accenture

Innovation delivered.

Roadmap to a Safer Wireless World

Security Report

• Consulting • Technology • Outsourcing • Alliances

Roadmap to a Safer Wireless World

2002 Security Visionary Roundtable

Jointly Sponsored by:

Accenture

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

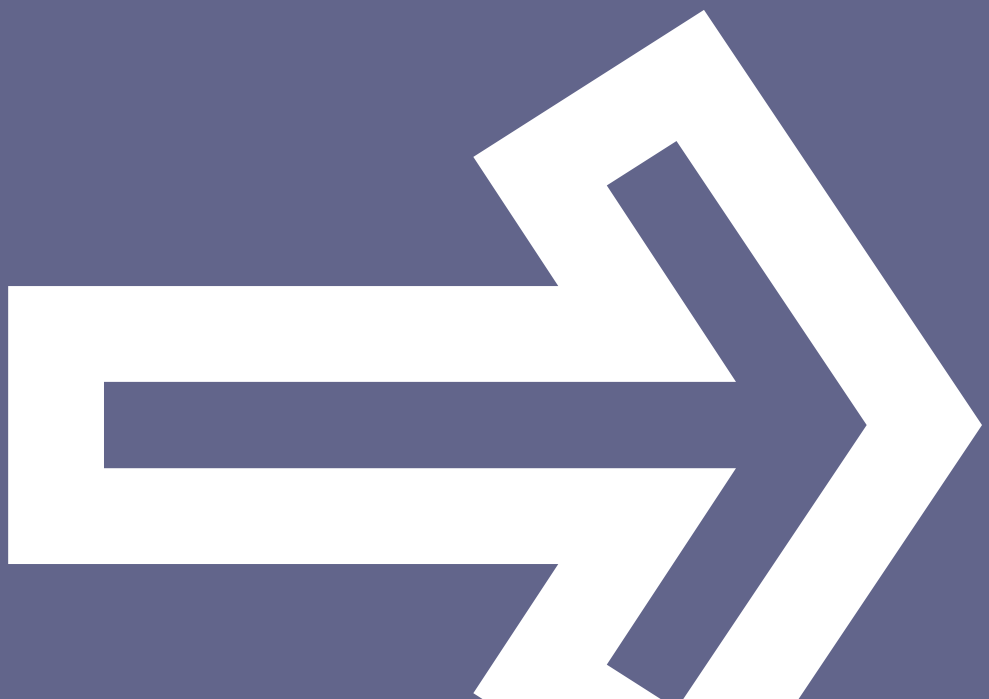

Table of Contents

I. Executive Summary

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 require-ments 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 III and IV of this report.

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.

II. Introduction

We are in the midst of a wireless revolution — a stunning increase in wireless networks and wireless devices — that promises to allow people to connect in new ways to their homes, businesses, stockbrokers, soda machines, and prescription bottles anytime and from anywhere. Wireless technologies include cell phones, wireless PDAs, smart tags on clothing and products, and other devices that transmit signals and information absent of physical access.

This ongoing revolution presents a wealth of opportunities for businesses eager to exploit ubiquitous connectivity, and deliver new products and services to the growing online population. It also presents a number of serious challenges for businesses, governments, and individuals to protect sensitive information, ensure privacy, and prevent fraud.

In response to wireless growth, two leaders in different sectors of the fields of information and security, Accenture and the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), partnered to explore issues of consumer education, define problems associated with wireless, and recommend policies and procedures to increase security. Wireless brings with it the promise of flexibility and the ability to surpass the limitations of wired computing. The move to wireless technology, however, requires careful consideration of risks and security hazards that are a part of this exciting new technology.

On May 6-7, 2002, CERIAS and Accenture invited a respected group of national and international experts to sort through the issues, weigh the benefits and risks, and present a set of guidelines for wireless (see Appendix A). Eighteen leading security experts and researchers from the realms of technology, business, and government met in Washington, D.C., to explore these 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, prestigious and respected universities and research centers, as well as government agencies, this diverse group shared very different perspectives as they developed ideas for a secure wireless future. During this Roundtable, 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 guides and prescriptions:

- 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 where appropriate and necessary to meet consumer goals for technology and security.
- Reinforce to security technologists the importance of appropriate interfaces with existing wired technologies.

This document is organized to meet many needs when exploring and answering questions of wireless security. Consumers and the general public will benefit from the general primer approach and the information guide presented here. Business and industry leaders and technical experts will grasp quickly the need to treat the outcomes and findings of this report as a true guide for developing risk assessments and a set of principles to incorporate a wireless platform safely into their operations. Policy makers will understand why consumers, industry, and academia alike call for changes in the role that government plays in ensuring information security and product standards.

The report also provides a basis from which to frame additional and future discussions in academia, industry, and government. In this accelerating technology environment, the answers are not one-time solutions. The Accenture / CERIAS Roundtable recommendations include the need continually to review, evaluate, and respond to changes in technology with appropriate policies and approaches.

Following this brief Introduction, the report is organized into two sections and four appendices.

Section III:
2002 Security Visionary Roundtable Proceedings

Section IV:
Road Mapping Security in the Wireless World

Appendices:
A: Biographies of Security Visionary Roundtable Participants
B: Additional Discussion Items
C: Best Practices for Deploying Wireless Networks
D: Wireless Security Resources

This document is not intended to provide detailed technical background, but does reference several excellent papers and other resources that provide this information. The scope of the high-level recommendations will guide policy discussions, both organizational and legislative, toward short- and long-term solutions, improved standards, and a sense of urgency to address underlying causes and direct future efforts to ensure a more secure world.

III. Security Visionary Roundtable Proceedings

The Accenture / CERIAS Security Visionary Roundtable experts identified numerous issues of concern and developed recommendations for short- and long-term approaches to understanding and planning for security in the wireless world. The Proceedings are organized into a discussion of the benefits and challenges of wireless technologies to each of the four affected groups, and present a set of guidelines useful in meeting the security needs of each group.

Evaluating the Benefits and Exposures of Wireless Adoption

Wireless is being embraced as a means to improve productivity, reduce costs, and move into new markets. As enterprises, service providers, industry, manufacturers, and consumers develop strategies to take advantage of these benefits, they also will need to consider areas of risk that affect consumers and significantly impede their ability to reach their goals safely.

Government agencies and social institutions are looking to wireless as a means to increase services and reduce costs. "Digital" governments and service organizations use wirelesstechnologies to reduce infrastructure costs and create responsive Internet tools, both of which are positive actions that, if lacking appropriate security protocols, can lead to detrimental outcomes.

Benefits of Wireless Adoption

Enterprises, employees, and consumers are eager to exploit the benefits of untethered communication promised by the wireless revolution. Many business enterprises invest in wireless technology with the goal of savings and the promise of improved employee productivity. Service providers let consumers connect from anywhere—hotels, airports, restaurants, and shopping malls. Supply-chain businesses improve customer service by using wireless to enhance mobility and share real-time information. The retail industry, educational institutions, and medical and healthcare organizations transform their environment through increased mobility and flexibility. Software developers and manufacturers deliver new products that capitalize on growth in the wireless marketplace and capture new customers. Home users appreciate the ease with which they can network multiple home computers

through a single Internet connection without cables. Government and institutions increase the quality of constituent interaction and reduce infrastructure expenses by speeding response time, providing 24/7 access, and facilitating improved emergency responses.

The many real and perceived benefits drive early adopters to speed ahead, unaware or ignorant of the dangers. The experts at the Accenture / CERIAS Security Roundtable, while acknowledging and embracing many of the positive aspects of wireless, used this forum to examine these hazards and develop a set of guidelines for entering the wireless world.

Security Challenges to Wireless Adoption

The road leading to untethered communications—the EverNET (the EverNET was originally defined in the first Accenture / CERIAS Roundtable; for more information refer to <http://cerias.purdue.edu/securitytrends>), always connected, anytime and anywhere—exhibits many security hazards. Unsafe "driving protocols, poorly designed vehicles, and weak traffic rules" cannot ensure the confidentiality, integrity, and availability of these electronic resources.

As a result, users unwisely place a great amount of trust in wireless tools that may betray that trust with unsecured protocols and poor assurance design. Dissatisfied consumers may become disillusioned and move away from wireless technologies that they do not trust, thereby creating a backlash that manufacturers can avert.

The participants at the Security Roundtable focused on security issues that must be addressed to make the widespread deployment of wireless safe for most users. The rapid shift to wireless connections significantly affects consumers' ability to protect critical information and even personal safety. Consider, for example, how the wireless trend has created security challenges for different segments of the population—enterprises, consumers, suppliers, and government organizations.

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 require-ments increase complexity	Protection of personal information	

Challenges For All Segments
Trained and knowledgeable security personnel Appropriate resources, tools, and protocols

Wireless Security Issues in the Enterprise
The business enterprise may adopt wireless technologies to reduce costs and improve productivity and flexibility, looking for a positive and healthy return on investment (ROI). But when network and device manufacturers fail to provide adequate security, when service providers operate unsecured networks, or when employees operate out of ignorance and carelessness, enterprises find themselves spending more on security "after the fact," thereby reducing ROI.

Enterprises confront the following vulnerabilities in developing approaches to wireless:

- Wireless networks expose wired networks.
- Wireless systems expose corporate secrets.
- Businesses do not always control electronic assets.

Wireless networks expose wired networks.
A single wireless "jack" can turn a private corporate network into a public network open to anyone near the access point. Possessing cheap equipment and minimal skills, seemingly anyone can navigate from the wireless to the wired network, stealing secrets, launching attacks, and compromising the integrity of networks, data, and electronic services.

Wired networks require physical access and can be protected with security guards, keys, badge access, even biometric access into a physical room. However, rogue users can connect to a wireless access point (AP) by detecting a radio signal. Sometimes the access points are added to the network when employees purchase and use an inexpensive AP, plugging it directly into the network from the data jack at their desks. This wide-open door to the network is largely undiscoverable to network operators, who use traditional network mapping techniques, but may well be advertising itself to the world of users armed with wireless detection equipment.

With the elimination of barriers to the internal network, security personnel will seek to "fix" and protect the wired environment from exposures caused by the wireless connections. The costs can be great, requiring higher security budgets for configuring security on new devices, installing firewalls at every access point, enabling virtual private networks (VPN) on every device, tightening security on every host, increasing network security analysis, conducting periodic perimeter sweeps, and enhancing practices to respond to policy compromises and intrusions.

Wireless systems expose corporate secrets.
The proliferation of devices and the increase in computing power puts a growing amount of critical information in the user's hands, where data can be damaged, stolen, or lost easily in public places. The ability to transmit and store multiple large documents containing market plans, trade secrets, or medical records is increasing, potentially placing an organization's wealth and knowledge capital in the hands of any employee.

Lost devices are easy targets when the user has failed to enable security features that protect confidentiality in case of loss or theft. Unsecured devices make attractive targets for "hijacking attacks"—remotely directing the device to launch attacks. Viruses can be sent over the air to mobile devices, thereby corrupting and destroying information, and potentially infecting other devices and networks.

Quick "theft, taint, and return" physical attacks are a concern as well. These attacks involve stealing the device long enough to compromise the system, possibly adding a Trojan horse, and then returning the device without the victim realizing it has left his or her possession.

Add to this the risk of someone eavesdropping on a wireless communication, personal digital assistant (PDA), or cell phone, and capturing sensitive information. Users are not always aware of the value of information they carry and the need to protect it with even more diligence than they protect their wallets. Employees must understand that losing a PDA containing a $40 million trade secret has greater repercussions than losing a personal wallet with $40. They also need to recognize that discussing a $60-million deal on a cell phone in an airport lounge is a high-risk activity if a competitor is sitting in the chair nearby.

Businesses and organizations do not always control electronic assets.
Businesses begin to lose control as users interconnect personal devices with business, home, and recreational networks. In the wired world, more control generally exists in a centralized environment—control over what software is used, who has access, and where communications occur. In the distributed environment, with the growing proliferation of wireless devices connecting to the enterprise, some of that control is tacitly delegated to end-users. Control over access may be lost. Control over software is degraded. Significant decision-making "authority" is placed in the hands of end-users—a group with varying levels of expertise, and unknown motives and capabilities.

These vulnerabilities are compounded by vendors' default policies. Wireless devices often are purchased as end-consumer products with little to no configuration management, and a lack of standard synchronization software or middleware. Users install their own LANs at home and then connect them to the business enterprise. They also implement wireless information redirectors to send email from their PC to PDAs—all of which is done in the clear across the network.

While a business enterprise may trust its own employees, wireless devices provide the ability to combine personal and professional information. Unwittingly, the business now also must trust an employee's family and spouse's employer as the organization's information is combined with personal uses of the device. Mobile devices can connect to many networks and services, a trend that will only grow as new services are introduced.

Businesses will be further challenged as employees purchase multiple new mobile products and look for opportunities to integrate with company resources. Businesses will feel compelled to maintain a presence at the forefront of technology; failure to do so may create gaps that employees will fill with their own devices.

Wireless Security Issues for Consumers
Although security responses often are decided by ROI concerns for protecting business investments, the rapid integration of wireless into the consumer's daily life affects personal security. Consumers will need to become more vigilant and protect their own identities, personal information, cyber-relationships, and even their whereabouts.

The following section focuses briefly on issues of consumer awareness and control over their own personal security:
- Safety requires awareness and effort.
- Our concept of personal privacy will change.
- Personal information demands protection.

Safety requires awareness and effort
Many consumers perceive that wireless products are "safe," which creates a false sense of personal safety. Others may recognize the risks yet value convenience and flexibility over security. Therefore, consumers seldom configure basic security in a device that could easily be stolen, damaged, or lost.

Consumers also may be unaware that they can leak information through private conversations on cell phones in public places, or by connecting to a public, wireless, local area network (LAN) in an airport while managing their stock portfolios. Consumers do not always consider the potential for attacks that can take control of their devices and direct them to an activity unknown and unauthorized by the owner.

Consumers blend business, home, and recreational uses of such devices. Consequently, they need to develop personal security policies that decide who and how much their device trusts in all the connections they establish. Vendors cannot realistically deliver products that are safe "out of the box" when they do not know whom to trust and when that trust terminates.

There may be additional safety concerns regarding the potential for biological effects from wireless systems as well. Long-term safety issues concerning exposure to wireless signals have yet to be conclusively determined across the range of frequencies, power, and concentrations used in wireless products.

Concept of personal privacy will change
As wireless technology becomes embedded in products beyond the obvious, consumers may find their concepts of personal privacy changing. Consider new services that take advantage of accurate position location provided by wireless phone systems as part of enhanced "911" emergency communications. A mobile device might be broadcasting an individual's location to intelligent stores, to private investigators, or to local loan shark. As passive, miniature devices are incorporated into clothing, and readers are located in appropriate locations, consumers could be sharing information unwittingly about their participation in public and private activities. Technology, laws, and culture all will play a part in our adaptation to this new environment.

Personal information demands protection
The ability to permanently associate information and identity with consumer devices offers great convenience and increased safety. For instance, the built-in global positioning system (GPS) in next-generation cellular phones will allow police and rescue volunteers more easily to locate someone in distress. But "stalkers" and other criminals could abuse such tools. Sensitive personal information—such as bank accounts or health history—might be available to anyone looking for it, thereby putting privacy, finances, and even lives at risk. Additionally, imagine life in a world where anybody can know anything about you, including your precise location. Consumers risk a constant bombardment of advertising, as long as their devices remain active. This development will drive many people to keep those devices turned off, possibly suffocating the promise of wireless networking in its infancy. To take full advantage of wireless commerce devices, the technology needs to be able to broadcast personal information on request. For instance, a restaurant might receive automatic notification that an arriving customer is allergic to peanuts, without explicit user authorization. Balancing the need to broadcast such information while simultaneously protecting that information from eavesdroppers will be a critical issue.

Wireless Security Issues for Government
Government entities, similar to consumers and vendors, express many different concerns in the wireless arena. Government agencies need to protect their sensitive information, their communication infrastructure, and their mobile devices. Wireless technology can be used as a tool to improve some government operations and save costs.

Government offices and agencies become prime consumers of wireless solutions, as well as potential leaders in efforts to increase security requirements and initiate legislation when needed to set standards and identify expectations.

Government challenges with wireless technologies include the following:
- Law enforcement, military defense, and legislators have unique needs for and concerns about wireless technologies.
- Government needs and uses for wireless will increase pressure to secure wireless.

Law enforcement, military defense, and legislators have unique needs for and concerns wireless technologies
Law enforcement is charged with detecting and investigating crime by discovering what the attacker has done with the wireless network. Equally important are military and homeland defense, both requiring the ability to conduct communications intelligence in the wireless arena. Legislative bodies must react to the competing concerns of enterprises, consumers, suppliers, and government agencies, in addition to the social issues that arise from the cultural changes driven by the adoption of wireless technologies.

Government needs will increase the pressure to secure wireless technologies
Government has a need for secure wireless technology yet cannot always develop it. Commercial technology often can be applied to meet the needs of government. Government must consider the plausible risks of unsecured technology and ensure that classified networks cannot be hacked as a result of an unsecured wireless protocol. These government needs will increase the pressure to secure wireless technology in the near future.

Recent warnings attest to this concern. For example, on August 19, 2002, the National Institute of Standards and Technology (NIST) released a report and set of recommendations to the U.S. Government warning against the use of wireless LANs and advising government officials not to use

wireless LANs except in rare cases. NIST also advised officials to place LAN access points where unauthorized users will not have access and to use VPN clients and gateways (<http://www.nwfusion.com/news/2002/13487408-19-2002.html>).

The Defense Department wireless use policy should be finalized soon as well. The policy will address the use of wireless devices in and around the Pentagon and will prohibit wireless connections to classified networks or computers. Another policy submitted for formal consideration addresses wireless devices on the global grid. For more information: <http://www.govexec.com/dailyfed/0802/081602td2.htm>.

Wireless Security Issues for Suppliers

Suppliers include designers, developers, and providers of network protocols, wireless devices, and mobile services, including mobile commerce (m-Commerce). This population delivers solutions to the marketplace that allow enterprises and consumers to enjoy the benefits of wireless technology. Suppliers must be expected to consider market forces and consumer demands when developing and delivering products and services; however, the following limitations represent true challenges for suppliers in the wireless world:

- Market forces affect quality of security.
- Security concerns may slow acceptance.
- Security requirements vary by situation.

Market forces affect quality of security

Many issues may affect the quality of the security provided to consumers. The marketplace and nature of mobile devices often drive security decisions. Technical limitations of speed, power, and computing capacity in the mobile devices prevent simple transfer of security solutions from the wired to the wireless environment, and some solutions presented by wireless technologies have not even existed before in wired technologies. The tension between achieving security goals and getting to the marketplace ahead of the competition can result in decisions that deliver inadequate security.

Consumers influence market decisions by indicating their willingness to accept and even demand convenience over security. This in turn provides little motivation for product developers to include security as a part of fundamental design. However, this may be changing in the wireless arena. Providers of mobile commerce, for example, recognize the benefits of incorporating security solutions to overcome the obstacles of theft of service, non-repudiated payments, and unsecured application downloads.

Security concerns may slow acceptance

As business enterprises abandon projects because of security concerns or show unfavorable ROI because of the costs of add-on security after deployment, they may become disenchanted and reduce their investment in this technology altogether. Likewise, consumers may be hesitant to embrace mobile commerce until they feel comfortable that the security features will adequately protect their interests. Both enterprises and consumers alike seek security with less complexity, greater interoperability and improved ease of use.

Security requirements vary by situation

Vendors are being asked to deliver solutions for wireless that work with enterprise infrastructure to meet many security goals, including authentication of users and devices, authorization of users, confidentiality and integrity of data, and secure roaming and authentication. In addition, vendors are expected to recognize the fundamental differences among the security of a wired solution, a wireless cellular solution, and a wireless LAN solution.

Attempts to transfer security solutions from one area to another are not always successful. Complicating this effort is the lack of common security requirements for the platform owner, user, manufacturer, service provider, and content provider. A clear articulation of the security interest of each is needed to establish the right balance of interests before platforms are designed.

Underlying Factors that Make Security Difficult

In the previous section, we looked at how the trend toward wireless has exposed security issues that significantly impact our ability to protect critical information and ensure personal privacy. This section presents many of the underlying factors that make it difficult to ensure the safety of wireless systems.

The first joint Accenture / CERIAS Security Visionary Roundtable was conducted in 1999 (for details: http://www.cerias.purdue.edu/securitytrends). Experts in the field of information security identified several long-term trends, including complexity, market forces and security skills. These three trends are of particular relevance to this discussion of wireless and are critical to any organization or agency developing approaches and solutions to address security.

The Wireless Arena is Complex
The explosion of new devices increases the complexity of our systems to the point that it is not possible to comprehend all of the possibilities. The complexity itself will cause breaches to happen that will catch people unprepared and incapable of identifying causes.

Complexity creates unanticipated exposures
The complexity of the wireless arena makes security a difficult problem to solve because there are so many "moving parts," multiple types of technology, large numbers of players in the market, and increasing numbers of trust relationships. The security vulnerabilities exposed by this complexity present growing dangers in an always on, always connected environment.

The wireless arena is complex because it encompasses many protocols, networks, devices, programming languages, business models, etc. The multiple types of wireless networks, each with its own set of standards, bring with them a unique set of vulnerabilities. The numerous types of devices for voice or data, or voice and data combined, added to the plethora of different programming languages on various platforms, thereby multiplying the challenges and frustrating efforts to develop a cohesive approach to security.

Since many security solutions apply only to one component, the result is a collection of technical silos with little or no security where the components interact. People tend to assume that if they combine two secure components or systems together, then the resulting system is secure, perhaps doubly secure. Many fail to understand that security hinges on the relationship between components, how they are combined, and how they work together.

The number of these relationships grows with wireless, increasing complexity, and decreasing the ability to comprehend the systems we build.

Number of players increases confusion
Not only is the technology complex, but the number of players competing in the market is growing. There are many competing technologies with advantages in different environments. Businesses and customers invest in solutions with only limited life spans because of rapid market movement. The ability to exploit existing platforms, spectrums, and protocols safely while introducing new products is a key development issue. Integration of aging systems with new services presents operational security nightmares that can erode profitability and cause shareholders to scrutinize the introduction of new services and products.

Mobility introduces complex trust problems
Mobility introduces critical and complex trust problems that are greater than have existed before in computer networks. Mobility has increased the number of possible trust relationships, only a few of which have been examined or modeled. As the wireless device moves around, it establishes different trust relationships in different contexts, complicating the issue of standards. People using these devices in multiple types of context often require high trust and many levels of security. The relevant trust relationships vary with the application being executed (e.g., phone conversation, e-mail functions, financial transactions, Internet browsing, or a file transfer). The count of new trust relationships is exploding far faster than the industry's ability to understand them or support them.

Always on, always connected is itself a source of an unsecured system
A wireless LAN—with platform openness, application generality, and relatively inexpensive access points—provides much greater opportunity for attack than single-function devices such as cell phones. The future world of embedded devices, always-on connectivity, combined with anonymous access, presents additional challenges. Now arises the need to secure objects talking to objects, not simply people talking to objects. Solutions are needed to resolve issues of identity and authority when these devices conduct activities for people without human intervention, and when no one is around to notice.

Market Pressures Override Security Concerns
The economic pressure on suppliers to bring new products and services to market quickly and cheaply creates security problems with end-user devices and network protocols. Economic pressure tends to trump common sense, planning, and investment in security. It is an issue with which the security community continues to struggle and one that requires the involvement of forces that can and will counter-balance that pressure.

Competition delivers products without good trust models
Competition in the market results in end devices, produced and delivered without a good trust model, that are subject to many types of attacks. Dealing with theft is a significant issue in the wired world, but the concern rises to extraordinary levels when considering the proliferation of new devices already in the market and soon to enter the market. Many of these devices store large amounts of data and information and perform exceptionally critical business and personal functions. For these devices, virus and malicious code attacks are alarmingly simple and successful. Lack of good encryption leaks secrets. The market does not yet know how these issues will impact the growth of new technologies, but the losses can be staggering.

Enterprises miscalculate risk and cost over time
Companies feel pressure to install wireless LANs, but they may not research or recognize the associated risk or add-on cost to maintain security. Employees may wish to interconnect to their homes or replicate the flexibility they have created at home—connecting from any location around the house—in the office environment. Companies often look to wireless connections as a means to improve productivity and flexibility, by reducing the expenses of wired connections. Often neither business owners nor employees understand that one connection between a wired and unwired networks can make the entire corporate network as vulnerable and open as if they removed the firewall and plugged directly into the Internet. The associated costs can be measured in dollars spent, time of recovery, and the cost of lost or compromised data.

The problem of rapid implementation of a new technology into the corporate infrastructure and consumer market without proper attention to security will be costly for developers, business owners, and consumers. This may be the experience that focuses business efforts into considering security during the design process, rather than expecting enterprise owners and consumers to apply security successfully and cost-effectively after products are deployed.

Security Knowledge and Skills Are Inadequate
The lack of security knowledge and skills available in the market affect many participants in the wireless chain—users, owners, managers, content providers, service providers, and manufacturers. This lack of knowledge affects the way standards are written, products are developed, networks are deployed, and wireless applications are implemented.

Sufficient knowledge of security is lacking in design process
Business developers, product and service vendors, and standards bodies alike fail to include security in all aspects of development and planning. Security concerns are not addressed in the early stages of product design—when standards for the product or service are developed. Standards bodies often neglect to bring security expertise to the creation and review of standards. Engineers with insufficient knowledge in security are frequently forced to design products for networks, service providers, and wireless devices.

Companies that do recognize the need for significant levels of security in wireless technology (and not all do) express difficulty finding and hiring experienced security talent to analyze their risk and manage their wireless rollouts. Very few degreed programs exist to educate specialists in information security and assurance. There also are few software engineering programs that place emphasis on security in design and development.

The development of security for the Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 for wireless LAN protocol suffered from a lack of qualified security expertise. In an August 2001 attack, personnel at AT&T Laboratories proved that it took less then one week and $100 to recover the encryption key on a production network, concluding that it was the poor implementation

of reasonably secure technologies that was responsible for protocol weaknesses. Cryptographers were not involved in its design and, as a result, weak encryption and key exchange algorithms were adopted that did not meet appropriate security requirements.

Organizations deploying wireless networks are unaware or ignoring the risks

The New York Electronic Crimes Task Force (NYECTF) recently ran a scan to determine the level of security on wireless networks in the Manhattan financial district. While some networks did have appropriate security measures, 50 percent of all the wireless networks were completely unprotected, providing full access to anyone. Networks often are left unprotected when wireless vendors deliver products with default settings that repeatedly and automatically broadcast service set identifier (SSID), if businesses do not assign trained personnel to evaluate and manage the wireless deployments, and when uneducated employees install rogue access points. If the wrong people are allowed to make security decisions, then the entire organization is at risk.

Information security is not recognized as an area of specialty

Expertise in information security and assurance requires a breadth of knowledge beyond that which is available in training classes that build computing or programming skills. Broader knowledge is required to evaluate risk, develop security models, and build security architectures.

Evaluating security expertise is equally difficult because the industry does not have a shared body of knowledge or a common method by which to qualify security expertise. Security experts must possess the experience and knowledge necessary to apply scientific rigor to security solutions. Scientific approaches are needed to bring discipline and metrics into the evaluation process when determining the validity of security methods. Knowledgeable and skilled professionals are essential to developing the appropriate processes and human resources to identify, quantify, communicate, and mitigate the increased risks of the wireless world. Business and government leaders can play a crucial role in encouraging the education and professionalism of security experts by increasing the demand for security specialists whose primary focus is information security and assurance. In addition, strong emphasis must be placed on improving the security skills of those practicing system management, network and software engineering, and product development.

IV. Road Mapping Security in the Wireless World

This roadmap recommends several actions that will lead to the desired destination: a safer wireless world. The 2002 Accenture / CERIAS Security Visionary Roundtable participants provided direction in four key areas—design, delivery, research, and education—articulating where stakeholders must focus their energies to develop short- and long-term solutions. The four recommended directions—improve the design process, enhance the delivery and deployment process, increase investment in scientific research, and educate all players in the wireless chain—are discussed in detail below.

The four critical recommendations are not intended to represent an all-inclusive list, but they do describe several paths that experts believe will lead to a safer wireless world. Many recommendations, identified as a critical action to improve wireless security, can apply in many other security environments. This roadmap provides a framework for setting direction and generating dialogue among those who wish to embrace wireless but recognize the need to understand the security challenges.

Complexity of technology, market forces, and lack of security expertise present obstacles in this roadmap that can be overcome with a security approach that focuses on simplification, understanding of true costs and risks, and improved education and awareness among all segments of the population. Many of the proposed actions deliberately recognize and address these pervasive issues.

In addition to the primary set of recommendations, the Roundtable experts also debated several additional concepts and concerns. These items ultimately were not supported as key recommendations by the entire Roundtable, but are discussed briefly in Appendix B.

Improve Design and Development Process

Security Focus: Improve the design and development process to achieve simplicity, secure interoperability and transparency.

The discussions among the Roundtable experts focused very heavily on design and development, resulting in the identification of the following primary concerns:

- Simplicity is the key to security. Complicated solutions only increase the risk of weaknesses to be exploited.
- Interoperability is crucial to reduce the costs of add-on security and increase the opportunity to develop a seam less 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 following actions prescribe a design and development process that incorporates security early and reduces costs for all players over time. Manufacturers can decrease the need to reengineer after security problems are discovered; business owners can reduce the costs of add-on security, incident response, insurance, loss replacement, liability, etc.; and consumers will gain confidence to expand safely into new products and services in the wireless world.

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 standard's development process

- Revamp the process of wireless security standards to ensure that enough security 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 standards process to meet the growing and robust security needs in the wireless arena.

Security should be a fundamental design consideration in standards development with a priority on obtaining broader security expertise. Citing the problems with the 802.11b standard, Roundtable participants agreed that the current process suffers from a lack of prepared security expertise. Good security models exist, but are not always well understood by those assigned to write standards.

Today, partly due to the high expense and time commitment required, most participation in standards creations is by vendors only. Changes are needed in the standards-development process to ensure appropriate expertise from academia, private foundations, independent consultants, and research labs.

One challenge is to find ways to bring independent experts together to help design and review security solutions that actually meet security goals. Suggestions ranged from involving independent experts in standards meetings to the development of nonprofit groups, to be supported by stakeholders such as insurance companies, commercial vendors, and government, that could award funds to worthy security research and applied projects. Other suggestions included the need for standards bodies to examine their bylaws and encourage greater participation by security experts and representatives from commercial vendors.

The participants also addressed the role of government in setting standards. Government bodies are significant consumers of wireless products, which they use for communication-security functions. They also have a strong stake in the need for security assurance in the products and services they purchase. Government involvement and articulation of requirements will ensure that security goals are designed carefully from the beginning, and can meet government and commercial needs.

Design for Ease of Use

Ease-of-use should be the outcome of a good security design, not the trade-off that results in a poor security decision. Roundtable participants disputed the commonly held belief that ease of use and security are mutually exclusive. Instead, they argued that improved ease-of-use actually can promote better security. Participants recognized that, in many cases, security requires a decision for feature enablement. It often is difficult to find and set the security parameters for very common user programs because the settings are not user-friendly. User prompts should be

understood, and the software should enable the appropriate features. 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 a primary goal.

Strive for consistency in security development
As vendors develop new products and services, they should ensure that all development teams are following a similar security model. One very practical and beneficial recommendation is for companies to bring all developers together to communicate and create a common understanding of the role security plays in all development. This could be achieved 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
Roundtable experts suggested the need to improve the security functionality of network base stations, which provide wireless access to corporate networks. Manufacturers should consider adding the following functions to their products: access points with built-in firewalls that have auditing, rate limiting on outgoing SMTP, and logging of wireless packets to Network Forensics Analysis Tool (NFAT).

Enhance the Delivery and Deployment Process
Security Focus: Manufacturers and vendors can improve the products they develop through enhanced delivery and deployment processes to 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.

Create and enable trusted devices
Creating and enabling trusted devices will create an environment on which to build privacy, authentication, integrity, and non-repudiation. Trusted devices, with 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 that ensure secure configurations
Processes must ensure secure configurations and be cognizant of the roles played by the different populations (manufacturer, access provider, consumer). The process also must clarify issues of enforcement and validation. The Roundtable experts emphasized the value of secure configurations as a method to reduce the risks when deploying products and services in the wireless arena.

When debating the costs to manufacturers, Roundtable participants agreed that these guidelines also make business sense. Manufacturers that reduce security risks will differentiate themselves in the market by delivering products with default configuration profiles. Their product and market position will be strengthened when they combine ease of use with default security by creating standardized security profiles (e.g. home, enterprise, hotel, airport) that are easy to install out of the box in a particular environment.

Develop and 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 today. With that audience and need in mind, the Roundtable Experts' discussions resulted in the development of the Best Practice for Deploying Wireless Networks guide as an additional deliverable from the Accenture / CERIAS Security Visionary Roundtable.

The best practice guide provides specific guidelines for use of firewalls, automated tools, and settings for wireless-network cards. This document is included in its entirety in Appendix C. The guide also is available as a separate document on the Accenture website at http://www.accenture.com/securitytrends, and the CERIAS website at, http://www.cerias.purdue.edu/securitytrends.

Increase Investment in Scientific Research
Security Focus: Investment in research is critical to understand, anticipate, and address issues of security.

Institutions must plan to invest in education and research to ensure that neutral and informed organizations continue to explore and discover security issues and solutions that will help build a more secure world. Long-term research

frequently gives way to profit concerns and real-time needs for directors and administrators. 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 where research will provide benefits.

The participants also emphasized the need for good 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 also may provide the impetus to address security earlier in the design phase.

Fund research to produce easily understood metrics for code quality and system security.
Metrics are the basis for forming judgments about the level of quality provided by vendors in the wireless arena. These metrics could lead to the development of tools and methodologies that can be adopted by organizations. The fundamental idea of creating metrics that reflect different aspects of security is crucial and implies some categorization of the elements of security. The metrics need to be small in number so virtually everyone from the average consumer to the knowledgeable expert can understand and compare them. The major software vendors must agree on these to provide a quality-assurance program respected by the masses.

The metrics provide a means of comparing and examining the capabilities of systems. Coding would provide a means for the consumer to understand the collection of information on a gross scale. Systems also need to be evaluated within the environment under which they operate. We need a better way to characterize different network topologies and assign security risks associated with each. A network without any wireless and managed by a professional information technology staff trained in intrusion detection has very different characteristics than an unmanaged home network based on wireless. A platform based on widely available open operating systems has different characteristics than a closed device (e.g., basic cell phone).

Fund research to produce metrics for trust, risk, and ease of use.
Security must be built on sound mathematical principles to quantify risk. 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 but critical problems. The first step is to create a process capable of collecting data of sufficient clarity. With this, there are both legal and privacy issues to overcome. By working with service providers in telecommunications, who already come together under a pledge of trust and confidentiality, security experts can share events to help the entire industry. Current laws would need to be reviewed and appropriately modified to allow this sector to share data anonymously with the research community for purposes of building metrics.

The U.S. National Science Foundation (NSF) would be a likely funding source for this type of research. Respected members of the research community must step forward to begin a dialogue about ways to solve this problem. Good metrics will lead to service levels and service-level agreements.

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 would help provide a model for the industry to use when developing secure applications and networks. The participants considered (but did not universally support) such a model that provides for authentication end-to-end.

This model assumed trusted devices as the communication end points. It 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. The device needs to know it is really you, and you need to know it is your device. Physical possession of the device is not sufficient. Further research also 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, research is needed to understand more about achieving service levels and service-level agreements that would make this work. In the other areas, solutions exist but need to be implemented.

Educate All Players in the Wireless Chain
Security Focus: Provide appropriate levels of security education for each player in the wireless chain.

The stakeholders in wireless include users, owners, managers, content providers, service providers, and manufacturers. These players need to understand their risk and obligation, relying upon security experts to evaluate and articulate these issues. The education of all players starts with the educating 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 personal privacy or safety.

Support notion of security as a distinct profession
Today there is a demand for security knowledge, but there is no common understanding about what qualifies an expert. Decision makers are hiring experts with limited experience, driven by a tendency to believe there is no need for specialists to fix the problem. People are self-certifying based on limited reading in narrow areas. With no common standard of due care, no reliable method exists to judge or determine the value of advice being offered by "security professionals."

Security must be elevated to the level of a profession, different from related technical fields, with well-recognized and supported qualifications. An effort needs to be initiated to define the discipline, including common terms, knowledge, and skills needed. Degrees and exams should be developed to define and test a standard of excellence. The discipline should recognize that skill sets are not only technical, but also include business skills, communication skills, and legal skills.

The regulatory and insurance bodies could participate by requiring that a set of minimum skills be required to provide advice. Government agencies and new laws could support educational and professional opportunities to encourage people to pursue this profession. Organizations need to differentiate IT professionals from security professionals and give more credence and weight to security skills and certification.

Teach security in all disciplines at universities
Universities should require coursework in security and assurance before conferring any information technology, engineering, or software development degree, exactly as they require a minimal level of math background for these disciplines. Security problems occur in all types of applications. For example, coders who are ignorant of basic security issues cannot prevent vulnerabilities. The new generation of wireless products and services will require enhanced knowledge of security to ensure secure end devices and secure transactions. In addition, business school, law schools, and medical schools should incorporate some aspect of security awareness in their curricula. Business owners, lawyers, and doctors will find themselves involved at some level in ensuring security and privacy of their customers and stakeholders.

Develop programs to increase level of awareness of security responsibilities in wireless world
Consumers need to understand how their actions put them at risk, and how they can take positive steps to reduce risk. Just as health education informs people about behaviors that prolong health and life, security education could inform people about behaviors that extend their rights to privacy and protection from malicious activities on their personal

computing devices. Consumers need to be informed about risks and encouraged to purchase appropriately secure machines and activities. Government and industry support, possibly even from the insurance and financial services industries, would be needed to develop a broad and useful security awareness campaign.

Summary

The Wireless Security Roundtable covered a broad range of issues related to wireless security. The participants reviewed current questions and concerns, and drew upon their expertise to anticipate future issues that will be faced by all players in the wireless arena: enterprises, consumers, suppliers, and government.

By using the principle findings of this and other Accenture / CERIAS Security Visionary Roundtables, the experts articulated guidelines to address the three major challenges—complexity, market forces, and lack of security skills—that impact the ability to address the primary problems of wireless. The 2002 Roundtable recommendations focused on several actions that can be taken to improve design and deployment, and identified areas that require 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 help realize the benefits by protecting valuable resources amid untethered communication.

Appendix A:

Biographies of Accenture / CERIAS Security Visionary Roundtable Participants

William Arbaugh, Ph.D., University of Maryland
William Arbaugh is a member of the Computer Science faculty at the University of Maryland, where his research interests include information-systems security and privacy, with a focus on wireless networking, embedded systems, and configuration management. He also currently serves on the editorial board of IEEE Computer, where he edits a bimonthly column on information security. Prof. Arbaugh spent 16 years with the U.S. Department of Defense. In his previous position he served as a senior technical advisor conducting advanced networking research and engineering.

David K. Black (Roundtable Facilitator), Accenture
David Black is a security technologies specialty manager with Accenture. He has more than 17 years of experience in computer technology and information security. Black is well known for his work at the National Computer Security Center (NCSC), where he contributed to the Center's in-depth analysis of commercial software offerings, including CA-ACF2, Novell Netware and Windows NT. Currently, Black's work is focused on wireless security solutions, secure Web-portal architectures, and risk-assessment methodology.

Jesse Bowen, Ph.D., Accenture
Jesse Bowen is the global lead for Accenture's enterprise security management offering, and focuses on assessment, design and deployment of security architectures for organizations in several industries. Jesse has also helped clients with planning and implementation efforts through workshops and consulting projects to achieve regulatory compliance with security and privacy requirements, such as the federal Health Insurance Portability Act (HIPA)information standards and the Food and Drug Administration CFR 21 Part 11 electronic signature standards.

Chris Briglin, Nokia
Chris Briglin is Director of Strategic Alliances, Americas. In this role, Chris is responsible for business development activities with key industry players related to Nokia's mobile terminal software solutions. Chris is also responsible for promoting the Open Mobile Architecture Initiative, which will stimulate innovation and freedom of choice for consumers, and will enable an open global market for the next generation of mobile services. Chris joined Nokia in 1994 and has held management positions in sales and marketing, including head of global marketing for Nokia's GPRS Business Program.

John Clark, Accenture
John Clark founded and currently leads Accenture's Global Security Technologies Specialty. He co-authored Netcentric Computing, a book that provides visionary and pragmatic direction to information technology professionals moving to Web-based systems. In addition to providing consulting services to Accenture clients, Clark is responsible for developing and executing the business plan for the company's security practice, defining security market offerings, creating and overseeing go-to-market alliances, and directing all Accenture research and investments in the security area.

Michael Cockrill, Qpass
Michael was the fifth employee at Qpass and as Vice President of Product, led the engineering, development, and design teams that created the Qpass service. Prior to joining Qpass, Michael spent nine years at Microsoft, where he led product management on the Microsoft Network's original e-commerce efforts, and client strategy for Microsoft Merchant Server and Commerce Server.

David J. Farber, Ph.D., University of Pennsylvania
David Farber is the Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania, and he holds appointments in the Departments of Computer Science and Electrical Engineering. He was one of the principals in the creation and implementation of CSNet, NSFNet, BITNET II, and CREN. His background includes positions at Bell Labs, the Rand Corp, Xerox Data Systems, University of California—Irvine and the University of Delaware. He is a member of the U.S. Presidential Advisory Committee of Information Technology. In addition, he is a Fellow of the IEEE and serves on the Board of Directors of both the Electronic Frontier Foundation and the Internet Society.

Joseph Ferra, Fidelity e Business

Joseph Ferra is chief wireless officer of Fidelity e Business (FeB), a division of Fidelity Investments. In his current role, Ferra is responsible for the overall product management and business development of Fidelity Anywhere, a service enabling wireless access to personalized investment information and trading via a number of wireless devices, including two-way pagers, Internet enabled mobile phones, PDAs), and the OnStar in-vehicle information system. Before joining Fidelity, he was with Drexel Burnham Lambert in New York, and previous to that was a second vice president with Smith Barney in New York.

Russell Flowers, National Security Agency

Mr. Flowers is currently the Chief of the Secure End-User Technologies Office (V3) in the Information Assurance Solutions Group at the National Security Agency. He is also the Senior Executive Account Manager (SEAM) for U.S. Central Command and U.S. Special Operations Command. Mr. Flowers has more than 30 years of information systems security experience, including design, engineering, program management, and management roles on a wide range of tactical, strategic, and defensive information operations initiatives. In 1996 he was on a Brookings Institute Legislative Fellowship with U.S. Congressman Jack Kingston of Georgia.

Simson Garfinkel, Sandstorm Enterprises

Simson Garfinkel is Chief Technology Officer at Sandstorm Enterprises, a computer security company that develops offensive information-warfare tools used to probe the security of computer systems and test defenses. As a journalist and author, he is a regular columnist for Technology Review Magazine, was a founding contributor to Wired magazine, and has written articles for numerous publications including ComputerWorld and Forbes. Garfinkel is the author or co-author of 10 books, including, Database Nation: The Death of Privacy in the 21st Century and Web Security, Privacy and Commerce.

Russell Housley, RSA Laboratories

Mr. Housley is a Senior Consulting Architect at RSA Laboratories and coauthor of Planning for PKI, . He has more than 20 years of communications and computer security experience. His expertise is in security protocols, system engineering, system security architectures, and product definition. He is the chairman of the IETF S/MIME Working Group. He contributes to the development of security standards (ANSI X9F) for the financial industry and is currently working with IEEE 802.11 on security for wireless LANs.

J.F. Mergen, Genuity

John-Francis Mergen is the Vice President - Chief Information Officer and Chief Security Officer for Genuity, an Internet infrastructure services provider offering an eBusiness Network Platform. As CIO, Mergen led massive changes in the Internet service provider and hosting market. Mergen has more than 15 years of experience managing information technology infrastructures and systems security for various companies and organizations, including SAIC, BBN, General Electric Information Systems, and Alex Brown & Sons.

Avi Rubin, Ph.D., AT&T Labs

Dr. Avi Rubin is Principal Researcher at AT&T Labs and a member of the board of directors of USENIX. Rubin is the author of two books on computer security: White-Hat Security Arsenal (Addison Wesley, 2001) and Web Security Sourcebook (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is the author of dozens of refereed conference and journal papers, and co-authored two chapters of Peer-to-Peer (O'Reilly, 2001). Rubin is a member of the research team that was the first to demonstrate a serious flaw in the 802.11 Wired Equivalent Privacy protocol standard.

Richard P. Salgado, J.D., U.S. Department of Justice

Richard P. Salgado is Senior Counsel with the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice. Mr. Salgado specializes in investigating and prosecuting computer network cases and technology-driven privacy crimes. He participates in policy development for emerging issues, including the growth of wireless networks, voice-over Internet protocol, surveillance tools, and forensic techniques. Mr. Salgado is an adjunct law professor at Georgetown University Law Center, where he teaches a Computer Crime seminar, and is a faculty member of the SANS Institute.

Richard Siber, Accenture

Richard Siber is a partner in Accenture's Communications & High Tech practice focused on managing worldwide wireless communications efforts. He provides a broad range of marketing, strategic, and industry-oriented consulting services to carriers, equipment vendors, and content providers in the wireless industry. His 17 years of wireless expertise cuts across all wireless technologies, including cellular, PCS, paging, mobile data, wireless LAN, wireless PBX, wireless local loop, and satellite. Richard is a frequent industry speaker and has chaired, moderated or spoken at more than 250 wireless conferences worldwide.

Eugene H. Spafford, Ph.D., Purdue University

Eugene H. Spafford is a professor of Computer Sciences at Purdue University and is Director of the Center for Education and Research in Information Assurance and Security (CERIAS). He has published more than 100 articles and reports on his research, has written or contributed to over a dozen books, and he serves on the editorial boards of most major information security -related journals. Dr. Spafford is a Fellow of the ACM, Fellow of the AAAS, Fellow of the IEEE, and is a charter recipient of the Computer Society's Golden Core award. He is co-chair of the ACM's U.S. Public Policy Committee and of its Advisory Committee on Computing Security, is a member of the Board of Directors of the Computing Research Association, and is a member of the U.S. Air Force Scientific Advisory Board.

Byron Thompson, State Farm Insurance

Byron Thompson is a security analyst at State Farm Insurance in Bloomington, Illinois. He is the team leader for remote access security, and has worked on all major wireless initiatives at State Farm for the past two years. He recently was given an achievement award for securing State Farm's first credit-card implementation. Currently on sabbatical, he is conducting research to define State Farm's long-term strategy for secure pervasive computing.

Jesse R. Walker, Ph.D., Intel

Jesse R. Walker is a network security architect at Intel. Currently, Walker focuses on 802.11, IPsec, and platform security. Walker joined Intel in 1999 as part of the company's acquisition of Shiva, where he was security architect for VPN products. Prior to Shiva, he was with Raptor Systems, where he built firewall and VPN products. He is the technical editor for the IEEE 802.11 security standards.

Parviz Yegani, Ph.D., Cisco Systems

Dr. Yegani, a technical leader of the Mobile Wireless Group at Cisco Systems, is currently engaged in 3G architectures and standards activities. Dr. Yegani chairs the IP-in-the-RAN working group (WG) of the Mobile Wireless Internet Forum, where he is leading an industry-wide effort to define an Internet Protocol-based Open Radio Access Network Architecture. He is also involved in standards activities in TIA, 3GPP2 and IETF, and has served as the chair of the All-IP Ad Hoc group and the vice chair of the 3G access Network architecture working group in 3GPP2 TSG-A subcommittee. Dr. Yegani has worked for Ericsson, Qualcomm, and IBM. He has held faculty positions at the State University of New York and Michigan State University.

Appendix B:

Additional Items of Discussion

The participants debated several additional recommendations that were not broadly supported. Nevertheless, these deserve mentioning as items of discussion in a forum with such diverse representation of the stakeholders in the wireless arena. These ideas were developed in small group breakout sessions and proposed to the full group. After discussion and priority voting, these items did not achieve strong consensus as primary recommendations among the participants.

Encourage consumers to begin to hold vendors accountable for faulty development and inclusion of known security vulnerabilities. Encourage vendors to develop securely and stand behind their products. In particular, take stands against laws that allow vendors to shield themselves from liability by license. Arguments for this position stated that product liability is necessary to hold vendors accountable and provide motivation for building security into products. Arguments against stated that product liability could kill the market and new entrants, thereby discouraging innovation.

Identify an organization to develop a common-criteria profile for wireless systems. Arguments for this position stated this would help develop protection profiles that deliver end performance result, and independent labs could validate products against the profile. Arguments against stated that common criteria for a wireless system would not provide all the benefits expected. Because a wireless system is part of a larger system, and composing larger systems from evaluated components is far from simple, a higher-level system must be profiled. Other arguments recognized that common-criteria certification is very expensive for small companies.

Encourage a government organization (e.g. NIST in the United States), to spearhead an effort to create a metastandard involving all stakeholders in wireless, including government (law enforcement, emergency response, defense departments, state government, transportation), academia, vendors, content providers, service providers, business entities, and consumers. Arguments for this position stated this would articulate common security and interoperability issues that could guide development of future standards in specific layers. Arguments against expressed concern with the difficulty in focusing only on wireless and in cross-engaging other network standards groups such that the metastandard has some context and relationship with commercial technology and de-facto standards.

Encourage standard-making bodies to use an abstraction approach for interim design. Design new standards from scratch and design a wrapper for transition. In the 3G approach to security, improve simplicity. Arguments for this position stated that new standards developed from scratch could focus more on good solutions and less on interoperability with old standards. The wrapper approach would include an explicit transition plan for development. Arguments against this position stated that development of two-track standards would increase the time needed to develop standards.

Provide the research needed to allow law enforcement and national security the access they need without degrading authentication. Arguments for this position stated the need to ensure that law enforcement has needed access, but that inhibits corrupt or misguided agents from abusing power. Research is necessary to ensure careful, thoughtful execution rather that settling for a hasty, last-minute edict. Concerns with this approach were that it should not deter the export of technology and systems, and that system abuses could be prevented so that people would not distrust the overall system.

Address quality-of-life concerns about physical health, impact on lifestyle, and using devices in unsafe places. The breakout group identified several possible actions, such as research into health effects, laws that enforce hands-free technology, cell phones integrated into autos, passive detection of use of wireless technologies in sensitive areas, and active counter-measures such as remote turn-off and jamming. Although this topic was recognized as an interesting problem, the group did not support further action on these ideas because they were considered out-of-scope for wireless security experts.

Appendix C:

Best Practices for Deploying Wireless Networks

Introduction

The May 2002 Security Visionary Roundtable created a unique opportunity for 18 leading security experts and researchers from the world of technology, business and government to meet to explore the challenges of wireless and develop a roadmap for a safer wireless world. These prominent individuals were invited to participate in a Security Visionary Roundtable sponsored by Accenture and Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS).

The experts developed a set of guidelines during the Security Roundtable that charted one path in this roadmap to safety — the path to improved security when deploying wireless networks. Many large and small enterprises are investing in wireless LANs to meet the goals of reduced costs, improved productivity, and increased flexibility. Recent reports of major security flaws should cause all of these organizations to pause and consider the unexpected risks.

The protocol for wireless LANs and end device products most in use in the United States is based on the IEEE 802.11b standard, also referred to as WiFi. Wireless vendors have developed and are marketing products that meet the standard for security. Unfortunately, the standard is flawed, and the security mechanisms used to support the standard perpetuate these flaws. Therefore, the products do not meet security goals, and all wireless networks based on this standard are at risk of providing unauthorized use of private networks through wireless access points. Several papers, cited in the reference section at the end of this document, provide detailed analysis of the flaws and demonstrate how easily and inexpensively these flaws can be exploited.

Wireless networks and handheld devices present several risks to organizations. NIST is releasing a Special Publication, 800-48, Wireless Network Security, http://csrc.nist.gov, that identifies the following list of specific threats and vulnerabilities to wireless networks and handheld devices. The Roundtable participants derived a similar list and fully endorse the use of NIST's list of vulnerabilities and approach to evaluating the threats of wireless technologies.

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users, and masquerade on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activity.
- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

Best Practice Guidelines for Wireless Networks

Security best practices can help mitigate the risks when deploying wireless networks. The use of these guidelines will improve the security of wireless LANs and the safety of wireless devices connecting to enterprise networks, whether using 802.11b or other network protocols. Organizations should continue to review and implement security best practices as a reasonable measure against unknown and future flaws and exploits.

The following guidelines are intended to cover a range of actions that can be taken today by organizations to reduce the risk of compromise when deploying current wireless networks. Keep in mind that these guidelines are not foolproof, and a determined attacker with the appropriate tools can defeat most current security measures. Furthermore, such tools are becoming increasingly available to less sophisticated attackers. The best defense for highly sensitive data is to avoid wireless networks entirely.

As organizations evaluate and determine their approach, administrators and security specialists should make decisions based on their particular organization and situation, the value of the resources they are protecting, the level of threat to which they are exposed, and a clear understanding of the ever-changing risks. The level of threat changes over time, and additional actions may be required as new threats are discovered.

1 Determine and illustrate the magnitude of the problem. Survey employees to determine their current and projected use of personal devices, as well as business plans for deploying mobile services. Include awareness questions to discover employees' level of attention to security. Employ automated tools to discover rogue access points and to illustrate security weaknesses in the current network. This information should help develop a risk assessment, identifying the level of security required and communicating the urgency of the problem to management.

2 Develop a security strategy that treats all wireless connections as Internet connections. This implies placing all wireless connections outside the firewall, or minimally on separate network segments to keep arbitrary protocols from being inserted into internal networks and to restrict traffic from wireless networks to the world at large. It also implies a monitoring policy to search for policy violations, access points installed directly on internal LANs. Develop requirements for the use of VPNs from mobile endpoints to authenticate trusted users and to protect against eavesdropping when communicating between the unsecured wireless access points and the internal network.
a) Install firewalls between wireless networks and wired networks. The firewall gateway is already equipped to manage traffic and

authenticate users coming from untrusted networks.
b) Install VPNs between trusted clients and trusted network gateways. VPNs help isolate traffic from untrusted locations until they can authenticate at a trusted gateway. In addition, they can encrypt traffic, protecting both confidentiality and integrity of information in transit. Many companies already have implemented VPNs for remote users accessing the protected network from the Internet.

3 Develop and communicate an employee wireless policy. Communicate employees' personal responsibility toward security. Educate them on appropriate behaviors and practices to protect the information they access and control.
a) Use only the company's standard wireless hardware. Identify and communicate company-wide standards for wireless hardware. Issue standard configuration instructions and test routinely for compliance.
b) Require personal firewalls on all computers connecting to wireless networks. Personal firewalls are needed to thwart attacks from unsecured and potentially hostile networks. Users should regularly monitor firewall logs to detect attacks and report unusual situations. Review and update this policy when personal firewall technology is available for wireless devices.
c) Require real-time virus scanning on all computers connecting to wireless networks and on mobile devices, if available. Real-time virus scanning should be enabled and monitored on all computers connecting to wireless networks. As virus-scanning features become available for mobile devices, they should be enabled and monitored.
d) Turn off drive sharing when accessing networks outside company boundaries. Consider writing a small application to alert employees when they are no longer connected to the home net. The application could ask them to close drives or applications with open ports, or it could execute these functions for them automatically.
e) Prohibit adding access points to the network. A major exposure is caused by employees who buy their own access points and plug them into the network as a rogue beacon for any wireless connectivity. Make it clear to all employees that this is a serious policy violation and could be cause for dismissal. If internal organizations are allowed to implement a wireless LAN, require approval by a central organization.
f) Regulate use of personal devices with internal systems. Identify criteria used to determine which mobile products and services will be supported by the enterprise, and expectations for version control and updates. Communicate this information to employees, along with guidelines for other unsupported mobile services. Deliver guidelines that emphasize the use of security features for proper authentication and protection of confidentiality. Test and recommend off-the-shelf products, such as encryption software, that are designed to improve security. Encourage frequent data backups, and communicate policy on improper storage or transmitting of corporate data.
g) Provide wireless-awareness training. Raise the level of awareness regarding the dangers of communicating, via voice or data, in public places, or from home networks. Communicate appropriate prevention and response for loss or theft of devices. Emphasize the need to password-protect and use encryption on mobile devices that contain critical company information.

4 Develop default configurations when installing wireless network access points. Implement the security features available in wireless network products. For 802.11b networks specifically, the following actions are relatively low-cost methods that increase the work factor for a casual attacker. These actions are not effective against a determined or sophisticated attack, as a little technical knowledge can overcome most of these measures.
a) Determine policy for naming the SSID. The service set identifier is a unique identifier associated with an access point or group of access points. Creating a unique SSID for base stations would require configuring clients with this unique SSID so they can find the network. Clients that attach to the network from multiple locations might need to know multiple SSIDs.
b) Disable the feature that broadcasts SSID to any clients who ask. This will reduce, but not eliminate, the ability for anyone to find the network. Someone with the appropriate technical sophistication can overcome this feature. In addition, the secret of the SSID is hard to keep when the population using that SSID is very large.
c) Use the unique MAC addresses of the clients to create an access allow list on the base station. This action is effective only against the least sophisticated attacker. This is not practical for situations with large numbers of clients or a high need for mobility.
d) Implement 128-bit encryption in Wired Equivalent Privacy (WEP). Change the keys frequently. Recognize

that tools exist to easily break this encryption, but it still provides protection from the lowest-level attackers. This action defends against casual hackers only and deflects them to sites that have not enabled WEP at all.

5 Deploy antennas designed to limit signal radiation to the desired coverage area. Omni-directional antennas should be used with care, and their radiation in the vertical plane should be taken into account. For example, instead of simple dipole antennas, collinear arrays, or other antenna designs may help limit signal strength on floors above and below the intended network area in multistory office buildings. Directional antennas, such as patch designs, can be used to limit radiation outside of buildings and help prevent interception in parking lots, surrounding streets, or adjacent buildings. Access point signal radiation can be measured with field-strength instruments, and the coverage area should be tested before production deployment of a wireless network.

6 Improve physical security of base stations. Ensure that network access points acting as base stations are not subject to tampering that could modify their configuration. When physical location in a secure room is impractical, consider adding a tamper-proof device with an audio alarm.

7 Test for Compliance. Use automated tools and physical checks to test for unknown networks. Spot check to determine if access control and encryption features are properly configured in base stations. Perform periodic audits on employee computers and personal devices to verify compliance with security policy. Inventory software running on mobile platforms to look for software that increases overall vulnerability. Review all servers that interface with mobile devices to ensure correct configuration. Run network forensic analysis tools to monitor traffic flow in and out. Conduct security audits and troubleshoot network security issues with network analyzer tools such as netstumbler (http://www.netstumbler.com). Review NIST Draft Special Publication 800-42, Guidelines on Network Security Testing (http://csrc.nist.gov).

8 Use Higher-level Security Mechanisms. Where possible, use other security mechanisms in other layers of the Internet Protocol stack, such as IPsec or Secure Sockets Layer (SSL). Consider the use of strong authentication, rather than simple passwords, to authenticate the user to the mobile device. Look for products that support the use of a RADIUS server for external authentication where access to the LAN now requires an account on the server plus the SSID and encryption key. Look for products that provide for mid-session re-authentication, inhibiting the hacker's ability to "sniff" packets and crack session keys. Review and enable security features in application servers and clients. Investigate potential for digital signatures and Public Key Infrastructure (PKI), especially with applications that involve financial transactions.

9 Emphasize the need for additional security requirements to manufacturers. Communicate to vendors that security is a priority in your networks.
a) Request access points that have built-in firewalls that allow for auditing, rate-limiting on outgoing SMTP and other connections, and logging of all wireless packets to an NFAT.
b) Ask manufacturers to develop a set of default configurations based on standard security policy for home or enterprise.
c) Indicate your interest in management tools, using RADIUS or other protocols, to manage wireless connections centrally with greater ease.

10 Continue to monitor issues of wireless security. Threats change as new attacks and vulnerabilities are discovered. Organizations need to evaluate and assess issues continually and adopt new best practices as necessary.

Appendix D:

Wireless Security Resources

Accenture / CERIAS Roundtables
<http://www.accenture.com/securitytrends>
<http://www.cerias.purdue.edu/securitytrends>

NIST Draft Special Publication 800-48
Wireless Network Security, release date-2002
<http://csrc.nist.gov>

NIST Draft Special Publication 800-42
Guidelines on Network Security Testing,
< http://csrc.nist.gov>

Helpful in identifying some of the pertinent legal doctrines that apply to vulnerability assessment, intrusion detection, wiretapping, hacking and other security-related issues.
<http://www.cybercrime.gov>

Papers on 802.11b Security Risks
CERIAS papers on wireless security
<https://www.cerias.purdue.edu/papers/archive/2002-17.pdf>

Includes papers written by Roundtable attendee, William Arbaugh, University of Maryland.
<http://www.cs.umd.edu/~waa/wireless.html>

Includes white papers written by Roundtable attendee, Jesse Walker, Intel.
<http://www.intel.com/ids/security>

Report that describes an attack to break WEP, by Adam Stubblefield,
Avi Rubin (Roundtable attendee), John Ioannidis
<http://www.cs.rice.edu/~astubble/wep>

Wireless security Webcast by Russ Housley, RSA Security, Roundtable attendee.
<http://www.rsasecurity.com/solutions/wireless>

Includes background information on the IEEE 802.b standard and discussion on the security issues. Includes links to papers that describe security threats in detail.
<http://www.cisco.com/warp/public/759/ipj_5-1/ipj_5-1_ieee_80211.html>

Short tutorial on configuring basic 802.11 security features
<http://www.dell.com/us/en/arm/topics/vectors_2001-wireless_security.htm>

White paper on wireless 802.11 security in a corporate environment; offers tips for deploying VPNs for wireless security.
<http://www.intel.com/ebusiness/products/related_mobile/wp012602.htm>

Article describing one corporation's approach to secure wireless – product selection and secure configurations.
<http://computerworld.com/securitytopics/security/story/0,10801,71448,00.html>

News Reports and Journals

<http://www.forbes.com/2001/05/22/0522wireless.html>

<http://news.com.com/2100-1033-898779.html>

<http://www.sbq.com/sbq/wireless>

<http://www.pcworld.com/news/article/0,aid,40442,00.asp>

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>

