International Working Group
on Data Protection
in Telecommunications

675.28.7 15 April 2004

Working Paper on potential privacy risks associated with wireless networks. Main Recommendations.

- adopted at the 35th meeting, 14-15 April 2004 in Buenos Aires -

Wireless communications offer many benefits such as portability and flexibility, increased productivity, and lower installation costs and are becoming increasingly popular. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices or homes without the need for wires and without loosing network connectivity.

Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems, application sharing between devices and eliminate the need for cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and mobile phones allow remote workers to synchronize personal databases and provide access to corporate services such as e-mail, and Internet access. Wireless technologies offer the prospect of greater functionality in the future.

However, there are risks associated with the use of wireless technology, in particular because the technology's underlying communications medium, the airwave, is open to intrusion unless appropriate security precautions are taken.

These risks include:

- The capture of location data and other personal data about the network user;
- Unauthorised and undetected access to corporate networks by external users;
- Bypassing of corporate firewalls and e-mail filtering by wireless users also connected to corporate networks, leading to loss of protection from virus attack and spam;
- Eavesdropping of personal communications and undetected connections between wireless network users, especially in public places;

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

The Working Group calls upon the IEEE Task Group[1] and the WI-FI Alliance[2] as well as the vendors involved in wireless products to give data security and privacy matters a high priority in the current and future development of wireless technology[3].

Recommendations

A) Risk Analysis and desired Security Level

Wireless network managers[4] should be aware of the technical and security implications of wireless and handheld device technologies.

Wireless network managers should perform a risk assessment and develop a security policy before considering wireless deployment in order to ensure that they have examined and can manage and mitigate the risks to their information, system operations, and continuity of operations.

Wireless network users should be made aware of the technical and security implications of wireless and handheld device technologies.

For their own concerns, all users should perform a personal risk assessment before purchasing, using or running wireless technologies and services, because their own and personal security requirements will determine which products or services should be considered.

B) Network Parameter Settings

Wireless network managers should carefully plan the deployment of wireless technology and set appropriate parameters on devices in order to guarantee both network functionalities and service security. In particular, network access should be covered by high security standards.

Users should be guided and should be made aware of how to configure wireless devices to ensure a high level of security and confidentiality.

C) Security management

Wireless network managers should establish security management practices and controls to maintain the security of the wireless network.

Wireless network managers must routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies. The authentication in wireless network is very important and could be based on a stronger access control with regularly modified passwords.

[1] IEEE 802.11 Working Group for Wireless Area Networks (WLANs). http://grouper.ieee.org/groups/802/11/. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters IEEE.

[2] Wi-Fi Wireless Fidelity http://www.wi-fi.org/ The Wi-Fi Alliance organization, a nonprofit industry group, promotes the acceptance of 802.11 wireless technology worldwide, and ensures that all Wi-Fi CERTIFIED 802.11-based wireless networking gear works with all other Wi-Fi CERTIFIED equipment of the same frequency band and features.

[3] "NIST Publication 800-48: Wireless Network Security 802.11, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf [NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs.

[4] Anyone who wants to deploy and use wireless networks.

Wireless network managers should inform the user of the level of security of the network and the measures available to safeguard the confidentiality of communication.

D) Other Considerations

Providers of wireless networks should comply with the legal requirements[5] which may differ from one jurisdiction to another.

The Working Group stresses also that security concepts are difficult for users to understand. Practical application may also be difficult even for experienced IT specialists. The industry as a whole should tackle the problem at both technical and informational levels in order to enhance confidence in technology. The default setting should provide for a high level of privacy protection.

Service providers over Internet, in particular WEB mailers, should offer the opportunity for application level encryption. If sensitive data are communicated through wireless networks strong encryption is indispensable.

Users should not be prevented from using pseudonymous or anonymous access to publicly available services.

[5] See Art. 4 par. 2 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).