

Plenary Keynote: "Web Services Depends on Interoperable Security Standards."

Dr. Nataraj Nagaratnam Chief Architect for Identity Management, IBM

The fundamental promise of Web demands predictable interoperability and security. This keynote would highlight the array of emerging Web services security standards (WS-Security), including those related to token types, headers, signatures and encryption. An overview of OASIS's in-progress security standards work will also be provided. In addition to the work of OASIS, the WS-I Basic Security Profile Working Group is tasked with producing Security Scenarios and a Basic Security Profile.

Keynote: "True Intrusion Prevention - Protecting Against Threats From All Vectors, At All Times."

Martin Roesch, CTO & Founder, SourceFire, Inc.

First generation Intrusion Prevention Systems (IPS) have failed to solve today's threat problem - breaches are occurring at an ever increasing rate, damaging organizations' reputations and costing revenue. Standalone IPS only protect against intrusions, coming from the perimeter, during the time of the attack. Today's blended threats require blended security systems that have more remediative options. Join Martin Roesch, founder of Sourcefire and creator of Snort, as he discusses how the combination of endpoint, threat and network intelligence provides true intrusion prevention by defending networks against threats from all vectors, all the time - before, during and after an attack.

Keynote: "Starting with Identity Management Systems for securing Web Services."

Mamoon Yunus, CTO & Founder, Forum Systems

Identity Management is the cornerstone of deploying secure Web Services. Application-to-Application & User-to-Application authentication and authorization are the primary steps in Web Services Threat Mitigation. Identity Management is also fundamental to Trust enablement of Web Services.

This session explores popular secure Web Services deployment scenarios through protocol-based (e.g., HTTP Basic Auth, SSL Mutual Auth) and message-based (e.g., WS-X509, SAML) identities. Practical Web Services Identity bridging, XML Threat Sensors, and Web Services Trust functions, such as WS-Signatures & WS-Encryption, are also presented as pillars of deploying comprehensive Web Services Security.

Topic: "McAfee NAC Solution: Gaining back your sanity and minimizing your Risk"

Andrew J. Berkuta, Senior Security Evangelist | Strategist McAfee, Inc.

You've already seen the CxO once this year...and for them it was enough! Why don't they understand that a good day in security is one where nothing happens? Now with the advent of zero day attacks, bots, and other ferocious types of malware, the industry is calling for end-point protection. What is it, and who is out there that can help me with a real flexible and scalable solution? Better yet, HOW can I go back to my CxO and ask for it THIS year?

Andrew J. Berkuta has been there. As a security director, as a "plank owner" for three startup companies, he understands that justifying another expenditure for security can be trying. He will talk about the latest trends in malicious events, the myth of ROI in security, and why a NEW paradigm is necessary to face the combative CxO, and still get what you need to security your enterprise!

Topic: "Security and Identity Issues in Cross-agency SOA."

Phil Walston, Layer 7 Technologies

Security and federation for SOA is a complex problem, and the standards are still evolving. This presentation takes a realistic look at what most services are being used for, and how to build secure, standards-compliant cross-agency solutions today.

Topic: "Web Services Security and BPM."

Phil Larson, Director of Product Strategy, Appian Corporation

The heavy adoption of service-oriented architecture (SOA) and Web services technology is driving demand for Business Process Management (BPM), and vice versa. However, legitimate security concerns arise when BPM is used to tie together disparate systems using Web services and make them accessible via a single application. Each web service may have its own security requirements reflecting the policies of the service provider. Moreover, the various "flavors" of Web service technology and the prevalence of poorly documented services makes implementing a holistic security paradigm more difficult.

BPM is empowering business users to be more responsible and involved in designing and managing their processes. However, most business users are unfamiliar with appropriate security measures to implement when designing application level security into the processes they are building. Conversely, BPM solutions that use Web services should carry over and enforce the same access privileges. This should be done in addition to standard organization security requirements, such as SSL encryption of network traffic, for effective authentication of users.

This session will feature Appian Corporation, the leading provider of human-centric business process management suites (BPMS) and will highlight the different security approaches organizations should look at when implementing BPM technology along with Web services. Appian's BPM suite solution is currently in use in tandem with Web services technology at leading Government agencies and commercial organizations.

Keynote: "Trusted Computing and its Impact on Web Services."

Steven Sprague, CEO, Wave Systems

Wave Systems has been involved in trustworthy computing since its inception in 1989. Wave has built a variety of security silicon implementations, with support infrastructure, which have been used in trusted computing in specific applications, and in 2003 was one of the first non-founding members of the Trusted Computing Group.

The Trusted Computing Group (TCG) is an industry organization formed in 2003, and currently is comprised of more than 100 companies representing security silicon manufacturers, platform OEMs, security middleware providers, and security application providers. The purpose of TCG is to develop, define, and promote open, vendor-neutral industry specifications for trusted computing. These include hardware building block and software interface specifications across multiple platforms and operating environments. Implementation of these specifications will help manage data and digital identities more securely, protecting them from external software attack and physical theft. TCG specifications can also provide capabilities that can be used for more secure remote access by the user and enable the user's system to be used as a security token.

At the core of TCG technology is a silicon security device, known as a Trusted Platform Module (TPM), which is embedded on the main processing board of a computing platform. The initial work on integrating TPM technology has focused on the PC, and workgroups are addressing incorporating TPM technology into PDAs, cellphones, servers, and trusted peripherals.

A TPM is a public key capable device which, when embedded in a environment to form a trusted platform, can be utilized by applications and infrastructure to:

- Store keys, digital certificates, passwords and data securely in hardware
- Enhance network security
- Protect online commerce transactions
- Help protect against viruses, worms and other malicious attacks
- Protect digital identities
- Provide authentication between systems and networks
- Allow for single sign-on to systems
- Enable digital signatures for financial and other transactions
- Support regulatory compliance for Sarbanes-Oxley, HIPAA and other federal requirements

The TPM is now shipping on millions of PC platforms driven by logo compliance for Windows Vista. The advent of industry standard security will change how the enterprise implements security. Strong multi-factor authentication and strong data protection is possible on every endpoint in the network.

Keynote: "Threat Protection in a Service Oriented World."

Andre Yee, President & CEO, NFR

It's increasingly becoming a service oriented world. The emergence of web services, service oriented architectures (SOA) and "software as a service" (SaaS) is rapidly changing the way software is designed, constructed, deployed and delivered. These exciting advances will also marginalize old security constructs and bring about new challenges in securing the enterprise. In discussing Threat Protection in a Service Oriented World, we will specifically look into the how the emergence of web services and SOA bring about exposure to new threats. This includes but not limited to the following:

- Real and potential attacks against web services based transactions.
- Problems with authenticating user identities in an SOA scheme
- Difficulty with authorization in a composite application service
- Challenge of end-to-end security across multiple traversal points.

We will discuss the nature of these threats and how to mitigate against them by effectively employing new emerging security standards, tools coupled with proven practices.

Keynote: "What are the realities of your legal risks?"

Melise R. Blakeslee, Partner, McDermott Will & Emery LLP

Court decisions, regulations and your company's own promises may be setting impossibly high standards for data, system and document security and management. This presentation will discuss:

- The surprising decisions from the courts
- The confusing regulatory environment
- The questions to ask about your company's obligations
- The sufficiency of technology solutions; and
- The most important steps you need to take to reduce the likelihood of legal liability.

Keynote: "eRisk and liability in Online Transactions – the impact of the Sarbanes-Oxley Act."

Ralph Bazilio, President, TCBA

In today's Internet Age, everyone must pay attention to the risks and liabilities in online transactions. For most, if not all of us, we are concerned not only as business professionals providing services to our client base but also as consumers ourselves. There are risks and liabilities to doing business online as they are with any type of business activity. There are also tremendous opportunities available to innovative businesses that understand the risks and take the appropriate measures to mitigate and reduce the risks and manage the potential for liability. The key is adequate planning and risk management.

To complicate matters even further, we have to be concerned with the relevant Federal Laws and Regulations such as the Sarbanes-Oxley Act of 2002. The Act has special significance related to erisk and liability in online transactions. The successful business executive in today's business environment must develop a plan to effectively manage these and other critical issues that impact our activities.

We will examine some of the most critical erisks and liabilities in online transactions in light of the Sarbanes-Oxley Act of 2002. We will also discuss and exchange ideas on how you can develop and implement a comprehensive strategy to address these and other issues. I will offer some insight on what TCBA has done to assist our clients address these and other related issues.

Topic: "Gartnerization of IDS/IPS Vending: Beyond the magic quadrant...What works? What Doesn't?"

Charles Iheagwara, Chief Technology Officer, Unatek, Inc.

Since the inception of the deployment of intrusion detection systems and lately intrusion prevention systems, more than 90 products have been/and are being touted as the ultimate solution(s) for enterprise deployment. In the rush to sale and attract customers, vendors have taken to the highway of producing bogus claims in their sales literature. In the process, different metrics have been used to describe the performance and potency of intrusion detection and prevention products. One of the most widely quoted metrics is Gartner's "Magic Quadrant." The quadrant ranks vendors in four categories and produces a leader board.

This presentation discusses the "pros and cons" and the implications of Gartnerization.

Topic: "IDS isn't dead, your implementation of it is! Lessons learned from an enterprise deployment: how to maximize your detection capabilities and investment."

Rohan Amin, Manager, Lockheed Martin

In 2003, Gartner said, "IDSs have failed to provide value relative to its costs and will be obsolete by 2005." Fast forward to 2006, their end conclusion has still not been realized; however, many of the shortcomings they noted in their controversial paper are not shortcomings of the technology but rather of the implementation. This presentation and paper will present a case study of IDS implementation from the world's largest defense contractor and review why Intrusion Detection, correctly implemented, is still a core component of enterprise security.

Topic: "Architectures for Detecting Service Intruders and Holding Them Accountable without Sacrificing User Privacy."

Prof. Ulrich Flegel, University of Dortmund, Germany

For a better digital world we need services and businesses that not only protect the security objectives of the service providers, but also respect the privacy objectives of their users. We examine the requirements of intrusion detection and response in a service environment regarding accountability and anonymity. Such requirements are partially of legal nature and partially mirror the expectations and demands of the users and therefore determine their choice of service providers. Designing or choosing the right technology is key, if we want to provide our service in and make business with countries that enforce restrictive privacy law, such as EU member states, as well as to get the desired share of the user community. Based on the examined requirements we develop an architectural model for secure and pseudonymous authorizations in service environments. Using the model and generic criteria we distinguish and compare distinct architectures, such we can make sound decisions when designing new systems. Also, existing architectures of secure authorization systems can be mapped to this model, and then analyzed and compared, in order to choose the right system for our purposes.

Keynote: "eFraud in Online Commerce: Impact on Business Reputation & Consumer Confidence."

Kerry G. (Kwasi) Holman, President, Prince Georges County Economic Dev. Corp.

The scope and target of Internet fraud in online commerce has seen an exponential growth in recent time. For this, there are unexpected consequences – which are not clearly discernable. By their basic nature, Internet fraud involves the use of the Internet as the target or as the means of perpetrating economic crimes of deception. Therefore, this keynote will examine the nature and extent of some of the principal types of business Internet fraud with concrete examples. The keynote will also highlight the impact on business reputation and consumer confidence.

Topic: "Spyware Exploits."

Donald DeBolt, Director, Computer Associates, Inc.

Don DeBolt, Director of Anti-Spyware Research for CA, will provide insight into the many exploit vectors used by manufacturers of Spyware to distribute their code. Botnets, toolbar bundles, rootkits, drive-by downloads, JavaByteVerify attacks, and social engineering are all tactics used by Spyware vendors today. Don will share "in the Wild" examples and provide empirical data to help quantify the treat.

Topic: "Security for Rich Media Collaboration: The Challenge of Balancing Network Security with the Need to Communicate."

John Starke, VP TransGlobal Business Systems

Security and network security are intended to serve customers, who need to communicate. Closing firewalls to complex traffic may keep the network safe, but it is also useless. Another popular alternative for secure communications is the safe proxy server. While providing some degree of security, it is expensive to scale and less flexible than peer-to-peer for personal collaboration. If security systems do not accommodate the need for complex collaboration, then the end users will find alternatives from professionals, who can provide secure and complex collaboration.

Topic: "Establishing A "Best Practice" Security Process: Setting the Standards From Assessment through Incident Response."

Omar Keith Helferich, Security Research Consultant, Department of Homeland Security and Faculty, Central Michigan University

Corporate commitment to protect the public as well as their brand image through risk assessment, planning, and more resilient supply networks is increasing given the recognition that the U.S. is vulnerable to a wide range of potential service disruptions from natural disasters, pandemic disease, disgruntled employees, special interest groups, and/or acts of terrorism. Michigan State University through a Department of Homeland Security Grant and in collaboration with industry is developing a strategic level methodology that defines a leading Brand Protection-Supply Chain Security Process. The objective of the process is to impact and prescribe brand protection/security controls to reduce or eliminate risks to the disruption of the overall supply chain. The process can serve as the cornerstone for the development of a brand protection program that identifies disruption risks that could affect business operations while prescribing cost effective solutions to mitigate these risks and optimize effective resilient networks. The process standard is dynamic, capable of being adapted to changing issues, new risks, or operational circumstances and business needs. The presentation will discuss the value, steps-"template" and metrics to achieve such a "Leading Practice" Process for overall Supply Chain Brand Protection/ Risk Management.

Topic: "Managing Identity Risk."

Bill Dutcher, Principal Consultant, Booz Allen and Hamilton

Identity credentials, such as a passport or a driver's license, allow us to cash checks, travel abroad, board airliners, and gain entrance to government and commercial buildings. The Department of Defense Common Access Card (CAC) and the forthcoming Personal Identity Verification (PIV) card will create government-specific identity credentials that can be used for both personal and electronic authentication to access government and military facilities, as well as to government IT systems.

Any identity credential, not matter how secure it may seem, carries with it some amount of risk. It may have been issued fraudulently, it may have been altered, it may be used by an unauthorized person, or systems it is used to access may not be protected adequately. This presentation will examine the risk elements in creating, using, and managing identity credentials, as well as what IT managers can do to reduce or mitigate those risks.

Topic: "Identity Bridging Techniques across SOA-based Business Service Networks"
Mamoon Yunus and Rizwan Mallal, Advisor and CEO, Crosscheck Networks

Identity Management is a critical aspect of deploying secure SOA-based Business Services Networks. Establishing trusted Business Services Networks require application- and user-level authentication and authorization of invoked services. In effective BSNs, service invocations should seamlessly traverse corporate boundaries. With loosely coupled and chained Web Services, building trusted Business Networks require flexibility in Identity Management across protocols and messages. As corporate boundaries become porous to trading partner interactions, identity enforcement and identity bridging become central in ensuring Business Service Network flexibility without compromising trust-based security.