



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



Category 'Best
Security Company'

Wireless Security Assessment (2)

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.

» RFID Security Testing

RFID tags are used primarily within the access control field, but can be used for inventory or stock control purposes.

Where encryption is not used, it can be trivial for an attacker to capture legitimate RFID data and clone tags to gain access to a facility. Even in cases where an encryption mechanism is used, it can still be trivial for an attacker to clone RFID assets and subvert security.

There have been a great deal of high profile press coverage surrounding the susceptibility of RFID technology to security flaws. Reviewing this area of wireless security should typically include the following techniques:

- » Evaluate the Business Need, Practices and Policies for RFID Tokens – Verify that the organisation has an adequate security policy that addresses the use of RFID tokens.
- » Evaluate RFID Token Attributes – Verify that RFID token serial numbers cannot be changed or modified by an un-trusted third party.
- » Evaluate Placement and Configuration of Scanners and Tracking Equipment – For the complete tracking of tagged products in a warehouse or other storage environment, ensure that RFID tag readers are in place at all entrances and exits, not just main arrival and departure points.
- » Evaluate the Configuration of RFID Backend Systems – Ensure that security vulnerabilities or weaknesses do not exist with backend systems that are intended to process data from RFID tokens or tags.
- » Evaluate the Ability to Intercept or Interfere with RFID Communications – Verify that RFID tag and reader transmissions do not interfere with wireless networks or other communications equipment. In addition, attempt to minimise the ability for an attacker to monitor and capture RFID scans.

» Microwave Radio Testing

Due to its relative inaccessibility when compared to 802.11 networks or Bluetooth, the security of microwave devices is often overlooked.

Incorrect assumptions within the communications industry can also lead to the misuse of terms such as 'encryption' and 'encoding' suggesting that security exists where it does not.

However, it is possible to intercept microwave point to point links providing an attacker can gain access to a point within the line of sight path.

This is often the case, notably where links terminate on buildings in relatively accessible public places. Reviewing this area of wireless security will normally include the following techniques:

- » Evaluate design and implementation – Verify whether or not the design includes appropriate levels of encryption or other controls to limit access.
- » Implementation – Verify whether the endpoints are in locations that might make them vulnerable to attack.
- » Terrain – Research the geography of the link to identify possible interception points along the path rather than near the endpoints.
- » Technology – Identify the technology in use and ascertain how readily available similar equipment is.



» SERVICES



Category 'Best
Security Company'

Wireless Security Assessment (2)

Wireless Security Assessment (2)

» Electromagnetic Radiation (EMR) Testing

Emissions Security (Emsec) is an often overlooked area of wireless security. It pertains directly to the remote testing of electromagnetic radiation from Information Technology devices. Electromagnetic radiation can be captured from common-place business devices such as CRT displays, LCD screens, printers, modems and cell phones to name but a few. It is possible for an attacker to utilise a technique known as Van Eck Phreaking to force data emanated from these devices to be displayed on a separate remote display or screen, thus potentially revealing sensitive company information. Reviewing this area of wireless security will likely include the following techniques:

- » Evaluate the Location of Sensitive Areas – Verify that the organisation has an adequate security policy to address EMR.
- » Evaluate Hardware and Placement – Verify that all Information Technology devices that must be protected are located in a suitable Faraday Cage or metal-shielded room.
- » Evaluate and Test Wiring Emissions – Verify that all wiring feeds into and out of a shielded environment are made of fibre where possible.

» 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 (1) - For Bluetooth Network Testing, Wireless Input Device Testing, Wireless Handheld Security Testing, Wireless Transaction Device Testing and Cordless Communications Testing.
- » Wireless Security Assessment (3) - Wireless Surveillance Device Testing and Infrared Systems Testing.

» Assessment Offer

If you feel that you are not receiving an adequate service from your existing security supplier, NGSConsulting would like to extend the opportunity of a no cost, no obligation 'mini-audit', provided under an NDA.

This allows our consultants to demonstrate their technical abilities and also allows future clients to assess the strengths and weaknesses of their existing suppliers.

For further details of this offer, contact info@ngsconsulting.com

» Contact Details

Web: www.ngssoftware.com

Support: support@ngssoftware.com

Sales: sales@ngssoftware.com

UK Head Office (London)
Next Generation Security Software Ltd
52 Throwley 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