Sensitive Information Protection on Mobile Devices Using General Access Structures

Tomasz Hyla, Jerzy Pejaś, Imed El Fray, Witold Maćków, Włodzimierz Chocianowicz
West Pomeranian University of Technology
Szczecin, Poland
e-mail: {thyla, jpejas, ielfray, wmackow, wchocianowicz}@zut.edu.pl

Marcin Szulga
Unizeto Technolgies SA
Szczecin, Poland
e-mail: marcin.szulga@unizeto.pl

***Abstract*- Mobility of users and information is an important feature of information systems that must be considered during design of sensitive information protection mechanisms. This paper introduces the architecture of MobInfoSec system. MobInfoSec is designed to be an information system that allows sharing documents with sensitive information using fine-grained access rules described by general access structures. The system is for users who want to use cryptographic data protection mechanisms to protect sensitive information on mobile devices with a specialized cryptographic module. MobInfoSec will be distributed, modular, and configurable cryptographic access control system to sensitive information that works in a public environment. The system will enable cryptographic protection of sensitive information in accordance with ORCON access control rules. The architecture is designed to be flexible enough, so several business scenarios can be implemented. The paper presents the MobInfoSec system, which the two main goals are to secure mobile information and to release the user from the obligation to monitor any classified information contained in his/her mobile device.**

Keywords-mobile device; sensitive information; access structure; ORCON.

I. INTRODUCTION

Mobility of users and information is an important feature of information systems that must be considered during design of sensitive information protection mechanisms. Mobility of information causes that level of information protection, regardless of its location, must be the same or at least not lower than in other locations. Obtaining such property is not a trivial problem and requires creation of a system that will prevent leakage of access rights to certain information.

Currently, information technology (IT) market does not offer a system that transparently enforces protection of sensitive information collected from various sources and stored on mobile devices. Moreover, the system should prevent its transmission to any third party without the originator consent. The major problem is the disclosure of such information to persons who are not authorized to view this information.

This paper presents the architecture of MobInfoSec system, which will be distributed, modular, and configurable cryptographic access control system to sensitive information. The system will enable cryptographic protection of sensitive information in accordance with Originator Controlled (ORCON) access control rules [1]. A user will be released from the obligation to monitor any information (especially against unauthorized copying). The system will allow building confidence to software and hardware components of popular mobile devices available at the market.

The MobInfoSec design takes into account the European Directive on Electronic Signatures and related standards developed by ETSI and CEN, and most representative of the ISO/IEC directives, recommendations and normative sketches available [2][3].

The paper is organized as follows. Section 2 contains description of the key theoretical elements that are used to build MobInfoSec system, i.e., ORCON access control model and general access. Section 3 contains description of MobInfoSec architecture. The paper ends with summary and conclusions.

II. BACKGROUND

A. Originator Controlled Access Control

The two main goals of MobInfoSec system are to secure mobile information and to release the user from the obligation to monitor any classified information contained in his/her mobile device. In practice, the mobile information should be protected and monitored in accordance with the ORCON requirements [1][4][5][6][7]. In this model, it is assumed that each resource (document) has its owner. A document owner has the authority to manage his/her documents, for example, he/she may have read, write or update right to his/her documents. However, the access control is done by an originator of the document (i.e., the entity which has, on behalf of the document owner, the right to share a document, or entity to which the originator has delegated that right). The owner can determine who can share a document, but the final decision is up to the document originator. It is assumed that any copy of the document must have the same access restrictions as the original document. A user with a read right to a document cannot share or make a copy of a document (i.e., it should be technically impossible).

The implementation of ORCON rules is difficult (and on the IT market practically do not exists any system allowing to manage and secure documents according to ORCON

 ISBN: 978-1-61208-319-3

model), because in commonly used computers users has a wide access to operating system and memory. When the user has access to memory, he can access decryption key. However, few solutions to that problem exist. One of them, proposed by Yu-Yuan and Lee [1], shows that ORCON requirements might be enforced by a hardware-software mechanism provided by Secret Protection (SP) architecture [5][6], which protects directly Trusted Software Module (TSM). SP architecture consists of a trusted software module, operating at the application layer, and the SP mechanism in the system microprocessor. The authors present a text editor application that contains TSM implementing ORCON. TSM module cannot be bypassed or manipulated by the operating system, because of a direct connection with the SP mechanism. Also, Hoole and Traore [8] present a tool for the exchange of documents according to the ORCON model requirements. However, the solution uses only the software working in the OS environment and because of that, it does not provide complete security, but it is useful from business point of view.

B. Access structures

The MobInfoSec system use two main innovative elements to support ORCON model and information mobility requirements: a) a specialized cryptographic module for secrets protection on mobile devices, b) an access policy built over general access structures. The cryptographic module will be the source of trust and will support ORCON requirements. The module will protect directly Trusted Software Module (TSM) compliant with ORCON rules. In turn, the general access structures will allow generating appropriate information protection mechanisms, including group encryption schemes with an arbitrarily pre-defined access structure.

An access structure [9] is a rule that defines who has access to particular assets in IT system. Access structures can be classified into structures with and without threshold [10][11]. Although threshold access structures are frequently used (e.g., the most familiar examples are (*n*, *n*) and (*t*, *n*) secret sharing schemes given by Shamir [12] or by Asmuth-Bloom [13]), the non-threshold structures are more versatile. It is especially visible when the sender of the information defines special decryption rules, which have to be met by the document recipient.

C. General Access Structure

Assume that $U = \{u_1, u_2, \ldots u_n\}$ is a set of *n* participants. The set $\Gamma = \{ A \in 2^U$: *a set of shareholders, which are designated to reconstruct the secret*$\}$ is an access structure of *U*, if the secret can be reconstructed by any set $A \in \Gamma$. The access structure $\Gamma_{(t,n)}$ of the threshold scheme (*t*, *n*) is defined as follows:

$$\Gamma_{(t,n)} = \left\{ A \in 2^U : |A| \geq t \right\} \quad (1)$$

It is easy to notice that in case of the access structure $\Gamma_{(t,n)}$ of the threshold scheme (*t*, *n*), all users have the same privileges and credentials. Simmons [11] generalized a secret threshold sharing scheme (*t*, *n*) and gave the definition of hierarchical (multilevel) and compartmented threshold secret sharing. In an approach, in contrast to the classical threshold secret sharing, trust is not distributed evenly among the members of the participants' set *U*. Multilevel access structures are particularly useful in organizations with a hierarchical structure and compartment access structures might be used in the cases that require the consent of various parties. Both structures are multilateral access structures, which mean that the set of participants is divided into several subsets and all participants belonging to the same subset have an equivalent role.

When it is possible to implement the access structure Γ, we say that the structure is useful. An example of the access structures realization is the approach proposed by Benaloh-Leichter [14]. However, the application of access structures to build a group-oriented decryption scheme is effective only when it is possible to reuse shares being in possession of participants. Solutions to meet this requirement are discussed in the work [4][15]. In this paper (Section III), the MobInfoSec system is based on the approach combining certificate public-key cryptography with general access structure [16][17].

D. Our contribution

The main issue related to the ORCON model is of an architectural and implementation nature. In the case of the MobInfoSec system, the architecture supporting the ORCON model is based on the following innovative elements:

- a specialized SP cryptographic module;
- an access policy built over general access structures and assertions confirming permission to access sensitive information;
- a group encryption scheme, in which the decryption operation is preceded by a strong mutual authentication between the SP modules involved in the sensitive information decryption.

The components mentioned above are partially consistent with a solution shown in [5][6]. In contrast to [5][6], MobInfoSec system uses a group encryption scheme based on a general access structure [16][17] and on a single secret stored in each SP module. Access structures might have different topologies (e.g., threshold, hierarchical) and may also change over time. The SP module can be used by its owner only after two conditions are fulfilled:

1. all users belonging to the privileged shareholders set, which plays the combiner role, are authenticated with their SP modules.
2. access rights authorization of the SP owner to sensitive information, which is going to be decrypted, is positive.

III. MOBINFOSEC SYSTEM

This section contains brief description of general MobInfoSec architecture followed by description of its subsystems. The subsystems are divided into three categories: subsystems that work on server-side of the system (at service provider site), subsystems that are used

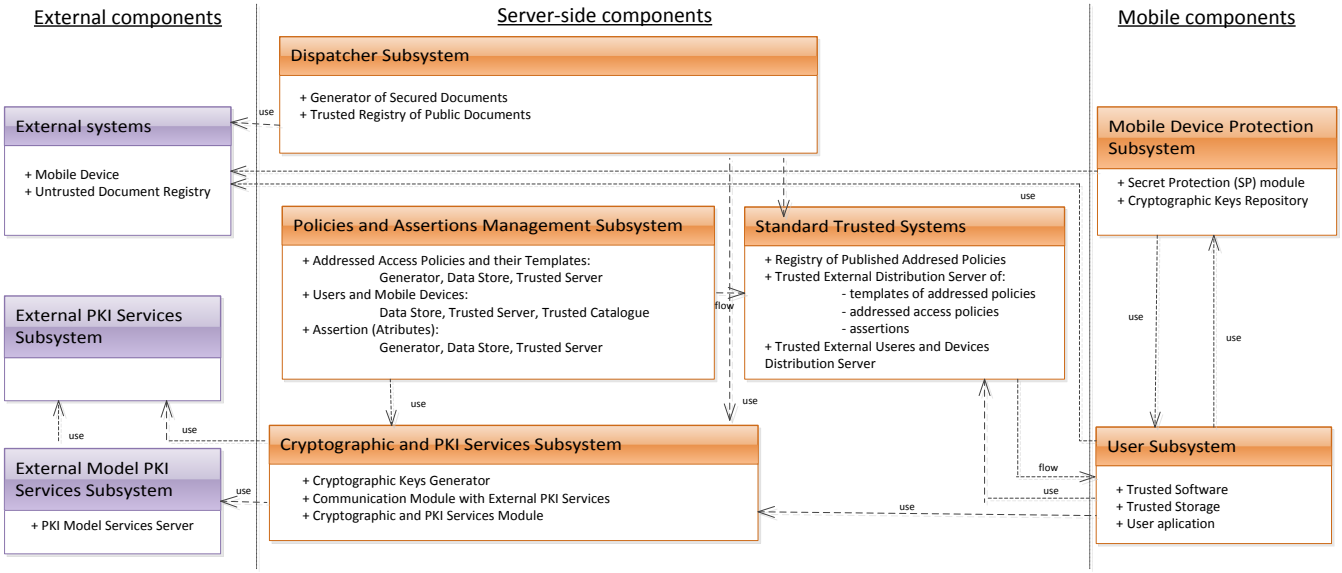

Figure 1. MobInfoSec high-level architecture

by mobile users and external subsystems which include services used by MobInfoSec.

Architecture of MobInfoSec system consists of six logical subsystems connected with three subsystems in external environment (Figure 1). Physical elements of individual subsystems might be shared. Deployment of subsystems into physical elements will depend on the target number of documents that system will manage and on the existing services used by a MobInfoSec provider.

The MobInfoSec consists of the following subsystems:

- User Subsystem;
- Mobile Device Protection Subsystem;
- Dispatcher Subsystem;
- Standard Trusted Systems;
- Policies and Assertions Management Subsystem;
- Cryptographic and Public Key Infrastructure (PKI) Services Subsystems.

A. *Server-side components*

Policies and Assertions Management Subsystem (PAMS), Standard Trusted Systems (STS), and PKI and Cryptographic Services Subsystem (PCSS) will be implemented on server-side of the system, probably in cloud environment. Moreover, in basic MobInfoSec version Dispatcher Subsystem (DS) will be implemented on the stationary part of the system.

1) Policies and Assertions Management Subsystem

PAMS contains several components that provide key features and can be divided into three categories. The first is related to management of targeted access policies and their templates. It includes generation, storage and distribution. The second group of functions is related to management of users and mobile devices. The third category contains functions related to assertions (attributes) management. This subsystem only distributes the data to Trusted Standard Services and is not available directly for mobile devices. The subsystem stores targeted access policies and targeted access policies templates, users and devices information.

2) Standard Trusted Systems

During decryption process the user system (located on a mobile device) need information, for example, about other devices or other users' assertions. The STS is the source of that information via the trusted components providing the following features:

- distribution of addressed access policies and assertions from PAMS to mobile devices (user systems);
- distribution of trusted devices and trusted user IDs to mobile devices (user systems);
- central users and devices authentication (e.g., MS Active Directory);
- provision of secure access to cryptographic services and PKI services.

3) PKI and Cryptographic Services Subsystem

This subsystem is a service provider for the authentication and encryption schemes. It will be integrated with existing PKI services.

4) Dispatcher subsystem

DS is used to generate targeted access policies and to encrypt documents with sensitive information in accordance with those policies. Generated policies are published in the repository located in STS. An encrypted document linked with a target access policy is published in External Subsystem in an untrusted document registry.

B. *Mobile components*

User Subsystem (US) and Mobile Device Protection Subsystem (MDPS) are two logical subsystems that are located in Mobile Device.

1) User Subsystem

US contains components that perform authentication and

 ISBN: 978-1-61208-319-3

authorization of users and mobile devices and distributes access policies to the mobile devices as well. Finally, US enforce access policy in the case of decryption. Additionally, in US may be located a trusted or untrusted (produced by external suppliers) application that presents the data subjected to access policy. US contains the trusted software configuration data set. The integrity of trusted applications and trusted data sets is protected by MDPS. If a trusted code requires using specific cryptographic keys, it receives them from MDPS through Secret Protection module.

2) Mobile Device Protection Subsystem

MDPS contains a dedicated cryptographic module called SP module. The module is a source of trust (at various levels depending on SP type). SP protects directly trusted US components implementing ORCON rules. This protection is possible by controlling the integrity of the code and configuration data. Different possible variants of specialized SP module are considered, including:

- a software SP module;
- a software SP module supported by the device with a built-in crypto processor (e.g., smart card with a crypto processor);
- a software token SP supported by the safety mechanisms built in mobile devices, e.g., laptops with TPM modules, tablets, and smartphones.

SP module should provide: the protection of cryptographic keys; building confidence to software components in the device; the authentication of the mobile device; the protection of information exchange between the device and the network environment where there are other devices of this type.

The whole device is managed by a trusted program module (Trusted Software), which has exclusive access to the functionality provided by SP module and to a reliable data storage module, i.e., TSM module. SP module should provide the following functionalities:

- TPM functionality, i.e., two keys (one for authentication and one for storage), the encryption and decryption keys from the store;
- registers and a code needed to verify the integrity (i.e., the integrity of mobile device hardware, system components and trusted code);
- the code that forces certain behaviour in the case of incorrect integrity verification.

SP module must be unambiguously assigned to the mobile device. Moreover, in its most secure form, a transfer of SP to another device should be impossible. From the business point of view it should be permitted to reset the connection between SP module and mobile device, or even more: the ability to derive trust from one SP module to many devices. This means that one SP module, which is owned by the user, can protect all mobile devices in the local range.

C. External components

External PKI Services Subsystem provides PKI services, and External Model PKI Services Subsystem provides PKI services which are not available in External PKI and Cryptographic Services Subsystem and are necessary for the functioning of new algorithms and protocols. External Model PKI Services Subsystem is not a part of MobInfoSec system and belongs to its environment.

External Systems subsystem contains untrusted mobile device that can be an untrusted device vulnerable for attempts that tamper its integrity. The mobile device is a platform that can be used to place dispatcher and user subsystems. Mobile Device Protection Subsystem (containing SP module) is integrated with a mobile device. Another system in external systems is an untrusted document registry**.** The untrusted document registry contains encrypted documents. It might be public http or ftp server or services intended to store files in a cloud, e.g., Dropbox.

IV. CONCLUSION AND FUTURE WORK

The main role of MobInfoSec is to secure documents that contain sensitive information. The system is designed to work in mobile environment. This is especially important when the most of the computer' users use mobile devices. The architecture is designed to be flexible enough, so several business scenarios can be implemented. The system is intended, for example, for small companies that want to protect they business information, as well as for healthcare organization to allow physicians to work with medical documentation outside the healthcare site.

The most difficult part in the creation of MobInfoSec is the design of Secret Protection module. From the information security point of view, it will better to design a new Secret Protection device from a scratch. However, it could be difficult to connect it with popular mobile devices and development costs would be initially too high. This is the reason why the system is targeted to use security mechanisms available in current devices or in devices that are easy to connect. The most difficult requirement to fulfil is prevention against unauthorized dissemination. This requirement implies that a special trusted application is needed for document viewing. The popular applications can be used, obviously after they are adjusted to MobInfoSec requirements and certified by a local system operator.

MobInfoSec should achieve commercial status in 2015, preceded by a prototype in 2014. Current works are carried out in two areas simultaneously. The first area is related to authentication and authorization issues and the second one to group encryption algorithms.

ACKNOWLEDGMENT

This scientific research work is supported by NCBiR of Poland (grant No PBS1/B3/11/2012) in 2012-2015.

REFERENCES

[1] C. Yu-Yuan and R. B. Lee, "Hardware-Assisted Application-Level Access Control", In: P. Samarati et al. (Eds.): ISC 2009, LNCS 5735, 2009, pp. 363-378.

[2] NIST, "SP 800-164 Guidelines on Hardware - Rooted Security in Mobile Devices (Draft)", 2012.

[3] IETF, "RFC 6749 The OAuth 2.0 Authorization Framework", October. 2012.

 ISBN: 978-1-61208-319-3

[4] Y. Sang, J. Zeng, Z. Li, and L. You, "A Secret Sharing Scheme with General Access Structures and its Applications". International Journal of Advancements in Computing Technology, vol. 3, no. 4, May 2011, pp. 121-128.

[5] J. S. Dwoskin and R. B. Lee, "Hardware-rooted Trust for Secure Key Management and Transient Trust", In: ACM Conference on Computer and Communications Security (CCS'07), 2007, pp. 389-400. Alexandria, VA, USA.

[6] R. B. Lee, P. C. S Kwan, J. P. McGregor, J. Dwoskin, and Z. Wang, "Architecture for Protecting Critical Secrets in Microprocessors", In: ISCA '05, Proceedings of the 32nd Intl. Symposium on Computer Architecture, 2005, pp. 2-13.

[7] J. Park and R. Sandhu, "Originator Control in Usage Control", In: Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks, (POLICY'02). Washington, USA, 2002, pp. 60-67, IEEE Computer Society.

[8] A. M. Hoole and I. Traore, "A Secure Document Management Tool for Scalable Collaborative Environments", In: International Conference on Trust Management. Moncton, New Brunswick, Canada, (12 pages), 2007.

[9] A. Renvall and C. Ding, "The access structure of some secret-sharing schemes" In: LNCS vol. 1172, 1996, pp. 67-78. Information Security and Privacy, Eds.: Pieprzyk, J., Seberry, J.. First Australasian Conference, ACISP'96.

[10] V. Daza, J. Herranz, P. Morillo, and C. Ràfols, "Extensions of access structures and their cryptographic applications", Applicable Algebra in Engineering, Communication and Computing, vol. 21, no. 4, 2010, pp. 257-284.

[11] G. J. Simmons, "How to (really) share a secret", In: Advances in Cryptology - CRYPTO 88, LNCS 403, 1990, pp. 390-448.

[12] A. Shamir, "How to share a secret", Communication of the ACM, vol. 22, no. 11, 1979, pp. 612–613.

[13] C. Asmuth and J. Bloom, "A modular approach to key safeguarding", IEEE Trans. on Information Theory, vol. 29, issue 2, 1983, pp. 208–210.

[14] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", in S. Goldwasser (ed.) Advances in Cryptology - CRYPTO '88, LCNS no. 403, Springer-Verlag, London, 1990, pp. 27-35.

[15] C. Chum and X. Zhang, "Hash function based secret sharing scheme designs", Security and Communications Network, vol. 6, issue 5, May 2013, pp. 584-592.

[16] T. Hyla and J. Pejaś, "A practical certificate and identity based encryption scheme and related security architecture", K. Saeed, R. Chaki, A. Cortesi, S. Wierzchon (Eds.), CISIM 2013, Lectures Notes on Computer Science, vol. 8104, Springer-Verlag, 2013, pp. 178-193.

[17] T. Hyla and J. Pejaś, "Certificate-Based Encryption Scheme with General Access Structure", In: Cortesi, A. et al. (Eds.), CISIM 2012, LNCS, vol. 7564, 2012, pp. 41–55.

 ISBN: 978-1-61208-319-3