Trust and Confidence in Open Systems: Does Security harmonize with Mobility?

Uwe Baumgarten, Claudia Eckert, and Harald Görl
TU Munich, Faculty for Informatics
D-80290 Munich, Germany
Tel.: +49 89 289 23259, Fax: +49 89 289 22037
{baumgaru,eckertc,goerl}@in.tum.de

Abstract

Mobile devices like organizers, mobile phones, notebooks, other personal appliances and equipment as well as traditional PCs and workstations interconnected by wireless and other networks make up today's computing and communication environments (see [3], [1]). By now, mobile devices are in use for business work as well as for personal applications like private e-mails and electronic commerce. As mobile devices will play an important role in our social and business life, studying their trusted and confidential usage in possibly untrusted and unconfidential environments is urgently required.
The intention of this position paper is to stimulate discussion about the relevance of trust and confidence in the usage of mobile devices. In this sense we try to explain the characteristic situations of mobile devices, to explain their special needs, to give a short overview of some relevant OS in this area including the distinction to similar approaches in embedded systems, to focus on some selected needs in mobility and security (here Trust and Confidence), to present a short overview of the solution architecture for these needs within our research project. We then focus in this paper on the requirements the operating software of such systems should fulfill.

Keywords

Mobile Device, Operating Software, Mobility, Security

1 INTRODUCTION AND MOTIVATION

Trust and confidence (for short TC) are key attributes in the field of mobile secure communication and mobile secure computation. In the next paragraphs we give a short motivation in terms of a scenario and some questions all around our theme and our major objective *"Usage of Mobile Devices with Trust and Confidence"*.

Mobility here means physical mobility of a device operating in different physical environments. In addition software components may be mobile being executed on different mobile devices and/or in various places. Beyond the general security aspects – like information confidentiality, information integrity, information and service availability and non-repudiation – security for mobile devices involves problems originated in their size, weight, and personal usage, in the heterogeneous environments, they are part of, and their dynamic extensions.

(1) What are the Questions of Usage to be asked?
Situation: We are using our mobile device (for short MD) anywhere and anytime. Some interesting questions are:
(Q1) We want to send a confidential message to a certain person and nobody else, and we want to get an acknowledgment of its delivery. Does our MD work in this way anywhere and anytime?
(Q2) Are we able to defend our MD against any attacks of any third party? Is unauthorized disclosure of information possible?
(Q3) Some day we use our MD in order to control our TV. The next day we are in our credit bank, try to control our banking account, and start a new financial transaction with our next TAN (transaction number). Is the current working environment OK and can we start that transaction now?

(2) What is TRUST, what is CONFIDENCE?
Many subjects (persons, active devices) exist in our environment. Two questions may give a first feeling for trust and confidence.
(TC1) Whom can we trust?
What are Third Parties? (known / unknown) ? (trusted / untrusted) ?
(TC2) We look at our MD and ask: "Is it that, what we mean, it is?"

(3) Assumptions.
We have to make some assumptions about the MD in its environments.
(A1) We don't have and we don't expect an *all-in-one* device suitable for every purpose (in german: *"eierlegende Wollmilchsau"*) in the (near) future.
(A2) But, devices which we can dynamically customize and personalize will come very soon.

(4) Consequences.
In order to use a MD anytime with trust and confidence the following is necessary.
(C1) It is necessary to be able to make a Trust and Confidence Test anytime the user wants.

(5) What is the model?
In order to state trust and confidence we need a simple model for this situa-

tion.
(M1) The simple model includes the following components: the mobile devices, the users, and third parties. Confidence should be stated between users and MDs, trust should be stated between mobile devices and the environment with third parties.

(6) TC-Approval – the key issue.
Now, our main task is to enable controlling of trust and confidence via TC-Approval. We are going to describe the stages of this approval later.

(7) What are the parts needed for TC-Approval?
Today's mobile devices are not well prepared for approving TC. Necessary support is needed of
(N1) Specifications (of various properties concerning trust and confidence),
(N2) States (of execution, attributes of components, etc.),
(N3) Prove rules (for matching specifications and states),
(N4) Assumptions (about the system and the environments), and
(N5) Assertions (about the base; MDs, users, environments)

(8) Proposed Architecture.
With respect to our objectives the central questions are now:
(K1) What is necessary in the design and implementation of such a MD?
(K2) What are the concepts for the operating software of a MD in order to support TC?
Figure 1 shows our proposed architecture. It is a simple layered architecture (with four major layers) combining components of computing, communication, and security. The layers are levels of abstraction, comprising the hardware, operating software, services and middleware, and applications. (With mobility aspects this model is described in [2]). Like a 'supporting pile' security features are based upon special hardware. In each layer security features are incorporated, based upon the layer below, but just as well allowing access and usage across the layers. In each layer these security features are required as a base (basic security features, enhanced security features, and application security features).

2 MOBILITY AND SECURITY: SOME ASPECTS

In this section trust and confidence will be explained with some degree of detail.
Trust and *Confidence* are the key terms here. In general, we use our mobile device anytime and anywhere. Anytime we want to be enabled to make a test of trust and confidence of the whole system and its components.
This is necessary, because we use personal information, some very sensitive information, and sometimes very valuable expensive information, which has

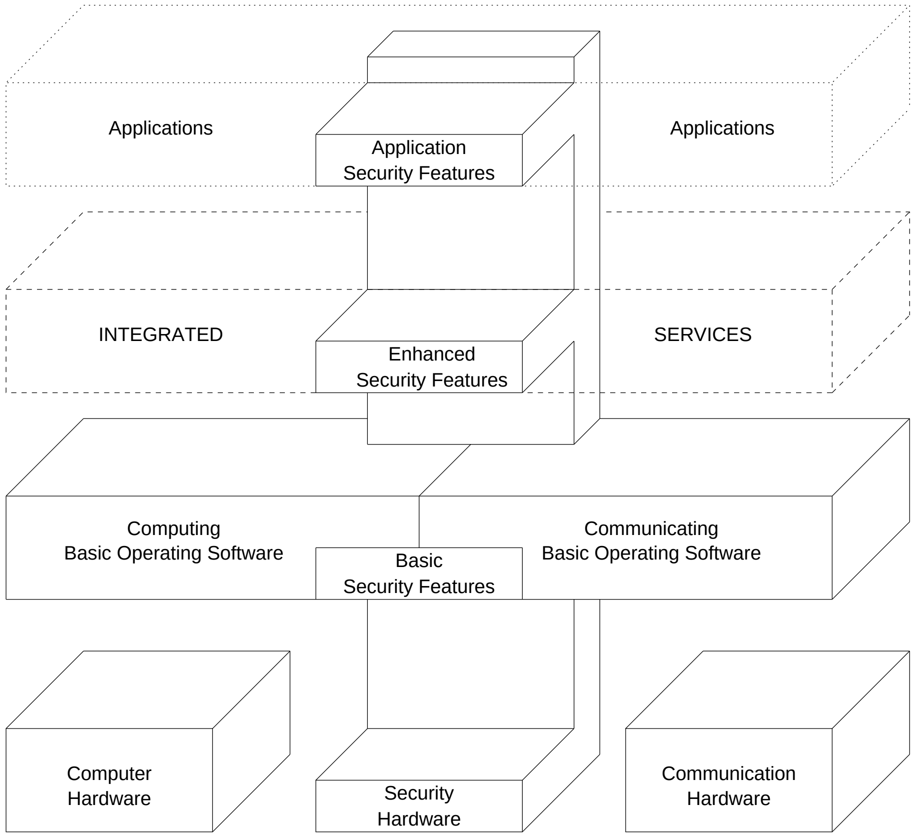

Figure 1 COMP + SECU + COMM Architecture

a high value. So it is very important for the user, to be aware of MD's trust and confidence every time. In order to differentiate individual requirements and situations stages of TC are established. Only two of these TC-stages are mentioned here.

TC-Approved: static and forever!
Is it possible to prove TC once before using the MD, so that TC holds forever for all components? No, this is impossible, because hardware and software may change, configuration, data, and requirements of the user may change, too.
... (many other stages) ...
TC-Provable: dynamic and everytime!
This is the objective!
Main Task: build a mobile device and environment, which supports TC-Provability.

Besides these stages different qualitative aspects may be defined. These may be documented in (in an unsorted manner): Provable assertions, certificates, documents from official sites, certified documents, signed documents, attestations, passports, and so on.

3 REQUIREMENTS

For the TC-approval some basic features are required. We will describe the necessary functions in an top-down manner. But we are going to describe only a few steps of refinement here. Let us first describe the simplest case.
One-Button-General-Answer
The mobile device has a special button. Once pressed (by a random user) a green light shows its user, that it is ok, whereas a red light indicates loss of TC.
The result of the TC-Approval may be statically found (printed as TC-label on the MD) or it may be computed dynamically.
One-Button-Individual-Answer
In our case MDs are personalized. Additional requirements arise.
(R1) User-to-MD and MD-to-User Authentication is necessary.
Until now we see the MD as a black box. In the next step we differentiate between various environments, like trusted home environment, trusted foreign environment, untrusted foreign environment. Additional requirement:
(R2) MD and User are able to distinguish between a foreign-trusted and a foreign-un-trusted working environment.
(R3) Every environment may observe only those attributes of an MD it allows.
Based upon the architecture as shown in figure 1 all higher layers are assembled from (interacting, depending) components. These components may be exchanged (dynamically, on the fly, with or without awareness of the user, with or without test of TC-Approval upon exiting or entering the system, and so on). An additional requirement is:
(R4) States, which are TC-approved, are necessary, transitions between those states, perhaps TC-approved transitions, are necessary.
Besides changes in the systems, user's criteria for TC-Approval may change. In addition:
(R5) Specification of criteria is necessary.
(R6) The MD has those functions, the User expects from the MD.

4 POSSIBLE SOLUTIONS

Mobile devices (at the moment and in the near future) will be (very) small and have to handle resource shortages in all of their basic facilities, namely computing, storing and communicating facilities. In addition, they will have a

short product life time. Nevertheless, many upgrades in software and hardware will be installed. They have to work in very different environments under different conditions.
At the moment, a MD with TC-Approval does not exist on the market, but many necessary components are available. This statement holds both for the hardware layer as well as the software layers above the hardware.
Components at the hardware layer of a TC-approved system (in both areas: mobile device and environment) could be a Microprocessor / Microcontroller (Computing Hardware), a DSP (Communication Hardware), a ChipCard and PIN-I/O-Interface or Biometric-Input-Interface (Security Hardware). The ChipCard may be tested for TC-approval inside the mobile device. Alternatively the ChipCard may be tested outside, perhaps in a trusted home environment or in a trusted third party environment.
The mobile device as a whole may have 'fixed' and 'dynamic' parts, each of them may be TC-approved in a trusted home environment or a trusted third party environment.
At the operating software layer algorithms and techniques for Cryptography, Authentication, Invariants, Sandboxing, User-Definded-Conditions, Trusted-Stable-Available-Storage (Online-Bank-Safe) may be used.
Especially these areas, where mobility meets security in mobile devices, are of most importance with respect to the operating software.

5 OVERVIEW, RELATED WORK, CONCLUSIONS AND FURTHER WORK

There is nothing appropriate at the market today. Neither the mobile devices, like appliances, PDAs, embedded systems, nor the operating systems, like PalmOS, Symbian, WindowsCE, or other, provide any substantial support for TC-approval.
Therefore, we have begun to make a detailed threats analysis, evaluate existing operating systems and tools, define an appropriate architecture (see figure 1), and to fill up their layers with approriate abstractions and components.

REFERENCES

[1] B. R. Badrinath, Arup Acharya, and Tomasz Imielinski. Impact of Mobility on Distributed Computations. *ACM Operating Systems Review*, 27(2):15–20, April 1993. VORHANDEN.

[2] U. Baumgarten. Personal assistance by means of mobile objects. In *Proceedings of ECOOP'96 Workshop on Mobility and Replication*. ECOOP, August 1996.

[3] M. Weiser. Some computer science issues in ubiquitous computing. *Communications of the ACM*, 36(7):74–84, 1993.