Stay Ahead

Technology moves at the speed of light in the world of cyber security attacks and defenses. Black Hat DC will once again gather the world's information and computer security elite to share their knowledge and experience with you.

Two days. Ten Classes. Thirty presentations.

Black Hat®

Briefings & Training DC 2007

February 27-March 1 • Sheraton Crystal City

www.blackhat.com

sponsors

diamond

Microsoft®

platinum

BAE SYSTEMS

QUALYS® On Demand Security

gold

BlackBerry

FORCE10

ARBOR NETWORKS

CORE

ArcSight

NORMAN®

IOActive

Training

Hacking by Numbers: Combat Training by SensePost

Hacking By Numbers Combat Edition is SensePost's flagship course. Combat is an unique new concept — a series of carefully crafted Capture-The-Flag 'missions', each designed to teach a specific hacking skill or concept. This course is all hack, no talk. Combat has been described as 'Zen' for hackers. This is an advanced level course.

Early: $2200 / Regular: $2400 / Late: $2500

Tactical VoIP: Applied VoIPhreaking by the Grugq

This course addresses exploiting VoIP—from end user devices through carrier grade servers—including protocol level attacks, application bugs and common dangerous deployment mistakes. The course provides deep coverage of a broad spectrum of VoIP relevant security threats.

Early: $1800 / Regular: $2000 / Late: $2100

Ultimate Hacking: Black Hat Edition by Foundstone

Ultimate Hacking: Black Hat Edition begins from a "zero-knowledge" perspective. Start by profiling your target, then learn how to identify and exploit well-known and obscure vulnerabilities in the most popular operating systems including Windows and multiple Unix flavors. Foundstone challenges you with countless hands-on exercises to demonstrate your expertise as you race other students to achieve the ultimate goal...getting root.

Early: $2000 / Regular: $2200 / Late: $2300

Analyzing Software for Security Vulnerabilities by Halvar Flake

This is an intense course encompassing binary analysis, reverse engineering and bug finding. The C programming language gives the programmer a lot of rope to hang himself with - and C++ just adds to the featurelist. Both languages have an impressive number of subtle pitfalls, and many of these can be leveraged by a skilled attacker to execute code on a computer on which these vulnerable programs run. But while almost everybody seems to understand the significance of these programming mistakes, few actually sit down and analyze code from the security analysis perspective. This workshop focuses on teaching security-specific code-analysis, both in source and in binary form.

Early: $2000 / Regular: $2200 / Late: $2300

Reverse Engineering on Windows: Application in Malicious Code Analysis by Pedram Amini & Ero Carrera

This class is meant to impart cutting-edge understanding of malicious code analysis upon attendees, ultimately taking them to an advanced level of reverse engineering skills applicable to other security domains. As this course is focused on malicious code analysis, students will be given real-world virus samples to reverse engineer. The details of executable packing, obfuscation methods, anti-debugging and anti-disassembling will be revealed and re-enforced with hands-on exercises.

Early: $1800 / Regular: $2000 / Late: $2100

ROOTKIT: Advanced 2nd Generation Digital Weaponry by Greg Hoglund and Jamie Butler

Rootkits are the primary tool used by malware to hide on a computer system. Rootkits can also be used to tamper-proof your own software against attackers. Take the next step in rootkit technology. This new 2nd generation class teaches advanced techniques such as memory subversion, kernel mode process infection even of "hardened" processes, simple "shellcode" techniques, creating processes from Ring 0, subverting the Windows Object Manager, and kernel mode covert network channels.

Early: $1800 / Regular: $2000 / Late: $2100

Live Digital Investigation – Investigating the Enterprise by WetStone Technologies

Upon completion of this intense two-day course, forensic examiners, private investigators, digital auditors, corporate security personnel, federal, state and local Law enforcement investigators, prosecutors and corporate IT personnel will have a complete understanding of the latest methods and techniques for acquiring, analyzing and investigating "Live" running enterprise computers.

Early: $2000 / Regular: $2200 / Late: $2300

Hands-On Hardware Hacking and Reverse EngineeringTechniques: Black Hat Edition by Joe Grand

This course is the first of its kind. We focus entirely on hardware hacking. It's hands-on. Not only do we, as hackers, explore reverse engineering and hardware hacking techniques, we also look at defense mechanisms and technologies that we, as designers, can use to protect our products from attackers. We'll guide you through an introduction to reverse engineering, explore the basic electronics fundamentals and common test equipment, and then dive into the step-by-step processes of successful circuit modifications and hardware hacking.

Early: $2200 / Regular: $2400 / Late: $2500

NSA InfoSec Evaluation Methodology (IEM) - Level 2 by Security Horizon

This course presents the methodologies used by the National Security Agency when conducting information security evaluation on organizations. This is a tools-based course that walks students through the use of tools and manual processes designed to provide a baseline of activities for comprehensive security evaluations. This is the followup course to the IAM.

Early: $2000 / Regular: $2200 / Late: $2300

ISA Ninjitsu by Timothy Mullen and Jim Harrison

This action-packed, two-day immersion into ISA technologies not only gets "under-the-hood" of hot topics like client configuration, server publication, application filtering, advanced logging procedures and troubleshooting techniques, but will also reveal many powerful, real-world DMZ configurations and design concepts you can leverage to deploy deeply secure, robust firewall solutions.

Early: $2000 / Regular: $2200 / Late: $2300

Advanced Database Security Assessment by NGS Software

This course teaches how to recognize the insecurities present within common database systems and how these flaws can leave you wide open to attack. It is tailored to teach security consultants, database administrators and IT professionals how hackers discover and exploit vulnerabilities to gain access to your data and further penetrate internal networks. By learning these techniques, we can discover the flaws for ourselves and effectively develop strategies to keep attackers out.

Early: $2000 / Regular: $2200/ Late: $2300

Breakable: Secure Your Oracle Servers By Breaking Into Them by David Litchfield & Mark Litchfield

Never has the need for understanding Oracle database security been so great as it is today as the boundaries between networks become less defined and web applications provide direct inroads through any firewalls and into the backend. This course will teach you how to hack into Oracle database servers; only by truly grasping the mechanics of attacks can a complete and effective defense be built.

Early: $2000 / Regular: $2200 / Late: $2300

For more information and to register:
www.blackhat.com

Briefings

Firmware Rootkits and the Threat to the Enterprise

John Heasman

This presentation discusses the technical and operational difficulties that must be overcome in order to persist a rootkit onto a PCI device. A common assumption is that attacks against firmware are highly specific not only to every vendor but also down to specific models of hardware. This in turn suggests that a large scale automated deployment of firmware rootkits is difficult to accomplish even in homogeneous environments. This session analyzes the "security through diversity" assumption in detail.

Software Virtualization Based Rootkits

Sun Bing, Research Scientist, McAfee (China)

We will discuss the complete technical scheme of a novel VM Based Rootkit. The VMBR itself is sort of light weight VMM. After the VMBR is loaded, the VMBR will ensure the target system is still running by placing it into a rootkit created virtual execution environment. It then becomes very difficult for the victim to perceive the rootkits' presence or to find any virtualization footprint. Although this novel VMBR is just a proof of concept, it has at least achieved the coexisting transparently and perfectly with the target system.

RFID for Beginners

Chris Paget, Director of R & D, IOActive

RFID tags are becoming more and more prevalent. From access badges to implantable Verichips, RFID tags are finding more and more uses. Few people in the security world actually understand RFID though; the "radio" stuff gets in the way. This presentation aims to bridge that gap, by delivering sufficient information to design and build a working RFID cloner based around a single chip - the PIC16F628A. Assuming no initial knowledge of electronics, I'll explain everything you need to know in order to build a working cloner, understand how it works, and see exactly why RFID is so insecure and untrustworthy. Covering everything from Magnetic Fields to Manchester Encoding, this presentation is suitable for anyone who is considering implementing an RFID system, considering hacking an RFID system, or who just wants to know a little more about the inductively coupled, ASK modulated, back scattering system known as RFID.

Secure Processors for Embedded Applications

James D. Broesch

There are many aspects to security in computing environments. In this presentation we look at some of the options for incorporating security at the hardware level by using variety of secure processor options. Traditionally, developers have relied on FIPS compliant processors when looking to secure processors. While there are many advantages to the use of standard FIPS devices, it is also true that these devices are often relatively expensive and limited in their processing capability. This presentation will discuss how to achieve both a secure computing environment and high performance.

Agile Incident Response: Operating Through Ongoing Confrontation

Kevin Mandia, Founder, Mandiant

Many government agencies and organizations are the targets of ongoing efforts to infiltrate their networks and pilfer sensitive data. If an intruder is ever successful, dealing with the incident becomes a protracted effort that can seriously impact operations and unnerve leadership. This session will review techniques to handle ongoing incidents with agile, cost-effective and rapid countermeasures to best diminish the resource drain and psychological wariness that ensues when a network is compromised by a persistent threat.

Volatools: Integrating Volatile Memory Forensics into the Digital Investigation Process

AAron Walters, Senior Engineer, Komoku, Inc.
Nick L. Petroni, Jr.

In this presentation, we will demonstrate the integral role of volatile memory analysis in the digital investigation process and how that analysis can be used to help address many of the challenges facing the digital forensics community. As part of this presentation, we will discuss the shortcomings of the popular tools and techniques currently used for live response. We will also release and discuss Volatools, a set of tools that can be integrated into the digital investigation process. The presentation will demonstrate how investigators can leverage the context found using Volatools to focus investigations with large volumes of evidence. Finally, for the technical audience, we will demonstrate the extraction of cryptographic key material from a volatile memory image that can then be used to access encrypted file systems without knowledge of the password.

Beyond The CPU: Defeating Hardware Based RAM Acquisition Tools (part I: AMD case)

Joanna Rutkowska

Many people believe that using a hardware based acquisition method, like e.g. a PCI card or a FireWire bus, is the most reliable and secure way to obtain the image of the volatile memory (RAM) for forensic purposes. This presentation is aimed at changing this belief by demonstrating how to cheat such hardware based solutions, so that the image obtained using e.g. a FireWire connection can be made different from the real contents of the physical memory as seen by the CPU. The attack does not require system reboot. The presented technique has been designed and implement to work against AMD64 based systems, but it does not rely on hardware virtualization extensions.

Web Application Incident Response and Forensics—A Whole New Ball Game!

Chuck Willis, Principal Consultant, MANDIANT

Web applications are normally the most exposed and the most easily compromised part of an organization's network presence. This combination requires that organizations be prepared for web application compromises and have an efficient plan for dealing with them. Unfortunately, traditional techniques for forensics and incident response do not take into account the unique requirements of web applications. The multi-level architecture, business criticality, reliance on major database and middleware software components, and custom nature of web applications all create unique challenges for the security professional. Responding to a web application attack brings many unique issues, often with no clear right and wrong answers, but this talk will provide useful information to guide attendees down this bumpy path.

Botnet Tracking: Tools, Techniques, and Lessons Learned

Dr. Jose Nazario, Senior Security Engineer, Arbor Networks' Arbor Security Engineering & Response Team (ASERT)

In this session Dr. Jose Nazario, author and security researcher, will discuss his research on botnet attacks and the increase of attacks made on government agencies and corporate America. Attendees will learn how botnet attacks have increased in frequency and malice through various forms such as DDoS attacks, new malware outbreaks, and high volume scanning and exploit activity. Attendees will also be supplied with a complete picture of the threats posed by botnets. They will learn how through actively monitoring a large number of botnets specialized tools and techniques have been developed to infiltrate a large number of botnets for long periods of time.

GS and ASLR in Windows Vista

Ollie Whitehouse

The following presentation is two parts, the first covers aspects of Microsoft's GS implementation and usage. The second is a complementary section dealing with ASLR in Windows Vista, its implementation and some surprising results...

360° Anomaly Based Unsupervised Intrusion Detection

Stefano Zanero, CTO, Secure Network

In this talk, after briefly reviewing why we should build a good anomaly-based intrusion detection system, we will briefly present two IDS prototypes developed at the Politecnico di Milano for network and host based intrusion detection through unsupervised algorithms.

We will then use them as a case study for presenting the difficulties in integrating anomaly based IDS systems (as if integrating usual misuse based IDS system was not complex enough...).

We will then present our ideas, based on fuzzy aggregation and causality analysis, for extracting meaningful attack scenarios from alert streams, building the core of the first 360° anomaly based IDS.

Data Seepage: How to Give Attackers a Roadmap to Your Network

David Maynor
Robert Graham, co-founder & CEO, Errata Security

Long gone are the days of widespread internet attacks. What's more popular now are more directed or targeted attacks using a variety of different methods. Since most of these attacks will be a single shot styled attack attackers will often look for anyway to increase the likelihood of success.

This is where data seepage comes in. Unbeknownst to a lot of mobile professional's laptops, pdas, even cell phones can be literally bleeding information about a company's internal network. This can be due to applications like email clients that are set to start up and automatically search for its mail server, windows may be attempting to remap network drives, an application could be checking for updates.

All this information can be used by an attacker to make attacks more accurate with a higher likelihood of success.

Danger From Below—The Untold Tale of Database Communication Protocol Vulnerabilities

Amichai Shulman, co-founder and CTO , Imperva

This presentation delves into the background of database communication protocol development and testing and explains how these vulnerabilities continue to proliferate. I will highlight some interesting information from our extensive research and testing and demonstrate examples of attacks and describe mitigation techniques.

Smashing Web Apps: Applying Fuzzing to Web Applications and Web Services

Michael Sutton, Security Evangelist, SPI Dynamics,

Fuzzing is not a new technique for vulnerability discovery yet it has been a highly successful black box testing technique arguably responsible for the majority of vulnerabilities that we see today. While fuzzing tools for network vulnerabilities have been around for some time, similar tools for web applications and web services are still in their infancy. In many ways, web applications are better suited for fuzzing. Web apps freely reveal information about expected user inputs, making the generation of (in)appropriate test cases far more streamlined, while web services go one step further by openly providing a structured blueprint for the data that is expected.

In this talk we will contrast fuzzing at the network and application layers. We will address some of the unique challenges faced when fuzzing web applications such as automating the identification of data structures and handling exception detection. Fuzzing will be broken into different categories including headers, methods, web services and AJAX. Included throughout, we will reveal open source applications that have been developed to automate the methodologies behind fuzzing web applications and services.

NAC

Ofir Arkin, CTO, Insightix

The threat of viruses, worms, information theft and lack of control of the IT infrastructure lead companies to implement security solutions to control the access to their internal IT networks.

A new breed of software (Sygate, Microsoft, etc.) and hardware (Cisco, Vernier Networks, etc.) solutions from a variety of vendors has emerged recently. All are tasked with one goal—controlling the access to a network using different methods and solutions.

This presentation (updated with new material) will examine the different strategies used to provide with network access controls.

Flaws associated with each and every NAC solution presented would be presented. These flaws allows the complete bypass of each and every network access control mechanism currently offered on the market.

Being Explicit about Software Weaknesses

Robert A. Martin, Principal Engineer, MITRE

The secure software development community is developing a standard dictionary of the weaknesses that lead to exploitable software vulnerabilities. The Common Weakness Enumeration (CWE) and related efforts are intended to serve as a unifying language of discourse and act as a measuring stick for comparing the tools and services that analyze software for security issues. Without a common, high-fidelity description of these weaknesses, efforts to address vulnerabilities will be piecemeal at best, only solving part of the problem. Various efforts at DHS, DoD, NIST, NSA, and in industry cannot move forward in a meaningful fashion or with any hope of their efforts being aligned and integrated with each other so we can protect our networked systems starting with the source - the software development lifecycle. While the current driver for CWE is in code assessment tool analysis, we believe that CWE and its related efforts could a have broader impact.

Attack Patterns: Knowing Your Enemies in Order to Defeat Them

sbarnum

This session will present the concept and construct of attack patterns including their background, structure and content, how they are generated, how they can be leveraged across the SDLC (Policy, Requirements, Arch & Design, Implementation, Test, etc.) and current efforts to collect, classify and make them an available and valuable tool for the software development community.

This session will be a more detailed and updated covering of the material included in the series of attack pattern articles published on the DHS Build Security In website with the addition of discussion of the Common Attack Pattern Enumeration and Classification (CAPEC) effort currently underway and funded by the Department of Homeland Security. It doesn't make much sense to cut and paste a 70 page whitepaper here so I figured I would give you a reference to go check it out.

This material closely aligns with the session proposed by Robert Martin of Mitre covering the Common Weakness Enumeration (CWE). It would make sense to have this session directly follow the CWE session if possible.

Reversing C++

Paul Vincent Sabanal, Researcher, IBM Internet Security

Mark Vincent Yason

As recent as a couple of years ago, reverse engineers can get by with just knowledge of C and assembly to reverse most applications. Now, due to the increasing use of C++ in malware as well as most moderns applications being written in C++, understanding the disassembly of C++ object oriented code is a must.

This talk will attempt to fill that gap by discussing methods of manually identifying C++ concepts in the disassembly, how to automate the analysis, and tools we developed to enhance the disassembly based on the analysis done.

Practical 10 Minutes Security Audit–The Oracle Case

Cesar Cerrudo, Founder, Argeniss

This paper will show a extremely simple technique to quickly audit a software product in order to infer how trustable and secure it is. I will show you step by step how to identify half dozen of local oday vulnerabilities in few minutes just making a couple of clicks on very easy to use free tools, then for the technical guys enjoyment the vulnerabilities will be easily pointed out on disassembled code and detailed, finally a oday exploit for one of the vulnerabilities will be demonstrated and explained.

While this technique can be applied to any software in this case I will take a look at the latest version of Oracle Database Server: 10gR2 for Windows, which is a extremely secure product so it will be a very difficult challenge to find vulnerabilities since Oracle is using advanced next generation tools to identify and fix vulnerabilities.

Practical Malware Analysis: Fundamental Techniques and a New Method for Malware Discovery

Kris Kendall, MANDIANT

Chad McMillan, Principal Security Engineer within the Federal Services Division of MANDIANT

IT environments are under constant assault by malicious software. Protection and detection systems are increasingly ineffective in dealing with this threat. Modern Incident Responders need to be able to identify and analyze malicious code in order to implement protections in their environments. This session will review analysis fundamentals for malware on Windows platforms.

This session will also include a discussion of a new technique developed by Mandiant for identifying suspicious data on a compromised system based on characteristics of modern malware armoring methods.

Exploting Similarity Between Variants to Defeat Malware

Andrew Walenstein, Research Scientist, Center for Advanced Computer Studies at the University of Louisiana at Lafayette

Most malicious programs that are seen by anti-malware companies are minor variations of some previously released version. This reuse of prior programs should be exploitable in defense. However, in order to do so, one must have an efficient and effective way of comparing new programs against a database of previously-seen versions. We present a method for measuring the similarity of malicious programs, which allows search against a database. It is adapted from text-based search, and uses scaled vectors of code feature frequencies. The method involves first disassembling the programs and then extracting features called n-grams and n-perms from the disassembled text. These features are then counted, and their histograms are scaled and then compared as vectors according to their cosine angle. The scaling is based on the frequency of the features within the database, with common features weighted less heavily. A small study illustrates that the approach is feasible at industrial scales (a database of tens of thousands of samples). False positive rates are also shown to be acceptable for anti-malware analysis. The potential impacts on malware analysis and automated detection are discussed.

Diamond Sponsor

Microsoft

Microsoft is proud to be a continuing sponsor of the Black Hat Security conference. We appreciate Black Hat providing a unique forum in which security researchers from all over the world, IT Pros and industry luminaries can gather to share insights, knowledge and information to advance security research. Microsoft remains dedicated to software security and privacy and continues to collaborate with the community of people and technology organizations helping to protect customers and the broader ecosystem, Microsoft is also dedicated to software security and privacy. Since the onset of Trustworthy Computing we have fostered a culture of security within Microsoft that includes developing secure code, building strong relationships with industry researchers and partners, and providing guidance to help protect customers. We would like to thank all of the customers, partners and security researchers who have worked with us to advance the state of the art in security science. Only by working together with partners, researchers and the community can we all ensure the advancement and success of the technology industry. www.microsoft.com/security

Microsoft

Platinum Sponsors

BAE Systems

BAE Systems Advanced Information Technologies develops advanced technologies and software solutions that enable individuals and organizations to make and execute better decisions faster—particularly in real-time, data-intensive environments. Our solutions provide integrated, high performance capabilities for the entire information chain, from raw sensor management to strategy formulation, planning and execution. Advanced Information Technologies staff work at the cutting edge of technology to develop, transition and exploit breakthroughs and innovations in information assurance & security, networking & communications and a broad range of other disciplines. www.baesystems.com

BAE SYSTEMS

Qualys

Qualys, Inc., the leader in on demand vulnerability management and policy compliance serves more than 2,200 enterprise subscribers around the world including 200 of the Forbes Global 2000. QualysGuard Software as a Service (SaaS) solutions help security managers effectively strengthen the security of their networks, conduct automated security audits and ensure compliance with internal policies and external regulations. Qualys' cost effective on demand technology requires no capital outlay, infrastructure or maintenance and can be deployed in a matter of hours anywhere in the world. Qualys global customers include AXA, DuPont, eBay, ICI Ltd, Kaiser Permanente, Novartis, Oracle and many others. Qualys is headquartered in Redwood Shores, California, with business units in Europe and Asia. www.qualys.com.

QUALYS® On Demand Security

Gold Sponsors

Arbor Networks

Arbor Networks® solutions enable government agencies to secure and maintain the availability of critical data and information systems. Through network behavior analysis and anomaly detection, Arbor Peakflow delivers unmatched network-wide visibility and scalability to defend against a wide range of threats, including worms, data theft, DDoS attacks, botnets and more. The Peakflow platforms are complemented by our Arbor Security Engineering & Response Team (ASERT). What makes ASERT unique is the combination of sophisticated, automated data collection techniques with the technical and analytical expertise of our security researchers, enabling them to distill mountains of technical information into actionable business intelligence for network and security professionals. Arbor's industry-leading security services bring context to the content, helping government agencies solve real business problems. www.arbor.net

ARBOR NETWORKS

ArcSight

ArcSight, a leader in Network and Security Information Management delivers mission-critical solutions for security, network, and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today's complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, responding and managing security and network data, ArcSight solutions mitigate information risk for real-time threat management, fraud intelligence, compliance reporting and automated network response. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs. www.arcsight.com

ArcSight

Core Security Technologies

Since 1996, Core Security Technologies has been committed to delivering breakthrough software and services that address the information security (IS) needs of corporations and government organizations worldwide. Our customers seek to protect their information assets from unauthorized access while complying with industry and governmental regulations, both today and as their networks expand in the future. Our Flagship product CORE IMPACT is the first automated, comprehensive penetration testing product for assessing specific information security threats to an organization. By safely exploiting vulnerabilities in your network infrastructure, the product identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments. www.coresecurity.com

CORE SECURITY TECHNOLOGIES

Force10 Networks

Force10 Networks is the pioneer in high performance networking and security. Founded in 1999, Force10 revolutionized networking with the first product to deliver true line rate 10 Gigabit Ethernet. With the introduction of the P-Series security appliance, Force10 again leads the industry with true line rate Gigabit and 10 Gigabit intrusion detection, intrusion prevention, and firewall. The P-Series integrates the openness of Snort software with a custom massively parallel deep packet inspection engine built into FPGA. Force10 is a global company with offices throughout the US, as well as the UK, the Netherlands, Japan, China and Korea. www.force10networks.com

IOActive

Established in 1998, IOActive is a professional security consulting firm specializing in information risk management and application security analysis for global organizations and software development companies. To our credit, IOActive is one of three firms in the world that were tasked by Microsoft with the security code review of the Vista client operating system. Unlike commoditized network security services and off the shelf code scanning tools, IOActive performs gap analysis on information security policies and protocols, and conducts in-depth analysis of information systems, software architecture and source code using leading information risk management security frameworks and carefully focused threat models. As a home for highly skilled and experienced computer security professionals, IOActive has attracted the likes of Dan Kaminsky, Chris Paget, Dinis Cruz, Jason Larsen, Josh Schmidt, Theodore Ipsen, key advisors like Steve Wozniak, and a crew of unequivocally talented "white-hat" hackers who, before being asked to host the infamous Capture the Flag at Def Con, owned the competition three years in a row. www.ioactive.com

Norman

Norman is a world leading company in data security, Internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection. While focusing on its proactive antivirus technology, the company has formed alliances that enable Norman to offer a complete range of data security services. Norman was established in 1984 and is headquartered in Norway with offices throughout Europe and the United States. www.norman.com

Research In Motion

Research In Motion is the designer, manufacturer and marketer of BlackBerry®, the leading wireless solution for the worldwide mobile communications market. Through the development of integrated hardware, software and services that support multiple wireless network standards, the BlackBerry® Enterprise Solution provides seamless and secure access to time-sensitive information including email, phone, SMS messaging, Internet and intranet-based applications. Research In Motion is committed to independent, third party approvals and certifications of BlackBerry security. BlackBerry solutions have received more security accreditations globally than any other wireless solution. The BlackBerry solution is approved for storing and transmitting sensitive data by the North Atlantic Treaty Organization (NATO) as well as government organizations in the United States, Canada, the United Kingdom, Austria, Australia and New Zealand. www.blackberry.com/security

Media Partners

Cisco Press