

www.**blackhat**.com

stay connected

RSS:
blackhat.com/BlackHatRSS.xml

TWITTER:
@BlackHatEvents *(real time event updates)*
@BlackHatHQ *(the staff at Black Hat)*

FACEBOOK:
facebook.com/blackhat

LINKED.IN:
search groups, Black Hat

speakers

Chema Alonso is a Computer Engineer by the Rey Juan Carlos University and System Engineer by the Politecnica University of Madrid, working as security consultant last six years, awarded as Microsoft Most Valuable Professional.

Jorge Luis Alvarez Medina is a Computer Engineer experienced in hardware and software development and security assessment (network and web applications penetration testing) and development.

Colin Ames is a security researcher with Attack Research LLC where he consults for both the private and public sectors. He's currently focused on Pen testing, Exploit Development, Reverse Engineering, and Malware Analysis.

Mike Bailey is a Senior Security Researcher and penetration tester with Foreground Security. His exploits are many, but rarely discussed. Generally, that's the way he likes it. He has been described as "a good guy, with an evil mind."

bannedit or David D. Rude II, is a security engineer with Affiliated Computer Services Inc. (ACS Inc.) where he conducts penetration tests for governments and various business clients.

Dionysus Blazakis has been breaking software since 1994, playing with debug.com and Ralf Brown's Interrupt List. Now he is a software developer, writing code for embedded devices for the last 8 years.

Bill Blunden (MCSE, MCITP:Enterprise Administrator) began his journey into enterprise computing over ten years ago at an insurance company in Cleveland, Ohio. Gradually forging a westward path to Northern California.

Elie Bursztein is a post-doctoral researcher at the Stanford Computer Security Lab. He holds a PhD in computer science and an Engineering degree in computer systems, networks and security. His research focus is network and web security, game theory and artificial intelligence.

Ben Butler: As the Director of Network Abuse for GoDaddy.com Ben Butler has, in this capacity, become an expert in spam, phishing, hacking, copyright violation, child exploitation issues, and related network security problems.

David Byrne is a Senior Security Consultant within the Application Security practice at Trustwave's SpiderLabs. SpiderLabs is the advanced security team responsible for Penetration Testing, Application Security, and Incident Response for Trustwave's clients.

Chris is is a Security Consultant and Researcher with Secure DNA. Chris specializes in web based application development security.

Richard Cox joined Spamhaus in 2003 after working for a number of UK Telcos and ISPs in the "compliance" sector, and has been CIO of Spamhaus since May 2005.

Tom Cross is the manager of IBM Internet Security System's X-Force Advanced Research team. Tom's team is engaged in a daily effort to identify, analyze, and mitigate computer security vulnerabilities.

Andrew Fried is currently a security researcher with Internet Systems Consortium (ISC), a nonprofit 501(c)(3) public benefit corporation dedicated to supporting the Internet community with software and professional services essential to its infrastructure.

Joe Grand is an electrical engineer, hardware hacker, and president of Grand Idea Studio, Inc. (www.grandideastudio.com), where he specializes in the invention, design, and licensing of consumer products and modules for electronics hobbyists.

Vincenzo Iozzo is a student at the Politecnico di Milano where he does some research regarding malware and IDS. He is involved in a number of open source projects, including FreeBSD due to Google Summer of Code. He works as a reverse engineer for Zynamics GmbH.

Christian Kendi will soon graduate from the Technical University of Munich (TUM) and the Universidad Politécnica de Madrid (UPM). He has been working as a security consultant for 11 years and is currently CEO of Iron Software.

David Kerb has worked in the computer security arena for the past ten years. He has specialized in reverse engineering, malware research, and penetration testing.

Mike Kershaw is the author of Kismet and several articles on wireless security. Mike also works for Aruba Networks, where his full-time job is to break things and pick up the pieces.

David Litchfield is the founder and chief research scientist of NGSSoftware Ltd., a UK-based security solutions provider. He has been recognized as the world's premier expert on Oracle database security, and is the designer of NGSSQuirreL.

Moxie Marlinspike does research with the Institute For Disruptive Studies and holds a 50 Ton Master Mariner's license.

Joshua Marpet is an ex-cop from Louisiana, an ex-volunteer fireman from New Jersey, Joshua Marpet has had every Career he dreamed of in childhood, except astronaut, and is now a Physical-and Information-Security analyst.

Joseph Menn is the author of "Fatal System Error," for *Financial Times,* and has reported on security and other technology issues for more than a decade at *Financial Times* and the *Los Angeles Times.*

HD Moore is Chief Security Officer at Rapid7 and Chief Architect of Metasploit, the leading open-source penetration testing platform, founded the Metasploit Project in 2003.

Leonardo Nve is a senior security auditor, involved in computer security since 1996, working as consultant auditor and from 2000, 2002 managed several research on various security technologies such as DOCSIS and Wireless.

Deviant Ollam: While paying the bills as a security auditor and penetration testing consultant, Deviant Ollam's first and strongest love has always been teaching. A member of the Board of Directors of the US division of TOOOL (The Open Organization of Lockpickers).

Jose Palazon (palako) is globally responsible for mobile security at Yahoo!. With more than 9 years experience in security auditing, consulting and trainning for the public, private and academic sectors.

Nicholas J. Percoco is Senior VP of SpiderLabs at Trustwave. He has more than 14 years of information security experience. In his role at Trustwave, he leads SpiderLabs, the team that has performed more than 500 computer incident response and forensic investigations globally.

Jean-Michel Picod is currently working for EADS Defence & Security and has an engineering degree in computer systems, networks and security. Over the past years he has been more focused on windows systems and their security.

Shane Powell is the Principle Systems Security Engineer, Raytheon – Network Centric Systems. As an Information Systems Security Engineer he specializes in detailed vulnerability assessment and post intrusion analysis.

Jason Ross has been performing application, host, and network based attack and penetration testing for 6 years, and has more than 10 years experience hardening systems and IP networks.

Nicolas Seriot has been an enthusiastic Mac user since 1986. He recently worked as a software engineer at Sen:te, Lausanne, Switzerland, where he created Cocoa applications, taught iPhone classes, wrote set-top-box embedded applications and custom web applications.

Val Smith has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on a variety of problems in the security community.

Kevin Stevens is a Threat Intelligence Analyst with the SecureWorks Counter Threat Unit. He has four years of experience in the security field and almost 10 years of experience in IT. Kevin has worked for such companies as Data General, EMC, and CNN.

Matthieu Suiche is security researcher who focus on reverse code engineering and volatile memory forensics. Matthieu actually works for the Netherlands Forensic Institute in The Hague.

Rohini Sulatycki is a Security Consultant within the Application Security practice at Trustwave's SpiderLabs. SpiderLabs is the advanced security team responsible for Penetration Testing, Application Security, and Incident Response testing for Trustwave's clients.

Bryan Sullivan is a Security Program Manager on the Security Development Lifecycle (SDL) team at Microsoft. He is a frequent speaker at industry events, including Black Hat, BlueHat, and RSA Conference. Bryan is also a published author on web application security topics.

Christopher Tarnovsky runs Flylogic Engineering, LLC and specializes in analysis of semiconductors from a security "how strong is it really" standpoint. Flylogic offers detailed reports on substrate attacks which define if a problem exists.

Qing Wang is a security engineer from Product Security team in Symantec. The daily work of this team includes identifying and responding reported vulnerability, penetration testing and security coding/testing training inside of Symantec.