MULTILATERAL SECURITY CONSIDERATIONS FOR ADAPTIVE MOBILE APPLICATIONS

Adrian Spalka, Armin B. Cremers
Institute of Computer Science III
University of Bonn
Römerstr. 164, 53117 Bonn, Germany

Marcel Winandy
Horst Görtz Institute for IT-Security
Ruhr-University Bochum
Universitätsstr. 150, 44780 Bochum, Germany

Keywords: Multilateral security, mobile computing, adaptive applications.

Abstract: Adaptive mobile applications are supposed to play an important role in the future of mobile communication. Adaptation offers a convenient and resource-saving way of providing tailored functionality. But to make this technology a success, the security of all concerned parties must be addressed. This work presents a multilateral security examination in two stages. We first introduce a co-operation model and state the security requirements from the perspective of each party. In the second stage we investigate the set of all requirements with respect to conflicts, state each party's role in the enforcement and suggest a realisation. The result is a comprehensive picture of the security aspects of adaptive applications in mobile environments.

1 INTRODUCTION

Today's applications in mobile computing consist of voice, text and video communication. Several Java or operating system specific applications exist as well. All applications are installed by the hardware manufacturer or must be downloaded by the user.

Network operators and service providers are engaged in fierce competition. They constantly enhance their services to satisfy customer needs: the requirements change, services evolve and software applications must be adapted. Therefore, flexible software architectures and adaptive applications are needed to quickly adopt these changes.

Future applications in mobile computing must allow for unanticipated evolution. In particular the support of context-sensitive behaviour, eg location-based services, requires a frequent adaptation of the software. To avoid re-installation of the whole application, adapting parts of it is more convenient and resource-saving. New techniques for software adaptation are developed now (Mügge et al., 2005).

To give an example, consider a user equipped with a smart-phone running a adaptive application. He can take the application to any other device, eg a desktop computer or a laptop. His mobile device will also be able to connect to external displays with different properties. The application should be automatically adapted according to the changing environment. If new features are introduced, the application must be adapted accordingly.

This work considers technologies for mobile applications with adaptable and replaceable components. To make them a success, the security of all involved parties must be addressed. The following parties are regarded as stakeholders: users (U), software producers (SWP), content providers (CP), service providers (SP), network operators (NO), and hardware manufacturers (HWM).

The aim of this work is to identify party-specific security requirements and to extract non-conflicting and possibly conflicting requirements in a multilateral examination. In the subsequent section we identify individual security requirements from the perspective of each party. In section 3 the requirements are examined with respect to conflicts. We state each party's role in the enforcement and suggest a realisation.

2 MULTILATERAL SECURITY REQUIREMENTS

In adaptive mobile applications components thereof can be replaced or adapted. We assume that a party does not trust the other parties.

Spalka A., Cremers A. and Winandy M. (2005).
MULTILATERAL SECURITY CONSIDERATIONS FOR ADAPTIVE MOBILE APPLICATIONS.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 133-137
DOI: 10.5220/0001420101330137

2.1 Stakeholder 1: The Users

In our scenario the user has a mobile device which can execute adaptive applications and receive updates. The user wants to make the best use of the services at the least cost. The user also wishes to retain integrity, confidentiality, availability and privacy of his data. These constraints result in the following security requirements with respect to the other parties.

Software producer

1. The software is written by the intended authors ⇒ Verification of the authors' authenticity.
2. The software accesses and modifies only authorised resources ⇒ Preservation of confidentiality and integrity of his data.
3. The software passes only data admitted by the user ⇒ Respect for his decisions on his privacy.
4. The software performs only intended modifications ⇒ Verification of the semantic integrity of data (safety of the software).
5. The software does not block access to previously accessible data ⇒ Preservation of availability.
6. The software does not prevent future adaptations ⇒ Preservation of availability of software adaptations.

The first requirement can be satisfied with digital signatures. Access control mechanisms can be used to enforce requirement 2, or cryptographic hash functions can be used, at least, to discover a violation of integrity. Data outside the intended working set can be encrypted to preserve confidentiality. To satisfy requirement 3, the user must be able to confirm or object to a data transmission. This implies the provision of a trusted input and display by the hardware and the operating system. Since the general user cannot verify the safety of software, a recovery mechanism is indispensable to achieve requirement 4. This also supports requirements 5 and 6.

Content provider

1. Software is not modified during distribution ⇒ Verification of software integrity.
2. The process of the software transmission is not revealed for privacy reasons.

The first requirement can be satisfied with digital signatures. The second requirement implies the ability to buy content anonymously. On the other hand, content providers may need to identify a user to process payment.

Service providers and network operators Here, the requirements are the same as for the content providers. If the user's identification is not needed, encryption of the transmission preserves privacy.

Hardware manufacturers

1. The software does not disable critical hardware functions ⇒ Maintenance of their availability.
2. The hardware device prevents the execution or adaptation of software at the user's request.
3. The software transmission process is not revealed for privacy reasons ⇒ Prevention of identification.

To partially satisfy requirement 1 the manufacturer can provide a function to reset the mobile device in a safe state. Requirement 2 cannot be enforced by the user without the help of the hardware manufacturer. Requirement 3 calls for a device which can switch off hardware identification at the user's request. However, (Rannenberg, 2000) mentions that it may not solve the problem.

2.2 Stakeholder 2: Software Producers

The software producer can be author of a complete program or a part thereof. We assume a traditional vendor model, in which software is sold as a product.

Content providers, service providers and network operators

1. The producer's profit depends on his reputation ⇒ Proof of software integrity and authenticity.
2. To charge for software usage, the producer wants to prevent unlicensed software distribution.

Again, requirement 1 can be satisfied with digital signatures along the distribution chain. The second requirement can be satisfied in this setting in several ways (the detailed description of which will be given in a separate paper).

Users and hardware manufacturers

1. Licence compliant usage ⇒ Verification of licenses.

This requirement relies on the verification of the execution environment, eg, device identification.

2.3 Stakeholder 3: Content Providers

The content provider's role resembles that of a merchant in the traditional world. His primary goal, profit, implies the following security requirements.

Software producers

1. Reputation of selling genuine software ⇒ Verification of authenticity and integrity.

   Simple solution: digital signatures.

Service providers

1. Reliability of the services.
2. Genuineness of the offered products.

While requirement 1 cannot be enforced by the CP with technical means, digital signatures are sufficient for the second one.

Network operators[1] Should distribute CP's data:

1. without modification (integrity)
2. in a timely fashion (availability)
3. only to the designated address (fraud prevention)
4. having access only to data germane to the transmission (business privacy).

Solutions are already presented.

Users We take the users to be the primary source of profit for the content provider.

1. Self-verification to build up reputation
2. Licence compliant usage ⇒ Verification of licenses.

Solutions already discussed.

Hardware manufacturers No apparent security requirements.

2.4 Stakeholder 4: Service Providers

A service provider offers technical services to content providers for the distribution of products to customers. To put it simple, a service provider puts the products of content providers in data packages, which can be transmitted by network operators. Its main objective, profit, dictates the following security requirements.

Network operators

1. The profit depends on the availability of its services

The satisfaction of this requirement relies on quality-of-service mechanisms. Otherwise, compensation of downtime can be regulated by contract.

Content providers

1. Authentication of the content provider for accounting purposes ⇒ Digital signatures.

[1] In contrast to a traditional carrier, eg UPS, a network operator need not have access to the contents or value of a package.

Software producers

1. Software updates or adaptations do not affect the availability of the services. If it cannot be enforced, the service provider must verify the origin of the software ⇒ Digital signatures.

Hardware manufacturers No apparent security requirements.

Users

1. Identify users and devices for billing purposes.

2.5 Stakeholder 5: Network Operators

A network operator exchanges data between a service provider and a user. Its main goal is profit, which he generates by charging fees for network usage. It is also inclined to provide services, which attract customers. From its perspective there is no need to discern between the service provider and the user.

1. No bypassing of the billing mechanism.
2. High quality of transmission.
3. Provision of attractive services.

The first requirement is stated on the grounds of recent fraud, cf (Prasad et al., 2003). Requirement 2 calls for quotas, eg limited bandwidth allocation. The last requirement is optional; to give an example, registered mail can be realised with digital signatures and express delivery resorts to a priority-based allocation of resources.

2.6 Stakeholder 6: Hardware Manufacturers

A hardware manufacturer provides to a user a mobile device with an operating system. Its basic objective is profit. In view of this article's focus, it is directly concerned only with its reputation among users. Indirectly, it can be favoured by other parties if its devices provide trusted functions or services that support their security requirements.

Users

1. The device remains operational irrespective of software behaviour.

This requirement relates to the quality of the design and manufacturing, which is the sole responsibility of the manufacturer and does not imply any specific techniques.

Table 1: Multilateral evaluation of security requirements.

Requirement	*Required by*	*Objected to by*	*Participation*	*Supported by*	*Conflict*	*Possible realisation*
1) Authenticity of the software producer and integrity of the software product	CP and U	no party	SWP	SP	no	Software product is digitally signed by SWP; digital signature can be verified by each party in the distribution chain.
2) Limitation of access to data	U	no party	HWM	SWP	no	Access control in the operating system.
3) User privacy: Limitation of distribution of data by the application	U	no party (possibly U)	HWM	SWP	no	Access control in the operating system; manual confirmation data transmission; trustworthy hardware display and input.
4) Safety of SW functionality.	U	no party	HWM	SWP	no	Undo function of the operating system.
5) Privacy of software transmission/purchase	U (optionally)	CP, optionally SWP	no party	no party	yes	Mediated payment scheme.
6) Availability of equipment	U, HWM	no party	HWM	all parties	no	Reset function of the operating system.
7) Limitation of sources of software	U (optionally)	no party	HWM, CP, SWP	N/A	no	Selective installation of digitally signed applications from white-listed sources.
8) Unlicensed distribution of software by the content provider	SWP	no party	U	N/A	no	User must register the application at the software producer.
9) Unlicensed software usage/redistribution by the user	SWP and CP	no party	HWM and U	N/A	no	User must register the application with an ID of the execution environment, which is provided by the HWM, at the SWP.
10) Availability of services	resp. party	no party	no party	all parties	no	Controlled resource allocation.
11) Accounting for services	resp. SP	possibly U (privacy)	service-using party	N/A	possibly	Authentication of service-requesting party.
12) Fraud prevention by eavesdroppers and business privacy	SWP and CP	no party	U	all other parties	no	Encryption of the software by CP with the user's public key.

Other parties

1. The mobile device provides security related functions, which are not under the control of the user.

This optional requirement depends on the manufacturer's commitment to perform security related operations on behalf of other parties, eg, the provision of a serial number or a service, which limits the usage of an application to the terms of its licence.

3 MULTILATERAL EVALUATION

We now extract the intersections, ie non-conflicting security requirements. They constitute the minimum set of requirements that can be supported in an environment with adaptive mobile applications. And, secondly, we extract conflicting security requirements, ie those that are demanded by one party but opposed by another. See table 1 for the evaluation results.

4 CONCLUSION

The idea to use adaptive applications in mobile environments is in its early stage. This provides a unique opportunity to include security techniques in their design. The starting point for this paper is the assumption that the security requirements of all parties must be considered in order to make it a success. We have introduced a co-operation model, in which all parties are considered: the software producer, the content provider, the service provider, the network operator, the user and the hardware manufacturer. The first stage of the investigation concentrated on the statement of all individual security requirements from the perspective of each party. In the second stage we have combined all these requirements into a set. We have found that nearly all security requirements are satisfiable without a conflict and that most of them can be enforced with accredited security mechanisms. We have identified the role and effort of each party in the enforcement with the insight that a concerted contribution results in a secure mobile environment for adaptive applications.

REFERENCES

Mügge, H., Rho, T., Winandy, M., Won, M., Cremers, A. B., Costanza, P., and Englert, R. (2005). Towards Context-Sensitive Intelligence. In *Proceedings of EWSA 2005, LNCS Vol. 3527*. Springer.

Pfitzmann, A. (2001). Multilateral Security: Enabling Tech-

nologies and Their Evaluation. In *Informatics - 10 Years Back. 10 Years Ahead.*, pages 50–62, London, UK. Springer-Verlag.

Prasad, A., Wang, H., and Schoo, P. (2003). Network Operator's Security Requirements on Systems Beyond 3G. In *Proceedings of WWRF 8*. Wireless World Research Forum.

Rannenberg, K. (2000). Multilateral Security - A Concept and Examples for Balanced Security. In *Proceedings of the 2000 Workshop on New Security Paradigms (NSPW '00)*, pages 151–162. ACM Press.