Secure Communication Using SDEx Method

Piotr Milczarski, Artur Hłobaż, Krzysztof Podlaski
Faculty of Physics and Applied Informatics
University of Lodz
Pomorska str. 149/153, Lodz, Poland
{piotr.milczarski, artur.hlobaz, Podlaski}@uni.lodz.pl

***Abstract*—In the paper the communication security is discussed. Nowadays applications mainly do not support end-to-end security. In the paper we show the solution (SDEX method) how to maintain end-to-end encryption in the data transferring basing on public key distribution using social media. The application of elaborated SDEX method is shown.**

Keywords— secure communication, data encryption, public key distribution,mobile applications, social networks, secure data exchange method.

I. Introduction

Nowadays, the Internet security is more and more crucial and even normal Internet users are becoming more and more conscious of the problem [1][2]. In recent years, there have been several major stories about how easy is to eavesdrop and breach our data or communication privacy like emails, e.g. secret documents leaked by former U.S. National Security Agency contractor Edward Snowden, WikiLeaks, HeartBleed OpenSSL, etc. Majority of users is not conscious what encryption is and that applications they use does not support it. It will not help to change it by simply saying or advertising that we users should rise our security level. There are some research that show that your friends can raise your awareness and make you more willing to implement the security measures [2]. The research done by Electronic Frontier Foundation (*EFF*) has shown that only 6 out of 39 popular messengers fulfills 7 criterions that may support end-to-end security properly [4].

In Sec. II the end-to-end security is described. In Sec. we present Secure Data Exchange (*SDEx*) method. In Sec. IV. an example of the method application is shown and possible security problems briefed. Finally, Sec. V. concludes the paper.

II. End-To-End Messengers security

The sophisticated online surveillance techniques used by the spy agencies pose the same problem as hackers. If the governments can do it, hackers maybe can do that as well. The problem of different types of attacks is described in several publications, e.g. session hijacking. Facebook has said it could enable end-to-end encryption between users exchanging data, but said such technology is complicated and makes it harder for people to communicate [5].

In the recent research [4] (Nov 2014) done by Electronic Frontier Foundation (*EFF)* 39 services were checked including popular tools from Apple, Google, Facebook, BlackBerry, Microsoft and Yahoo. According to the EFF research, only 6 applications pass the security test. The EFF was interested in 7 possible questions/features [4]: is data encrypted in transit; is it encrypted so the provider can't read it; can the service verify contacts' identities; are past communications secure if keys are stolen; is the code open to independent review; is security design properly documented; and has there been an independent security audit?

All 39 examined by EFS applications encrypt content in transit, but only six satisfied all of the EFF's security requirements and managed to fulfill all seven EFF requirements: ChatSecure + Orbot, Cryptocat, Off-The-Record (Windows), RedPhone, Silent Phone, Silent Text and TextSecure. Basing on the EFS criterions we prepared the outline of the method that supports end-to-end security. The idea of using the well-known methods of encryption to support end-to-end security is presented in [6][7]. We show some new methods how to strengthen the security of data exchange.

III. Method Secure Data Exchange (*SDEx*)

In the *SDEx* method that general outline is presented in [6][7][8], we have sketched the idea of creating secure channel that supports end-to-end secure connectivity. That method also fulfills all of the *EFS* criterions supposing that we have the code open to independent review and there has been an independent security audit. It does not need the special architecture because it uses existing Social Medial Networking users profile. In the papers [9][10][11] we have also shown several methods and techniques how to make end-to-end users communication more secure.

A. The Method SDEx and Their Applications Prerequisites

The method Secure Data Exchange (*SDEx*) was presented generally in [6][7] and [8]. The *SDEx* method is designed so it can fulfill the first five requirements of the EFS research.

The application prerequisites that uses the SDEx method [8]: (1) have the Internet and Social Medias Network access; (2) can upload and download files/ images from them; (3) can save data (keys) locally on the device; (4) can generate QRcode, process QRcodes; (5) can capture and send text and data from SMS, messengers; (6) can capture voice telephony agent to work with the voice transmission; (7) can encrypt and decrypt using well known methods. The prerequisites of the applications can be widened or shortened due to the application's functionality.

B. Frame formats

Frame format of the published QRcode as a public key was designed especially to find QRcodes in Social Media galleries.

Frame metadata header of QRcode contains set number of 16 bytes [8]: unique set of bits for filtering the gallery – 4 bytes; header length in bytes – 1byte; timestamp of key generation in milliseconds – 8 bytes; version of the key – 1byte; key length in bits – 2 bytes. The QRcode is storing only the data without any tags. That data can be anything like names, phone numbers, web page links, etc.

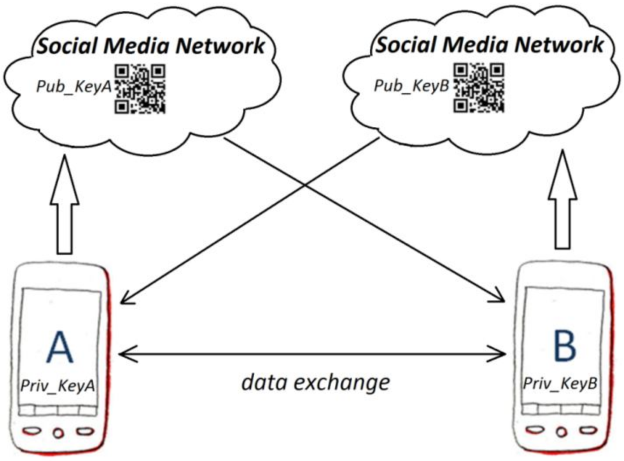

Fig. 1. General scheme of mobile applications using SDEx method

The designed frame metadata header of the message is important part of the SDEx and it contains set number of 14 bytes [8]: application ID – 4 bytes; special unique code - 2 bytes; - message type and controls like new key request, key received, key acknowledged, unrecognized key, etc. – 1 byte; timestamp of key generation of the public key (user B) in seconds – 4 bytes; version of the key used – 1 byte; message length in bytes – 4 bytes.

IV. Applications of SDEx Method

At the Fig. 1 it is shown the general scheme of applications that use SDEx method. In the paper [8] the whole method is described thoroughly.

The example of implementation for the encrypted SMS exchange is shown at the Fig. 2. The proposed header can vary depending on the medium used, e.g. phone calls. In the text messaging using SMS it can be simplified by omitting the message length part of it. During the process of data exchange it is possible to change the keys or change the communication medium. For more details see [8].

The problems that need the research is how to protect the initial exchange of the keys because of the possible man-in-the middle attacks, lack of IT infrastructure and how to have the keys that authenticate (and confirm) the end user.

Conclusions

The proposal of secure data exchange with everyday social network as key store solves both of the problems. On the other hand usage of images from social network gallery makes it easy to accept by ordinary mobile user. The proposed method can be implemented in mobile applications and description of such application was presented. The application will be presented in more details in next articles.

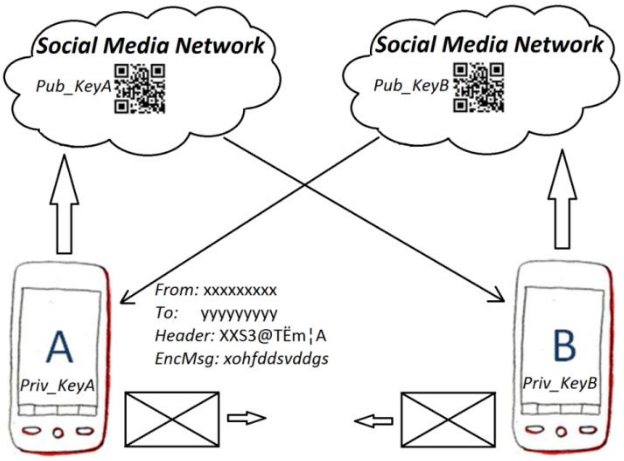

Fig. 2. Text exchange using SMS

The problems that need to be examined are: (A) how to protect the initial exchange of the keys because of the possible man-in-the middle attacks, (B) lack of IT infrastructure and (C) how to have the keys that authenticate (and confirm) the end user.

References

[1] N. Nikifrakis, W. Meert, Y. Younan, M. Johns, and W. Joosen, "Sessionshield: lightweight protection against session hijacking," Engineering Secure Software and Systems, pp. 87–100, 2011.

[2] I. Threats, " New Challenges to Corporate Security," Research Journal of Applied Sciences, 8, 3, 2013. Becker, A and Paar, I: Bluetooth security & hacks, Ruhr-Universität Bochum, 2007.

[3] S. Das, A.D.I. Kramer, L. A. Dabbish, and. J.I. Hong, "Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation," Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14), ACM, New York, pp. 739-749, 2014.

[4] Electronic Frontier Foundation, https://www.eff.org/secure-messaging-scorecard, November 2014.

[5] The Verge, http://www.theverge.com/2013/6/26/ 4468050/facebook-follows-google-with-tough-encryption-standard. Accessed March 2015.

[6] K. Podlaski, A. Hłobaż, P. Milczarski, "New Method for Public Key Distribution Based on Social Networks," CoRR abs/1503.03354, 2015.

[7] K. Podlaski, A. Hłobaż, P. Milczarski, "Secure Data Exchange Based on Social Networks Public Key Distribution", in proceedings 2nd SaSeIoT, Rome Italy, Oct 2015.

[8] P. Milczarski, K. Podlaski, A. Hłobaż, "Applications of Secure Data Exchange Method Using Social Media to Distribute Public Keys," in Computer Networks, Communications in Computer and Information Science Vol. 522, Springer International Publishing, pp. 389-399, 2015.

[9] A. Hłobaż, K. Podlaski, P. Milczarski, "Applications of QR Codes in Secure Mobile Data Exchange," Communications in Computer and Information Science Vol. 431, pp. 277-286, 2014.

[10] A. Hłobaż, "Security of measurement data transmission - message encryption method with concurrent hash counting," SEP 1/2007.

[11] A. Hłobaż, "Security of measurement data transmission - modifications of the message encryption method along with concurrent hash counting," FSNT NOT Vol. 1, pp. 39-42, 2008.