CYBER NETWORKS

Blackhat Briefings Europe 2004
White Paper : Smartphone Security Issues

Luc Delpha *Consultant Manager*
Maliha Rashid *Security Consultant*

Cyber Risk Consulting

May 2004

Abstract

Mobile phones are becoming more and more like computers today, resulting in smartphones that combine processing power with always on connectivity to the Internet.
Mainstream availability makes these devices potentially dangerous to organisations, extending the information system beyond the frontiers of the traditional trusted perimeter.
This white paper discusses the security issues surrounding the use of these devices.

TABLE OF CONTENTS

1 INTRODUCTION

Access to information and communication on the move is not only possible today, it is critical to maintain a competitive edge.
Emerging wireless technologies make it possible to access the web, email, business applications and to synchronise calendars, contacts and other applications, in real-time, anytime, anywhere.
Today's mobile phones combine these wireless technologies with dedicated operating systems and advanced multimedia functionalities, thus the term smartphone.
Smartphones facilitate the flow of information over heterogeneous networks, through untrusted domains. This flow of information represents risks for the owner of the smartphone and for the owner of the information.
Given their growing popularity, smartphones need to be acknowledged when considering an information system, and more particularly when considering the security of any information system.

After an introduction to the functionalities and architecture of smartphones (Symbian…), an overview of the technical risks associated with smartphone connectivity to wireless networks (Bluetooth, GPRS…) and malicious mobile code (Java MIDP) amongst others will follow.
Legal issues will then be addressed, with a focus on the legal limits on controlling the use of such devices, and the share of legal responsibility.

1.1 *Why smartphones?*

Given the gadget appeal of smartphones and their mainstream availability, smartphones are growing in popularity. Since smartphones are primarily used and sold for their phone function, they target a much wider population than traditional PDAs (Personal Digital Assistants).

Although smartphones are primarily acquired for personal use, their organiser and mail functions tend to be used for professional purposes. In a corporate setting, it is difficult to control the use of these devices to that effect. This difficulty is due to practical and legal limitations, and remains even when the smartphone is acquired for corporate purposes because of the highly personal level of interaction with the device.

1.2 *Smartphone caracteristics*

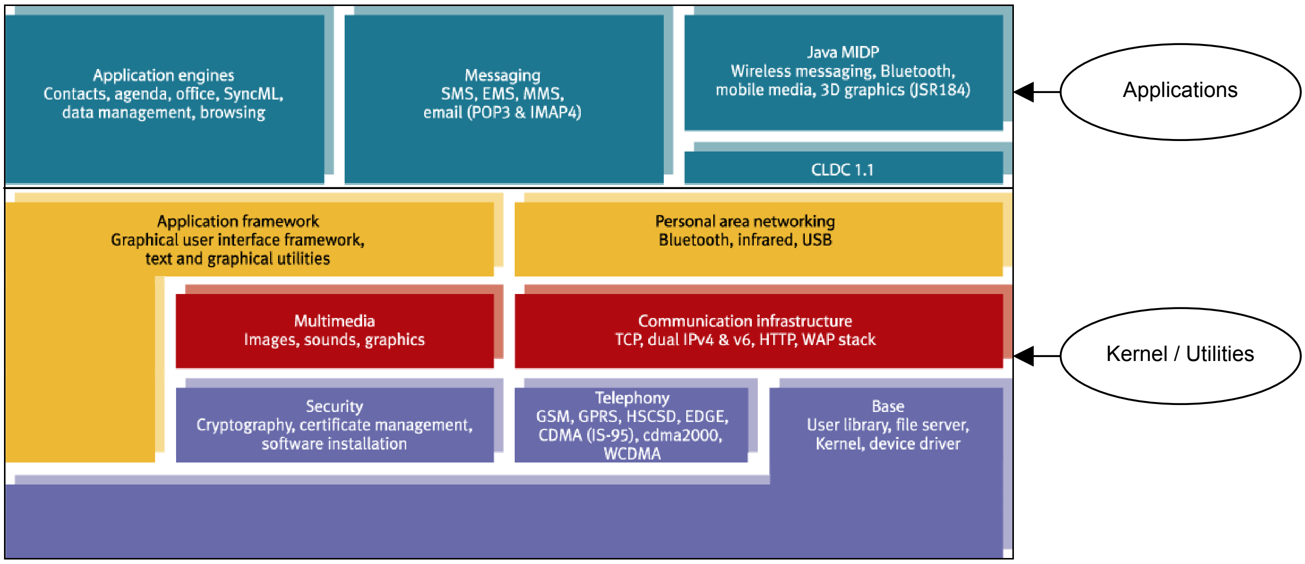
Aside from vocal communications over GSM and GPRS networks, smartphones provide web browsing, email and organiser functions, as well as advanced multimedia capabilities such as high resolution colour screens, digital cameras, mp3 players as well as support for Java applications.

Smartphones allow users to synchronise PIM (Personal Information Management) Data (calendar, contacts, tasks) and email using protocols such as SyncML, HotSync, ActiveSync or IntelliSync over Bluetooth, IrDA or GPRS.

Smartphones today are equipped with full fledged, purpose-built operating systems, designed for optimising resources. The dominating operating systems are Symbian, Windows Mobile and PalmOS. Smartphones running Linux are also available today (Motorola A760).

Figure 1 details the architecture of version 8.0 of Symbian OS [1].

Figure 1 : Architecture of Symbian OS version 8.0


Application engines
Contacts, agenda, office, SyncML, data management, browsing
Messaging
SMS, EMS, MMS, email (POP3 & IMAP4)
Java MIDP
Wireless messaging, Bluetooth, mobile media, 3D graphics (JSR184)
CLDC 1.1
Applications
Application framework
Graphical user interface framework, text and graphical utilities
Personal area networking
Bluetooth, infrared, USB
Multimedia
Images, sounds, graphics
Communication infrastructure
TCP, dual IPv4 & v6, HTTP, WAP stack
Kernel / Utilities
Security
Cryptography, certificate management, software installation
Telephony
GSM, GPRS, HSCSD, EDGE, CDMA (IS-95), cdma2000, WCDMA
Base
User library, file server, Kernel, device driver

Symbian OS version 8.0:

- Is based on a hard real-time micro kernel that implements multi threading and multi tasking (variant EKA2)
- Provides support for the latest CPU architectures, peripherals, internal and external memory types
- Comes equipped with application engines for PIM, messaging, browsing, utility and system control, Java, Bluetooth, gaming, 3D graphics (Open GL libraries)

1.3 Smartphones and wireless networks

Smartphone design is focused on facilitating the exchange and flow of information, using the latest wireless technologies to this effect. Wireless technologies used today range from Wireless PANs such as Bluetooth to Wireless WANs such as GPRS (General Packet Radio Service). Details of the protocols that stand out today are listed below.

1.3.1 Bluetooth

Bluetooth is defined by a core specification and a set of profiles related to different use cases.

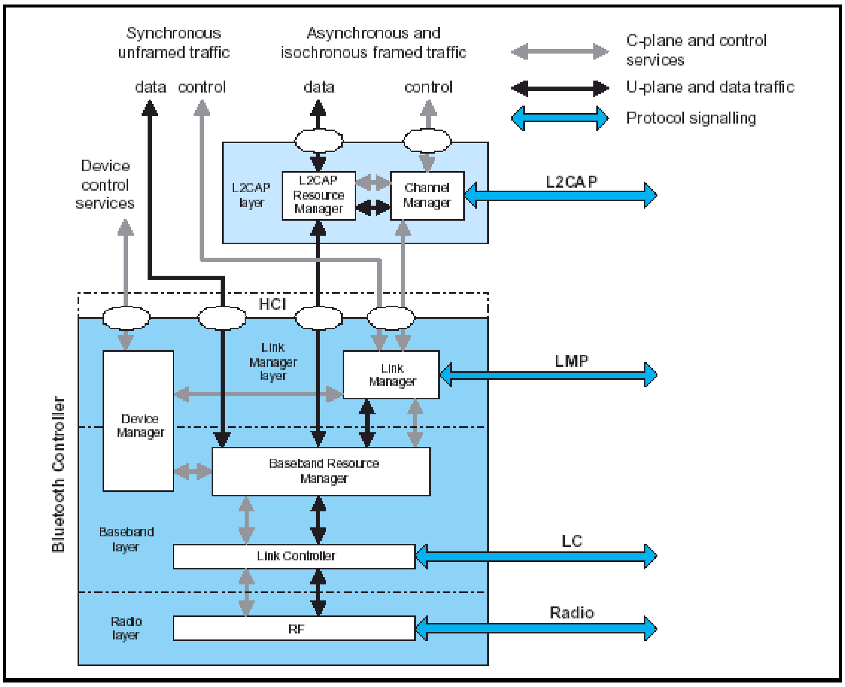
As described in Figure 2, the core system outlines the four lower layers and their associated protocols [2]:

- Radio Layer
- Baseband Layer
- Link Manager Layer
- L2CAP (Logical Link Control and Adaptation Protocol) Layer

The core system also covers :

- A common service protocol : SDP or Service Discovery Protocol
- the overall requirements for profiles : GAP or Generic Access Profile

Figure 2 : Core specification 1.2



The profiles commonly used in smartphones are :

- Service discovery application profile
- Synchronization profile
- Generic Object Exchange Profile

The Generic Object Exchange profile uses the OBEX protocol designed by the IrDA association [3]. The OBEX or Object Exchange Protocol is a binary equivalent of HTTP, providing object exchange services through Push (PUT method) and Pull (GET method) functions.

Because interoperability of devices is a priority in Bluetooth, the specification is deliberately not explicit about implementation.

1.3.2 GPRS

The General Packet Radio Service makes use of the GSM infrastructure, allowing higher data rates through a packet switched IP backbone.

GPRS networks provide always on Internet connectivity, as described in Figure 3, through two main elements :

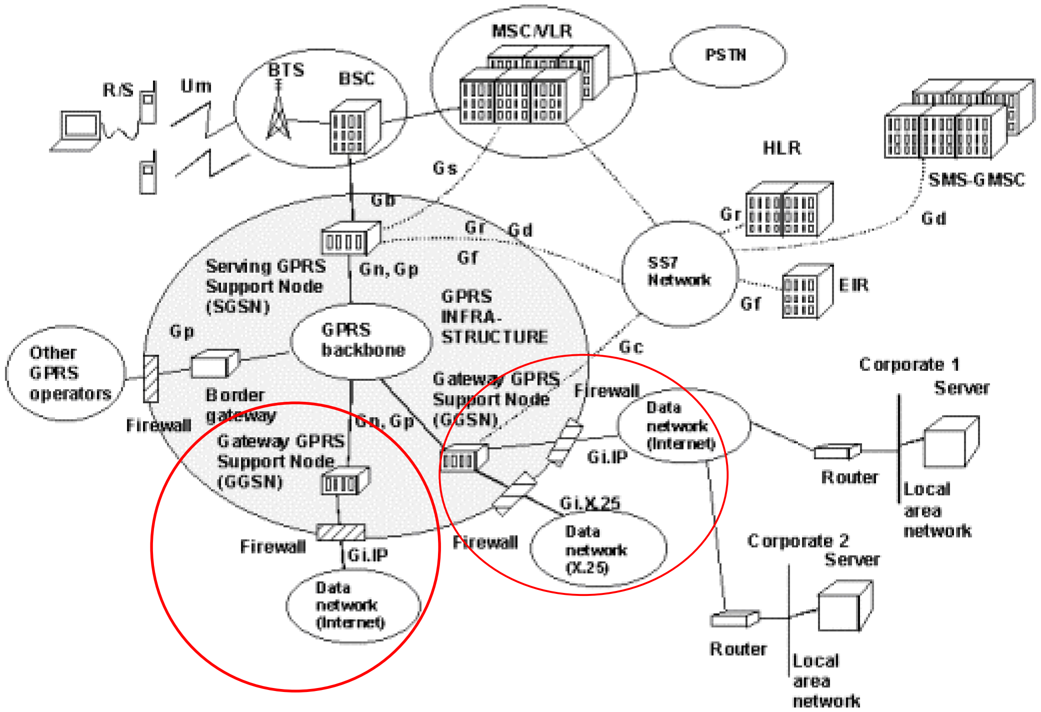
- The SGSN or Serving GPRS Support Node for :
  - ❑ Monitoring the state of the mobile device and tracking its movements
  - ❑ Establishing and managing the data connections between the mobile user and the destination network

©2004 CYBER NETWORKS
Reproduction interdite sans autorisation écrite préalable

- The GGSN or Gateway GPRS Support Node which provides the point of attachment between the GPRS domain and external data networks such as the Internet and corporate Intranets

A firewall is placed between the GGSN and external data network to protect the GPRS domain from attacks from the Internet

Figure 3 : General Packet Radio Service Architecture



The areas circled in red in Figure 3 show the interconnection between the GPRS domain and external data networks.

2 The risks

Smartphones, be it through their inherent characteristics, their use (or misuse) or the technologies associated with their use, bring forward risks.

2.1 *Security risks related to the inherent characteristics of smartphones*

As described above, smartphones come equipped with dedicated operating systems. This in itself will induce new risks such as the emergence of security holes and bugs, mainly due to the complex architecture of these operating systems. For example, known issues in the implementation of Java MIDP 2.0 in the Nokia 6600 have been documented in [4]. Bugs have also been documented on Windows based smartphones in [5]. It is possible to exploit these bugs to jam devices and provoke a reset. This would erase the data stored on the device. System-based vulnerabilities will be making their way in smartphones, just as they do on computers as smartphone operating systems will grow in sophistication.

Another issue linked to the inherent nature of smartphones revolves around access control and data security.

As there is no form of encryption used to protect the data inside the devices, the information remains at hand for anyone that can gain physical access to the device. Other than the PIN code, there is no native form of authentication for the most widely used smartphones despite the fact they are very often used to store personal and maybe confidential data (see Figure 4).
This is a kind of risk manufacturers and users of smartphone may have to consider…

Even if a pin code is protecting access to the telephone features, sometimes the data remains unprotected. Moreover data is (in most of the devices) stored on flash chipsets (or removable memory cards) so, with physical access to the chipset anyone can bypass the access controls and steal data (the device may be destroyed by the way ;-)))

2.2 *Security risks related to the users*

According to a mobile usage survey conducted by Pointsec Mobile Technologies :

Figure 4 : Mobile usage survey conducted by Pointsec Mobile Technologies

85 % of handhelds are used as business diaries
80 % of handhelds are used to store business names and addresses
79 % of handhelds are used to store personal names and addresses
75 % of handhelds are used as personal diaries
48 % of handhelds are used for entertainment - games & music
35 % of handhelds are used for documents/spreadsheets
33 % of handhelds are used to store passwords/PIN numbers
32 % of handhelds are used to receive and view emails
25 % of handhelds are used to store bank account details
25 % of handhelds are used to store corporate information

These figures show that users store confidential information on their handhelds without necessarily being aware of the risks they are taking.

Data stored on the device can easily become accessible to a third party whether it be by illegitimate connection, loss or theft of the device.

Consequences can be serious, ranging from identity theft to leakage of sensitive personal, corporate and client data.
Such was the case of the Blackberry RIM device sold on eBay for $15.50 by a former vice president of mergers and acquisitions for a major bank who had left the bank months earlier. The device contained a trove of confidential corporate and client data, from email addresses of the bank's representatives world wide, to emails discussing loan terms for the bank's clients, amongst others. It turned out that the Blackberry belonged to the VP but he had not given the bank the device for removal of the information before leaving the bank, as he assumed it had already been removed remotely.

Moreover, smartphones can easily be configured by the user for access to corporate email and data. Synchronisation using a cradle or infrared port does not require any authentication in most cases and can pose a threat to the information system if the device is compromised (by a virus contained in an attachment for example).

2.3 Security risks related to wireless networks

Connectivity of smartphones to a variety of different networks presents risks due to the inherent nature of the wireless medium and the always-on connectivity provided by 2.5 et 3G networks. The interconnection of different types of wireless networks incurred by 4G networks will escalate these risks by factoring in rebound and complexity.
The following paragraphs detail the risks related to two types of networks : Bluetooth and the GPRS.

2.3.1 Bluetooth

Bluetooth provides security features. However, very often these features are not implemented nor activated on smartphones.
In most cases, the implementation of Bluetooth security in smartphones is restricted to the pairing mechanism and setting the Bluetooth mode to "non-discoverable".
Tools such as Redfang [6] and BTscanner bypass the non-discoverable mode by brute-forcing the last 6 bytes of the Bluetooth address and calling the read_remote_name() function [7]. Redfang works on a Linux platform.
Other tools such as BTbrowser developed for the Nokia 6600 and SonyEricsson P900 (both running Symbian) allow a user to list surrounding devices and browse available files as well as PIM data.
It won't be long before smartphone versions of Redfang are out in the wild, given the growing interest in Bluetooth stirred by the bluejacking craze. Bluejacking refers to putting a message in place of one's Bluetooth device name and sending it to a nearby device through a pairing request. This in itself is harmless, but the message can also prompt the "victim" to press a key or compose a number, which if done by the victim would allow the bluejacker access to the files on the device.

Moreover, vulnerabilities in the Bluetooth implementation of certain smartphones have been discovered recently.

A certain number of Bluetooth enabled Nokia phones are vulnerable to a buffer overflow provoked by a mal-formed OBEX message (CAN-2004-0143) [8].
Other documented vulnerabilities include trust relationships established through the pairing mechanism that persist even after the relationship is no longer in the list of trusted devices, allowing an attacker to gain unauthorized access to the files on the device, without the knowledge of the victim [9].

Given the complexity of the protocol, implementation errors on devices will continue to induce security holes in devices.

2.3.2 GPRS

Smartphones connected to the GPRS are exposed to risks originating from the GPRS IP Backbone. Security of the GPRS backbone depends on the measures the operator has taken to secure the GGSN (Gateway GPRS Support Node). If the GGSN is compromised, the GPRS operator's subscribers become exposed to attacks from the Internet.

An attack on the NAT of the GPRS Network has been documented in [10], and is simple to implement. The same article also describes attacks that consist in flooding the GPRS connection with unnecessary TCP traffic from the Internet.

What GPRS allows - always on connectivity, be it for email Push, Synchronisation or OTA provisioning - is what makes smartphones all the more vulnerable to attacks from the Internet.

Smartphones that support multiple active PDP (Packet Data Protocol) Contexts present risks. Allowing simultaneous public and private contexts can lead to exposure of the private context to the public context, making the private context vulnerable to attacks from the public context. Symbian OS version 8 allows support for multiple active PDP Contexts.
This would allow an attacker to gain access to the information system simply because the smartphone user is simultaneously connected to the information system and browsing the web or using instant messaging. The risk here is the same as connecting the LAN directly to Internet with a modem.

2.4 Security risks related to the applications : stand-alone (Java MIDlets) – browser-based

Application development on smartphones is set to explode, mainly for games and mobile commerce applications. These applications can take the form of stand-alone applications, or be browser-based.

2.4.1 Java MIDlets

J2ME or Java 2 Platform, Micro Edition technology provides an optimised Java runtime environment for small devices, through the CLDC or Connected Limited Device Configuration which defines a base set of APIs for resource-constrained devices such as smartphones and the MIDP or Mobile Information Device Profile. The Java stand-alone applications for smartphones are called MIDlets. Two versions of MIDP exist to date : MIDP 1.0 and MIDP 2.0.

Java MIDP 1.0 applications have only limited access to system resources, as per the sandbox model. However, bytecode verification is limited as full bytecode verification would be too heavy an operation for smartphones. The same applies to the security manager and a number of security packages. Moreover, MIDP 1.0 does not include HTTPS and is limited to HTTP as a network protocol. Due to these limitations, using the device to access data across the network presents a real risk regarding Privacy or Confidentiality.

Given the limited possibilities and lack of security of MIDP 1.0 applications, the Java MIDP 2.0 specification aims to provide better security features thereby offering more possibilities to MIDlets [11].

Java MIDP 2.0 introduces the concept of trusted MIDlets. If the MIDlet is untrusted, it will run in the sandbox environment. If the MIDlet is trusted, MIDP 2.0 allows MIDlets greater access to system resources with APIs for PIM, network access, phone calls and messaging.

There are two sets of permissions for MIDlet access to sensitive APIs :

- Allowed (without explicit user authorization)
- User (prompt for authorization mode : blanket, session, oneshot or refuse).

Permissions are automatically attributed according to the domain that MIDlet belongs to. If the MIDlet belongs to a trusted domain (operator or manufacturer), permissions will be set to allow. If the MIDlet belongs to an untrusted domain (third party or unsigned), the user will be prompted for authorization.

These permissions are left to the discretion of the developer of the MIDlet and the end-user. An end-user that downloads and installs a free midlet most likely will say yes to any prompt and may very well end up authorizing access to the PIM API for example, giving the midlet access to the user's contacts and calendar. The midlet could then forward this information to a remote server.

2.4.2 Browser issues

Security issues also arise from the use of web browsers on smartphones. If a vulnerable version of Internet Explorer or Opera is running on the smartphone, the smartphone can be compromised in the same way as an ordinary desktop.

3 THE CHALLENGES

3.1 *Legal issues and security policy*

As discussed above, the use of smartphones by employees extends the information system beyond company control. Control is also limited by legal considerations, especially when the smartphone belongs to the employee.

In this case, a number of options are available to companies :

- Banning the personal use of smartphones
  - Unrealistic : in the same way as banning personal use of the internet
  - Impossible to physically control and enforce
- Setting limits to the personal use of smartphones
  - By clearly defining the authorized interactions between the smartphone and information system
  - Impossible to physically control and enforce

When leakage of confidential information or occurs due to theft or loss of the smartphone, the enterprise may be held responsible for the subsequent losses, even though the smartphone may belong to the employee. This is true especially when the enterprise has not taken the required measures to prevent losses in accordance with the current state of the art.

The first step in countering the risks induced by smartphones in the enterprise is to acknowledge their existence and adapt security policy to the use of smartphones, and more particularly to the users of smartphones.

When the users happen to be upper management, which is the case most of the time, the key is to get these users into the loop, and inform them not only of the risks their use of smartphones generates, but also of the limitations of the devices and their associated technologies.

The security policy should set forth recommendations for each type of risk, and distinguish between dangerous and harmless actions.

The main actions that are important to define in the security policy are related to:

- Synchronisation (PIM, email with or without attachments)
- The use of the device in public areas (beware of hotspots, deactivate Bluetooth)
- Downloading and transferring files from the device to the information system

3.2 *A secure framework for smartphones*

Incorporating smartphones as elements of the information system implies a secure framework that includes :

- A centralized administration solution
- Mutual Authentication between the devices and servers
- End to End Encryption
- Hardening the smartphone

A centralized administration solution will allow better control of the devices and their interaction with the information system, using mutual authentication between the information system and the smartphone.

Encryption for communications and the data stored on the smartphone combined with central administration will help mitigate the risk of leakage of confidential information. In case of loss or theft of the device, the central administration solution would be able to remotely remove the data stored on the device.

And finally, smartphones need to be hardened in the same way as laptops, with the help of an anti-virus and personal firewall.

3.3 *Perspectives*

Smartphone security is complex. Its model implicates a number of actors, ranging from device manufacturers to telecommunications operators to software & protocol designers on one end and users, corporate policy makers and administrators on the other end.

For this model to work, it is important for this entire range of actors to take into account the risks associated with the use of smartphones and to take the adequate actions to mitigate these risks.

This however is difficult to coordinate, and legislation may be required to accompany the different actors in their actions.

The future of smartphone security is all set to be challenging. Will 4G networks, which will interconnect existing wireless networks from WPANs to WWANs, be secure?

4 CONCLUSION

Smartphones are complex in design and architecture, and the same goes for the network protocols used by smartphones. This complexity opens the doors to implementation errors and structural weaknesses, making smartphones vulnerable to different types of attacks. Attacks are simple to implement, and the growing interest in the technologies associated with smartphones will lead to the discovery of more weaknesses and multiply the risk of attacks. To secure a framework incorporating smartphones as part of the information system against attacks, the first step for organisations to take is to communicate with the users on smartphone security issues and work on and adequate security policy. Taking measures to secure the interactions between the smartphones and the information system and harden the smartphone can then help mitigate the risks associated with their use.

5 REFERENCES

[1] http://www.symbian.com/technology/symbos-v8x-det.html

[2] Bluetooth Core Specification 1.2

[3] http://www.irda.org/standards/specifications.asp

[4] http://ncsp.forum.nokia.com/downloads/nokia/documents/Known_Issues_in_the_Nokia_6600_v1_0_en.pdf

[5] http://www.cewindows.net/bugs/wm2003netsec.htm

[6] http://www.atstake.com/research/tools/info_gathering/

[7] http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf

[8] http://www.pentest.co.uk/documents/ptl-2004-01.html

[9] http://www.bluestumbler.org/

[10] Attacks on GPRS – Candolin, Lundberg.

[11] MIDP 2.0 Security Enhancements – Kolsi, Virtanen.

6 ABOUT THE SPEAKERS

Luc Delpha is a Consultant Manager at Cyber Risk Consulting, a French consultancy specialised in Information Systems Security. Cyber Risk Consulting is part of Cyber Networks, itself a leader in Information Systems Security on the French market, with proven experience in mobility and wireless security architectures and issues.

Luc Delpha has extensive experience in the field of cyber security, advising various government organisations and financial institutions on complex security issues and architectures. He was previously CSO of Citizentrade (financial portal-broker).

Today he leads a team of consultants working on security projects ranging from security audits, pen-testing, risk assessment, disaster & recovery plans, security policy and Public Key Infrastructure to wireless and mobility issues, as well as security architecture design and Netscoring© through a partnership with Marsh.

Maliha Rashid is the author of white papers on PDA and smartphone security. As a Consultant in Information Systems Security with Cyber Risk Consulting, she performs pen-tests, audits, risk assessment and works on security policies with a focus on security issues raised by emerging mobile and wireless technologies.

Contact information :

Luc Delpha : ldelpha@cyber-networks.fr

Maliha Rashid : mrashid@cyber-networks.fr