



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



Category 'Best
Security Company'

Wireless Security Assessment (3)

Wireless Security Assessment (3)

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.

» Wireless Surveillance Device Testing

Increasing numbers of security cameras, microphones and other surveillance equipment is being replaced with wireless equivalents.

The obvious consequence is that these devices may now be susceptible to wireless vulnerabilities.

Where these devices are used for security purposes in their own right, security vulnerabilities within can have a greater effect.

An attacker may be able to utilise wireless vulnerabilities to view security cameras which themselves are used as part of a larger monitoring system.

By accessing these feeds, it could also be possible for an attacker to use this information to launch a physical attack when an organisation is at its most vulnerable.

Reviewing this area of wireless security should include the following techniques:

- » Evaluate the Business Need, Practices and Policies for Wireless Surveillance Devices – Verify that there is a company policy that effectively addresses the secure use and deployment of wireless surveillance equipment.
- » Evaluate Wireless Surveillance Devices and Device Placement – Verify that the surveillance equipment is truly disguised or is not visible to an intruder where this is a priority for deployment. Also verify that the surveillance equipment is able to monitor all it is intended to.
- » Evaluate the Ability to Intercept or Interfere with Wireless Surveillance Communications – Verify the perimeter of wireless surveillance device transmissions.

» Infrared Systems Testing

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

However, it is possible to issue commands to infrared systems without needing to supply 'credentials' or use any form of encryption.

In some cases this can lead to an attacker compromising an element of security, wherever infrared systems are used by an organisation.

Reviewing this area of wireless security will likely include the following techniques:

- » Evaluate the Business Need, Practices, Policies and Location of Sensitive Areas for Infrared – Verify that the organisation has an adequate security policy that addresses the use of wireless technology, such as infrared devices.
- » Evaluate Hardware, Firmware and Updates for Infrared Devices – Perform a complete audit of all infrared enabled devices to determine where infrared is intended to be used.
- » Evaluate the Ability to Intercept or Interfere with Infrared Devices – Verify the distance that infrared communication extends beyond the physical boundaries of the organisation.
- » Evaluate Infrared Device Configuration – Verify infrared client authentication methods.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

Wireless Security Assessment (3)

Wireless Security Assessment (3)

» 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:

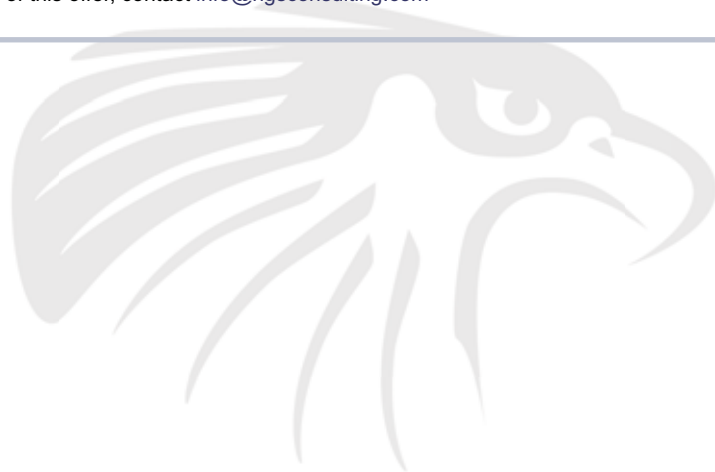
- » Wireless Security Assessment (802.11) - For 802.11 Networks.
- » Wireless Security Assessment (1) - For Bluetooth Network Testing, Wireless Input Device Testing, Wireless Handheld Security Testing, Wireless Transaction Device Testing and Cordless Communications Testing.
- » Wireless Security Assessment (2) - For Electromagnetic Radiation (EMR) Testing, RFID Security Testing and Microwave Radio 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