accenture

Innovation delivered.

Roadmap to a Safer Wireless World

Best Practices

• Consulting • Technology • Outsourcing • Alliances

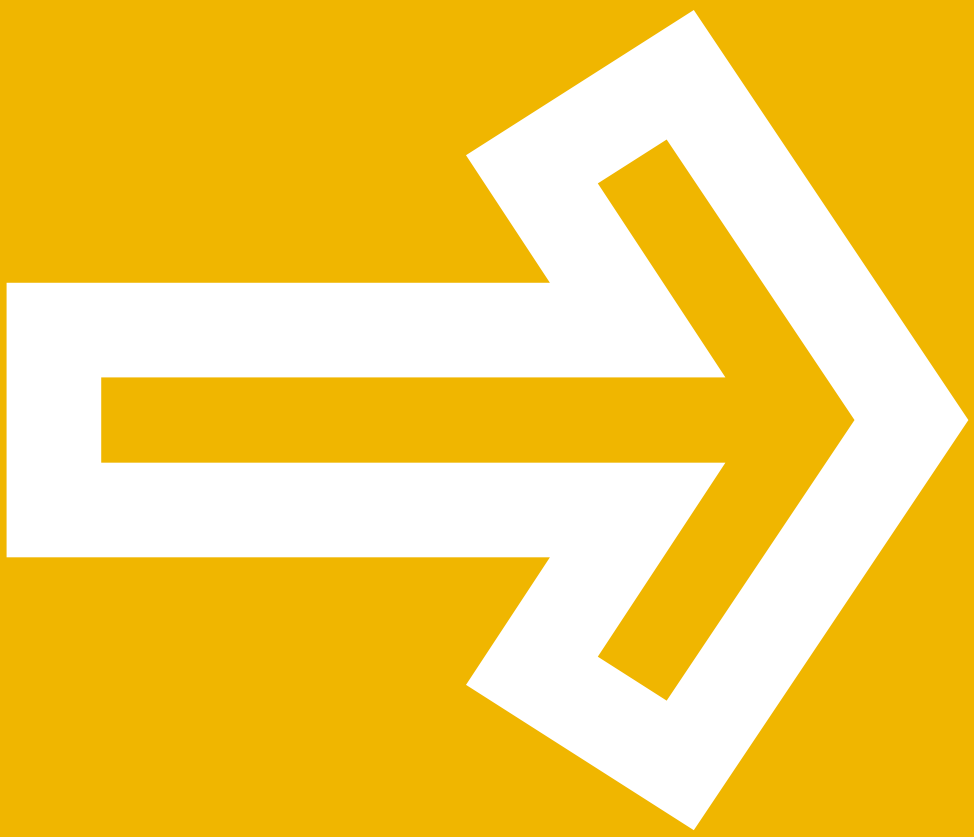
Best Practices for Deploying Wireless Networks

2002 Security Visionary Roundtable

Jointly Sponsored by:

Accenture

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



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.

Wireless Network Security Guidelines

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.

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>

Roundtable Roster

William Arbaugh, Ph.D., University of Maryland
David K. Black, Accenture
Jesse Bowen, Ph.D., Accenture
Chris Briglin, Nokia
John Clark, Accenture
Michael Cockrill, Qpass
David J. Farber, Ph.D., University of Pennsylvania
Joseph Ferra, Fidelity e Business
Russell Flowers, National Security Agency
Simson Garfinkel, Sandstorm Enterprises
Russell Housley, RSA Laboratories
J.F. Mergen, Genuity
Avi Rubin, Ph.D., AT&T Labs
Richard P. Salgado, J.D., U.S. Department of Justice
Richard Siber, Accenture
Eugene H. Spafford, Ph.D., Purdue University
Byron Thompson, State Farm Insurance
Jesse R. Walker, Ph.D., Intel
Parviz Yegani, Ph.D., Cisco Systems

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.

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>