available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Future consumer mobile phone security: A case study using the data-centric security model

André van Cleeff

University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands

ABSTRACT

Consumer mobile phone security requires more attention, now that their data storage capacity is increasing. At the same time, much effort is spent on data-centric security for large enterprises. In this article we try to apply data-centric security to consumer mobile phones. We show a maturity model that can be used as a roadmap for improving their security. Additionally, several shortcomings of the data-centric approach are discussed.

1. Introduction

In the interconnected world that we live in, traditional security barriers are broken down. Developments such as outsourcing, increased usage of mobile devices and wireless networks each cause new security problems.

To address the new security threats, a number of solutions have been suggested, mostly aiming at securing data rather than whole systems or networks.

However, these visions (such as proposed by the Jericho Forum, 2005 and IBM (Grandison et al., 2007)) are mostly concerned with large (inter-) enterprise systems. Until now, it is unclear what data-centric security could mean for other systems and environments. One particular category of systems that has been neglected is that of consumer mobile phones. Currently, data security is usually limited to a PIN number on startup and the option to disable wireless connections. The lack of protection does not seem justified, as these devices have steadily increased in capabilities and capacity; they can connect wirelessly to the Internet and have a high risk of being lost or stolen (Mailley, 2006). This not only puts end users at risk, but also their contacts, as phones can contain privacy sensitive data of many others. For example, if birth dates and addresses are kept with the contact records, in many cases a thief will have enough information to impersonate a contact and steal his identity.

Could consumer mobile phones benefit from data-centric security? How useful is data-centric security in this context? These are the core questions we will try to address here.

2. The current status of mobile phone security

How serious the physical security threat to mobile phones is, becomes clear when we look at theft statistics. In the UK, an estimated 710,000 mobile phone thefts occurred in 2001 (Mailley, 2006), which increased to over 2.6 million in 2006 (Haurant, 2006), or one phone every 12 s. The direct costs of loss and theft were estimated at pounds 390 million. Two particular mechanisms that have been implemented to counter theft are the blocking of the phone from the network using the phone's unique IMEI number, and tracking the phone's location while it is still connected to the network (Ristenpart et al., 2008). However, these mechanisms cannot solve the physical security problem; small items like mobile phones that are carried around will be lost and stolen, no matter how much effort is put in prevention. Phone loss can even be an unintended consequence of a car or bag theft.

Another issue is that mobile phones are becoming the target of viruses, worms, and Trojan horses: Even if the phone is under physical control of the user, data could still be stolen

E-mail address: a.vancleeff@ewi.utwente.nl

1363-4127/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2008.10.003

from it. Already, several phones (Apple's iPhone, Nokia's N95) have storage capacity that is measured in gigabytes. How to keep all this data secure should therefore be a core objective for improving mobile phone security.

To understand what data security actually entails, we will discuss one particular model called the ''data-centric security model'' or DCSM (Grandison et al., 2007) and as a case study, apply it to mobile phones.

3. The data-centric security model

The DCSM was developed by IBM to solve two major problems in achieving (cost) effective security:

1. how to apply security measures proportionally to the value of the systems they protect.
2. how to allow high-level specification of IT policies that can be implemented at lower (technical) levels without distortion.

These problems are solved in the following way:

> As a paradigm, the focus in the DCSM is on deriving the right security level, based on a business analysis of the data being handled. This data classification then drives the properties and access control policies governing the use of data by applications that implement business processes. Security services and their underlying mechanisms can be abstracted into interfaces that directly support data management policies. (Grandison et al., 2007, p. 86)

If we look into the details of the model and how to interpret it, we find that the 'model' of the DCSM actually consists of several different elements:

1. The DCSM as a paradigm for managing security, as discussed before
2. The DCSM as a methodology for implementing appropriate security
3. The DCSM as a means of deployment for security mechanisms
4. The DCSM as a maturity model for IT security.

Here we look at the latter three.

3.1. *Methodology*

In applying the DCSM, the first step is to gather business requirements and regulations. These are used to classify the data, for example based on the owner and given security requirements. Classification can be done using criteria such as origin, ownership, control, data holder and data type. Next, we formulate policies about how the data should be handled. We define who can use the data, how long it can be stored and what safeguards should be in place. In turn, these policies can be implemented using the appropriate security mechanisms. This is illustrated in Fig. 1.

3.2. *Deployment*

Secure operation is made possible by a security infrastructure that handles tasks such as identity management, access control and safe transport. Access to the data is only possible via the data control layer or DCL, which utilizes the security infrastructure. This is illustrated in Fig. 2.

3.3. *Maturity model*

To help organizations implement the DCSM gradually, it comes with a maturity model of four adoption levels. These levels are shown in Table 1.

4. Case study on mobile phones

Now that the DCSM has been discussed, we will do a case study on its application to mobile phones. Obviously, this requires a case study subject - we need a reference mobile phone implementation to which we can apply it. Here, our reference point is loosely based on the Nokia N95 8 GB. Its market introduction was in the first quarter of 2008; at that time, it was the Nokia flagship consumer mobile phone. Network connections are possible via 3G mobile networks, WLAN, Bluetooth, infrared and USB. Data synchronization with a PC is possible for items such as contacts and calendar events. The entire file contents are accessible via USB. Additional software is available to connect to sites such as Flickr to upload photos. A schematic overview is given in Fig. 3.

In applying the DCSM, we also need to consider what viewpoint should be used; the deployment, the paradigm, the methodology, the maturity model, or a mixture of these? Here we choose to concentrate on the maturity model. The intent is to show how consumer mobile phone security can be improved step by step, using a data-centric approach. For each level, we state the requirements of the DCSM and elaborate how they could be implemented.

4.1. *Adoption level 1: basic*

4.1.1. *DCSM requirements*

At this level a baseline security infrastructure is in place, covering all information assets, ranging from critical to non-critical. As a result, some assets will be over protected, while others are insufficiently protected. The baseline security infrastructure provides the foundation on top of which more complicated policies can be enforced later.

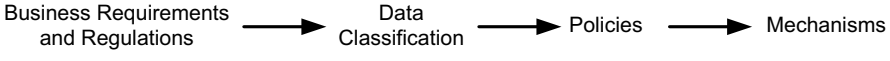

Fig. 1 – High-level view of DCSM methodology.

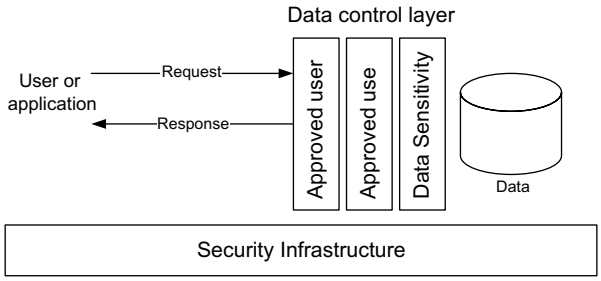

Fig. 2 – DCSM deployment model (Grandison et al., 2007, p. 89).

4.1.2. *Elaboration and implementation*

For PCs there is already a consensus about what the essential security mechanisms should be, such as a firewall, anti-virus, anti-spyware and automatic patch management. These would also be required for mobile phones. Added to that, the basic security infrastructure for mobile phones should provide extra authentication and data storage security mechanisms.

Concerning authentication, there is a problem with password authentication. Mobiles phones are not used continuously and for adequate security, the user should authenticate again after every break. This hinders usability and therefore most users only type in the password (the PIN number) when the device is powering up. It would be better to complement the password with a fingerprint reader (so called two-factor authentication). This allows for quick authentication. For example, when a mobile phone is lent out to other persons to make a phone call, there would be no need to access all content on the phone. Fingerprint readers have already been implemented in a limited number of devices such as those from Toshiba (www.3G.co.uk, 2007) (Fig. 4).

An additional feature could be to implement different user accounts. As mobile devices are personal, they normally have just one account; For example Windows Mobile only has privilege levels (Microsoft, 2007).

Other required data security mechanisms would be:

- Encryption of all content on the device
- Automatic and remote backups
- Remote wiping software

Encryption is already available for BlackBerry smartphones (Research in motion limited, 2008). Backup functions are also becoming more common, but then in the form of synchronizations; For example the iPhone can be used in combination with the MobileMe website (Apple, 2008) using so called 'Push technology', all servers are notified of changes in one location, which are then propagated to other sites. With wireless 3G connections this can even be done remotely. Remote wiping is also an interesting addition to the security: In case the phone is stolen but a network connection is still present, the phone can be controlled remotely to prevent possible data theft. This is already implemented in some applications, such as Guardian Mobile (2008).

Table 1 – DCSM maturity model (Grandison et al., 2007, p. 93).

Adoption levels	Basic	Intermediate	Advanced	Full
Security infrastructure	X	X	X	X
Business data classification		X	X	X
Role definitions		X	X	X
Policies by classification		X	X	X
Labeled data			X	X
Data flow analysis			X	X
Automatic policy provisioning				X

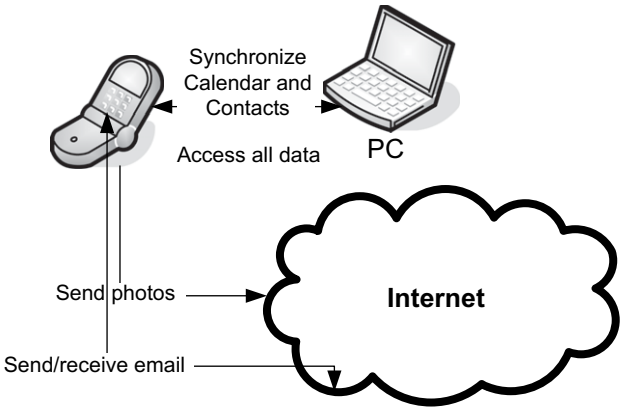

Fig. 3 – Reference phone in context.

4.2. *Adoption level 2: intermediate*

4.2.1. *DCSM requirements*

The second maturity level includes all requirements from the previous level. Added to that, data is classified and the protection levels are determined for each data category. Each system (or component) is protected based on the most critical data that is handled by it.

4.2.2. *Elaboration*

The first step is to define the requirements and applicable regulations.

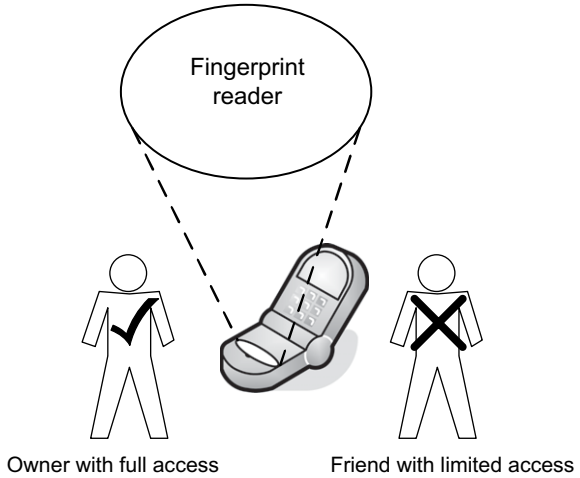

Fig. 4 – Application of fingerprint reader.

4.2.3. *Requirements*

For business, this step starts with assessing the business value of the data, for example in terms of losses when confidentiality, integrity and availability are breached. Data classification is ideally driven by the value of the data, which is related to the business processes that are supported by it. Security measures are taken proportionally to the value of the data; It is up to a business to determine the appropriate security and cost level.

For consumers, the situation is different, as the data does not serve a business process and is not linked to any profit. There is no CEO or CIO that can state business rules and regulations. The cost-security tradeoff is also different; One of the reasons that consumer mobile phone security is at such a low level is that few individuals are willing to pay for additional security measures; extra security precautions might be effective but hinder usability. Some noticeable differences between the business and consumer situation are shown in Table 2.

Regarding confidentiality, the most obvious consumer requirement would be privacy protection. Unfortunately, it is hard to place any monetary value on privacy (for an attempt to price on-line privacy, see Hann et al., 2002). Regarding integrity and availability, we need to consider the hassle of data loss and the value of a personal archive of data - such as vacation photos and emails. Items such as contact data can be recovered from other sources in many cases, for photos this might not be possible. Another requirement is that of usability: The device should provide adequate security for privacy sensitive data, with as little user intervention as possible. In addition, data integrity and availability must be assured.

4.2.4. *Regulations*

There are many regulations about data storage and processing. As for data security requirements, one of the most notable in the EU is the data directive (Council European Parliament, 2006), but this is not concerned with data usage by individuals and households. Some exceptions include regulations concerning copyright and adult content. Other problems arise when the device is also used for business purposes. Data gathered for a business could be subjected to privacy regulations. An example would be sent and received email. As a whole, regulations (and enforced compliance) are not a big concern for consumers and we will ignore them accordingly.

Table 2 – Differences between business and consumer situation.

Aspect	Business	Consumer
Data value	Related to business value	Related to personal needs such as privacy
Applicable rules	Top-down, from the CEO and legal requirements	Personal, undefined
Impact of security breach	Financial losses, threat to business continuity	Loss of privacy, extra work to recover data
Main security tradeoff	Security - cost	Security - cost/usability

4.2.5. *Data classification*

The next step in the DCSM is to classify the data.

4.2.6. *Type of data*

Typical data items stored on mobile phones are:

- Calendar events (including todo items and notes)
- Contacts
- Messages (text and multimedia messages, emails)
- Images
- Sound files (music, voice memos)
- Video clips (movies, clips)
- Office documents (PDF, MS Word, MS Excel)
- Logs (call and synchronization records)
- Preferences settings (alarms and backgrounds)
- Security settings (email connection and passwords, WLAN keys).

4.2.7. *Ownership and control*

Because the mobile phone is a personal device, the owner will normally be the main user. However copyright might reside at another party, as is the case for received emails and music. (Again, the situation is different when the phone is used for business purposes.) As a whole, ownership of the files is of no particular interest here - what is on the phone should be fully accessible to the phone owner.

4.2.8. *Data origin*

The first distinction here is between data that is captured using the device (audio, images, videos) and data that is transferred to it. The latter could be divided into three parts:

- Personal data
- Data from friends or personal contacts (such as pictures sent by Bluetooth)
- Third party data (with whom there is no direct relation, such as music).

4.2.9. *Data value*

Next we determine the particular value of the data. We propose to do the valuation based on the potential impact of a security breach:

- In terms of loss of confidentiality
  - disclosure of private information of the owner
  - disclosure of private information or from other persons
  - disclosure of security information for other systems
- In terms of loss of integrity
- In terms of availability
  - Loss of useful data that can be recovered from other sources
  - Loss of useful data that cannot be recovered from other sources.

Integrity will be ignored here, and we group the data together in two dimensions: Public (non-confidential or third party) versus private, and recoverable versus non-recoverable (Table 3).

Table 3 – Data groups.

	Public (non-confidential)	Private (confidential)
Recoverable	I	III
Non-recoverable	II	IV

Data in group IV has the highest value, followed by III, II and I. Next we put the data types in the different groups (Table 4).

4.2.10. *Policy aspects*

For each of the data groups we need to define policies. In this case study we will focus on just three policies:

- How are backups made? (daily/on creation or change)
- Is the data encrypted or not?
- What rules apply on export? (user confirmation, target system must be trusted)

This could lead to the following policy-data matrix shown in Table 5.

4.2.11. *Implementation*

Each application that uses one of these data items would need to apply the highest security level of all the data items it handles. When a user installs a new application, the application will request permissions for certain data items and connections. For example, a map application might use the Internet connection to download updated map information, but is not capable of accessing any contact data.

4.3. *Adoption level 3: advanced*

4.3.1. *DCSM requirements*

The third maturity level includes all requirements from the previous two levels. Here, all data and communication channels are labeled at runtime. An application processing a particular data item will select the appropriate policy automatically.

4.3.2. *Implementation*

Newly received images, emails and SMSes are all labeled according to their source of origin and other classifications. One way to achieve this is to attempt to link the data to a particular person or group of persons - then specific policies could be applied which hold for this person. This results in a more refined security model than was described at the second maturity level. Unclassified data (for example images) resides in a queue, for later processing.

Table 4 – Data types and groups.

Group	Data type
I	Multimedia - third party
II	Preferences settings
III	Messages, Calendar, Contacts, Multimedia - received from friends, Logs, Security settings
IV	Multimedia - user created, Notes

Table 5 – Data types and groups.

Group	Backup policy	Encryption policy	Export policy
I	Daily	Unencrypted	None
II	Daily	Unencrypted	User confirmation
III	On creation or change	Encrypted	User confirmation, trust required
IV	On creation or change	Encrypted	User confirmation, trust required

4.3.3. *Connections*

Connections with other devices and applications such as PCs and online-sharing websites are also labeled. For example, personal pictures cannot be sent to a sharing website unless SSL is used and authorization controls are in use on that site. The same is true when connecting the device using USB to an unknown computer. Pictures can be watermarked before export, such that in case of a security breach, the source of the breach can be found.

4.4. *Adoption level 4: full*

4.4.1. *DCSM requirements*

The fourth maturity level includes all requirements from the previous three levels. At this level, policy management is automated. A generic policy can be specified top-down and automatically implemented by different systems. Vice versa, policies from different systems are gathered bottom-up and checked for compliance with the high-level policy.

4.4.2. *Implementation*

The phone provides a unified security configuration, to which all applications must conform. The operating system employs a capability security model, meaning that each application can request data items, but the OS decides whether this is allowed. Data access is also logged, and periodically checked for compliance with the policies.

5. Conclusions

We have discussed the data-centric security model in detail, and demonstrated its application in a case study of consumer mobile phones. This resulted in a model for stepwise improvements of their security.

On the whole, we found the DCSM to be quite well applicable in a consumer situation, outside of its intended business scope. It was possible to split up the different types of data, and define appropriate security levels. One noticeable problem is the second maturity level; if an end-user device or application has to be configured at the highest security level of the data it is going to handle, the usability will be very low. In this case, intermediate and advanced levels could better be merged.

A point for discussion is how much effort should be put in classifying data. If the baseline policy is to encrypt all data, is it worth to spend additional effort in securing different types of data with specific encryption methods?

One omission of the DCSM seems to be that it does not take the program data itself into account. Data can only be secure if the programs that use it are also secure - but these programs consist of data themselves. This program data might not have direct business value, but when compromised (for example due to a rootkit), the security of other valuable data is at risk. Securing program data could be a requirement for baseline security, but maybe a more elegant solution is possible, by treating program data as a special data type.

As for the maturity model itself, we see several applications. First, it could be used to create a guideline for consumers. With it, they can make informed decisions about which phone to buy and afterward determine how much effort they want to put in securing their data; In general, the higher the maturity level, the more configuration needs to be done.

Obviously, it is up to developers to implement the security mechanisms first. For this, the maturity model can serve as a roadmap for the development of more secure mobile phones. The first step in the implementation would be to create the data control layer in the operating system. Secondly, a standard model for policies is needed, that could be implemented by different applications. One interesting development here is the Android operating system, the new and open source mobile platform from Google (2006). Its availability would allow to implement new security features and distribute them to end users at little cost.

Combined, this puts security in the hands of both developers and end users: Ultimately, mobile phone security is their call.

Acknowledgments

We thank Pieter Hartel, Pascal van Eck, Siv Hilde Houmb, and Trajce Dimkov for their help with the paper.

This research is supported by the Sentinels program of the Technology Foundation STW, applied science division of NWO and the technology programme of the Dutch Ministry of Economic Affairs under project number TIT.7628.

REFERENCES

Apple. MobileMe. Available from: http://www.apple.com/mobileme/; 2008.

Council European Parliament. Directive 2006/24/ec of the European parliament and of the council. Official Journal of the European Union. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, 2006;L 105:54–63.

Google. Android – an open handset alliance project. Available from: http://code.google.com/android/; Tuesday 16 May, 2006.

Grandison T, Bilger M, O'Connor L, Graf M, Swimmer M, Schunter M, et al. Elevating the discussion on security management: the data centric paradigm. *Business-Driven IT Management, 2007*. BDIM'07. 2nd IEEE/IFIP International Workshop on, pp. 84–93, 2007.

Guardian Mobile. Guardian mobile usage. Available from: http://www.guardian-mobile.com/usage.pdf; 2008.

Hann IH, Hui KL, Lee TS, Png IPL. Online information privacy: measuring the cost-benefit trade-off. 23rd International Conference on Information Systems, 2002.

Haurant Sandra. Mobile stolen 'every 12 seconds'. Available from: http://www.guardian.co.uk/money/2006/may/16/internetphonesbroadband.phones; Tuesday May 16, 2006.

Mailley Jen. UK mobile phone theft costs at least £1Bn. Available from: http://www-staff.lboro.ac.uk/ssgf/PDFs/2006_Cost_of_Mobile_Phone_Theft.pdf; 2006.

Microsoft. Understanding the windows mobile security model. Available from: http://technet.microsoft.com/en-us/library/cc512651.aspx; 10 January, 2007.

Research in motion limited. BlackBerry enterprise solution security version 4.1 technical overview. Available from: http://www.resourcecenter.blackberry.com/resource/xHCO-BlackBerry_Enter prise_Solution_Security_version_4.pdf; 2008.

Ristenpart T, Maganis G, Krishnamurthy A, Kohno T. Privacy-preserving location tracking of lost or stolen devices: cryptographic techniques and replacing trusted third parties with DHTs. USENIX Security '08, to appear, 2008.

The Open Group Jericho Forum. Jericho whitepaper. Available from: http://www.opengroup.org/jericho/vision_wp.pdf; 2005.

www.3G.co.uk. Fingerprint touch controls enable data protection and usability enhancements in Toshiba 3G phones. Available from: http://www.3g.co.uk/PR/Feb2007/4258.htm; 12 February, 2007.