ОФЛАЙН-БЕЗОПАСНОСТЬ ДЛЯ КОРПОРАТИВНОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ

Т. Галибус[1], В. Краснопрошин[1], Э. П. Де Фрейтас[2], Р. О. Альбукерке[3], Р. Т. Де Соуза Жуниор[3], А. Залесский[4], H.E.R.M. Vissia[4]

[1]Белорусский государственный университет
Минск, Беларусь
e-mail: tan2tan@gmail.com, krasnoproshin@bsu.by
[2]Федеральный университет Рио-Гранде-ду-Сул, UFRGS - INF - CP: 15064, 91501-970,
Порто-Алегре, Бразилия,
e-mail: edisonpf@gmail.com
[3]Университет Бразилиа, UnB - FT - Эне - CP: 4386, 70910-900,
Бразилиа, Бразилия
e-mail: robson.pesquisador@gmail.com, desousa1961@gmail.com
[4]Byelex Multimedia Products BV Argon 1, 4751 XC
Oud Gastel, Нидерланды
e-mail: azalesky@by.byelex.com, h.vissia@byelex.com

Эта статья представляет собой новый подход к безопасности корпоративных мобильных устройств, в частности в автономном режиме. Защита используемых конфиденциальных данных в ситуациях, когда мобильный клиент не подключен к корпоративному облаку, обеспечивается за счет комбинации криптографических методов. Предлагаемая архитектура безопасности поддерживает минимальный трафик и пониженную коммуникацию с облаком.

Ключевые слова: мобильная безопасность; автономный режим; ABE; разделение секрета; защищенное облако.

OFFLINE SECURITY FOR CORPORATE MOBILE APPLICATION

T. Galibus[1], V. Krasnoproshin[1], E. P. De Freitas[2], R. O. Albuquerque[3], R. T. De Sousa Júnior[3], A. Zaleski[4], H.E.R.M. Vissia[4]

[1]Belarusian State University
Minsk, Belarus
[2]Federal University of Rio Grande do Sul, UFRGS – INF – CP: 15064, 91501-970,
Porto Alegre, Brazil
[3]University of Brasilia, UnB – FT – ENE – CP: 4386, 70910-900,
Brasília, Brazil
[4]Byelex Multimedia Products BV Argon 1, 4751 XC
Oud Gastel, The Netherlands

This paper presents a novel approach to the security of the corporate mobile devices, in particular the offline mode. The protection of the confidential data in use when the mobile client is not connected to the corporate cloud is provided by the combination of the cryptographic methods, such as AES file encryption, ABE authorization based both on user and share attributes, user key secret sharing (SS) based protection between the device and the user as well as MOS-based analytics methods to prevent the malicious user behavior. The proposed security architecture supports the minimized traffic load and reduced communication with the cloud.

Keywords: mobile security; offline mode; ABE; secret sharing; protected cloud.

INTRODUCTION

Special security issues and requirements have to be considered when mobile devices are actively used in corporate cloud environment [1]. Today more and more organizations and enterprises are functioning in the Bring-Your-Own-Device (BYOD) paradigm. The protection scheme used on a mobile device should be both computationally secure as well as resource-constrained due to battery power limitations [1]. On the other hand, the protection schemes with good computational qualities lack the security analysis in many cases [2]. Due to the resources constraint, there is a crucial difference in strategy of online and offline mode protection. This paper proposes a novel approach based on powerful cryptographic preventive methods, such as secret sharing [3] and ABE encryption [4]. The key expiration period is safely incorporated into the proposed system solution in order to enhance security. To the best of our knowledge, the offline mode security problem has not yet been deployed, neither in academia nor in the industry [1, 5, 6]. Therefore, the main concern of this proposal is the protection of the device and app in offline mode when the functions of data protection cannot be offloaded to a cloud or a trusted party. The approach proposed in this work describes and implements the complete lifecycle of the mobile app security infrastructure.

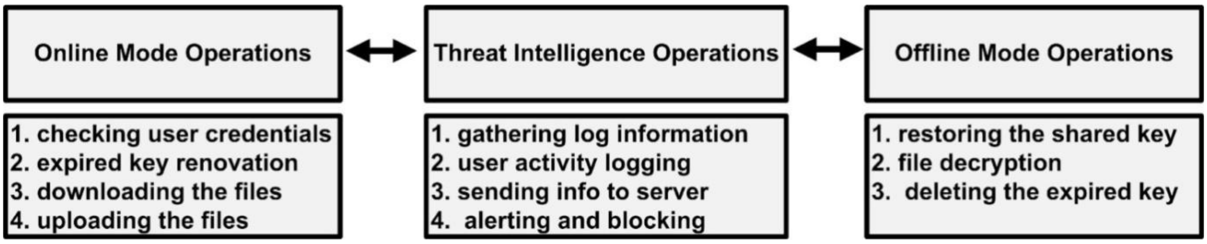
Online Mode Operations
Threat Intelligence Operations
Offline Mode Operations
1. checking user credentials
2. expired key renovation
3. downloading the files
4. uploading the files
1. gathering log information
2. user activity logging
3. sending info to server
4. alerting and blocking
1. restoring the shared key
2. file decryption
3. deleting the expired key

Fig. 1. Block diagram of the core set of functions and protocols of the mobile app security infrastructure

The proposed offline mode functional architecture includes:

1. *The protected storage*: the storage is protected with the shared user key and contains the ABE keys giving access to the file keys which allow decrypting the stored files.
2. *Key management center:* it includes the functions for maintaining the key expiry period and deleting the expired keys.

The client app performs all the cryptographic calculations in the shadow. These calculations include the key storage, key restoring, decryption and showing the decrypted files in the client area. To finalize the description of the offline mode, fig. 2 shows the complete workflow of the proposed mobile application in the offline-mode.

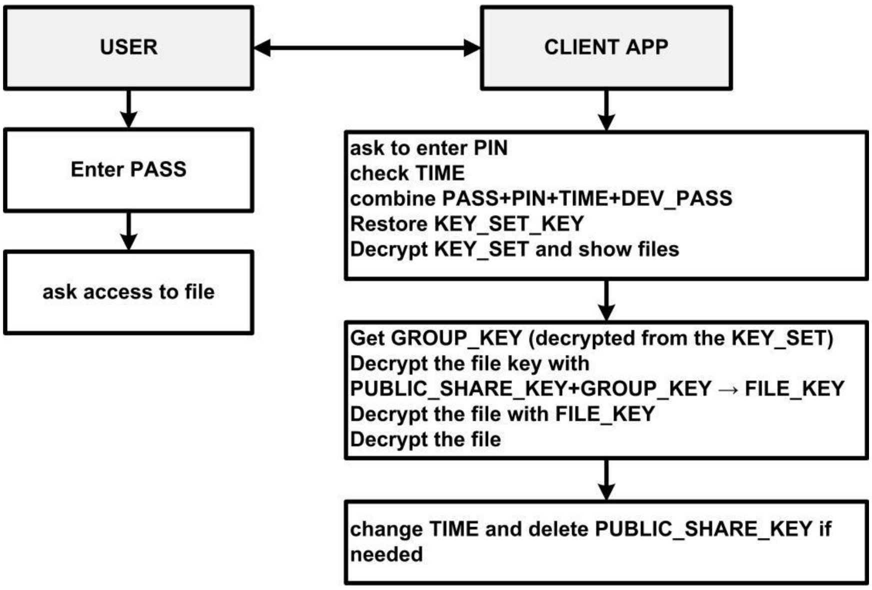
USER
CLIENT APP
Enter PASS
ask access to file
ask to enter PIN
check TIME
combine PASS+PIN+TIME+DEV_PASS
Restore KEY_SET_KEY
Decrypt KEY_SET and show files
Get GROUP_KEY (decrypted from the KEY_SET)
Decrypt the file key with
PUBLIC_SHARE_KEY+GROUP_KEY → FILE_KEY
Decrypt the file with FILE_KEY
Decrypt the file
change TIME and delete PUBLIC_SHARE_KEY if needed

Fig. 2. Offline mode authorization workflow

The core cryptographic module of the implemented solution is based on the combination of AES-ABE-SSS methods. The key feature of the offline security is that the client app does not actually store any part of the user password to be verified. The client app combines its own key with the user share (PIN and password-derived) in order to restore the initial KEY_SET_KEY. If the user provides the wrong share the client will not be able to recognize it, but will decrypt the files incorrectly. Additionally, the password entering is tracked and too many tries in a short time are considered a threat. In the proposed approach, the kernel encryption scheme in the mobile device is a combination of several methods of security. The files are encrypted with 128/256-bit AES, while the permanent file keys are encrypted with the attribute-based encryption. The set of expiring ABE keys corresponding to the set of files accessible by user in encrypted with a single expiring AES key (KEY_SET_KEY). This key is expiring and is split by the server into 4 parts (2 are stored on the device and 2 belong to the user) by the method of secure secret sharing. The encryption workflow is outlined in the fig. 3.

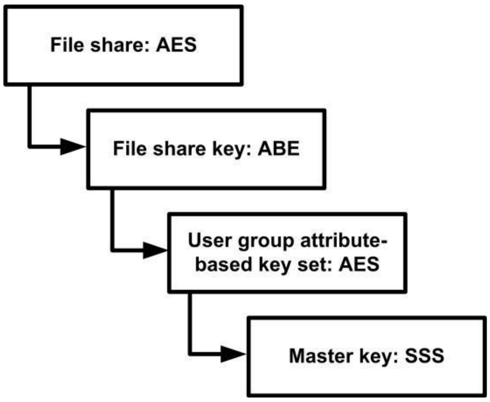

Fig. 3. Encryption workflow

The attribute-based private keys D_i should be protected while being stored in the device memory. Therefore, server encrypts the set of D_i with a single AES key before sending it to the user device. This AES key (master key) is denoted by the value KEY_SET_KEY in accepted notation. KEY_SET_KEY is a secret value and it is split by the secure method of polynomial modular secret sharing [7], [8] into the set of 4 shares:

$$\text{KEY\_SET\_KEY} = \text{PASS}+\text{PIN}+\text{TIME}+\text{DEV\_PASS}.$$

Since the underlying sharing scheme is perfect [7], the adversary cannot get any information of the KEY_SET_KEY unless he possessing all 4 key parts. Here the values PASS and PIN are predefined similar to the construction in [8].

The proposed authentication system is based on the shared storing of the user key. Also, the device acts as a dealer in the SSS. Using the SSS ensures that the key can only be accessed by an authenticated user. The participants of the (2, 2)-threshold SSS are the user and device.

The proposed concept of mobile client security has been implemented in the Storgrid protected cloud environment (available via http://www.storgrid.com). Therefore, the approach is correlated with the practical usability requirements: the corporate user continues to use the mobile storage app in offline and does not need to reload the files every time the key is renewed. This methodology can be used in other mobile apps. The common advantage is that the mobile client performs the operations both in the offline and online mode and uses the key expiry and ABE to protect the privacy of the corporate data.

Acknowledgements – The authors thank the Brazilian research and innovation agencies FAPDF (Research Support Foundation of the Federal District), FINEP (Agreement RENASIC / PROTO 01.12.0555.00), CAPES and CNPq under the FORTE Project – CAPES Forensic Sciences Announcement 25/2014, under the productivity grant number 303905/2014-0, under the PVE project number 88881.030392/2013-01 and the project number 207644/2015-2 of the program CSF – Aerospace Technology.

REFERENCES

1. Khan A. N., Kiah A. M. Shahaboddin Shamshirband and Atta ur Rehman Khan. A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach // J. of Grid Computing. 2015. 13 (4). P. 651–675.

2. Abdul Nasir Khan M. L., Mazhar Ali Mat Kiah, Sajjad A. Madani, Atta ur Rehman Khan and Shahaboddin Shamshirband. BSS: block-based sharing scheme for secure data storage services in mobile cloud environment // J. of Supercomputing. 2014. 70 (2). P. 946–976.

3. Galibus T., Matveev G. Generalized Mignotte Sequences in Polynomial Rings // ENTCS. 2007. 186. P. 39–45.

4. Goyal V., Pandey O., Sahai A. and Waters B. Attribute-based encryption for fine-grained access control of encrypted data // Proceedings of the 13th ACM conference on Computer and communications security, New York, 2007. P. 89–98.

5. Khan A. R., Othman M., Madani S. A., Khan,S. U.: A survey of mobile cloud computing application models // Communications Surveys & Tutorials, IEEE. 2014. 16. P. 393–413.

6. Khan A. N. Towards secure mobile cloud computing: a survey. Futur. Gener. Comput. Syst. 29, 2013. P. 1278–1299.

7. Galibus T., Matveev G. and Shenets N. Some structural and security properties of the modular secret sharing // Proceedings of IEEE SYNASC, Timisoara, 2008. P. 197–200.

8. Galibus, T., Gafurov, S., Kaganovich, D., Vissia, H. Mobile security based on the secret sharing // The J. of Brest state technical university. 2015. 5 P. 33–36.