International Working Group
on Data Protection
in Telecommunications

675.41.18 7 September 2010

Working Paper on

Mobile processing of Personal Data and Security

48th meeting, 6 – 7 September 2010,

Berlin (Germany)

Background

In April 2004, the Working Group adopted a Working Paper on the potential privacy risks associated with wireless networks.[1]

Since that time, due to the strongly increasing dissemination and diversity of mobile devices such as, for example, mobile phones, smart phones, laptops and PDAs, accompanied by the constant availability of public communication networks, data processing of all manner of confidential and personal data on potentially insecure devices in potentially insecure public environments is becoming increasingly easy.

The use of mobile devices is not solely limited to the maintenance of contact data and processing of calendar entries. Rather, it makes confidential and personal data in corporate databases or the use of cloud computing services easily accessible.

The constantly increasing storage capacities of mobile devices and the ever-increasing speed of wireless networks allow mobile data processing in a way that was only possible in fixed and more secure environments in the past. The increased integration of mobile applications in conventional company IT infrastructures and processes increasingly results in confidential, personal, as well as business critical data not just being stored in the central system, but also being processed on the mobile devices. This can have a direct impact on the integrity, confidentiality and security of the data.

Furthermore, mobile devices are being increasingly used for archiving and temporary storage of data, which entails risks of data loss or disclosure.

Data protection and data security risks

By their very nature, mobile devices are small in design and light in weight. The major risks for data security lie in the manipulation, loss and theft of data. In order to recognise data manipulation, suitable mechanisms for securing data integrity exist. Whereas the loss of data is immediately recognisable, data theft often goes unnoticed until the data itself or a processing result reappears at a different location.

[1] http://www.datenschutz-berlin.de/attachments/197/1_en.pdf?1215693444

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.berlin-privacy-group.org

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

A series of specific risks result due to the use of mobile devices:

- Connection to public network access points (e.g. open Internet access points in restaurants, hotels, Internet cafes, etc.), irrespective of the type of connection (e.g. connection via network cable or Wireless LAN), solely due to the untrustworthy network. At the very least the connection data or, possibly, even the content data can be intercepted and tapped. The interception of confidential information in the communication is not only possible for the network operator, but also, in the event of insufficient security precautions in the relevant network segment, from every network connection.

- The use of open unencrypted wireless access, even in otherwise secure networks, enables communication between users to be spied upon unnoticed.

- The ongoing unnoticed evaluation of a mobile device's location data, e.g. by location based services (LBS) running in the background, allows a user movement profile to be created.[2]

- Attacks on the availability of mobile devices are, possibly, easier to implement (e.g. interference signals on the relevant frequency bands) than comparable attacks on workplace computers.

- Under certain circumstances, the use of short range communication, such as Bluetooth, can allow an attacker to gain control of an unprotected device.

Furthermore, risks often arise in connection with storage and direct data processing on mobile devices:

- Mobile devices often already come with numerous additional applications from the supplier. A reputable supplier would be expected to eliminate deficiencies and vulnerabilities discovered in the software before publication. However, partially open and documented programmer interfaces and development environments allow other companies and private persons to develop software (so-called "Apps") for mobile devices and disseminate them easily and inexpensively via the Internet. The installation of such external applications from third-party providers increases the risk of infection by malware or damage to data by insecure applications. The entire system's stability can be adversely affected by the retroactive installation of uncertified third-party software.[3]

- The development of uniform operating systems and standards for mobile devices is indeed simplifying software development. But in the event of vulnerabilities, this uniformity can lead to an increased risk of malware dissemination, as is already evident in the personal computing world. However, uniform operating systems facilitate the implementation of uniform security measures.

- "Push service" or "server push service" describes a method of content dissemination that is usually Internet-based. In the process information is outsourced from a central server directly to the mobile device where it is immediately processed. An unchecked dissemination of the incoming messages generates risks, which are already known today from the field of e-mail processing on workplace computers (e.g. malware in attachments, exploitation of weak points in the processing software, etc.).

[2] Common Position of the IWGDPT on Privacy and location information in mobile communications services, http://www.datenschutz-berlin.de/attachments/193/local_neu_en.pdf

[3] All privacy aspects regarding third-party software are not considered in the current Working Paper.

Experience shows that a balance needs to be found between the implementation of too restrictive security requirements in dealing with mobile data carriers as well as devices on one hand, which may then not be accepted by users, and the provision of a secure environment with sufficient data protection on the other hand.

The mere encryption of the data and sensitive information *without* employing accompanying measures and behavioural standards is *not* an effective way to counter any risks and security considerations.

Recommendations

Based on the above-cited risks the Working Group makes the following (preliminary) recommendations addressed to suppliers and users of mobile devices.

Suppliers

When delivered, the default security settings of the mobile device should implement the maximum security in line with the purpose for which the device is marketed.

One or more configurable user profile settings with limited privileges should exist, together with a super user who can control and limit access to the security settings for a user profile.

The user should be informed in a simple way about any change in the security settings. This could, for example, happen when updating system software (e.g. firmware or operating system update) or due to the installation of additional applications.

The manual should include a chapter dedicated solely to the topic of “security” and “security settings”. The latter should deal with the risks of the use of mobile devices and give the user a transparent and comprehensible guideline for secure handling.

Built-in hardware components and interfaces used for the collection and transmission of data (e.g. camera, GPS, microphone, IrDA, Bluetooth, WLAN, etc.) should be disabled by default; these interfaces should be available for the user to activate when needed, dependent on the privileges associated with the user profile.

In the case of mobile phones, a PIN on the SIM card can offer protection against unauthorised access. This access protection should be able to be extended to the telephone memory via an appropriate security setting. A user should be able to specify an interval of time after which the device blocks the inactive display/keyboard and only releases it again once the PIN or a freely selectable password is re-entered.

With regard to communication

A user should be warned when possibly insecure communication channels are being used for data transfer.

If the device loses contact with a secure WLAN and subsequently automatically re-connects to an insecure WLAN, a warning should be issued to the user.

A user should be able to easily recognise whether external communication channels and interfaces are active or inactive. Additional services on a mobile device, such as e.g. interfaces for communication, should be easily switched on and off by the user.

With regard to storage and data processing

In the event of subsequent installation or downloading of untested (uncertified) software from a third-party provider, a corresponding warning notice should be output to the user.

Before downloading and installing applications, a user should have the opportunity to inform himself in a simple way and in a self-selected language specifically about name and the electronic signature of the provider, the terms of use, access rights to hardware components and other pre-installed software necessary for running the application, directions for de-installing the application, and additional warning notices and other information relevant to security

A user should have the option of restricting the access of every installed application to the available device hardware (e.g. network interface card, camera, etc.) as well as to the stored data (e.g. to the calendar or the address book).

The user should be able to easily understand which data in the mobile device are encrypted and which are unencrypted when saved.

User

The raising of awareness is a first important step towards preventing misuse, data loss and theft. The users' own responsibility in connection with data security and integrity should be pointed out to them. The following recommendations are meant as a guide:

Users should review the local security settings of the mobile device following any system software upgrade (e.g. firmware update) and, if necessary, adjust them to meet their own needs.

When using a mobile device in a public area, users should make every effort to ensure that the screen and keyboard of their device are not observed by passers-by or surveillance cameras.

When using a company's mobile devices, compliance with the organisational measures developed by the technical department is imperative. Technical manipulations and changes to system settings should be prohibited.

With regard to communication

Public Internet access points should be used with caution. Confidential information and data should not be processed via insecure network connections unless the transmission is adequately protected by additional security measures, e.g. a virtual private network (VPN) tunnel.

Before exchanging confidential information, the communication partner's identity should be checked. Every unknown message or inconsistency in the operation should be questioned and, in case of doubt, an expert, or the responsible office in a corporate environment, should be informed or consulted.

Interfaces not required for actual use should be deactivated via the mobile device settings (e.g. facilities for transmitting data via Bluetooth, infrared signals (IrDA), wireless networks (WLAN), etc.). Location based services specifically should be deactivated, if they are not actually being used.

With regard to storage and data processing

Before installing external applications, the source should be meticulously checked. Signatures and manufacturer's specifications can minimise the risk of an infection. In case of doubt, an installation should be abandoned.

Access from installed external applications should be restricted to the data required for orderly operation. Thus, for instance, not every application needs access to the address book or calendar of the mobile device.