Certified vs Secure

Chair -

Jon David
Lehman Brothers

Panelists -

Sarah Gordon
IBM

Tim Polk
NIST

Dan Woolley
Global Integrity Corporation

Fred Kolbrener
Xacta Corporation

We all need properly working products, but few of us can determine how "good" a product is. Certifications are touted (by vendors with them) ad indicators of quality. Is this true, though?

Organizations such as Consumers Reports are buyer sponsored, but don't treat security products (of our type, anyway). Not-for-profit certification processes may treat only the criteria of interest to the certifiers. For-profit certifiers may be prejudiced in favor of vendor sponsors. How might the criteria used be different for each type of certification group?

If a vendor chooses to expand a security product to meet current and important threats, rather than spend those efforts and monies to satisfy out-of-date certification criteria, is such a vendor to be penalized for having a better product? Should/do vendors design for optimum security or certification (if they can only do one)?

Just what is certification, i.e. does "certified" mean (or even imply) "good," or merely that certain tests/evaluations have been completed without horrible results? With our dynamic technology, how current can criteria be/remain? Certification is an inherently slow process that doesn't really fit today's world. How you use a system is at least as important as what it does; is this taken into account in certification processes and, if so, how?

What's the difference between not being certified & failing to get certified? Is having an adequate product enough to get a certification, or are other things (paperwork, fees, whatever) also required? With both hardware and software becoming out of date within a week or two of installing it, and obsolete within a few months, how long should certifications be deemed valid? What metrics, if any, are used in certifications? Do certifications require passing all in a set of tests, or is there some combination of all tests that can overcome specific shortcomings? (Think of a product failing one test while acing all others, vs. a product that barely passes all tests ... If the area of failure is of no importance to you, isn't the failing product better than the passing one?)

This session investigates all these issues in a real world context.

Jon David

Jon David is an officer in the Security Engineering group at Lehman Brothers. With over 30 years in security, he was a pioneer in both computer and network security. Prior to Lehman Brothers, he was Director of Network Security for an ISP, and spent a depressingly long time as a security consultant. He is a frequent author and speaker, and has repeatedly been in the van of security technology. Well past his prime and clearly at the pre-dotage stage of life, he lives off of the knowledge and abilities of friends these days. In an attempt to disguise his street kid tendencies, he did his undergraduate work at Queens College and his graduate work at Columbia University.

Sarah Gordon

Sarah graduated from University with special projects in both UNIX system security and ethical issues in technology. She is currently working with the anti-virus science and technology team at IBM's Thomas J. Watson Research Center. Her current projects include impact of vulnerability and exploit publication, profiling techniques and methodology, certification standards for security software. Her on-going projects include ethical implications of technology, with an emphasis on computer viruses and malicious code. She has been featured in publications such as Forbes, IEEE, Time Digital, The Wall Street Journal, and WIRED; her work appears regularly in technical and generalist publications. She has won several awards for her work in various aspects of computing technology. Sarah is on the Virus Bulletin Advisory board and serves on the Board of Directors of both The WildList Organization International, and The European Institute for Computer Antivirus Research. She provides consultancy services to corporate, educational and government organizations. Read about her work at www.badguys.org

Tim Polk

Tim Polk has been a member of the Computer Security Division at NIST for eleven years, and has been a member of the PKI Project Team for five years. He was co-editor of RFC 2459, the PKIX Certificate and CRL Profile. Tim currently edits several NIST and IETF PKI specifications. Before joining the PKI Team, Tim focused on system security tools and techniques.

Dan Wooley

Dan Woolley is President, Chief Operating Officer and acting Chief Executive Officer Global Integrity Corporation, and brings over than 25 years of experience in the information technology industry.

Prior to joining Global Integrity, Mr. Woolley was the National Security Services Leader for Business Development and Operations for Ernst & Young’s National Information Security Services Practice, where he was responsible for business strategy and direction for the 12 area practices in the United States and Europe. Mr. Woolley has also held senior management positions at Memco Software Inc. as vice president of business development; International Computers Limited as director of North American Business Operations, Marketing and Sales; and Computer Consoles Inc. where he was the Chief of Staff for Worldwide Operations. He is also a retired United States Air Force Reserve Lieutenant Colonel who served on multiple technical advisory and acquisition teams in the Office of Secretary of the Air Force at the Pentagon.

Over his career, Mr. Woolley has managed or been closely involved with taking to market a number of state of the art leading edge technologies. They include X.500 and X.509 technologies; Single Sign-On and Secure Single Sign-On, Secure Authentication and Enterprise distributed Network Authorization, UNIX Access Control and access monitoring tools, UNIX SVR5, and Network Security Infrastructure and Interoperability Tools. He also managed the US product requirement involved with automated dynamic link analysis technologies for various intelligence and law enforcement organizations.

Fred Kolbrener, GCIA

Fred Kolbrener is Senior Network Security Analyst for Xacta Corporation.

He is currently at the Network Infrastructure Services Agency (NISA) Directorate of Security where he devises and implements certification criteria and processes. He is a retired colonel in the army where he was heavily involved in security areas.