Robust Data Management in Mobile Environments

Prof. Dr.-Ing. Wolfgang Lehner

Faculty of Computer Science / Database Technology Group

01062 Dresden, Germany

Motivation

Mobility gains more and more importance from a technological as well as social perspective. On the one hand, mobility is required from the personal and professional environment in order to keep pace with the developments in a global world. On the other hand, the existence of wireless networks and the success of cell-phones enable a wide usage of mobile communication infrastructure. While mobile devices (especially cell-phone) are becoming more and more a general vehicle to perform a wide spectrum of applications like internet browsing, etc. many, many issues are still unsolved in order to provide a technologically solid and well accepted mobile infrastructure. In the following, we focus on the term of robustness as a mean to achieve this goal. No only the general possibility to communicate via mobile devices using wireless networks is the question, but the reliable, secure, and finally simple way of doing it must be the core research in the context of mobile environments.

Currently on the one side, the wireless networks are neither secure against interception nor reliable with regard to the required functionality. On the other side, which will be addressed by the described research project, mobile devices are not safe with regard to secure storage of (private) data, are not protected against data loss in the case of loss of theft of the mobile device, etc. In general, the term robustness is defined using the following properties:

- Robust systems exhibiting a friendly, well known, and well defined behaviour. The properties of friendly and well defined are implying the assertion of reliability, trust, and integrity.
- Robust systems are working even under problematic conditions. Examples of problematic conditions are the failure/break down of parts of the systems, change of parameters describing the environment, and finally and most obstructive, attacks from outside and inside.

In general, the notion of robustness has an impact on the infrastructure (Database Systems, Operating Systems, Wireless Data Transmission, …), the physical perspective (Theft, Reconfiguration,…), and finally on the lifecycle (design, etc.) of software programs.

Sample Applications

The demand for mobile and robust infrastructure increases with the comprehensive usage of wireless network technology. The context of the ‘Connected Home’ can be seen as a primary example requiring robust networks and mobile systems. In the Assistant Living scenario, movements and interactions, and physical conditions of people are monitored and transmitted to a central observation system. Data mining algorithms are used to evaluate the data on-the-fly and trigger appropriate actions. Another scenario in this context is related to consumer electronics. Recent development in the operating systems context (Windows Media Center, http://www.microsoft.com/windowsxp/mediacenter/default.mspx) can only be seen as a first attempt to provide one single integrated platform for to connect different MFDs (multi functional devices).

Dagstuhl Seminar Proceedings 04441
Mobile Information Management
http://drops.dagstuhl.de/opus/volltexte/2005/164

The general attempt to introduce home automation already results in first standards (like ZigBee Alliance, http://www.zigbee.org).

A completely different application scenario demanding for really robust systems can be found within the automotive sector. A Mercedes S-class already has 17 antennas to communicate with the outside. The application of wireless communication in this context ranges from remote diagnoses of the engine to the interaction of onboard-computers of multiple cars (e.g. to propagate news according to traffic conditions, etc. without having a centralized server system).

The Research Challenge

From a research point of view, many challenges exist with respect to robustness in mobile environments. The spectrum ranges from protecting a user from loss of mobile devices. A solution might consist on the one hand of a capability to reconstruct the (more or less) latest state of the device (software configuration plus locally stored data sets). On the other hand, loss/theft should imply the self-destruction of the device (at least an extinction of the data and software programs). If there is a requirement to reconstruct states of specific devices, it has to be possible to download software updates and perform reconfigurations. Robust devices have to ensure that none of these actions exhibit any impact on the correct behaviour of the device. The same has to be true for systems in difficult environments. Jamming (intentional interference) or the change of parameters ranging from the quality of a physical connection to soft factors like trust, privacy, etc. have to yield in a dynamic reconfiguration. More importantly, all solutions have to be developed under the constraint of limitation regarding energy consumption of mobile devices.

The academia as well as the related industry is currently focussing on different perspectives of the more general problem of robustness of mobile networks and devices. In the context of dependable systems, mobility is not a main issue. Work which is currently carried out in the context mobile networks focuses on low emission, the creation of ad-hoc networks, and the problem to provide high data rates to enable high-quality video or music transmission. On the device sector, there are multiple efforts going on to create a secure operating platform as a base for more advanced secure system and application-oriented software. The main force in this context is TCPA (trusted computing platform alliance) as a consortium founded by Microsoft, IBM, HP, and Compaq in 1999 or the successor, TCG (trusted computing group, https://www.trustedcomputinggroup.org/), founded in 2003, pushed by AMD, HP, IBM, Intel, Microsoft, Sony, and Sun. The general goal of this initiative is to provide specifications for a secure PC-based platform. Interestingly, the goal especially addresses applications as well as data sets securely stored on a computer.

Robust and Secure Data Management

The research issue of robust and secure data management on mobile devices provides a huge portfolio of interesting research questions. Some of them are already discussed in related projects. Secure data management relies on the integration of crypto technology built into data systems in order to gain access to the required information only in combination with the required privilege (esp. keys, passwords, etc.). Robust data management is also addressed in the context of ad-hoc data replication and mobile transaction, i.e. that each operation with regard to the local database is propagated to a backend server machine. This backend server records all transactions and provides a single point of complete data in order to provide a recovery of the data set if the mobile device gets lost.

The current research project conducted at the institute of system architecture at Technische Universität Dresden focuses on an integration approach across multiple system layers in order to provide a solid base for

secure data storage, efficient retrieval, and recoverability by propagating changes to the background server with respect to the current network infrastructure.

The overall architecture of the secure data management infrastructure is depicted in figure 1. The core of the approach is an operating system providing a small set of functionality which is based on an ARM hardware platform[1].

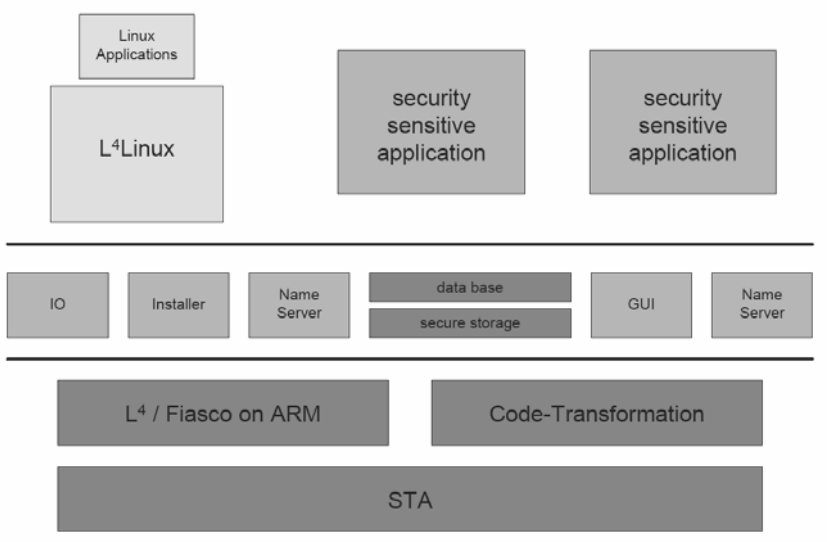

Figure 1: Overall architecture of the integrated approach for secure data management.

The basic idea is that the set of trusted operating software modules is as small as possible so that security sensitive applications are able to run directly on top of this "pure" operating system. All "convenient" infrastructure mechanisms are outsourced to a regular Linux running like any other application on top of this "pure" operating system. This architectural approach leads to the more detailed view given in figure 2.

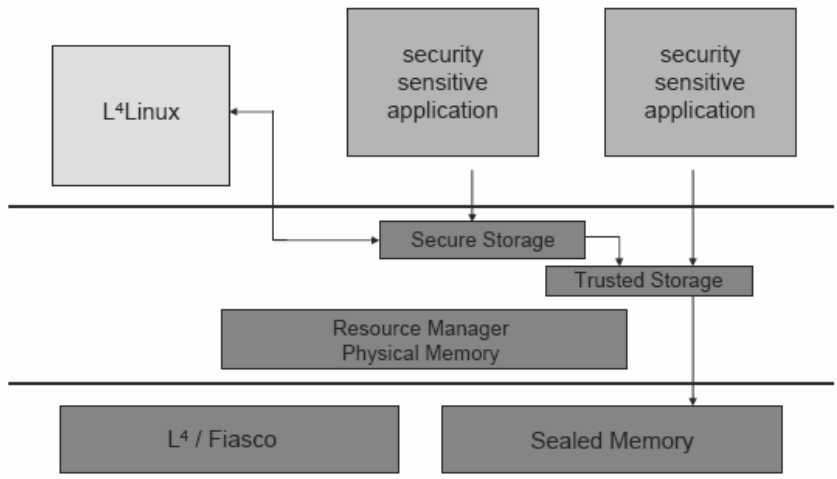

Figure 2: Detailed architecture of secure storage

[1] It is worth mentioning here that a second project is dealing with energy-efficient hardware platforms. The basic idea is to simulate different CPU behaviour on top of that specific chip set (STA). The simulation (code morphing) can be seen in figure 1 as code transformation. This technology provides an abstraction with regard to the specific hardware so that only a single set of operating software modules are required.

Security-sensitive applications are referring to a secure storage module which is part of the small and "pure" operating system platform and provides all necessary functionality of data management (i.e. set oriented access, storage and retrieval of semi-structured data, etc.). The secure storage module again is based on a more general and low-level operating system module called trusted storage, which again exploits techniques of the hardware-oriented Sealed Memory technology. This detailed view enables the discussion of the two major points with are subject of the secure data management project:

- Use of sealed memory infrastructure. As can be seen, a major issue is the question of how to exploit the technology provided by Sealed Memory infrastructure (as part of the TCG base) from a database architecture point of view. Within the project, different approaches are investigated to inquire at what level in the architectural hierarchy, a signature or crypto-graphic algorithm can be exploited.

- Use of trusted wrapper to benefit from the "legacy" Linux environment. As already outlined, a regular Linux system runs on top of the "pure" operating system base and provide all well-known file and network system amenities. The second question in that context from a database perspective is, how to define a secure tunnelling system through the "legacy" Linux environment and take advantage of file systems and network capabilities to propagate transactional changes.

The architecture of the robust and secure data management project enables the construction of a reliable database service to locally manage huge amount of data and synchronize them with backend servers. The very specific difference to other research projects consists in the integrated approach considering hardware technology (power consumption, sealed memory infrastructure, …), operating system technology (trusted wrappers to tunnel secure data through un-trusted operating system environments), and data management issues (embedding data management into secure operating system environments).

Summary

Robustness is a key issue in order to make ubiquitous computing a success from a social (and - as a consequence - economical) point of view. Dealing with mobile devices in general has to become so simple like using a regular standard (wired) telephone. The multi-functionality of the individual devices and the capability of storing GigaBytes of data locally raise many open issues from a technological point of view. Robustness comprises the simple use of the devices and therefore demands for adaptive applications and intuitive user interfaces. Robustness also demands for energy-efficient hardware platforms in order to enable real mobility (and not being tied up to a power plug). Finally, robustness means a secure and reliable data storage so that neither the individual data sets nor the identity of the user can be intercepted.

The current ongoing research project aims at providing a comprehensive and integrated solution across multiple software layers. Integrity of data is not only local to application software but also integrated into low-level system software relying again on hardware mechanisms. The goal is to come up with a secure platform for local data management with special focus on tight integration into operating system.

Contact Address

Wolfgang Lehner
Technische Universität Dresden
Faculty of Computer Science / Database Technology Group
D-01062 Dresden, Germany
Phone: +49 351 463 38383
Email: lehner@inf.tu-dresden.de