Global Information Assurance Certification Paper

Melanie Lantz
GIAC Certification Version 2.0
GSEC Practical Assignment Version 11.2f
December 5, 2001

Power Inc. (Fictitious Name) Wireless Security Policy – Version 1.0

The corporate policy documented here is intended as a position paper dealing specifically with wireless technology. It is intended to be part of the overall security policies for Power Inc. so that security risks are minimized and if they occur they can be recognized and controlled.

Wireless is fast becoming part of our working environment. When you consider the possible cost avoidance that wireless offers over the cost of wiring buildings where running wires just isn't practical (i.e. older buildings), combined with the convenience of a mobilized workforce, it is easy to foresee wireless becoming a solution of choice. But with the cost avoidance, and higher productivity comes what many consider a serious threat to the security of our private network.

This policy will provide guidelines if you are considering a wireless solution, which include CDPD, wireless point-to-point, and wireless LANs. Currently Power Inc. has both CDPD applications and wireless point to point. We are including wireless LANs in this policy due to the possible requirement to use this technology in the near future.

Securing Wireless Networks and Wireless Devices

Security of Wireless Networks and Wireless Devices

Document Version Control Log

Version Number	Date	Author	Modification Description	Notes
1.0	December 5, 2001	Melanie Lantz	New	Review/Revision required by June 1, 2002

1. Purpose

1.1 To set forth the policy for adding wireless devices and wireless networks to Power Inc.'s existing network, and to define the administrative responsibilities and controls related to this policy.

2. Applicability

2.1 This policy applies to all Power Inc. operating units and partners.

3. Policy

3.1. Power Inc. personnel are not to design, build, or install any wireless point-to-point circuits without approval from Power Inc.'s Telecom Group, Corporate IT Network Group and the Security Officer.

3.2 Power Inc. personnel are not to design, build, or install any CDPD applications without approval from Power Inc.'s Telecom Group, Corporate IT Network Group and the Security Officer.

3.3 Power Inc. personnel are not to design, build, or install any wireless LANs without approval from Power Inc.'s Telecom Group, Corporate IT Network Group and the Security Officer.

3.4 Only standard based wireless solutions are to be considered in any wireless design. Currently, the standard recognized by Power Inc. for wireless networking, is 802.11b. Newer wireless standards and solutions are being developed at the time of writing this policy. In an effort to keep this policy current, a revision date of six months is required.

3.5 Corporate IT's Data Network Group will conduct periodic inspections on all wireless LANs and networks. These inspections will look for, but not be limited to, wireless communication designs that lack proper encryption, insecure systems, and unacceptable leakage of antennae beam.

CDPD

3.6 All wireless devices (Mobile End System, MES) using CDPD will require authentication and authorization from the vendors' (Cellular Inc.) Mobile Data Intermediate System (MDIS).

3.7 All wireless devices, MES, using CDPD will require authentication and authorization from Power Inc.'s VPN.

3.8 All CDPD networks will require the encryption provided by the vendor (Cellular Inc.), and Triple-DES provided on the Power Inc. WAN.

3.9 Lost or stolen wireless devices that connect to the CDPD network i.e. laptops, must be reported immediately to the Help Desk at 1-800-555-5555 or 555-5555.

3.10 VPN accounts of lost or stolen wireless devices that use a CDPD network, must be disabled immediately by the VPN administrator.

3.11 VPN accounts inactive for a period of ninety (90) days are to be reviewed by the VPN administrator, and disabled or removed if not required.

3.12 VPN accounts of terminated employees must be disabled immediately by the VPN administrator. Files authored by this employee are to be retained for thirty (30) days, and then reviewed with the employee's previous management.

3.13 The VPN administrator will review the authentication logs daily on the authentication server to identify users attempting to access the system or data that they are not authorized for.

3.14 Repeated failed logon attempts are to result in disabling the account by the VPN administrator. This account is to remain disabled until the IT Help Desk authorizes reactivation.

3.15 The VPN administrator must review the authentication logs daily to identify any unusual patterns or trends that require attention.

Wireless Point to Point

3.16 All wireless point-to-point connections must enable WEP 128-bit encryption on access units.

3.17 All wireless point-to-point connections must be configured to allow connection to only one other access unit. The access list should have only one entry.

3.18 WEP keys are to be changed by the network administrator at least once a month.

3.19 Wireless point to point is only used when cost justified and risk of scanning by intruders is minimal due to location of wireless circuit.

3.20 All security event traps are to be configured and enabled on all wireless point-to-point access units. Alarms are sent to Power Inc.'s *HP OpenView* system. The Network Administrator monitors these events.

3.21 The Network Administrator reviews access unit logs once a month.

3.22 When any wireless point to point is considered compromised, the Network Administrator will immediately disable the wireless point-to-point access units in question.

Wireless LANs

3.23 All wireless LANs must enable WEP 128-bit encryption on access point.

3.24 WEP keys are to be changed by the network administrator every six months.

3.25 All wireless LANs must have MAC address based access lists. The Network Administrator will be responsible to manage these access lists.

3.26 All wireless LAN access points will be connected to Power Inc.'s WAN via VPN. This VPN will be set up to service only wireless workstations operating on wireless LANs and will use Triple-DES encryption.

3.27 All wireless LANs connecting to the Power Inc. WAN via a dedicated VPN will authenticate using Corporate IT's authentication server.

3.28 Lost or stolen wireless devices that connect to a wireless LANs i.e. laptops must be reported immediately to the Help Desk at 1-800-555-5555 or 555-5555.

3.29 VPN accounts of lost or stolen wireless devices that connect to a wireless LAN, must be disabled immediately by the VPN administrator.

3.30 VPN accounts inactive for a period of ninety (90) days are to be reviewed by the VPN administrator and disabled or removed if not required.

3.31 VPN accounts of terminated employees must be disabled immediately by the VPN administrator. Files authored by this employee are to be retained for thirty (30) days, and then reviewed with the employee's previous management.

3.32 The VPN administrator will review the authentication logs daily on the authentication server to identify users attempting to access the system or data that they are not authorized for.

3.33 Repeated failed logon attempts are to result in disabling the account by the VPN administrator. This account is to remain disabled until the IT Help Desk authorizes reactivation.

3.34 The VPN administrator must review the authentication logs daily to identify any unusual patterns or trends that require attention.

3.35 When any wireless LAN is considered compromised, the Network Administrator will immediately disable the access device's connection to the dedicated VPN.

Questions regarding this policy should be directed to Original Signed by:
Power Inc. Information Technology
December 5, 2001

Definitions

VPN – Is a process where a connection is established across the Internet in such a way that a private link exists between two distant locations. This Virtual Private Network or VPN allows separate locations within a corporation to safely communicate on internal matters without concern their information will be intercepted and read. This private link or "tunnel" is kept secure by encrypting the data being exchanged between the two locations.

Triple-DES – The Data Encryption Standard (DES) was developed by an IBM team around 1974 and adopted as the national standard in 1977. Triple-DES is a minor variation of this standard. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple-DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted with the third key. It takes three 64-bit keys, for an overall key length of 192 bits. (Triple-DES Encryption Overview) **http://www.tropsoft.com/strongenc/des3.html**

MES – Every client connected to the CDPD wireless network is considered a Mobile End System or MES. (CDPD: A look at a Secure Wireless Network. Barry Cox, April 11, 2001)
http://www.sans.org/infosecFAQ/wireless/CDPD.html

MDIS – This box is the heart of the CDPD network. It manages the connections for all of the MES clients. It is responsible for authentication and authorizing connections and providing the encryption services for the airlink communications. (CDPD: A look at a Secure Wireless Network. Barry Cox, April 11, 2001)
http://www.sans.org/infosecFAQ/wireless/CDPD.html

Encryption (& decryption) – Software security algorithms that digitally encode passwords/pass phrases and data to provide secure transaction over a non-secure network such as the Internet. Encryption & decryption provide confidentiality, helping prevent unauthorized individuals from stealing information. IBM Security Definitions http://www.pc.ibm.com/ww/security/definitions.html

802.11b - IEEE Standard for Wireless Networking . Currently, this is the most commonly used wireless standard.

WEP – Wired Equivalency Protocol

CDPD – Cellular Digital Packet Data

WAN – Wide Area Network

LAN – Local Area Network

MAC – Media Access Control

References

Triple-DES Encryption Overview
http://www.tropsoft.com/strongenc/des3.html

Cox, Barry. "CDPD: A look at a Secure Wireless Network". SANS Institute. Information Security Reading Room. April 11, 2001
http://www.sans.org/infosecFAQ/wireless/CDPD.html

IBM – Security Definitions
http://www.pc.ibm.com/ww/security/definitions.html

Griffen, Sean. "Security and the 802.11b Wireless LAN". SANS Institute. Information Security Reading Room. September 16, 2001
http://www.sans.org/infosecFAQ/wireless/80211b.html

Posluns, Jeffrey. "Wireless Communications Technologies: An Analysis of Security Issues". April 26, 2001
http://www.sans.org/infosecFAQ/wireless/sec_issues.html

van der Walt, Charl. "Introduction to Security Policies, Part One: An Overview of Policies". August 27, 2001

http://www.securityfocus.com/infocus/1193

van der Walt, Charl. “Introduction to Security Policies, Part Two: Creating a Supportive Environment”. September 24, 2001
http://www.securityfocus.com/infocus/1473

van der Walt, Charl. “Introduction to Security Policies, Part Three: Structuring Security Policies”. October 9, 2001

http://www.securityfocus.com/infocus/1487

van der Walt, Charl. “Introduction to Security Policies, Part Four: A Sample Policy”. October 22, 2001
http://www.securityfocus.com/infocus/1497

Fennelly, Carole. “Let Security Hound You”.
May 2001.IBM - Security in Wireless.
http://www-106.ibm.com/developerworks/library/wi-sec.html?dwzone=wireless

Leyden, John. “Wireless Security is Even Flakier Than We Thought”. August 7, 2001. The Register
http://www.theregister.co.uk/content/55/20877.html