Cyber Security Awareness Day

Presentations/Speakers

SAFE
Security Awareness For Everyone

Cyber Security Awareness Day
Wave Systems will present information on Trusted Platform Modules (TPMs), semiconductor chips that conforms to the industry security standards set forth by the not-for-profit Trusted Computing Group. Topics will include how this powerful security technology is the basis for strong authentication, identity management, data protection and network access control. This presentation is a must for any IT professional considering authentication and/or data protection solutions as the industry continues to migrate toward industry-standard, open platform technologies. Leveraging industry-standard, open-platform technologies has been the backbone of IT for many years with ethernet, TCP/IP and many other technologies. The advent of industry-standard hardware security in the client will lead to enhanced interoperability and standardization of security practices. With over 50 Million TPMs shipping inside PCs by the end of 2006, it is time to leverage this new and powerful technology in securing the network.

Steven Sprague is president and CEO of Wave Systems Corp., based in Lee, MA (www.wave.com). A pioneer of the Trusted Computing movement, Sprague has been an executive and technology developer in computer security and e-commerce since the late 1980s. Wave Systems addresses critical security issues facing businesses and government today, with trusted computing solutions that work with all PC security chips compliant with Trusted Computing Group specifications for strong authentication, data protection, advanced password management and enterprise-wide trust management services and more. Wave holds a portfolio of significant fundamental patents in security and e-commerce applications and employs some of the world’s leading security systems architects and engineers. Sprague has a B.S. in mechanical engineering from Cornell University.
Law Enforcement Trends in Cyber Crime
10:30 a.m. - 11:30 a.m.

This presentation will provide a law enforcement overview of trends in cyber crime with an emphasis on terrorism, intrusion investigations, and identity theft.

Special Agent (SA) **Christopher J. Lester** began working for the FBI over 16 years ago in the San Francisco Division. In 1994, SA Lester was assigned to the Minneapolis Division to work white collar crime and computer intrusion investigations.

In 1995, SA Lester headed up the Minneapolis Division’s Evidence Response Team, a group of agents extensively trained in the collection of physical evidence from crime scenes. He has been a member of the Computer Analysis Response Team (CART), a team assigned for the forensic collection of data from computers for almost seven years.

In 2002, SA Lester was Acting Supervisory Special Agent for the high tech computer crime squad of the Minneapolis Division for six months. He has been the primary relief supervisor for more than four years. For the past six months, SA Lester has been the Acting Supervisory Special Agent for the FBI Cyber Crimes Squad.

Identity Theft: When bad things happen to your good name
12:30 p.m. - 1:30 p.m.

Identity theft is a growing problem in nearly every community in the world. The Postal Inspection Service will discuss the size of the problem, current trends used by thieves to gather and manipulate information and what people and victims can do to protect themselves. The final segment of the presentation will be left for fielding questions or comments from the audience.

**Matt Schmitz** is a United States Postal Inspector responsible for investigations in North Dakota and western Minnesota. Before his appointment as a Postal Inspector, Matt served as a police officer and detective in Wisconsin. He has been involved in numerous identity theft investigations and is a member of the International Association of Financial Crimes Investigators.
Introduction to Personal Internet Safety & Security

2 p.m. - 3 p.m.

More than 75% of Americans today have Internet access at home and about 65% of those have broadband access. With this increase in connectivity, however, come the inevitable bad side effects of any technology. Threats to our personal safety, security and especially to that of our children have gone up dramatically. From identity theft to child predators, the Internet in some ways provides an easier avenue for these threats to be realized - often taking advantage of our lack of awareness and trust. After all, how many of us sit with the assumption that a faceless machine sitting in the study or kid’s bedroom can be a source of danger? This talk will introduce you to the major categories of problems plaguing web surfers today. Special focus will be paid to the risks posed to children and teenagers online. All through the presentation recommendations for protection will be made and illustrated.

Software Security in the Real World

10:30 a.m. - 11:30 a.m. (Red River Valley Room - sessions runs concurrent with Law Enforcement Trends in Cyber Crime)

This talk will attempt to convince the audience about the need to build security into software from the ground up rather than resorting to either just penetration tests to catch all problems or worse still on a patch mentality. The focus would be on efficient approaches for improving security during each phase of the software development lifecycle. Topics ranging from threat modeling to security code review and penetration testing will be covered. Using real world examples such as the improved security quality of large software systems, the speaker will attempt to convince the audience about both the need and the most efficient way to achieve security goals.

Dean H. Saxe is a Managing Consultant at Foundstone. He is responsible for conducting web application penetration testing, threat modeling, code reviews, secure software development lifecycle (S-SDLC) design and implementation, and project management. Dean also provides client education services as a lead instructor of these Foundstone

Dean has nine years of software development experience in a variety of industries, including banking, education, and quality control. Since 2001, he has focused on secure software development and web application security. Prior to working at Foundstone, Dean held the position of manager of web application security for a corporate cash-management application service provider. In this position, he implemented the company’s first secure software development and deployment guidelines, development frameworks to support secure coding paradigms, tools used for the semi-automated remediation of application vulnerabilities, and static code analysis tools to expedite conducting secure code reviews. Dean co-founded and remains active in the Atlanta ColdFusion User Group (ACFUG) and is an active member of the Open Web Application Security Project (OWASP) Atlanta Chapter.

At Foundstone, Dean has worked with multinational telecommunications providers, utility companies, and software manufacturers to perform threat modeling and code reviews of numerous business critical applications. He has identified the lack of developer training and the lack of formalized secure software development and deployment practices as the root cause of many critical application vulnerabilities. Dean’s findings have led to an ongoing effort at many organizations to incorporate security into the software development lifecycle (SDLC). Key factors of success in this effort include developer training on secure development practices through Foundstone courses, the addition of threat modeling to all phases of the SDLC, and the identification of “security evangelists” within each development organization.

Dean attained the Certified Ethical Hacker (CEH) designation in 2004 and the Certified Information Systems Security Professional (CISSP) designation in 2006. Dean holds a BA in biology from The Johns Hopkins University in Baltimore, Maryland.
Securing the Infrastructure
3:30 p.m. - 4:30 p.m.

Learn how to protect your IP Voice, Video and Data Infrastructure from unauthorized access.

Steve John has been a Systems Engineer with Cisco Systems, Inc. since 1999. He achieved the Cisco Certified Internetworking Expert (CCIE), Cisco’s highest certification level, in 2001. He achieved his Certified Information System Security Professional (CISSP) certification in 2006. His role includes technical consulting for government, education and commercial accounts in North Dakota. An expert in network security and IP voice, Steve has helped many companies securely architect their networks with emerging technologies.

Prior to Cisco, Steve worked as Network Engineer and Services Manager for a North Dakota systems integrator for nine years. The North Dakota office of Cisco Systems is located in Fargo.
The Cyber Security Awareness Day committee would like to thank all of the event’s presenters and sponsors for their time and generosity.