



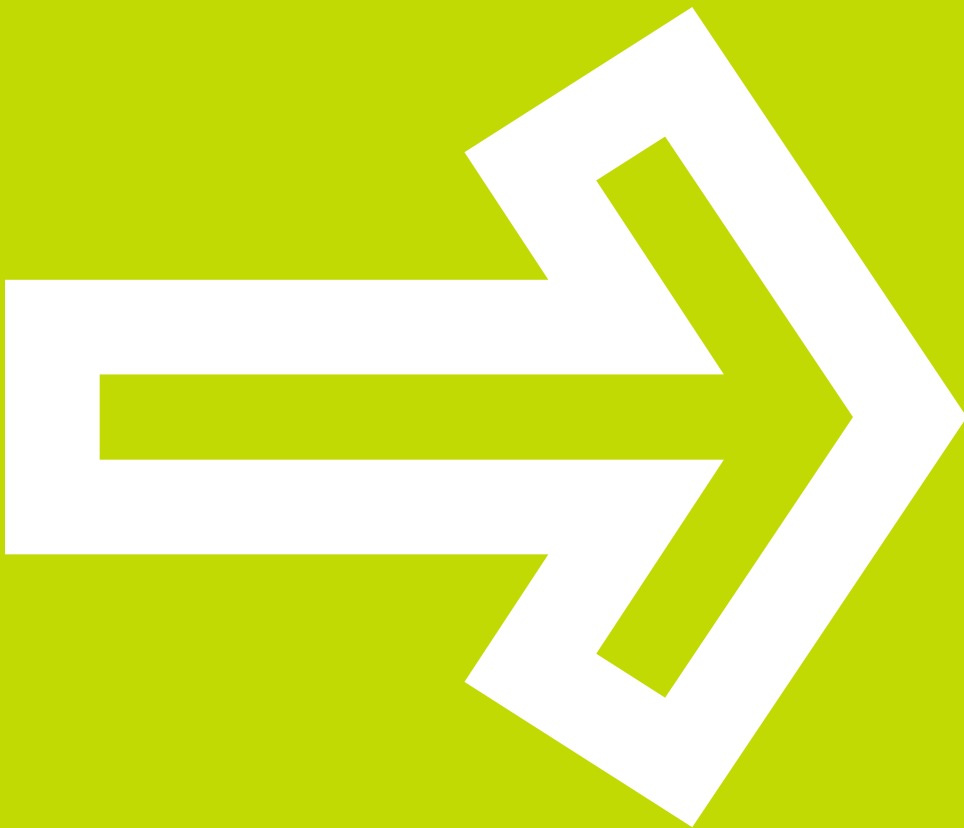
Innovation delivered.


Roadmap to a Safer Wireless World

Executive Summary

• Consulting • Technology • Outsourcing • Alliances

Roadmap to a Safer Wireless World



A person wearing a black suit is holding a silver laptop. The person's hands are visible, typing on the keyboard. The laptop is open and angled upwards. The background is a light-colored, textured wall.

2002 Accenture / CERIAS
Security Visionary
Roundtable

Roadmap to a Safer
Wireless World

Trillions of dollars of data traffic currently travel telephone and computer networks in the wired world.

Forecasts for growth in use by the public, business, government, and other institutions indicate that traffic will move to wireless products at an alarming rate. Use of wireless for communication, commerce, and computing needs is expected to grow, which will increase security vulnerabilities.

The enormous advantages of wireless networking — lower infrastructure costs, ease of installation, unlimited flexibility — are driving computer users to embrace wireless networking, despite the known risks of the technology. As a growing percentage of critical infrastructures, from healthcare facilities to power grid and the water supply, become computer-controlled, and those computers are networked to allow for remote operation and monitoring, information security issues will become increasingly important. Wireless networking further complicates those issues, making it easier for attackers to hide and creating unexpected new risks.

On May 6-7, 2002, the Center for Education and Research in Information Assurance and Security (CERIAS) and Accenture invited a respected group of national and international experts to sort through the issues, weigh benefits and risks, and present a set of guidelines for wireless. Eighteen leading security experts and researchers from the realms of technology, business, and government met in Washington, D.C.,

to explore the challenges and articulate a vision for a safer wireless world. Representing security and wireless expertise at some of the largest and most influential companies in the world, respected universities, research centers, and government agencies, this diverse group shared different perspectives as they developed ideas for a secure wireless future. For two days the group expressed concerns, identified key themes, and developed short- and long-term approaches to improve security in the wireless world.

The 2002 Security Visionary Roundtable Resulted in a Set of Guidelines:

- ▷ Increase awareness in the general public and educate consumers.
- ▷ Inform business and industry, both as end-users and as product and service providers, and challenge them to weigh and address the risks, demand safety and security of themselves, and create a sense of organizational responsibility and leadership in private-sector approaches to security.
- ▷ Encourage and support government participation when appropriate to meet consumer goals for technology and security.
- ▷ Reinforce to security technologists the importance of appropriate interfaces with existing wired technologies.

Discussion among the experts and the resulting guidelines and policy recommendations focused on challenges to several affected groups of "wireless consumers": business enterprises; suppliers of wireless technologies; consumers; and government, both as a consumer and a policy driver. Within each group, the experts identified numerous challenges and made corresponding recommendations to meet needs and address security concerns.

Wireless Security Challenges			
Enterprise	Suppliers	Consumers	Government
Exposure of wired networks	Market forces and rush to market can compromise quality of security	Safety requires awareness	Law enforcement and defense have unique needs
Lost, damaged and stolen devices	Security concerns, slow acceptance	Concept of privacy changes	Increased use and "digital" government processes increase need to secure
Loss of control over assets	Differing requirements increase complexity	Protection of personal information	
Challenges For All Segments			
Trained and knowledgeable security personnel Appropriate resources, tools, and protocols			

The existing problems of the current wired computer network infrastructure, including difficulties maintaining data privacy and the ability to impersonate others easily, only become magnified when viewed through the lens of wireless networking. Several critical issues must be addressed to make wireless technologies safe for most users, with various sectors facing unique challenges.

Businesses, government agencies, universities, and other organizations look to wireless networking as a way to improve the bottom line. But much of the security available on today's computer systems used by businesses and organizations depends on physical measures, such as keeping people out of critical buildings and rooms through the use of guards, keys, and tools such as fingerprint readers. In a wireless world, such techniques are useless. In addition, wireless devices can be lost, stolen, or sold by an unaware or disgruntled employee, potentially opening up a corporate system to an outside attack. Allowing employees to access corporate information assets with wireless devices reduces companies' control over the types of software tapping in to their systems, opening those systems to issues ranging from technical failure to a deliberate software attack.

Consumers have embraced wireless connectivity without clearly understanding the risks, either because they believe products are "safe" or because they value the immediate convenience and flexibility of wireless over a less immediate and somewhat amorphous

threat. The result is that they may unwittingly broadcast a great deal of personal information (e.g. personal tastes, physical location). Consumers will need a greater understanding of the hazards that exist so they can make informed choices.

Governments, especially those in free societies, face unique challenges. Citizens generally expect free and unfettered access to public documents, and governments have responded by making them available electronically. But governments also need to protect secret information and maintain the integrity of the communications infrastructure. While wireless technologies make it easier for citizens to access information—while lowering the costs of government—those same technologies also make securing the information much harder.

Suppliers are not likely to lead the way in addressing the critical issues facing wireless users, largely because of market forces, consumer demands, and the limits of the technology today. This situation does not differ significantly from conditions in the wired world. However, the critical nature of wireless issues demonstrates the need for other influencers and responsible parties to step in and demand safety and integrity in wireless systems.

In a world where many personal technology devices are always connected to the network, security vulnerabilities become even easier to exploit. The increasing complexity of the wireless network marketplace, with different types of technology and a wide variety

of developers, make security increasingly problematic. For instance, a small subset of technologies may offer reasonable security, but connecting that system to another system or systems may open a large security hole. Seamless interoperability between disparate components, the goal of modern computing, has proven to be something of an Achilles heel for secure computing.

A large part of the problem can be blamed on a lack of security knowledge and skills among users, providers, and manufacturers. As a result, systems are designed badly, installed incorrectly, and used foolishly. Consumer awareness can be the first and best line of defense, creating new knowledge and demand.

To combat these problems, the Accenture / CERIAS Roundtable experts identified four steps:

- ▶ Design secure wireless systems with the aim of simplifying solutions.
- ▶ Build interoperability into the systems from the start.
- ▶ Make the technology transparent enough for any user to understand.
- ▶ Educate users about the choice between safety and convenience.

To achieve these four steps, all parties must invest both human and financial resources in greater awareness and more investment in scientific research. Exploration of security issues and solutions must be ongoing and long-term.



Security Primer

The following concepts represent an overview of the wealth of discussion during the 2002 Accenture / CERIAS Security Visionary Roundtable. The Security Primer provides an outline of the key challenges identified by the experts as facing all segments in the wireless chain. The Primer is presented as a high-level briefing and should be used as reference by security experts, administrators, and developers alike when planning for a secure wireless system. Detailed discussions of these concepts are available in Sections II and III of the full report at www.accenture.com/securitytrends and www.cerias.purdue.edu/securitytrends.

Roadmap to Improved Security

The Roadmap to a Safer Wireless World recommends several actions that will lead to a safer wireless world. The directions focus on four key areas: improved design and development; an enhanced delivery and deployment process; increased investment in scientific research; and education for all players involved in wireless.

Improve the design and development process

The experts identified simplicity, interoperability, and transparency as primary areas of concern in the design and development process.

- ▷ Simplicity is the key to security. Complicated solutions only increase the risk of weaknesses to be exploited.
- ▷ Interoperability is crucial for reducing the costs of add-on security and increasing the opportunity to develop a seamless security infrastructure.
- ▷ Transparency allows users to embrace the wireless world while meeting their security goals, without having to learn the intricacies of security technology.

The design process should focus on incorporating appropriate mechanisms that provide for proper authentication of users and devices, ensuring only authorized use of services, protecting confidentiality and integrity of data, and providing for secure roaming and authentication of mobile users.

Improve the standards development process

- ▷ Revamp the process of wireless security standards to ensure that enough expertise is included, and security goals are strengthened as the first priority.
- ▷ Identify a mechanism to fund and encourage the participation of independent security experts.
- ▷ Include government in the standard-setting process to meet the growing and robust security needs in the wireless arena.

Design for Ease of Use

This recommendation centers on the need to develop processes that reduce the need for secure configuration, but when configurations are required, experts recommend that ease-of-use be the primary goal in security design.

Strive for consistency in security development

One very practical and beneficial recommendation is for companies to bring all developers together to communicate a common understanding of the role security plays

in development. This could be done by transferring developers into one organizational entity or creating a specific administrative position that is charged with integrating security training, requirements and security reviews among all the teams.

Improve functionality of network base stations

Manufacturers should consider adding the following functions to their products: access points with built-in firewalls that have auditing, rate limiting on outgoing Simple Mail Transfer Protocol (SMTP), and logging of wireless packets to NFAT (Network Forensics Analysis Tool).

Enhance the Delivery and Deployment Process

Many of the recommendations in this section can be applied today. Manufacturers and vendors can improve the products they develop, through enhanced delivery and deployment processes that reduce security risks. Businesses that deploy wireless technology can improve the development process to ensure secure installation and follow best practices to mitigate known risks.

The future of wireless holds promise for improvements in quality of life and work. Proper attention to the security issues will enable us to achieve those promises and protect our valuable resources, without losing any of the exciting benefits of wireless communication.



Create and enable trusted devices

Trusted devices create an environment for building privacy, authentication, integrity, and non-repudiation. Trusted devices, plus a secure place to store credentials, will enable a trusted device scenario. These devices also must be enterprise-ready, and include policy-management capabilities, logging, firewall abilities, and remote-kill.

Encourage processes to ensure secure configurations

Processes must ensure secure configurations and be cognizant of the roles played by various populations, (manufacturer, access provider, consumer). The process also must clarify issues of enforcement and validation. The Roundtable experts further emphasized the value of secure configurations as a method to reduce the risks when deploying products and services in the wireless arena.

Develop & Implement Best Practices

Recent news reports have illustrated the need to address security issues in the deployment of wireless architectures. Business enterprises will benefit from access to wireless security best practices that help them mitigate risks as they deploy wireless networks. With that audience and need in mind, the Roundtable experts developed the Wireless Security Best Practice.

Increase Investment in Scientific Research

Institutions must plan to invest in education and research, and ensure that neutral and informed organizations continue to explore and discover security issues and solutions to build a more secure world. Directors and administrators frequently must

sacrifice long-term research for profit margins and real-time needs. But while sometimes considered a luxury in the business arena, research that examines trends and increases overall security knowledge is necessary to move ahead of problems and plan for security. The Roundtable experts identified several areas of research that will provide benefits.

The participants emphasized the need for metrics to measure security and provide the basis for understanding the upfront costs of security, as well as the amortized costs over time. With good measurements, insurance companies can write policies, and business managers can plan for and evaluate technology costs. In addition to the benefits of stronger planning criteria, metrics may provide the impetus to address security earlier in the design phase.

Fund Research to produce metrics for code quality and system security that are easily understood

Metrics are the basis for forming judgments about the level of quality provided by vendors in the wireless arena and may lead to the development of tools and methodologies that can be adopted by organizations. Metrics are critical because they provide a tool with which to compare and examine system capabilities. Systems also need to be evaluated within their environments, allowing for different network topologies and the assignment of security risks associated with each.

Fund Research to produce metrics for trust, risk, and ease of use

Metrics, supported by a solid set of data, are a fundamental requirement to help support the development of processes that identify, quantify, communicate, and mitigate risks. Roundtable experts strongly supported the need for good metrics and research funding to solve these difficult and critical problems.

Fund Research to develop a model for a reliable and predictive communication network between trusted peers.

Trusted devices that ensure privacy, peer-to-peer authentication, integrity, and non-repudiation, combined with trusted storage of credentials, require high integrity in the network to achieve end-to-end security. Research in these areas is necessary to provide a model for the industry to use when developing secure applications and networks.

While security experts do not always agree on the approach, many agree that a model of trustworthy devices as the communication end-point is critical. This recommendation calls for mutual authentication in five areas:

1. human to device, device to human
2. device to network, network to device
3. peer to peer
4. sub-network to sub-network
5. re-authentication after roaming

The model should work whether the entire path is wired, wireless, or a combination of both. Those areas that require more advanced research include human to device mutual authentication. Further research is needed in the area of sub-network mutual authentication when networks are composed of different service providers. Although there are known solutions and methods, more knowledge is required to understand how to achieve service levels and service-level agreements appropriate to the model.

Educate all Players in the Wireless Chain

The stakeholders in wireless include users, owners, managers, content providers, service providers, and manufacturers. These players need to understand their risks and obligations, relying on security experts to evaluate and articulate the issues. The education of all players starts with the development of experts who meet a standard of professionalism. Education continues with training and awareness at different levels, depending on whether the player is developing applications and services, writing or interpreting laws, or using wireless services that could compromise their personal privacy or safety.

Support security as a distinct profession

The demand for security knowledge is high today, but many "security experts" actually have limited experience. Currently there is no reliable method on which to judge or determine the value of advice being offered by security professionals. Security needs to become a distinct profession, different from related technical fields, with

well-recognized and supported qualifications. Roundtable experts called for increased efforts to be initiated to define the discipline, including common terms, knowledge, and skills. Degrees and exams should be developed to help define and meet a standard of excellence. The discipline should recognize that skills sets are not only technical, but also include business knowledge, communication skills, and legal savvy. In addition to education and professional qualifications, government agencies should encourage professional standards, and organizations must differentiate information technology professionals from security professionals by giving more credence and weight to security skills and certification.

Teach security in all disciplines at universities

Just as they require a minimum level of math skills, universities should also require coursework in security and assurance before conferring any information technology, engineering, or software development degree. Security problems occur in all types of applications when coders remain ignorant of basic security issues that prevent vulnerabilities. The new generation of wireless products and services will require enhanced knowledge of security to ensure secure end devices and secure transactions.

Develop a program to increase the level of awareness of security responsibilities in the wireless world.

Consumers need to understand how their actions place them at personal risk, and how they can take positive steps to reduce the risks. Consumers need to be informed about risks and

encouraged to purchase appropriately secure machines. Government and industry support, possibly even from the insurance and financial services industries, might be needed to develop a broad and useful security awareness campaign.

Outcomes

The Wireless Security Roundtable experts covered a broad range of wireless security issues, and based their discussions on the need to address both current and future concerns for all players in the wireless arena: enterprises, consumers, suppliers, and government. The experts identified major challenges, including complexity, market forces, and lack of security skills. Their recommendations focus on several actions that can be taken immediately and over time to improve design and deployment, and identified areas for enhanced research and improved education.

The future of wireless holds promise for improvements in quality of life and work. Proper attention to the security issues will enable us to achieve those promises and protect our valuable resources, without losing any of the exciting benefits of wireless communication.

About Accenture

Accenture is the world's leading management and technology services organization. Through its network of businesses approach—in which the company enhances its consulting and outsourcing expertise through alliances, affiliated companies and other capabilities—Accenture delivers innovations that help clients across all industries quickly realize their visions.

With approximately 75,000 people in 47 countries, Accenture can quickly mobilize its broad and deep global resources to accelerate results for clients. The company has extensive experience in 18 industry groups in key business areas, including customer relationship management, supply chain management, business strategy, technology and outsourcing. Accenture also leverages its affiliates and alliances to help drive innovative solutions. Strong relationships within this network of businesses extend Accenture's knowledge of emerging business models and products, enabling the company to provide its clients with the best possible tools, technologies and capabilities. Accenture uses these resources to serve as a catalyst, helping clients anticipate and gain value from business and technology change.

For the fiscal year ended August 31, 2001, Accenture generated net revenues of \$11.44 billion. Its home page is www.accenture.com.

Special thanks to Ruth Page Jones, Athena Consulting, for providing guidance on the development of the Security Roundtable and for drafting this report from the proceedings of the event. Special gratitude to Teresa Bennett, CERIAS- Purdue University, for assistance in organizing the Security Roundtable and for editing this report.

About CERIAS

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University is the world's foremost university center for multidisciplinary research and education in information security, privacy, and assurance. CERIAS conducts research in the areas of computer, network, and communications security and information assurance.

Mission Statement

To establish an ongoing center of excellence that promotes and enables world-class leadership in multidisciplinary approaches to information assurance and security research and education. This collaboration will advance the state and practice of information security and assurance. The synergy from key members of academia, government, and industry will promote and support programs of research, education, and community service.

CERIAS works with business and industry, government and other universities to bring attention to the problems of information security. As a research and education center, CERIAS leads the nation in its understanding of computer, network, and communications security and information assurance.

The goals of CERIAS are to:

Increase public awareness of security and privacy issues, and increase general knowledge through education and training. Partner with business, industry, and government. Investigate and develop the latest and most relevant research and technologies. Educate and equip professionals in the field of information security and assurance.

For more information about CERIAS:

Teresa A. Bennett
Manager of Strategic Relations
Center for Education and Research
in Information Assurance and Security (CERIAS)
Purdue University

tkbennet@cerias.purdue.edu
(765) 494-7806
<<http://www.cerias.purdue.edu>>

Copyright © 2002 Accenture
All rights reserved.

Accenture, its logo, and
Accenture Innovation
Delivered are trademarks
of Accenture.



1 2 4 5 2 9 2 5