DATA SECURITY IN A MOBILE ECOSYSTEM

Irina Noninska

Technical University of Sofia
e-mail: irno@tu-sofia.bg
Bulgaria

Abstract: The article deals with main dimensions in a mobile ecosystem security, discusses treats and damages which could be caused by the contemporary cyber attacks. The general structure of a mobile ecosystem is presented and three basic levels in it are defined. A mobile business application for the Android mobile ecosystem is designed and is used to analyze all information flows at the user level. For the purposes of information and communications protection the application is accomplished with a security module, designed to process personal data in accordance with privacy requirements and to guarantee secure transactions at the user level of a mobile ecosystem.

Key words: mobile ecosystem, data security, privacy, authentication.

1. INTRODUCTION

Today the new generation of mobile networks 5G gradually enters upon the global mobile industry. Together with the most widespread networks, designed over 3G- and 4G-technologies, they will shape the mobile economy next years. There is a tendency, more and more visible during last few years: people use mobile phones not only for voice calls, but preliminary for data, photo and video-exchange. Contemporary smart electronic devices (e-devices) are in fact light and convenient computers which are capable to use distantly different applications and services, customizing their basic functions according to the user's requirements. Different companies which propose their products – apparatus and e-devices; installations and infrastructure; operating systems; software and applications lay the foundations of a system, called mobile ecosystem. Using it, every customer could extend the functionality of employed e-devices, choosing one or more directions according his/her professional necessity and personal preferences.

Enhancing opportunities of the business partners and common users to generate, send and receive big amounts of data with heterogeneous structure and content, the mobile ecosystem faces to new and more complicated threats in the sphere of information and communications security [1, 2]. There could be defined four basic dimensions where security measures, tools and technologies have strategic influence on protection against contemporary cyber attacks. The first one

– *Information security* is responsible for protection against data theft or modification during their storage and transmission within a mobile ecosystem. The second one is *Communication security* which deals with protection of the infrastructure as a whole by avoiding any threats that are able to cause functional alteration of the components' characteristics. *Operations security* is obliged to keep protected procedures in a structure, bearing in mind specific requirements to different data flows and keeping interconnection between all communicated units according to the access rules of the security program. The fourth dimension is *Infrastructure Security* which is related to all measures and tools that could protect the basic components of a mobile ecosystem against physical threats as unauthorized access to servers, attacks on core hardware components and utilities, attempts for insertion of malicious hardware or software.

Recently many security programs rely on models, algorithms and technologies, where protection of privacy and user's security take part and have important place [3, 4].

The present article deals with main principles related to design and implementation of a mobile ecosystem, steady on cyber attacks and protected against unauthorized access to all types of data, kept or transferred via the system [5, 6, 7, 8]. Basic levels of the general structure are defined and analyzed in order to reveal main interdependences and interconnections between different components in it. As a result three separate levels in the structure are defined. For the security purposes at user level an algorithm for input data flow control is proposed. It is implemented in a module for customers' privacy to be part of a business application for push messaging, designed on Android OS. The second part of the security module deals with transactions security, implementing SSL protocol and digital certificate X.509 v.3 for authentication.

2. STRUCTURE OF A MOBILE ECOSYSTEM

A mobile ecosystem must be accepted as a compound complex of devices, tools and services, intended to facilitate users' access to the electronic communications market. It includes companies of different spheres – producers of e-devices, networks components and communication infrastructure; mobile operators; designers of operating systems, specialized software and applications; innovative platforms that provide wide spectrum of e-services and all other elements which take part in this environment, connecting customers by their mobile e-devices (smart phones, tablets). An important role of management the components and the processes of such complex structure have Operation Systems and corresponding browsers. Today customers choose mobile internet service mainly between Google and Apple, i.e. they employ Android OS or Apple iOS and relatively small part of this market hold the rest popular products Windows and Blackberry.

The Android OS is open source which give good opportunity of different producers to adapt it in their e-devices and to have access to service and applications provided by Google. Since Apple iOS is licensed, the producers of end devices are restricted, so the smart phones and tablets could use the only applications of Application store. In this way customers' devices and their mobile applications become capsulated in a system depending on the operation system. The policy of both companies is to enhance influence over mobile economy by implementing new technologies and services, especially over the new generation mobile networks 5G which will give opportunity to realize projects like smart city, smart healthcare, smart transport and make them closer to the citizens. Hence it might say that two companies - Google and Apple have created their own mobile ecosystems.

Figure 1 presents the general structure of a mobile ecosystem. As shown in it, every basic component has specific place in the structure according its functionality and connections with some of the rest elements. Their activities are put at the root of a conceptual analysis for interconnections and interdependences in a mobile ecosystem as a whole. The end user is directly connected with four of these components: Producers of e-devices (smart phones and tablets); Mobile operators; Internet-providers and Application stores. Every customer by his contract with a mobile operator has at his disposal system software and basic applications. Further in addition he is able to supplement the set with new applications, using the application store.

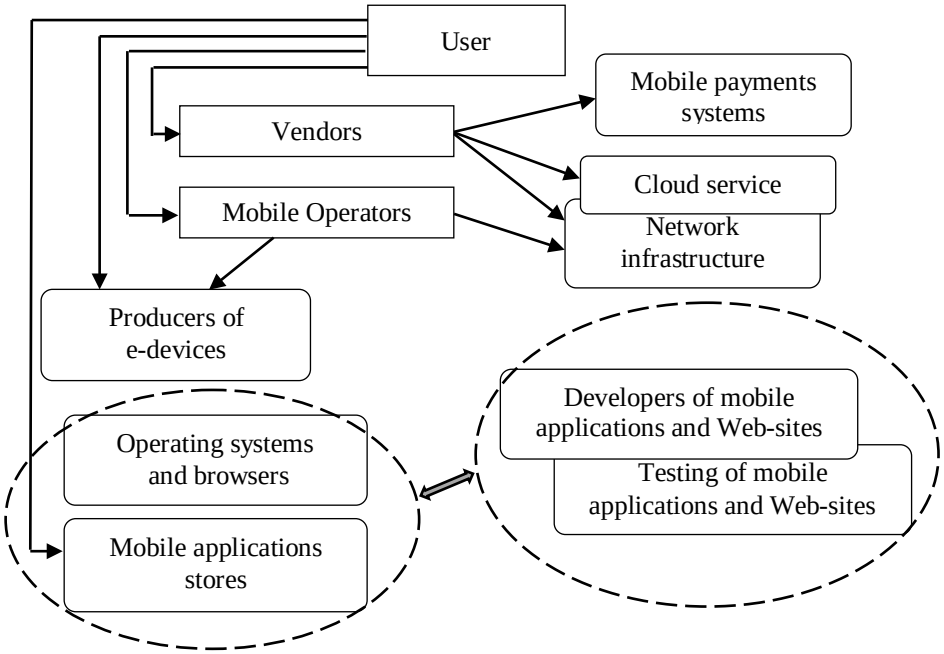

Fig. 1. General structure of a mobile ecosystem

All processes that are connected with customer service and corresponding components, obliged to ensure their prompt organization and control form the first level of a mobile ecosystem, called *User level*. This level could be adopted as an external part of the mobile ecosystem, comparatively independent, which represents the dynamic of consumption and requirements of the common customers and business partners. Detailed structure of the user level is shown in figure 2.

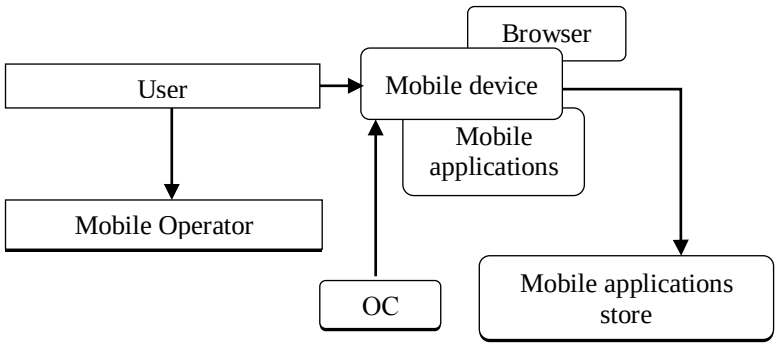

Fig. 2. User level of a mobile ecosystem

The second level includes companies which produce and sell apparatus, network infrastructure, system software – operation systems and browsers. Mobile operators take part in this part of the structure, as well. They design mobile networks, implementing new technologies as Long Term Evolution (LTE) for 4G-networks and LTE Advanced for 4,5G that give them opportunity to enhance and improve all their services, especially data and multimedia transfer by mobile Internet. This level includes all specifications and standards, proposed by standardization organizations in the telecommunications as American National Standards Institute (ANSI), European Telecommunications Standards Institute (ETSI), European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), etc. The structure of this second part of the mobile ecosystem structure, called *Basic level*, is shown in fig. 3.

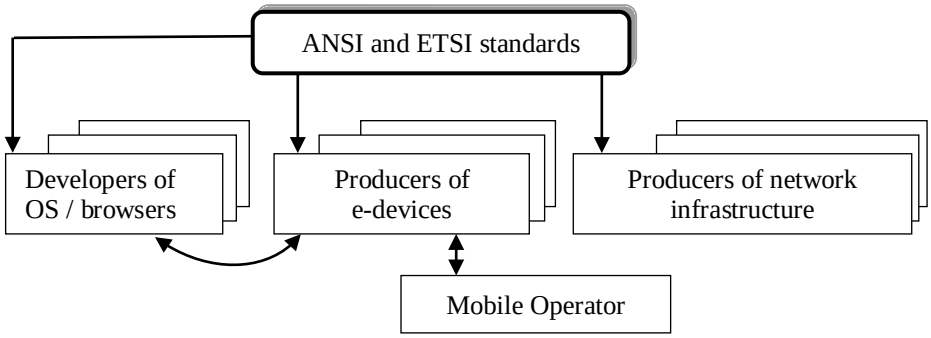

Fig. 3. Basic level of a mobile ecosystem

The third level of the mobile ecosystem unites designers of mobile applications, designers of Web-sites and closely connected with them testing systems, cloud services and mobile payment systems. This level, called *Application level* (fig. 4) and the *Basic level* construct the internal core of the mobile ecosystem. This internal core has flexible connections with the external one – the *User level*. As shown in fig.1, the application stores ensure direct connection between the two levels – the *Application* and the *User level*. As a connection unit between *Basic level* and the *User level* mobile operators and Internet providers give the consumers opportunity to access Internet and mobile services with high speed and raising quality.

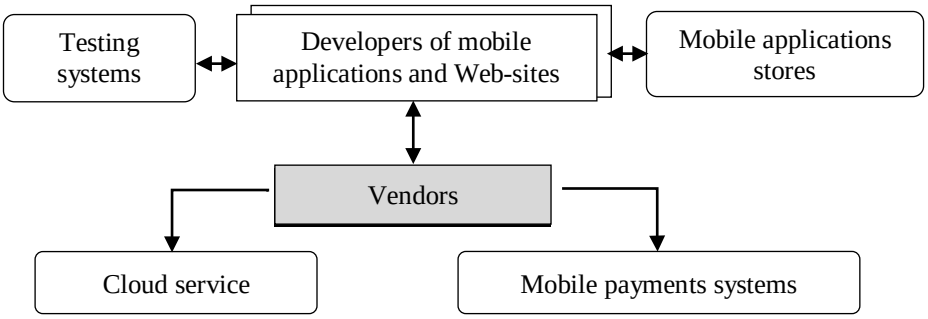

Fig. 4. Application level of a mobile ecosystem

Recently the technologies Machine to machine (M2M) and Internet of things (IoT) enlarge the scope and functionality of the mobile ecosystem with many innovative solutions, intended to propose devices and services for remote measurement and control in different spheres as transport, finance, public utilities, helping everyday human's life, healthcare and education. In this way the mobile ecosystem has great importance in the contemporary processes of transition from a connected consumer to a digital consumer.

3. SECURITY POLICY IN A MOBILE ECOSYSTEM

The mobile information systems could be considered as an object of different cyber attacks mainly in two dimensions. The first one is related to the end user. In fact the e-devices have been always in danger of unallowed access, personal data theft or identity fraud via the network. Nowadays besides traditional mobile applications customers could access IoT-platforms, where except customers' tablets and smart phones, computers and infrastructure, many units for monitoring and control are put together in a complex system. These systems propose personalized services, closely connected with private peoples' life as retail and healthcare domains, they deal with sensitive data which should be protected in a new, highly level of security. Hence this dimension, named ***identity protection*** ranges a variety of security measures and tools, obliged to keep human privacy.

The second dimension is connected with data processing by mobile applications. Except different types of data, input and storage in the system, they must keep secret also parameters, defined for users' identification, authorization and authentication. For this purpose several basic requirements should be put at the root of a security platform, as quality control of input data; passwords security by hashing; data encryption; cloud security for valuable copies of data and schemes for data recovery. These requirements must be implemented in accordance with the ***security policy of a mobile ecosystem***, intended to frustrate cyber attacks. All basic measures could be generalizes as follows:

♦ ***Mobile communication management in the frame of a single company***

This management has two sides. The first one is connected to hardware and software modules, intended to protect mobile devices of unauthorized access and use. The second deals with security measures of mobile applications' implementation, bearing in mind their characteristics to control their dissemination. Some of the popular big companies have succeeded to construct their own complex systems, proposing methods and tools for security management in it as Apple iOS applications security guide and iOS security development checklist, Best practices for Android applications security and privacy.

♦ ***Mobile operation system security***

The companies define all possible attacks, collect information concerning functional deviations, anallowed attempts to access system files and other subjective or objective violations that could destroy operation system functionality. Obtained results are analysed to make conclusion if the operating system works in accordance with its specifications, if it is stable to possible cyber attacks or it must be replaced with a new, revised version, as it happened to Android 2.3.

♦ ***SIM card security***

Since a SIM card identifies a user without any doubt of his/her personality all data that are kept in it should be protected by strong measures. The unique code, used to access mobile networks after personification everywhere in all over the world - International Mobile Subscriber Identity (IMSI) and other information in the SIM card as phone number, cryptographic keys for safe communication, personal data should be un important task for security by implementing cryptographic schemes.

♦ ***Infrastructure security***

This dimension includes all measures and tools that frustrate attacks to base transceiver stations of a mobile network and to the rest part of the network infrastructure. It must be taken into account that security requirements and implemented schemes should not disturb the functionality of the structure as a whole.

When the source of information in a system is just one, or there are a few constant sources, it is easy to control data and avoid different mistakes during their processing. Data Warehouse and recently Cloud Computing became widely used as organisational and technological extension of existing databases. They collect and

storage information from many and various sources and as a result the process of data security control becomes more complicated.

4. DATA SECURITY CONTROL AT USER LEVEL

A mobile application in the frame of the mobile ecosystem Android is designed. The target is to propose reliable and flexible trade advertisement and it is intended to help small and middle size companies to be more attractive for their clients by push messaging. This is the first goal of the application. The second is to be used as a foundation for an analysis of the information flows at the user level of a mobile ecosystem. The mobile application has several basic functions, as follows:

- push messaging management – the goal is to ensure this service 24 hours a day, every day without breaks. For this purpose the platform of one of the leaders in mobile marketing Urban Airship is applied;
- QR reading - Zxing is implemented to create barcode scanning application;
- easy and correct scanning of QR-codes from different sources and different places;
- optimal requirements for the Operation system – the application is able to deal with Target SDK as a well accepted Android version.
- function Scanning – it deals with bar-codes and QR-codes scanning – after processing, information of 1D and 2D-codes is displayed.
- function Notifications – it presents a list with all accepted messages which is connected with additional functions for their processing – view or delete.

The main purpose of analysis was to put over security control all processes that are closely connected with the customers' activities at the user level. As a result the application is accomplished with a security module, designed to process personal information of users in accordance with preliminary defined privacy requirements and to ensure secure transactions at the user level of a mobile ecosystem. The security module consists of two parts. The first one *Identification and Authorization* deals with input data flows, collecting and processing information for new customers and storage them after encryption. It is done on the base of an algorithm for data validity, which consists of 9 basic steps, as follows:

Step (1) Defining attributes

At this step different attributes obtain set of values which are acceptable, having in mind the nature of every separate item. As a result several sets from S_1 to S_N are defined. They will be used to present input data in a way, preliminary put over control to avoid grammar or logic mistakes.

Step (2) Data validity control

When a new customer fulfils the registration template, he/she is obliged to propose information which usually contains personal data. They must be checked for validity at first and after that the rest information of the template will be appended to the new user's profile.

Step (3) Data base actualization

All data, collected in accordance with the application's security requirements, are stored in a database, designed especially for the purposes of personal data storage. Some of the data which clients propose are not compulsory, but they could be very useful for service personalisation, having in mind education, occupation, specific professional interests and activities of each individual.

Step (4) Metadata base design

Data, structured at the *step (1)* and data from the accepted templates are processed to extract information about their origin, their semantic, features of their content and structure, i.e. at this step metadata are defined and stored in a metadata base.

Step (5) Profiles of the customers

When input data are checked, stored and corresponding identification parameters for secure access are defined every registered user has already his profile.

Step (6) Identification of a user

Parameters, generated to identify a user when his profile is completed at *step (5)* must be checked and proved before addressing any request to the application.

Step (7) Authorisation of the customers

After successful authorisation every user could deal with additional functionality of the application depending on access rights obtained during registration.

Step (8) Processing of a request

When the data, proposed by the user at the step (6) are checked and proved, i.e. the identification is successful request is ready to be processed.

Step (9) Sending results

User obtains results, information of his identification and authorization is kept in journal files to be checked subsequently, if it is necessary.

The second part of the security module *Authentication and Trust service* is designed to ensure secure transfer of data and files and reliable authentication by certificates. Data integrity is guaranteed by hashing, SHA-1 is applied. Typical client server application which implements SSL for encrypted data transfer and digital certificate X. 509 v.3 for prompt authentication is proposed. The scheme of the security module is shown in figure 5 where the two parts are outlined in accordance with their relations and interdependences. Customers could deal with mobile application stores in a secure environment with their everyday used devices – smart phone, tablet and PC. This approach gives good opportunity different applications to be integrated at this level of the mobile ecosystem, protecting personal data of the users, proposing them full functionality.

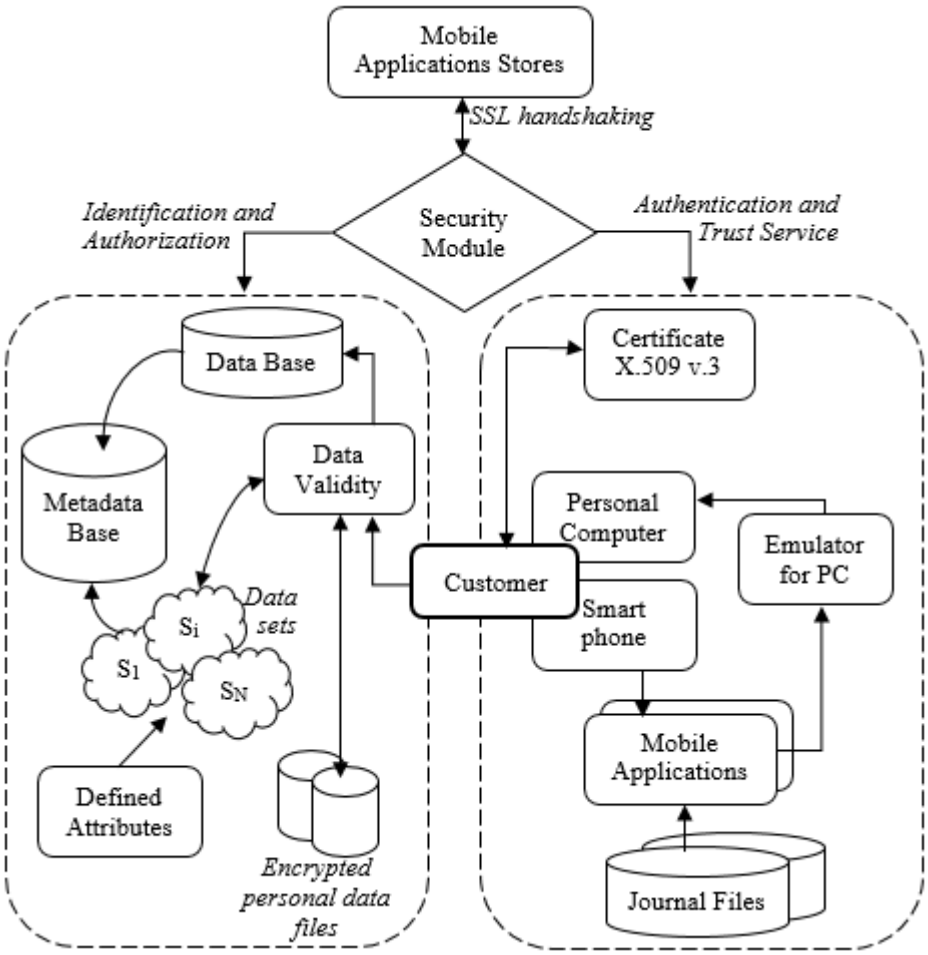

Fig. 5. Security module at User level

4. CONCLUSION

Mobile ecosystems are now and will be in the future an object of many attacks that could cause damages or destroy functionality of their components. Contemporary cyber attacks become more complex and more flexible in order to avoid or break defence mechanisms that have been already applied and sometimes these attacks succeed. For this reason the process of analysis the security level of a system must be permanent, new measures, tools and schemes should be implemented in time. The security module, proposed in this article is designed to be used as a part of a whole system for strong security at the user level of a mobile ecosystem which allows many different applications to be put over control in order to keep customers privacy and to guarantee reliable transactions.

REFERENCES

[1] Roman, R., J. Lopez, M. Mambo. Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. *Future Generation Computer Systems*, 1 (vol. 78, part 2), Jan 2018, pp. 680-698;
URL: https://www.sciencedirect.com/science/article/pii/S0167739X16305635

[2] Peev, St., Romansky, R. Technological Aspects of Mobile Payments Organization. *International Journal on Information Technologies and Security*, ISSN 1313-8251, 3 (vol. 6), 2014, pp.55-65.

[3] Toch, E. et al. The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Computing Surveys*, **2** (vol. 51), June 2018, Article No. 36. URL: https://dl.acm.org/citation.cfm?id=3172869&dl=ACM&coll=DL

[4] Romansky, R. Opportunities of the Digital Space and Challenges for Privacy and Individual's Security. *Proceedings of the 31st International conference on Information Technologies (InfoTech-2017)*, ISSN 1314-1023, Bulgaria, 20-21 Sep. 2017, pp. 169-178.

[5] Winter, J., S. Battisti, T. Burstrom, S. Luujjainen. Exploring the Success Factor of Mobile Business Ecosystems. *International Journal of Innovation and Technology Management*, **3** (vol. 15), 2018, pp. 1850026-1 - 1850026-23. URL: https://www.worldscientific.com/doi/abs/10.1142/S0219877018500268

[6] Burg, A., A. Chattopadhyay, K-Y. Lam. Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things. *Proceedings of the IEEE*, **1** (vol. 106), Jan 2018, pp. 38-60. URL: https://ieeexplore.ieee.org/abstract/document/8232533

[7] Abbas, R et al. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In: *The Network and Distributed System Security Symposium (NDSS 2018)*, 18-21 February 2018, San Diego, CA, USA, 15 p.; URL: http://eprints.networks.imdea.org/1744/1/trackers.pdf

[8] Bonneau, V., Evolution de l'ecosyseme Mobile, 13 Octobre 2016, https://fr.idate.org/evolution-de-lecosysteme-mobile/

Information about the author:

Irina Noninska - PhD, Associate professor in Cryptography and data security. She has obtained her PhD degree in Databases and Local Area Networks from Technical University of Sofia. Now she is a lecturer at Computer Systems Department, Technical University of Sofia, delivering courses "Cryptography" and "E-business technologies". Her scientific and research interests are in the area of Information and Network Security, Data Protection, Cryptographic Algorithms and Protocols, Quantum cryptography, Cyber security, Internet of Things, Telecommunication Standards. She is author and co-author of more than 90 scientific papers, articles and 9 books. She is a member of: Union of Scientists, Bulgaria; Union of Automatics and Informatics; International Editorial Board of International Journal on IT and Security; Organizing and Program Committee of Information Technologies.

Manuscript received on 12 April 2019