Global Information Assurance Certification Paper

An Initial Look at Audit & Control of Wireless Networks
Toni Dunning
2 January 2003

ABSTRACT
The material that follows is submitted as completion of the Practical assignment in partial fulfillment of the GSEC certification. The case study chronicles a technology auditor's information gathering, assessment, and high level control suggestions that were developed during an initial audit of "Wireless Networks" as portrayed in a hypothetical Company.

The environment described in the case study and the opinions rendered by the writer belong to the writer alone and do not represent those of colleagues or firms with whom the writer is or has been affiliated.

Special thanks to Janet Zhu for her assistance in gathering and assembling some of the preliminary resources required for completion of the analysis and case study that follows.

INTRODUCTION
During the last several months I've become increasingly aware of the proliferation and deployment of various types wireless technologies and the profound and sometimes subtle impact of wireless components on individuals, corporations, and government. Various aspects of wireless technology are topics of frequent discussion in trade, technical, and professional publications as well as government, legal, and regulatory pronouncements. But the catalyst for familiarization with the benefits and risks affiliated with wireless technology was direct: it was the Technology Audit Plan. The Technology Audit Plan simply called for an audit of "Wireless Networks."

Several questions quickly came to mind as I considered the scope of the audit. Mentally I sifted through my standard list of questions that began with: who, when, what, where, why and how and I tried to apply each to "wireless networks." For example:

- Who relies on and supports wireless technology and how is wireless technology controlled?
- When wireless technologies used?
- What risks do wireless technologies present?
- Where are/should wireless devices/components located?
- Why is an audit of "wireless networks" important?
- How are wireless networks defined?

I thought the answers to these questions, would help make the audit of "wireless networks" relevant to the Company. I knew that gathering this background information would require that I draw on resources internal to the Company in addition to external materials and publications. However, I had no means of anticipating how complex and varied the answers would be. The remainder of this paper addresses the previous questions in reverse, chronological order.

How are wireless networks defined?
I initially decided to focus only on wireless technologies that were either in use or planned for use in the immediate future so I interviewed members of the engineering, development, and emerging technologies staffs. The Company's emerging technology function based in Information Services (IS) evaluates and tests new technology and shares results with the development and engineering teams.

It was not surprising to learn that the engineering and technical staffs were among the primary users of wireless technology. However, it was interesting to observe that everyone that I spoke with struggled as much as I did when attempting to define "wireless networks." We easily agreed that an 802.11 wireless local area network (WLAN) and supporting devices could easily comprise a "wireless network." We also readily acknowledged that BlackBerry Personal Digital Assistants (PDA) have wireless capabilities. Then someone mentioned the cell phones which might have

web-browsing and/or email capability. Finally, someone mentioned the two-way pagers—which prompted an animated engineer to talk about a new wireless BlackBerry handheld device that combines Nextel® Direct-Connect™ functionality together with web-browsing, wireless access to email, calendars, and contact lists. The conversations demonstrated that wireless devices were plentiful, and likely in use by many colleagues, though they might not be connected to the network. My attempt to limit scope seemed to have stalled, but armed with this new information about the world of wireless devices, I began to research the features, control elements, and regulatory concerns.

Why is an audit of "wireless networks" important?

My research took me took me to a variety of resources. I read vendor literature that described features and functionality of various types of wireless devices as well as technical, trade, and regulatory documents that cited diverse vulnerabilities and risks. Some of the results of this effort yielded specific risk areas for certain wireless network devices. Specific detail is captured in Appendices A & B and there will be more discussion of how the Appendices were used later in this paper.

Generally, there was agreement among all of the literature that wireless devices and its communications are subject to interception by unintended parties and that such an interception has potential for additional compromise. Exactly what is at risk for a particular wireless device must consider the device type and capabilities as well as the physical and logical environment.

Regulatory concerns surfaced in an FDIC Financial Institution Letter dated February 1, 2002 (FIL-8-2002) with the subject: *Guidance on Managing Risks Associated With Wireless Networks and Wireless Customer Access* spoke directly to the WLAN environment and further stated, "wireless internet access is a standard feature on many new cellular phones and hand-held computers." FIL-8-2002 states, "Common risks include the potential:

- Compromise of customer information and transactions over the wireless network;
- Disruption of wireless service from radio transmissions of other wireless devices;
- Intrusion into the institution's network through wireless network connections; and
- Obsolescence of current systems due to rapidly changing standards. [1]

FIL-8-2002 goes on to say "these risks could ultimately compromise the bank's computer system, potentially causing:

- Financial loss due to execution of unauthorized transactions;
- Disclosure of confidential customer information, resulting in – among other things – identity theft…
- Negative media attention, resulting in harm to the institution's reputation; and
- Loss of customer confidence.[2]

Shortly after FIL-8-2002 was distributed, the Banking Industry Technology Secretariat (BITS) Financial Services Roundtable published a 38 page guidance document, *BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines*, dated March 15, 2002. The document specifically addresses network guidelines, software solution guidelines, and handheld device/mobile terminal guidelines. According to page 3 of the Introduction section, the BITS document:

> Details requirements for the three segments of the technology infrastructure needed for successful implementation of mobile financial service. BITS is making this material available to inform wireless network operators, mobile terminal and handheld device manufacturers, and mobile software solution providers of the standards and business requirements that will need to be met in order for financial services companies to continually improve the level of security of the financial applications they offer to mobile customers, professionals and

> workforce constituencies. In addition to providing guidelines for three mobile industry segments, this document includes general information on mobile applications and on applications networks used by financial services companies to support customer accounts, transactions, and financial services. Financial services companies must implement mobile financial applications in a way that is consistent with their responsibilities as providers of the US critical economic infrastructure. The guidelines are created with this very important role in mind.[3]

I was convinced that an audit of wireless networks was important.

Where are/should wireless devices/components located? What risks do wireless technologies present?
It is commonly known that wireless devices that are connected to a wired network are capable of exposing data on the wired network. To help prevent compromise of data and unauthorized access, proper configuration and logical location of wireless devices in relationship to firewalls, data stores, and data streams is very important. In addition, physical location of access points and antennae must also be addressed because wireless signals may be transmitted beyond the physical perimeter of a structure. Caution should also be exercised in placement of wireless devices, particularly access points, in the event that physical facilities, such as buildings, are shared by unaffiliated firms. In addition, a means of preventing the eventual sabotage should be considered as handheld wireless devices (PDAs, cell phones, two-way pagers, etc.) and their data will most likely eventually fall victim to viruses, Trojans, worms, and/or other malware that could introduce additional risk to data. It should be noted that both the potential for loss and the probability of realizing loss, are functions of the wireless device and network control environment as well as the business processes that depend on device and network reliability.

For this initial audit of "wireless networks" I gathered information required to complete the tables in the appendices focusing primarily on an 802.11b WLAN and centrally-controlled, BlackBerry PDA handhelds. The audit paralleled an 802.11b pilot project that was physically and logically separate from the wired network. The pilot project was successful in familiarizing engineering and development staffs with the technology as well as in identifying minimum requirements should the need for an 802.11b network present itself. The suggested logical control settings in the table at Appendix A were drawn from reviews of a number of publications, some from the SANS Reading Room, and the specific references used are cited within the Appendix.

In addition to the WLAN, PDAs that were centrally managed using the BlackBerry Enterprise Server were also researched and reviewed. The primary research supporting this effort was drawn from BlackBerry publications and resulting suggested minimum control settings were identified and are provided at Appendix B. References are included within the Appendix.

During the audit, I compared and documented the existing configuration with the suggested control settings to determine areas of potential risk completing the Control Environment Settings Observed, Specific Exposure(s), Loss Potential and Loss Probability columns. Completion of the Specific Exposure(s) fields required consideration of the specific control area, the control environment observed, and the nature of use of the wireless device with respect to business processes and function. Loss Potential is a subjective measure of the value that could be lost in the event of compromise. Loss Probability is a subjective measure of the potential for Loss Potential to be realized. Exposures, Loss Potential, and Loss Probability can al be useful in preparation of cost-benefit analyses that may be required to developing, implement, and support control solutions.

When are wireless technologies used?
During my research, I recognized a subtle but disturbing fact: *many wireless devices can be easily and inexpensively acquired, installed and configured, and used—without requiring the involvement of IS.* For example, many of my colleagues and I have personally-supplied wireless

devices, such as PDAs and phones that could be connected to the corporate network, or a network-connected device such as a desktop or notebook PC. In the event any of these devices were ever configured to connect to the wired network, they may contain proprietary or sensitive data. If connected and configured outside IS, there is little assurance that overall network security architecture would be considered as the devices are placed in service. Security of any proprietary data on the device itself would be paramount in the event the device is lost or stolen, and such an event may never be reported to IS if the device was personally-supplied.

In addition, many notebook PCs are delivered with an 802.11b integrated NIC, and those that don't have an integrated NIC, routinely offer a PCMCIA 802.11b NIC. An AirDefense White Paper, *Enterprise Approaches to Detecting Rogue Wireless LANs*, that was published in 2002 states, "In default mode, a wireless-enabled laptop running Microsoft XP automatically searches for an access point with which to connect. Wireless-enabled laptops can pose several security risks from accidental associations with neighboring networks and and-hoc, peer-to-peer networks." [4]

Who relies on and supports wireless technology and how is wireless technology controlled?
Existing standards may allow colleagues to acquire certain Company-supplied wireless devices as needed on a justified basis through IS. However, personally-supplied cell phones, two-way pagers, and handheld use are common at all levels of many organizational structures. In some situations, these devices could be configured and connected to network devices. They may also store, retrieve, or transmit Company data and could be used to either intentionally or unintentionally compromise proprietary data. It is not difficult to see why addressing the issue of personally-supplied devices is complex and this writer's opinion is that more research is needed in this area.

CONCLUSION
While unable to offer a silver-bullet controls solution, oversight that combines the use of monitoring and discovery tools and techniques with effective policies, standards, and business processes should establish and maintain IS ownership and responsibility for the network (wired or otherwise) and all connected devices. This writer believes that IS ownership of the network is vital to ensure data and network resources are available to properly authorized individuals when required to support of the Company business.

If not already in place, monitoring and discovery tools should be evaluated for cost and benefit. Though not tested during this study, it is noted that AirDefense, Inc. has products that may some of these requirements if effectively implemented and supported by staff that are adequately trained.[5]

Perhaps at the highest level of "policy" is a practice that was cited in an audit program that we found: the development and deployment of an Acceptable Use Policy (AUP) for wireless devices. [6] In an ideal world, the AUP specifically expresses the Company's expectations regarding use of wireless devices. It should address:

- Colleague/contractor responsibility and accountability.
- Business and personal use, including devices not supplied by the Company.
- Access to internal and external networks, downloads and file transfers, virus/Trojan protection, and data backup.
- Data ownership, handheld device and data disposition upon termination or transfer of colleague or contractor.

Naturally, an AUP needs to have corresponding support of Human Resources policies. Further, policies that are consistent with the Company culture and support the AUP should define roles and responsibilities for acquisition, development, and security of mobile computing and handheld devices. Collectively, the policies should address:

- Data qualities and characteristics acceptable for handheld access, storage, creation, and transmission including responsibilities for protecting confidential and proprietary data.
- Notifications and approvals required before physical or logical connection to company computing resources.
- Notifications, approvals, and security considerations required for development or implementation initiatives that provide access to applications and/or interfaces using handheld devices.
- Acquisition, configuration, maintenance, and management of handheld devices and their data.
- Use, maintenance, and management of any third-party security products and acceptable configuration.

Finally, security policies, standards and supporting business practices should be in place to ensure consistent and reliable engineering/rollout, configuration management, and change control for all wireless devices.[7]

APPENDIX A
802.11b CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
1	*Wire Equivalent Privacy (WEP)* [8]	In 802.11b, WEP is optional and not implemented by default.	If WEP is not used, network traffic will all be plaintext transmissions.	Implement WEP.				
2	*Wire Equivalent Privacy (WEP)*	The standard implementation of 802.11b WEP is weak and cracking tools that can decrypt WEP traffic (e.g., Airsnort[9] and WEPCrack[10]) are readily available in the public domain.	Network traffic may be "sniffed" and subsequently decrypted, disclosing proprietary data to unauthorized parties. [11], [12]	Implement IPSec with WEP. [13]				
3	*Wire Equivalent Privacy (WEP)*	In 802.11b, WEP relies upon a random 24-bit Initialization Vector (IV) with over 16 million possible values that is transmitted in plaintext with every frame. [14]	Because the IV is transmitted plaintext with each frame of data, there is potential for duplicate keystreams. An attacker can catalog keystreams, and upon detection of a duplicate, derive the underlying pre-shared key allowing decryption.[15]	Implement IPSec with WEP. Also periodically change keys.				

APPENDIX A
802.11b CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
4	*Service Set Identifier (SSID)*	SSIDs, unique identifiers that allow wireless access points and wireless nodes to communicate, are transmitted in plaintext in the header of each packet within the WLAN in 802.11b implementations.[16]	Eavesdroppers may intercept, then spoof SSIDs and gain unauthorized access to data.[17]	The AP should not broadcast the SSID.[18] In addition, the SSID should not entice an eavesdropper by clearly identifying the company name, affiliation, or WLAN purpose.				
5	*Access Points (AP) including servers*	The 802.11b standard provides for shared key authentication, rather than two-way, mutual communication. For example an access point authenticates a user, but because a user cannot authenticate an AP, a rogue AP can be placed on a WLAN.[19]	Rogue APs can be used to launch denial of service attacks and/or for unauthorized access to data available via the WLAN.[20]	Prevent access to the internet via the WLAN and limit internal and sensitive data accessible via WLAN. Achieve mutual authentication through use of Extensible Application Protocol (EAP) in conjunction with a RADIUS server on a wired LAN. Use firewalls that pass traffic only specified ports to limited networks or sub-networks. Actively use intrusion detection & monitoring tools.[21]				

APPENDIX A
802.11b CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
6	*Access Point (AP)*	The 802.11b standard provides for connection through the air using radio signals.[22]	Eavesdropping, interception, and interference are all potential threats to the WLAN data and environment. This may create exposures if APs can be accessed from outside the building (e.g., street) or from locations within company facilities that are leased to other businesses. When an AP is accessible from the street, an eavesdropper can use publicly available utilities such as NetStumbler from a laptop in a vehicle to discover characteristics of the WLAN, including potential decoding of traffic. This technique, commonly known as "war driving," has resulted in publication of the WLAN characteristics, including data that may be deemed proprietary to databases and maps that are accessible to registered users at NetStumbler.com. These conditions may lead to subsequent compromise of the WLAN and/or proprietary data.	Use encryption for network traffic, including authentication. Implement ACLs on all Access Points and disable DHCP. Segment the WLAN from the wired network. Periodically test to ensure Access Points are located where they are free from eavesdropping, interference, or interception. Change factory default Administrative ID and password. [23] Enable a VPN solution to access hosts inside the firewall when accessing the internal network over 802.11. [24] Ensure proper placement and settings for antennae supporting the WLAN.[25] Consider running NetStumbler[26], Nmap, Airsnort, [27]or a freely available wireless sniffing utility to determine what can be discovered,				

APPENDIX A
802.11b CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
7	*Key Management*	WEP uses pre-shared keys as a means of authenticating a device on an 802.11b WLAN. These pre-shared keys are stored on every device on the WLAN to enable WEP encryption/decryption. However, WEP does not specify how keys should be distributed or the frequency of change. [28]	Distribution of static keys increases the likelihood that keys might be discovered. Discovered keys can be used to decrypt traffic that was intended to be private, resulting in unauthorized disclosure of information.	Establish policies, procedures, and standards for key management. Consider distribution of keys via SSL before the required change date & train/require individuals to configure their own keys OR establish a key management standard and make someone responsible for the key management function.				
8	*MAC Addresses*	The 802.11b standard provides capability for restricting access to the WLAN based on MAC (Media Access Control) addresses stored in the AP's Access Control List (ACL). MAC addresses are generally set in Read Only Memory (ROM) on the Network Interface Card (NIC) by the manufacturer. MAC addresses are broadcast in plaintext on the WLAN. [29]	Eavesdroppers may intercept, then spoof MAC addresses and gain unauthorized access to proprietary data.[30]	A combination of MAC addressing and user-based authentication should be used. ACLs should be used to identify legitimate MAC addresses rather than allowing users to self-configure and register new NICs on the WLAN. Disable DHCP (Dynamic Host Configuration Protocol) to prevent an intruder from being assigned a valid IP address.				

APPENDIX A
802.11b CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
9	*Theft of Hardware/Key Disclosure*	The 802.11b standard for WEP requires storage of a pre-shared key on each WLAN device.	Loss or theft of devices configured for WLAN connection may expose keys to unauthorized personnel and/or allow unauthorized connectivity to the WLAN. This condition may increase the potential for unauthorized access to proprietary data.	Devise and follow policies, procedures, and standards that require notification of the key administrator and key modification any time a WLAN device(s) is/are lost or stolen. Modify ACLs to ensure the stolen device cannot reconnect to the WLAN via the old NIC. Implement controls that require WLAN users to authenticate to the WLAN by user as well as device.				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
1	Key Management & Exchange[31]	BlackBerry provides DES3 encryption for all communication between the handheld and the desktop by default. A private serial connection between the handheld and the desktop is used when the key is established to prevent interception of the key by eavesdroppers. The key is a random number that is generated based on a series of random mouse movements made by the user at the time the key is established. The configuration is established within the BlackBerry Desktop Manager at the desktop workstation. The encryption key is stored in a hidden folder on the user's Microsoft Exchange Message Store on the Exchange server.	Key might be discovered. Discovered keys can be used to decrypt data that was intended to be private, resulting in unauthorized disclosure of information.	Enable screensaver (or other desktop) lockout controls and prevent access to file structures where keys are stored. Additionally, implement password controls on the handheld to prevent unauthorized access to BES, Exchange, and other data. Ensure Exchange Server has appropriate physical and logical access controls.				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
2	Wireless Modem	The BlackBerry handheld employs a small wireless modem with a 2-watt transmitter that ensures constant connectivity to the desktop.	Transmissions between the desktop and laptop could be intercepted, potentially resulting in unauthorized and/or inadvertent disclosure of proprietary information.	Communication between the handheld and the desktop is encrypted by default using DES3. [32]				
3	Firewall Security	BES is a Windows NT service capable of concurrent user monitoring via a single Administrative connection to the Microsoft Exchange Server. BES also uses a direct TCP/IP connection (Server Routing Protocol or SRP) to the wireless network.	Penetration of the BlackBerry and/or Exchange servers using an Administrative account may result in unauthorized access to systems and data and may also result in downtime or system inefficiency.	Firewall configuration should permit only an outbound connection on port 3101.[33]				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
4	Theft/Loss of Handheld Hardware	Although BlackBerry is capable of requiring a password for access to data, a password is not required by default on the handheld device.	Unauthorized and/or inadvertent disclosure of proprietary data, potentially including strategic information or customer information subject to GLBA privacy laws.	Use a version of Exchange and BES that allow the BlackBerry administrator to force the password requirement on all handheld devices. Subsequent to setting the password, users can lock the handheld to protect against unauthorized access, including access through the serial port on the handheld. Once a password is set, an incorrect password entered more than ten times results in automatic erasure of the handheld's memory. Only the SHA-1 hash of the password is stored on the handheld.				
5	Access to IT Policy Files	Policy Files can be used to configure handheld settings, BlackBerry Desktop Manager settings and Microsoft Exchange Settings.	Alteration of policy files could introduce control weaknesses in the BlackBerry environment.	Permit access to BlackBerry Policy Files only to authorized personnel responsible for BlackBerry administration. Policies can be used to force password requirement at the handheld.				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
6	Unauthorized BlackBerry User	Users can use Desktop Redirect rather than Exchange, circumventing centralized management of the BlackBerry device.[34] Centrally managed BlackBerry handhelds must be configured with the BlackBerry Desktop Manager that is in turn connected to a valid Exchange user account to gain typical access to the wireless services.	Unknown devices capable of storing, retrieving, or transmitting Company data may be connected to network-connected devices. There is potential for unknown loss of proprietary, customer, and/or strategic data if the device is lost or stolen. Additionally devices that are not centrally managed may not have adequate security enabled.	The Company's Authorized Use policy prohibits installation of BlackBerry devices independent of Information Services. Human Resources policies require compliance with the Acceptable Use policy.				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
7	Access to BlackBerry Servers Properties[35]	BES is an NT Exchange service capable of concurrent user monitoring via a single Administrative connection to the Microsoft Exchange Server.[36]	Access to BlackBerry Servers Properties can allow people to change the administration settings. This account must full administrative rights to the message stores of the users served. Administrative control of the BlackBerry solution may be compromised if unauthorized individuals can access to the BlackBerry property window.	Controls over Exchange should be sufficient to restrict access to BlackBerry Exchange Server and the BES infrastructure. Access should be restricted and granted only to properly authorized individuals. Such access should be monitored to prevent security violations.				

APPENDIX B
802.11b CONTROL MATRIX
BLACKBERRY CONTROL MATRIX

No.	*Risk Area*	Standard Functionality	Potential Threat	Suggested Minimum Control Settings	Control Environment Settings Observed	Specific Exposure(s)	Loss Potential (H, M, L)	Loss Probability (H, M, L)
8	BlackBerry Enterprise Server Performance -Monitoring Counters[37]	By default, to ensure efficient and effective message routing, the BlackBerry administrator can monitor the performance of the BlackBerry Enterprise Server in the following categories: 1. Connection State. 2. Messages Expires 3. Messages Filtered 4. Messages Queued for Delivery 5. Messages Received 6. Messages Sent	If BES is not monitored messages that are not routed efficiently or effectively may go unnoticed for an excessive period of time.					

REFERENCES

[1] Federal Deposit Insurance Corporation. "Financial Institution Letter 8-2002: Guidance on Managing Risks Associated With Wireless Networks and Wireless Customer Access." 1 February 2002. URL: http://www.fdic.gov/news/news/financial/2002/fil0208.html (2 January 2003).

[2] Federal Deposit Insurance Corporation. "Financial Institution Letter 8-2002: Guidance on Managing Risks Associated With Wireless Networks and Wireless Customer Access." 1 February 2002. URL: http://www.fdic.gov/news/news/financial/2002/fil0208.html (2 January 2003).

[3] Banking Industry Secretariat (BITS). "BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines. 15 March 2002. URL: http://www.bitsinfo.org/BITSMob1.pdf (2 January 2003).

[4] AirDefense, Inc. "White Paper: Enterprise Approaches to Detecting Rogue Wireless LANs." 2002. URL: http://www.airdefense.net/whitepapers/roguewatch_request2.php4 (2 January 2003).

[5] AirDefense, Inc. "White Paper: Enterprise Approaches to Detecting Rogue Wireless LANs." 2002. URL: http://www.airdefense.net/whitepapers/roguewatch_request2.php4 (2 January 2003).

[6] Naidu, Krishni. "Audit Checklist for Handheld PDAs." 2001. URL: Unknown. (1 July 2002).

[7] Tanzella, Fred. "Wireless LAN Security – How to Protect WLANs." March 2002. URL: http://www.airdefense.net/wirelesslansecurity/wlan_secrity_whitepaper.html (2 January 2003).

[8] Voorhees, James. "The Limits on Wireless Security: 802.11 in Early 2002." 30 January 2002. URL: http://rr.sans.org/wireless/limits.php (11 April 2002).

[9] Shmoo, The Group. "Airsnort Homepage." 3 May 2002. URL: http://airsnort.shmoo.com/ (3 May 2002).

[10] Rager, Anton T. "WEPCrack- An 802.11 Key Breaker." Published before 15 April 2002. URL: http://wepcrack.sourceforge.net (15 April 2002).

[11] Huey, Benjamin. "Penetration Testing on 802.11b Networks." 24 February 2002. URL: http://rr.sans.org/wireless/test_80211b.php (11 April 2002).

[12] Keeney, Frank. "Vacation War Driving." Published before 15 April 2002. URL: http://www.pasadena.net/vacation/ (15 April 2002).

[13] Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy." 23 January 2002. URL: http://rr.sans.org/wireless;netsec.php (11 April 2002).

[14] Voorhees, James. "The Limits on Wireless Security: 802.11 in early 2002." 30 January 2002. URL: http://rr.sans.org/wireless/limits.php (11 April 2002).

[15] Voorhees, James. "The Limits on Wireless Security: 802.11 in early 2002." 30 January 2002. URL: http://rr.sans.org/wireless/limits.php (11 April 2002).

[16] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org/wireless/8021X.php (11 April 2002).

REFERENCES

[17] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org/wireless/8021X.php (11 April 2002).
[18] Huey, Benjamin. "Penetration Testing on 802.11b Networks." 24 February 2002. URL: http://rr.sans.org/wireless/test_80211b.php (11 April 2002).

[19] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org/wireless/8021X.php (11 April 2002).

[20] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org/wireless/8021X.php (11 April 2002).

[21] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org/wireless/8021X.php (11 April 2002).

[22] Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy." 23 January 2002. URL: http://rr.sans.org/wireless;netsec.php (11 April 2002).

[23] Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy." 23 January 2002. URL: http://rr.sans.org/wireless;netsec.php (11 April 2002).

[24] Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." Published in the proceedings of the ACM's Seventh Annual International Conference on Mobile Computing And Networking, July 16-20, 2001.

[25] Tanzella, Fred. "Wireless LAN Security – How to Protect WLANs." March 2002. URL: http://www.airdefense.net/wirelesslansecurity/wlan_secrity_whitepaper.html (2 January 2003).

[26] URL: http://www.netstumbler.com (3 May 2002).

[27] Kuehl, Kirby. "Detecting Rogue 802.11 Access Points Within the Enterprise." SANS 2001.

[28] Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP Algorithm." Published before July 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (11 April 2002).

[29] Mishra, Arunesh and William Arbaugh. "An Initial Security Analysis of the IEEE 802.1X Standard." 6 February 2002., Department of Computer Science, University of Maryland, College Park, MD 20742. CS-TR-4328, UMIACS-TR-2002-10.

[30] Stargel, Daryl. "Wireless LANs and 802.1x." 12 December 2001. URL: http://rr.sans.org./wireless.8021X.php (11 April 2002).

[31] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

[32] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

[33] Research in Motion Ltd., *BlackBerry* Enterprise Server Installation and Getting Started Guide, Version 2.1. Waterloo: Ontario, Canada; 3/19/2001; p.21.

[34] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

REFERENCES

[35] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

[36] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

[37] Research in Motion, Ltd., "Technical White Paper BlackBerry Enterprise Edition for Microsoft Exchange version 2.1." 1999-2001 URL: http://www.blackberry.net (11 April 2002).

Last Updated: October 17th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event