



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



Category 'Best
Security Company'

Wireless Security Assessment (1)

Wireless Security Assessment (1)

It should be no surprise that modern businesses, regardless of industry, are embracing wireless technologies to increase productivity. Wireless technology is also used to expand IT infrastructure to include areas not traditionally reachable from wired environments. Despite the benefits of wireless technologies, press coverage has shown that it is an area which contains many insecurities (making it a popular choice for malicious attackers). Whilst mainstream scrutiny has concentrated on the security problems within 802.11 based network architectures, there are many other areas of wireless capability that can be just as susceptible to security compromises. The following are some of the potential avenues or channels for the subversion of wireless technologies available to a prospective attacker.

» Bluetooth Network Testing

Bluetooth enabled devices are on the increase, for both enterprise and personal electronic accessories. Bluetooth ad-hoc networks (piconets) and low bandwidth intensive wireless personal area networks (PANs) can have an impact on wireless network security. Reviewing this area of wireless security will normally include the following techniques:

- » Evaluate Bluetooth Business Needs, Practices and Policies – Verify that there are organisational security policies which address the use of wireless technology and contain specific references to Bluetooth devices.
- » Evaluate Bluetooth Hardware, Firmware and Updates – Perform a complete inventory of all Bluetooth enabled wireless devices that are considered part of the inventory of assets.
- » Test for Common Bluetooth Vulnerabilities – Perform brute force attacks against Bluetooth access points to discern the strength of passwords in use. Verify that passwords contain numbers and special characters and therefore cannot be guessed easily by an attacker. Verify that ad-hoc Bluetooth devices do not have default PINs enabled and operate with the inclusion of encryption wherever possible.
- » Evaluate the Ability to Intercept or Interfere with Bluetooth Communications – Verify the perimeter of the Bluetooth network, and determine the level of physical access controls to Bluetooth access points and devices controlling them. Also review the potential to intercept Bluetooth wireless signals passively.
- » Evaluate Bluetooth Device Configurations – Verify that Bluetooth devices are set to the lowest possible power setting to maintain sufficient operation and to keep transmissions within the secure boundaries of the organisation. Configure all ad-hoc devices to use non-standard PIN numbers for pairing and to opt-in to encrypted solutions wherever possible.

» Wireless Input Device Testing

An organisation may make use of wireless input devices such as a mouse or keyboard. Whilst the popularity of these devices is on the increase, using such devices in an enterprise can introduce wireless privacy and security vulnerabilities. Reviewing this area of wireless security should include the following techniques:

- » Evaluate Wireless Input Device Business Needs, Practices and Policies – Analyse organisational security policies that address the use of wireless technology; ensure that these policies include the use of wireless input devices.
- » Evaluate Hardware, Firmware and Updates – Perform a complete inventory of all wireless input devices on the network, or any which are peripherals to other networked devices and/or hosts.
- » Evaluate the Ability to Intercept or Interfere with Wireless Input Device Communications – Perform a site survey to measure and establish the service range of the wireless input devices in use for an organisation. In addition, attempt to establish the potential for misuse for a given wireless input device.

» Wireless Handheld Security Testing

Many devices fall into the wireless handheld category such as smart phones, Blackberry handhelds, PDAs, cameras and MP3 players. As with all wireless devices and technologies there are many security and privacy concerns that could have an impact upon an organisation. Areas of concern include the education of users and the configuration of the handheld in line with business policies. Reviewing this area of wireless security will likely include the following techniques:

- » Evaluate Wireless Handheld Business Needs, Practices and Policies – Verify that there is an organisational security policy that addresses the use of all handheld devices in use within the organisation.
- » Evaluate Hardware, Firmware and Updates – Perform a complete inventory of all wireless handheld devices that are able to connect to an organisations business network.
- » Evaluate the Ability to Intercept or Interfere with Wireless Handheld Communications – Verify that there is external boundary protection around the perimeter of buildings or wireless networks.
- » Evaluate Wireless Handheld Device Configuration – Verify that devices use robust encryption to protect sensitive files and applications.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

Wireless
Security
Assessment (1)

Wireless Security Assessment (1)

» Wireless Transaction Device Testing

Wireless technologies are used increasingly within Point of Sale (POS) terminals to add flexibility and convenience around retail hotspots. As with wireless technology in the surveillance field, wireless technology around the POS transaction introduces potential security vulnerabilities that may have a significant impact upon an organisation. Where the POS or other general financial transactions can be subverted by an attacker, the loss to an organisation could have a direct monetary effect (which may also be in contravention of standards such as PCI DSS).

- » Evaluate the Business Need, Practices and Policies for Wireless Transaction Devices – Verify that there is a company policy that effectively addresses wireless transaction equipment.
- » Evaluate Hardware, Firmware and Updates for Wireless Transaction Devices – Perform a full inventory of all wireless transaction devices.
- » Evaluate Wireless Transaction Device Configurations – Verify that the data being sent by wireless transaction devices is encrypted and the level of encryption used is adequate.
- » Evaluate the Ability to Intercept or Interfere with Wireless Transaction Communications – Determine the possibility for an unauthorised third party to intercept transmitted data.

» Cordless Communications Testing

There are many cordless communications implementations that do not utilise wireless technologies such as 802.11 or Bluetooth. These technologies may rely upon other parts of the electromagnetic spectrum or cellular technologies such as GSM, GPRS or UMTS. In any case, these cordless communications technologies may expose an organisation beyond the desired perimeter, and may in some cases cause interference to other systems. Reviewing this area of wireless security will typically include the following techniques:

- » Evaluate the Business Need, Practices and Policies for Cordless Communications – Verify that the organisation has an adequate security policy that addresses the use of cordless communication technology.
- » Evaluate Cordless Communications Hardware, Firmware and Updates – Perform an inventory of all cordless communication devices in use within an organisation.
- » Evaluate the Ability to Intercept or Interfere with Cordless Communications – Verify the distance in which the cordless communication extends beyond the physical boundaries of the organisation.

» Further Wireless Security Assessments from NGSSoftware

NGSSoftware provides an exhaustive range of Wireless Security Assessments. For further details of other Wireless Security Assessment Services, please refer to the following brochures:

- » Wireless Security Assessment (802.11) - For 802.11 Networks.
- » Wireless Security Assessment (2) - For Electromagnetic Radiation (EMR) Testing, RFID Security Testing and Microwave Radio Testing.
- » Wireless Security Assessment (3) - Wireless Surveillance Device Testing and Infrared Systems Testing.

» Contact Details

Web: www.ngssoftware.com

Support: support@ngssoftware.com

Sales: sales@ngssoftware.com

UK Head Office (London)
Next Generation Security Software Ltd
52 Throley Way
Sutton
Surrey, SM1 4BF
United Kingdom

Australian Office (Sydney)
Next Generation Security Software Pty Ltd
Level 19, 2 Market Street
Sydney, NSW, 2000
Australia
ABN: 83 119804803
Regional Web: www.ngssoftware.com/au
Regional Sales: australiasales@ngssoftware.com

Tel: +44 (0)208 401 0070
Fax: +44 (0)208 401 0076

Tel: +61 (0) 448 692 022