CERIAS Security Visionary Roundtable

Call to Action

Executive Summary

Jointly Sponsored by

Accenture
(formerly known as Andersen Consulting)

and

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University

CERIAS Security Visionary Roundtable

Security Experts Issue **Call to Action** for More Secure World

Executive Summary

"A more secure future" for business and society is at stake, according to some of the world's top information technology security experts. Extraordinary changes in the way we do business and lead our lives in the ever-connected world of the future will create tremendous security challenges. These challenges will be shaped by many of today's emerging trends: the rapid acceleration of network speed, connectivity and the overall number of devices; the removal of the human element from many everyday transactions; and easier and cheaper collection of public and private information. More than ever before, we will demand security solutions that enable businesses to thrive and private information to be protected. The bottom-line is that "doing security right" requires the greater community of business leaders, technologists, educators and political leaders to look seriously at this Call to Action and to commit resources and energy to help lead us all to a more secure world.

On September 25-26, 2000, fifteen security visionaries met as guests of Accenture in St. Charles, Illinois, to participate in the CERIAS Security Vision Roundtable, jointly sponsored by Accenture and the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security). These invited luminaries included early pioneers in information security and security leaders at some the largest and most influential companies in the world. For two days, the group shared their deepest concerns, perspectives on significant trends affecting security in the future, and views on actions needed to move us towards a more secure world.

Deepest Concerns

In identifying primary concerns, almost everyone put the threat of a major disaster on the list. Will it happen? Will it affect our increasingly fragile infrastructure? Will it cause loss of life? How can the potential situation be averted? Why hasn't it happened already? High on the list was concern about the impact of poor quality software, widely distributed on the Internet, and the high potential for harm when software weaknesses are exploited en masse. The participants also expressed concern that the highly publicized security incidents were keeping us from focusing on really critical areas that address policy, process and people issues, such as personnel security, hiring and termination procedures, assurance technologies, and system safety issues. The experts agreed that businesses are more willing to buy technology solutions, yet they are forgetting to use good business practices to ensure employees act responsibly.

Trends

When they debated significant trends impacting security, the common themes included increased complexity and interconnectivity, device proliferation, a global economy, privacy vs. convenience, and the "always on" aspect of computing. The solutions, interestingly enough, did not focus on finding a "star wars" solution, but emphasized what the participants have been saying for long time, " We have to take the holistic approach and address this from many dimensions-- including policy, business process controls, law, personal behavior and technology." There was general recognition among a group of competing technological viewpoints that the problem of security really is as hard as we all believe it is, there are no silver bullets, and there is a lot that has to be done to address the problem.

Call to Action
The group agreed that more public debate is needed on the issues surrounding privacy so that organizations and individuals have well understood expectations. We need to improve the quality and assurance of software to eliminate security vulnerabilities. We need to better develop and deploy baseline security best practices and standard security architectures. We must pursue a well-rounded, integrated, and proactive approach that addresses business, social, technical and government problems. We have to recognize that this is, above all, a people problem and we must invest wisely in education and awareness.

The participants shared and absorbed an immense amount of information. This paper captures their input on deepest concerns, emerging trends, and a Call to Action for the next decade. This Call to Action must continue to engage leaders in debating and resolving these issues so we can look forward with optimism to a more secure world.

The following list includes the top ten trends impacting security that the group identified. A summary explanation and detailed description of each trend is provided in the full report.

Top Ten Trends

The EverNet:	Billions of devices proliferate that are always on and always connected.
Virtual Business:	Complex outsourcing relationships extend trust boundaries beyond recognition.
Rules of the Game:	Government regulation increases as lawmakers react to real losses that hurt.
Wild Wild West:	International criminals exploit lack of cooperation and compatibility in international laws.
No More Secrets:	Privacy concerns will continue to compete with convenience and desire for features.
Haste Makes Waste:	"Time to Market" increases pressure to sacrifice security and quality of software.
Talent Wars:	Lack of security skills will compound weaknesses of delivered solutions.
Yours, Mine or Ours:	Identifying intellectual property and information ownership will become key areas of debate.
Web of Trust:	Standard security architectures and improved trust will spur eCommerce growth.
Information Pollution:	Information exploitation becomes more lucrative than hacking.

CERIAS Security Vision Roundtable

Call to Action

The following is a list of action items viewed as most critical by the group of the visionaries. More explanation for each action item is included in the full report.

Improve Software Quality	Focus on improving the quality and assurance of software. Prevent distribution of weak software with security exposures. Conduct research to find better methods for designing and developing higher quality software.
Invest in Training and Awareness	Develop a sound educational program that focuses on security and ethics. Focus resources throughout the educational spectrum. Teach respect for electronic boundaries. Develop comprehensive curriculum to educate our next generation.
Implement Best Practices	Incorporate baseline safeguards and practices. Use best practices to ensure security is done right in development, implementation, testing, business processes, and consumer practices.
Initiate Public Debate	Initiate public debate on identification, ownership protection, use of personal information, and responsible use of computing.
Advocate Holistic Approach	Advocate and pursue a well-rounded and pro-active approach to the overall problems: business, social, technical, and government.
Package Security Architectures	Encourage packaging of a basic security architectures with standard services that integrate with applications and infrastructure.

Perspective on the Future

Whether we notice it or not, more and more aspects of our lives are gradually becoming virtual. A few years ago we started paying bills on-line. Today, we trade and shop on the Internet. Tomorrow will bring truly smart connected appliances: medicine cabinets that will monitor our health and communicate with our doctors and pharmacists, wardrobes that will know what clothing we have, cars that will know their positions and occupants, home entertainment centers that will know all our tastes and habits. All this personal information is increasingly stored, updated and communicated in digital form. In the right hands of our service providers it will bring wonderful conveniences and efficiencies into our lives. In the wrong hands, this information can be used to wreck havoc both financially and socially.

Today, we make sure that the doors of our houses are securely locked. We often use security services to protect our physical selves and our possessions. But are all our virtual doors secure? What can we do to protect them without causing great inconveniences for ourselves? This is not a theoretical threat of interest only to very rich people. Today, one can hire private investigators to dig up all kinds of personal information about a person. This is costly and inconvenient. Tomorrow, almost everything we do will be recorded electronically. With the right tools, this information can be collected and analyzed cheaply and efficiently. Businesses will do it to provide customized services that we demand. Others may use these same tools to commit crimes of fraud, impersonation, theft, vandalism, etc. on a large scale with a push of a button.

The new world and the new economic model of connecting everything electronically, requires us to trust in things we can no longer talk to or touch or see.

Whom do we trust?
We trust electronic systems to recognize what is authorized and unauthorized and to act only upon legitimate requests. We trust software vendors to write programs that work as we expect. We trust our service vendors to implement adequate business process controls that help us define what is authorized. We trust our communications infrastructure and our legal infrastructure to protect us and to respond when something fails. We trust those who have access to our personal data as it is stored and shared in cyberspace, i.e., software developers, commercial enterprises, medical providers, insurance companies, delivery service providers, law enforcement, to know what they are doing and understand the implications of this massive and complicated process.

Visionaries

Rebecca G. Bace
Infidel, Inc.

John C. Clark
Accenture

Daniel Deganutti
Avanade

Whitfield Diffie
Sun Microsystems

Glover T. Ferguson
Accenture

Daniel Geer, Sc.D.
@Stake, Inc.

Anatole V. Gershman,
Accenture

Michael J. Jacobs
National Security Agency

David A. McGrew, Ph.D.
Cisco Systems, Inc.

Fred Piper
University of London

John W. Richardson
Intel Corporation

Marvin Schaefer
Books with a Past

Howard A. Schmidt
Microsoft Corporation

Eugene H. Spafford, Ph.D.
Purdue University

Phil Venables
Major US Investment Bank

Can we achieve this seamless economic model? If we can, it is only when organizations and governments can assure us that our trust has been well-placed. It is not sufficient for our trust, though, to be in only one entity. In fact, our greatest need for assurance is in the interaction of businesses and the complex infrastructure that supports these transactions. Where are the potential failures that could erode our trust? Some could be technology failures, but many, if not most , will eventually be recognized as people and process failures.

Some of the potential failures could be in the software, but remember people write software and people test software. The management and delivery of immature and weak software products is a people problem. Software that is designed and developed without adequate security protections, safety assurances, and controls, is a people and process problem. Some of the potential failures could be in the process of authorization-, we authorize too much without setting reasonable boundaries. The failure could be our own lack of awareness, in that we trust too much and do not ask for appropriate assurances that our privacy and integrity will be maintained. The failure could be in careless employees who do not follow policies and share or sell confidential information (our medical records, our physical location, etc.) or who modify systems to perform unauthorized activities. The failure could be inadequate laws that do not require businesses to take proper precautions until enough failures and lawsuits motivate businesses to address security more aggressively.

Providing security that enables businesses to thrive and that protects both business assets and personal privacy must be approached multi-dimensionally. It requires good business practices and well-planned policies and procedures for software developers, business managers and customers to follow. It requires public awareness and training to ensure people understand their obligations and their risks. It also requires security technology solutions that we can trust to validate identity, ensure only authorized activity, protect privacy, and provide accountability. Security is complex, because failures can occur in so many different dimensions. We cannot rely only on policies, on laws, on personal behavior, or on technology. We must address each of these facets and understand how they impact each other as we focus on creating a more secure world in this new century.

About Accenture

www.accenture.com (As of 01/01/01)

Accenture, formerly known as Andersen Consulting, is an $8.9 billion global management and technology consulting organization. The firm is reinventing itself to become the market-maker, architect and builder of the New Economy, bringing innovations to improve the way the world works and lives. More than 70,000 professionals in 48 countries deliver a wide range of specialized capabilities and solution to clients across all industries. Under its strategy, the firm is building a network of businesses to meet the full range of client needs -- consulting, technology, outsourcing, alliances and venture capital.

Accenture is recognized as a leader in information security. Our proven approach clarifies the issues and provides a clear roadmap for security planning. We focus on business strategy and security implementation, not just audits. We offer full service security solutions and in-depth technical expertise to solve the complex challenges of the evolving business environment.

About CERIAS

www.cerias.purdue.edu

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University is the world's leading academic organization in its field. The Center's goal is to promote and enable world-class leadership in interdisciplinary approaches to information assurance and security research and education. This is accomplished through the financial and technical support of industry and government partners, and the active participation of researchers from across Purdue's many schools and departments. Over 100 faculty, staff and students at Purdue are currently involved in leading-edge efforts at improving the practice and knowledge of how to secure information systems in today's rapidly-changing environment.