

CYBER RISK CONSULTING

Blackhat Briefings Europe 2004

Smartphone Security Issues

May 2004

Luc DELPHA – Maliha RASHID



Summary

1. **Introduction**
 - Why smartphones?
 - Functionalities
 - Operating Systems
 - Supported Connectivity
 - Wireless Networks

2. **Risks**
 - Inherent nature of smartphones
 - Bluetooth
 - GPRS
 - Java applications

3. **Challenges**
 - Legal Issues
 - Security policy
 - A secure framework
 - Perspectives

4. **Conclusion**



Summary

- 1. Introduction**
 - Why smartphones?
 - Functionalities
 - Operating Systems
 - Supported Connectivity
 - Wireless Networks
- 2. Risks**
 - Inherent nature of smartphones
 - Bluetooth
 - GPRS
 - Java applications
- 3. Challenges**
 - Legal Issues
 - Security policy
 - A secure framework
 - Perspectives
- 4. Conclusion**

1. Introduction

Why smartphones ?



■ Why smartphones?

- Same functionalities as traditional PDAs
- More connectivity
 - GPRS : Always on
 - Bluetooth
- Mainstream availability – Gadget Appeal
- General tendency to become more popular than PDAs
- Highly personal interaction

1. Introduction

Functionalities



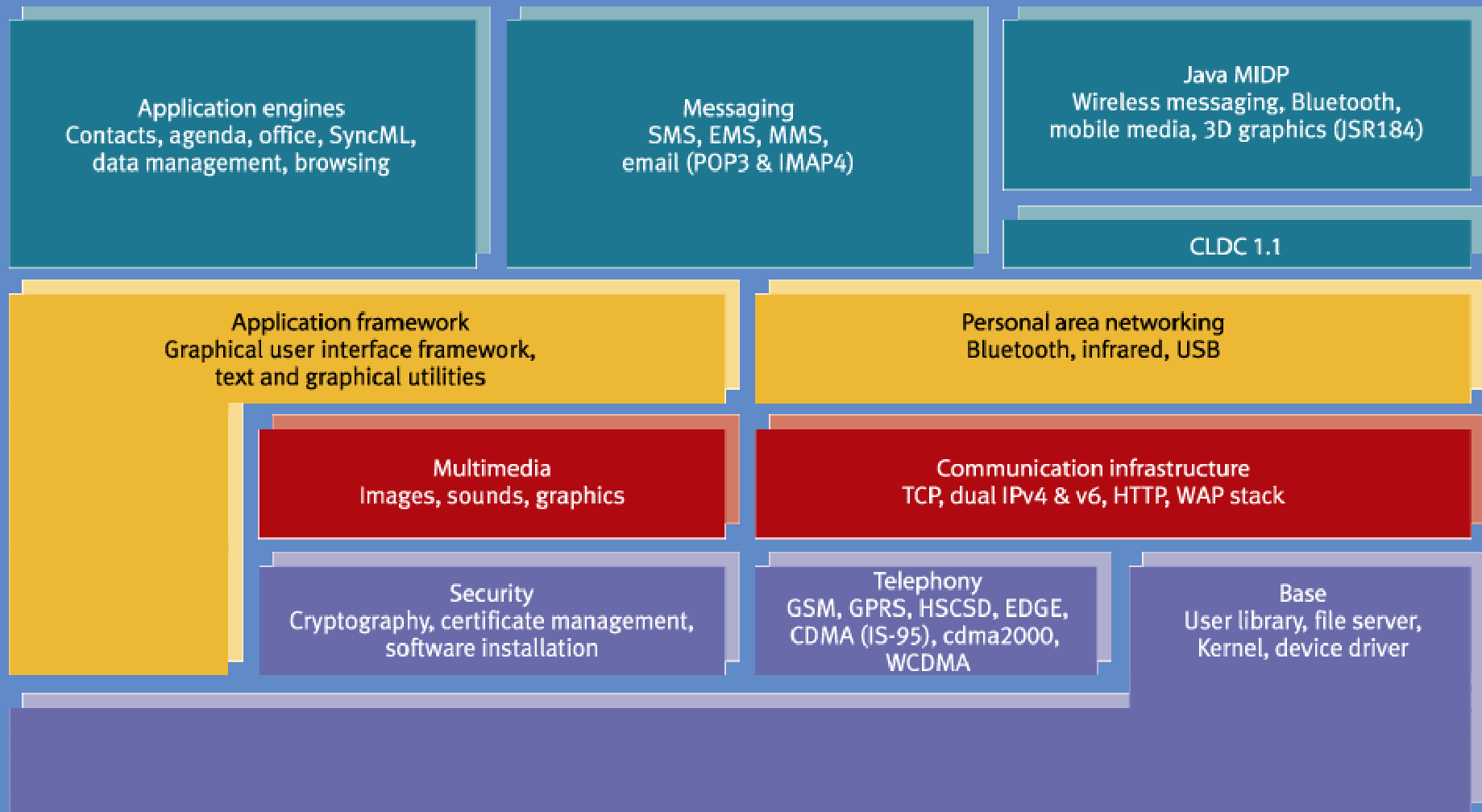
- Telephone : GSM / GPRS (in Europe)
- Camera
- PIM Data – (Personal Information Management)
 - Contacts
 - Calendar
 - Tasks
 - Synchronization
- Email client (POP3, IMAP)
- Web browsing
- Java Applications
- File exchange (vCard, photos...) via IrDA or Bluetooth
- Multi-player games with Bluetooth (N-Gage)

1. Introduction

Operating systems



- Symbian OS, Palm OS, Windows Mobile, Linux
- Symbian OS version 8.0



1. Introduction

Supported Connectivity



- GPRS : General Packet Radio Service

- Wi-Fi :
 - for PDAs
 - Symbian OS 8 supports Wifi

- Bluetooth

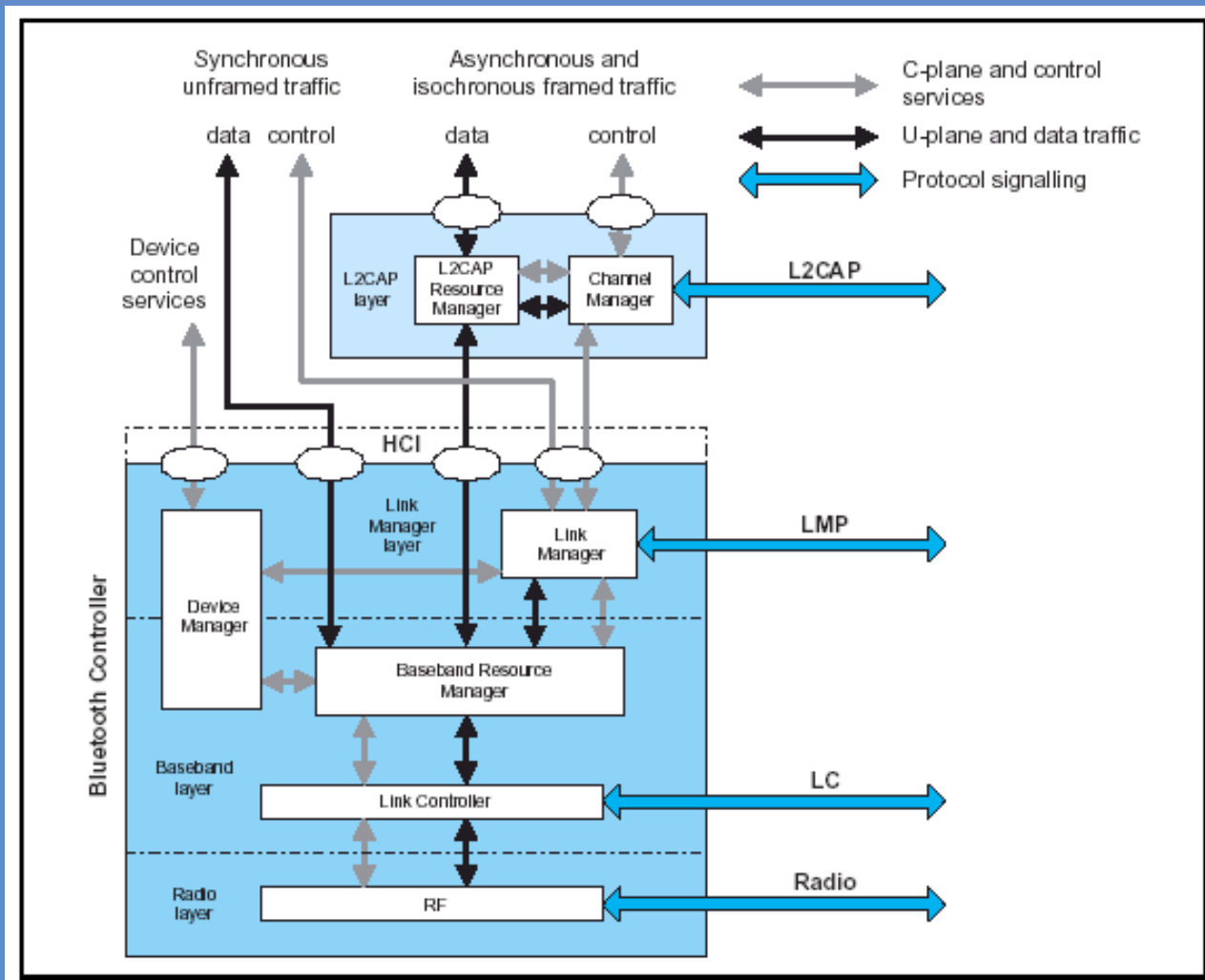
- IrDA

- ...

1. Introduction Bluetooth



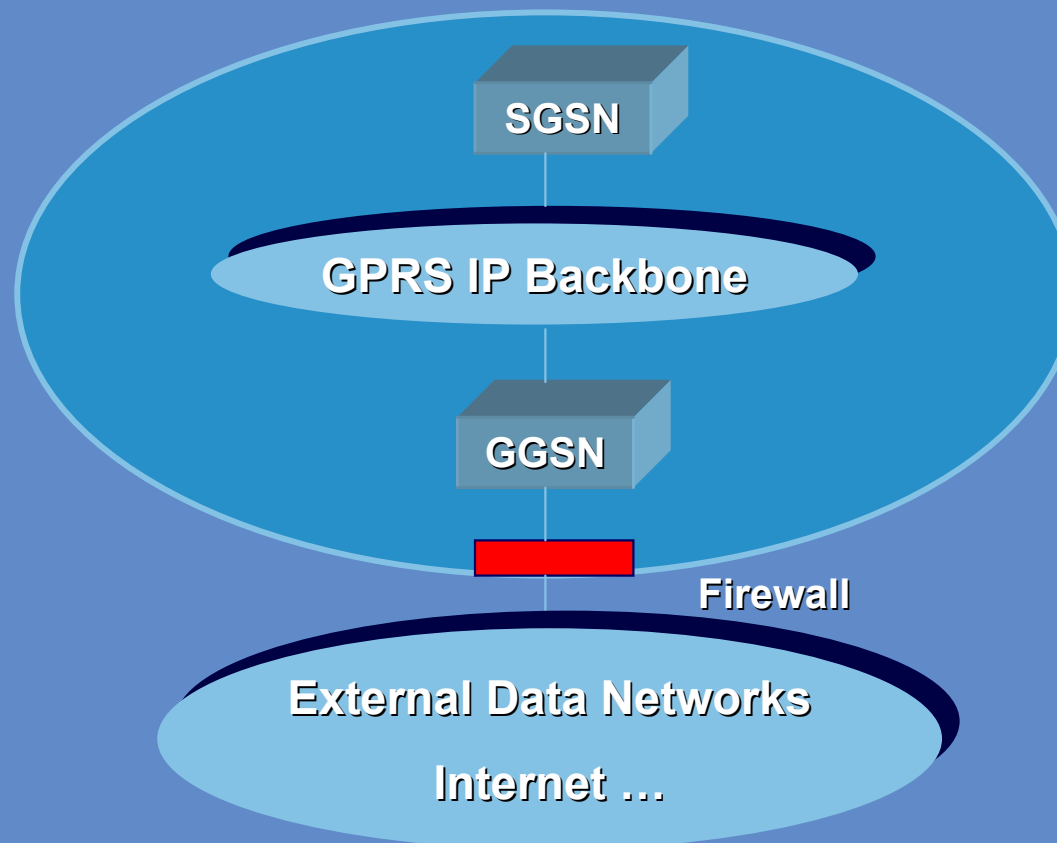
- Core specification more than a thousand pages
- Profiles : Synchronization - Service Discovery - Generic Object Exchange Profile ...



1. Introduction GPRS



- GPRS : Extension of GSM – IP Backbone
- Main Elements : GGSN & SGSN
- Firewall between the GGSN and external data networks





Summary

- 1. Introduction**
 - Why smartphones?
 - Functionalities
 - Operating Systems
 - Supported Connectivity
 - Wireless Networks
- 2. Risks**
 - Inherent nature of smartphones
 - Bluetooth
 - GPRS
 - Java applications
- 3. Challenges**
 - Legal Issues
 - Security policy
 - A secure framework
 - Perspectives
- 4. Conclusion**

2. Risks

Inherent nature of smartphones



- Dedicated operating systems
 - Bugs – Implementation errors – Security holes
 - MIDP 2.0 implementation issues on the Nokia 6600
 - Windows based devices

- Access Control
 - PIN Code
 - In most cases no native authentication for data stored on the device
 - With physical access to the device anyone can access the data (flash chipsets or removable memory cards)

- Device can easily be destroyed

2. Risks

The users



- Smartphone used to store confidential data
 - Corporate Diary, Email, Data
 - Personal Diary, Email, Data
- Risk of loss or theft because the device is not physically contained
- Synchronization with the information system
 - PIM Data – Email – Attachments ...
 - Difficult to control
- If the smartphone is compromised, the information system is exposed
- Back to corporate data... Understanding the user with the eBay example

2. Risks

Wireless networks - Bluetooth



- Bluetooth security implementation in smartphones restrained to :
 - non discoverable mode
 - pairing mechanism
- Non discoverable mode can be bypassed
 - Redfang – Btscanner
 - Brute forcing the last six bytes of the MAC Address and calling a `read_remote_name()`
- Ways to force the pairing – The Bluejacking craze
 - « U've been bluejacked » in place of Bluetooth device name
 - Send to surrounding Bluetooth devices
 - Watch surprised expression
 - Harmless but the message can prompt to pair
 - If pairing succeeds, bluejacker gets access to files on the victim's device

2. Risks

Wireless networks - Bluetooth



- Vulnerabilities in Bluetooth implementations
 - Nokia Bluetooth enabled phones vulnerable
 - CAN-2004-0143
 - Buffer overflow provoked by mal-formed OBEX message
 - Persistence of trust relationship even after the device has been removed from list of paired devices

- Bluetooth is a complex protocol
 - Interoperability of devices is a priority
 - Specification is deliberately not explicit on implementation details

- Implementation errors are bound to happen

- Increasing the risk of security holes

2. Risks

Wireless Networks - GPRS



GPRS security depends on measures taken by operator to secure the GGSN

If the GGSN is compromised, the GPRS network is exposed

- Possible GPRS Attacks :
 - Firewall
 - NAT : reserving all the ports
 - Flooding the GPRS connection with TCP traffic from the Internet

- Multiple PDP Contexts supported in Symbian OS v 8.0
 - Simultaneous private and public contexts
 - Private context can be attacked by public context !
 - Same as having a PC connected to the LAN and the Internet via a modem at the same time

2. Risks

Java Applications



- MIDlet : Java stand-alone application for mobile devices
- MIDP : Mobile Information Device Profile
- MIDP 1.0
 - Limited possibilities : Sandbox means limited access to the device
 - Limited security : No security manager, limited bytecode verification, security packages discarded due to performance issues, no support for HTTPS connexions
- MIDP 2.0
 - Concept of trusted MIDlet : If the MIDlet is trusted, access to PIM, Messaging, Bluetooth APIs amongst others
 - The user can decide whether or not to trust the MIDlet
 - Can the user be trusted to do this?

Third party malicious MIDlet can access information on the device and send it to a remote server, posing as an « innocent » application

- Game that prompts to connect to the Internet to put the highscores on a website



Summary

- 1. Introduction**
 - Why smartphones?
 - Functionalities
 - Operating Systems
 - Supported Connectivity
 - Wireless Networks
- 2. Risks**
 - Inherent nature of smartphones
 - Bluetooth
 - GPRS
 - Java applications
- 3. Challenges**
 - Legal Issues
 - Security policy
 - A secure framework
 - Perspectives
- 4. Conclusion**

3. Challenges Legal Issues



- Given the risks, the use of these devices by employees needs to be supervised
 - Forbidding use
 - Unrealistic
 - Impossible to control and enforce
 - Same dilemma as allowing personal use of the Internet at work
 - Privacy issues in France and most of Europe

- Even if the device belongs to the employee, responsibility belongs to the company to secure the data
 - In case of disaster – the eBay worst case scenario – Company responsible

3. Challenges

Security policy



- Inform employees of risks
- Clearly define interaction between smartphones and information system
- Clearly define harmless and harmful actions
- Clearly define what the smartphone infrastructure can and can't do
- Define the limits of existing technologies

3. Challenges

A secure framework



- Treat the smartphone like a laptop
- Centralized administration
- Mutual authentication between devices and servers
- End to end encryption :
 - VPN IPSec
- Harden the smartphone
 - Logon authentication
 - Encrypt the data
 - Antivirus
 - Personal Firewall

3. Challenges Perspectives



- Smartphone security model is complex because :
 - Implicates a variety of actors :
 - Manufacturers
 - Operators
 - Smartphone designers
 - Software designers
 - Protocol designers
 - Administrators
 - Policy makers
 - Last but not least : Users
 - Goals of these actors may conflict
 - Coordination is difficult
 - Legislation may be required



Summary

1. **Introduction**
 - Why smartphones?
 - Functionalities
 - Operating Systems
 - Supported Connectivity
 - Wireless Networks

2. **Risks**
 - Inherent nature of smartphones
 - Bluetooth
 - GPRS
 - Java applications

3. **Challenges**
 - Legal Issues
 - Security policy
 - A secure framework
 - Perspectives

4. **Conclusion**

4. Conclusion



- Smartphone design, architecture and associated network protocols are complex
 - Door open to :
 - Implementation errors
 - Structural Weaknesses

- Growing interest in GPRS and Bluetooth
 - Attacks simple to implement

- To counter these risks :
 - Communicate with users on the risks
 - Anticipate on incorporating these devices as part of the information system
 - Create a suitable environment in which these devices can be used

Questions / Answers

