Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 171–174
DOI: 10.15439/2014F319
ACSIS, Vol. 3

Send It Safe – A Novel Application for Secure Key Exchange Using Telecommunications Open Middleware APIs

Piotr Wawrzyniak
Orange Polska
Orange Labs
Research and Development Centre
ul. Obrzeżna 7
02-261 Warsaw, Poland
Email: piotr.wawrzyniak@orange.com

Łukasz Wronkowski, Damian Kuniszewski,
Adam Cackowski, Paweł Czapliński,
Karol Szymański
Faculty of Mathematics and Computer Science
Nicolaus Copernicus University
ul. Chopina 12/18
87-100 Toruń, Poland
Email: wronkowski.lukasz@gmail.com

Abstract— Common surveillance of citizens by various intelligence services every year becomes more dangerous threat to our privacy. Recently, number of security enrichment was developed that allows to increase privacy protection during pervasive network use. In this article we present a novel approach that uses telecommunications OpenMiddleware APIs to provide reliable public key exchange protocol.

I. Introduction

NOWADAYS security and privacy issues are getting more and more important for many people using state of the art communication tools like mobile smartphones or internet [1]. The growing need to increase security results in number of applications increasing the privacy and security.

Majority of existing telecommunication security solution generally are intended to be used in IP-based networks, such as internet. This is caused by several factors, among them widespread of internet communication is one of the key driver. However recently growing number of smartphone users results in growth of the importance of mobile security and privacy.

One of the important issues regarding secure communication is the key exchange process when asymmetric ciphers are to be used. Among several available protocols, the scheme based on Diffie-Hellman concept and its derivative Station to Station (STS) protocol [2, 3].

The possibility to use secured communications on mobile devices is often limited by insufficient device capabilities, lack of necessary software libraries or poor internet connectivity.

In this article we present novel application designed for Android-enabled mobile phones which allows to securely exchange cryptography keys with the use of Public Land Mobile Network (PLMN) operator's infrastructure. In fact, our solution makes use of Unstructured Supplementary Service Data (USSD) messages, which provides a finest level of reliability and confidentiality. Number of applications proves that USSD channel can successfully replace IP connectivity in a variety of fields [4-7]. Moreover due to OpenMiddleware Application Programing Interfaces (APIs) network resources, including USSD communication channel can be easily accessed by external services [8-10] with the use of state of the art protocols including RESTful web services.

The remainder of this paper is organized as follows:

- Chapter II provides description of the system architecture, it focuses on the key functions of the entire components,
- In chapter III our proposal of simple, efficient and secure key exchange protocol intended for USSD communication channel is presented,
- Chapter IV describes Human-System Interaction, in particularly focusing on the mobile applications developed for Android-enabled mobile phones.
- Chapter V summarizes the paper and provides possible further extensions.

II. System Architecture

Our system consists of two main parts: application server which act as message proxy between negotiating parties, and mobile application designed for Android-enabled smartphones that allows to exchange encryption keys and facilitate the communication protocol.

Application server act as simple proxy and is the key component of the solution. The importance of that element origins in a USSD communication constraints, which makes it impossible to send USSD datagram directly between two mobile phones (using operator service platforms only). In particular USSD messages can only be send between mobile phone and service platforms and vice versa thus it was necessary to develop proxy service that will enable USSD

© 2014, PTI

datagrams exchange between two mobile phones. On the other hand such strong dependency on operator infrastructure makes USSD messages highly reliable communication channel.

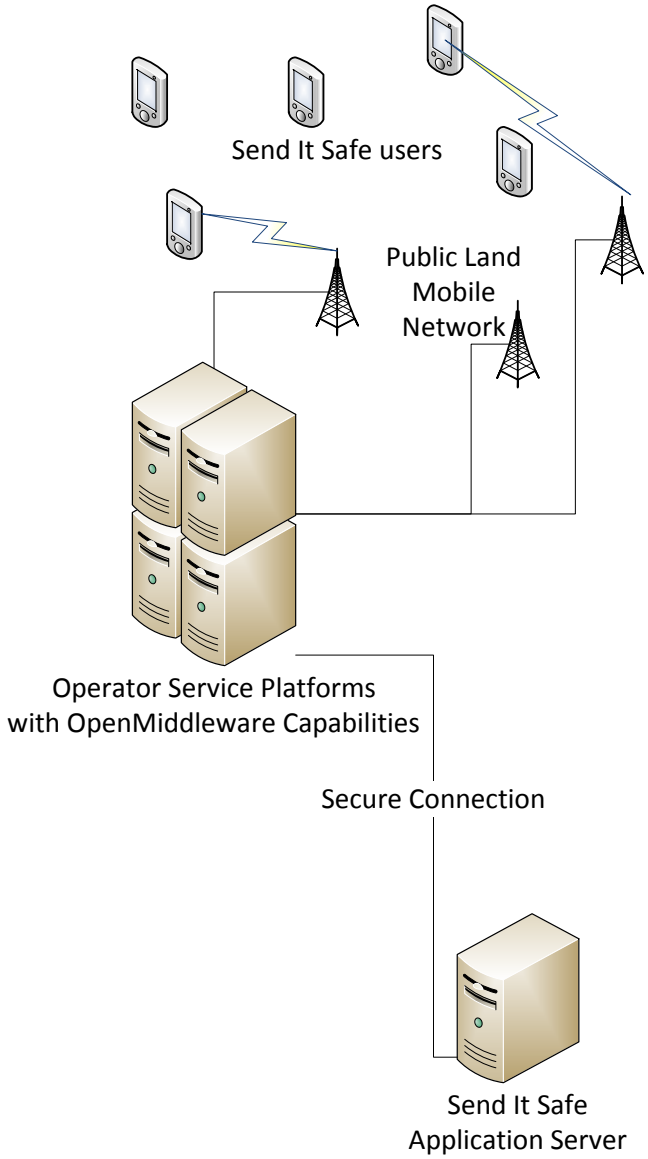

Fig. 1 The architecture of developed solution

Our proxy server allows to maintain the finest privacy and reliability level. In particular it do not violate the integrity of the payload of exchanged datagrams.

Developed mobile application is designed for Android 4.0 or newer smart phones. It is composed of two cooperating independent components. First one is Android system service that runs in the background. It is started together with the Android OS in independent process. Functionalities of the service includes but are not limited to:

- Capturing SMS messages from the system (before they appear on the screen)
- Capturing received USSD messages
- Categorizing of incoming messages
- Communication with external applications
- Modifying screen dialogs that accompanies USSD messages being sent (percentage progress is displayed instead of standard message)
- Displaying the progress in the system tray while receiving the key
- Supporting retransmission of individual packets when communication error occurs.

Latter part of Android components is Graphical User Interface (GUI) application that is responsible for:

- Concatenating incoming messages
- Encoding and encrypting the messages
- Confirming and checking the identity of the remote party
- • Communication with the Service
- • Dividing outgoing messages to parts that can be sent via USSD protocol
- • Managing key repository (reading stored keys, alternatively it is possible to load the public key of the remote party if we have any in the device repository, verifying whether our keys belong to one pair)
- • Encrypting and sending secured SMS messages and their reception and decryption.

The overall architecture of the proposed solution is provided in Fig. 1.

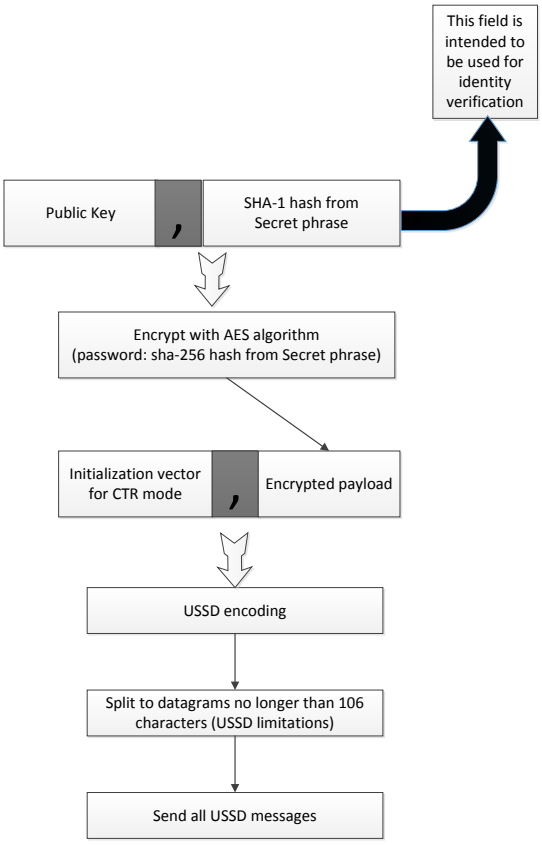

Fig. 2 Implemented key exchange message composing algorithm.

III. Key Exchange Protocol

In order to use USSD messages for key negotiation, key exchange algorithm was designed and implemented. It uses symmetric key to exchange asymmetric public key between involved parties, which significantly minimizes the number of messages to be exchanged during key negotiation. Minimization of number of datagrams is particularly important factor since it takes about three seconds to exchange single USSD message thus allows to make our system more responsive in human-system interaction experience.

Moreover our algorithm provides efficient mechanism of identity verification which is based on pre-known secret phrase. The secret should be agreed by both negotiating parties prior to entire key exchange. Such approach benefits in strict identity verification capabilities from the one side and allows to keep the number of exchanged datagrams as small as possible on the other. The algorithms for concatenating and initial processing of the key exchange algorithm are presented in Fig. 2 and Fig. 3.

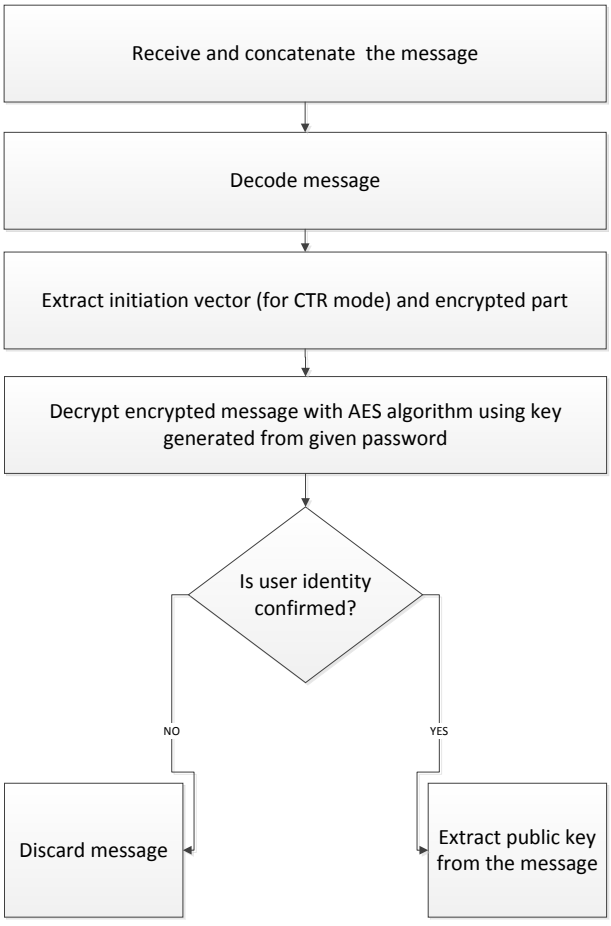

Fig. 3 Proposed public key exchange algorithm.

The simplification of the key exchange do not disturb the overall security of the system. Since we use USSD datagrams even this simple approach provides high reliability and security due to fact that entire communication channel is strongly secured.

Fig. 4 The "Load Keys" menu ("Wczytaj klucz" means "Load key"). In provided picture both keys were loaded and verified to be the same pair of public and private key.

IV. Human-System Interaction

User might interact with the developed solution with the use of sample application developed as a part of the project. It is primarily intended to be used for key repository management as well as managing and supervising key exchanges, as mentioned in chapter II. This capability is documented in Fig. 4

User interface provides simple visual aids for key management (whether the keys are loaded, validated, etc.) accompanied by the constant monitoring of the key exchange progress. Moreover it can be used to manage contacts (i.e. other people with whom public keys has been already exchanged). The sample menu intended for contact management is provided in Fig. 5.

Moreover exchanged public keys might be exported and easily used by other applications. This feature significantly expand application usability since it can be used for secure and reliable key exchange that are intended to be used by other application or services. This feature makes it also possible to easily incorporate our secure key exchange mechanism into existing services.

Nevertheless the main purpose of the application is to allow secure communication via encrypted SMS or USSD messages with other users. For securing user communication our solution uses RSA algorithm but as it was aforementioned it is possible to store exchanged keys and use them for any purpose.

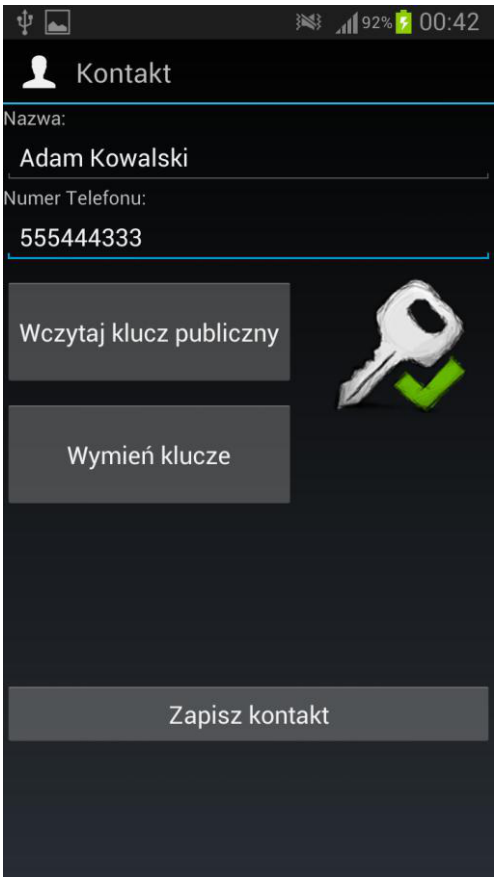

Fig. 5 The “Manage Contacts” menu (“Wczytaj klucz publiczny” means “Load public key”, “Wymień klucze” means “Exchange keys”, “Zapisz Kontakt” means “Save contact”).

Upon successful message decryption it remains secured. In particular it stored in dedicated secure storage of the application. Therefore it can be accessed only with the use of our application and is not being displayed in standard messaging application of the phone.

V. Summary

In this article we presented prototype solution designed for secure and reliable key exchange for mobile devices. It makes use of PLMN operator infrastructure which is accessible via OpenMiddleware APIs. Proposed solution is composed by three main parts:

- Android system service, which makes it possible to seamlessly use USSD and SMS communication channels for key exchange protocol,
- Android GUI application designed for key repository management, instant monitoring of the key exchange process and providing tools for communication with the use of secured SMS messages,
- Send It Safe application server, that acts as message proxy. Due to security reasons and in order to provide highest confidentiality level, the proxy do not modify payload of processed datagrams.

Since proposed solution makes extensive use of USSD messages for key exchange, lightweight key exchange protocol has been developed. It allows to minimize the number of exchanged datagrams and provide strong identity verification capabilities.

Moreover exchanged keys can be stored in device memory which makes them accessible to any external application. This approach strongly increase usability of proposed system.

Future system development plan includes implementation of mobile party for other smartphone operating system and implementation of server-side administration panel for performance monitoring.

References

[1] Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., Borgthorsson, H., & Vej, R. L., “Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use,” in ACM CHI Conference on Human Factors in Computing Systems, http://dx.doi.org/10.1145/2556288.2557421.

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition Pearson Education, Inc, 2011

[3] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography. CRC Press LLC, 1997.

[4] Bogusz D., Siewruk G., Legierski J., Kunicki J.S.,USSD communication channel as alternative to XML SOAP in mobile Unified Communication applications, Federated Conference on Computer Science and Information Systems. Place: Krakow. September 8-11, 2013

[5] Trusiewicz, P.; Legierski, J., "Parking Reservation - application dedicated for car users based on telecommunications APIs," Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.865,869, 8-11 Sept. 2013

[6] Litwiniuk, K.; Czarnecki, T.; Grabowski, S.; Legierski, J., "BusStop — Telco 2.0 application supporting public transport in agglomerations," Computer Science and Information Systems (FedCSIS), 2012 Federated Conference on , vol., no., pp.649,653, 9-12 Sept. 2012

[7] Trusiewicz, P.; Witan, M.; Kuzia, M., "Mobile Payment System - Telco 2.0 application dedicated for payments," Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.859,864, 8-11 Sept. 2013

[8] Legierski J., Korbel P.; Telco 2.0 -przykłady praktycznego wykorzystania interfejsów telekomunikacyjnych platform usługowych, KSTIT2011, Przegląd Telekomunikacyjny, 8-9/2011

[9] Wawrzyniak, P.; Korbel, P.; Borowska-Terka, A., "Student information delivery platform using telecommunications open middleware APIs," Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.871,874, 8-11 Sept. 2013

[10] Korbel, P.; Wawrzyniak, P.; Grabowski, S.; Krasinska, D., "LocFusion API - Programming interface for accurate multi-source mobile terminal positioning," Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.819,823, 8-11 Sept. 2013