SKEMON: A Simple Certificate-Less Method for Key Exchange by Using Mobile Network

C. Sakamoto[1], G. De Marco[1], R. Yaegashi[2], M. Tadauchi[1], and L. Barolli[3]

[1] Toyota Technological Institute, Tenpaku-Hisakata 2-12-1, Nagoya 468-8511, Japan
{demarco,tadauchi}@toyota-ti.ac.jp
[2] Shibaura Institute of Technology, 3-7-5 Toyosu, Toto-ku, Tokyo 135-8543, Japan
rihito@sic.shibaura-it.ac.jp
[3] Department of Information and Communication Engineering,
Fukuoka Institute of Technology (FIT)
3-30-1 Wajiro-Higashi, Higashi-ku, Fukuoka 811-0295, Japan
Tel.: +81-92-606-4970
barolli@fit.ac.jp

Abstract. Secure communications requires the exchange of keying material, which in general is not trivial problem. A simple solution is to use alternative communication channels to exchange the cryptographic keys, like standard mail services or reciprocal visual inspection of text strings. Here, we propose to use the standard Public Mobile Network (PMN) as an alternative channel, because the use of mobile phones has become pervasive and affordable for most of users. The basic assumption is that the PMN is more secure than other wireless and wired networks. We envision a system for subscribers who wish to exchange their cryptographic keys, which can be used afterwards for sending encrypted messages over other (insecure) communication channels, like Internet. We assume that every user or its mobile phone is able 1) to generate a public/private key pair, and 2) to store it inside his/her mobile phone rubric. The public key is exchanged by sending special requests by means of standard PMN services, like the text messaging system. We analyze the scalability of such a system, by assuming that the subscribers can send group queries, i.e. queries which request the whole (public) keys stored in the rubrics of a subset of the closest neighbors of an user. The performance of such an approach depends on the properties of the graph model of interactions among people. By means of simulations, we show that it is preferable to send few group queries instead of many single requests. This result can be used to dimension the service provided by the PMN.

1 Introduction

Nowdays, we can count a lot of solutions to tackle the security concerns of network based information systems. Perhaps, the most famous solution is the Public Key Infrastructure (PKI) which uses asymmetric cryptography, in order to provide confidentiality, privacy and perfect forward secrecy[1]. As representative public key cryptosystem, we cite S/MIME (Secure Multipurpose Internet

[1] For example, by using Ephemeral Diffie-Hellman.

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 108–117, 2007.

Mail Extensions) used to secure e-mails, IPSec (Internet Protocol Security)[10] used for establishing VPN connections (Virtual Private Network) [8] and TLS (Transport Layer Security)/SSL (Secure Socket Layer) [6] aimed at secure transactions on the Web. One of the problem of PKI is the distribution of keys [12]. The standard solution is providing users with signed certificates distributed by trusted Certificate Authorities (CA). However, CAs are single point of failure and deploying a lightweight PKI infrastructure even for simple and daily communications can be difficult. Furthermore, anonymity is not always guaranteed in PKI. In fact, the public keys must be known to both parties of the communication. If one of the party does not know the correspondent's public key, he/she must require a certificate. Sending a certificate over an insecure channel allows attackers to know the participants of the communication.

Here, we propose Simple Key Exchange by using MObile Network (SKEMON), a certificate-less system to distribute the encryption keys by using the Public Mobile Network (PMN). The invaluable advantage offered by the PMN with respect to the Internet is that the spoofing and/or the attacks are relatively difficult. In fact, wiretapping a communication over the PMN is very hard or at least costly, while it is very easy sniffing, analyzing and forging packets flowing through an IP network . For example, in wireless Ethernet as the IEEE 802.11, the `aircrack` tool can easily recover the keys used for encryption of the communication; in wired Ethernet, the `etthercap` tool can easily mount Man in the Middle (MiM) attacks [1]. Here, we assume that users trust one another, or rather their public keys are implicitly signed, as in the scheme of Günther. This self-certification is given by the reciprocal knowledge of cell phone numbers. Accordingly, the exchange of public keys can be executed by using cell phone themself. In this way, users inherently signed their public keys and a certificate server is not needed. The system uses only two messages and it is like a messaging system. We leverage the security of the PMN in order to exchange the encryption keys. We analyze pros and cons of the proposed architecture in case of one-to-one and one-to-many communications.

The rest of the paper is organized as follows. In Section 2, we briefly review related works about key exchange proposals. In Section 3, we discuss our proposal and in Section 4, we analyze the system both from the point of view of the security and the scalability. In Section 5, we give our simulation results, by comparing single queries against group queries, and we conclude the paper in Section 6.

2 Related Works

A classical way to exchange the key of two parties is the Diffie-Hellman (DH) protocol which requires two messages only. The DH protocol is vulnerable to MiM, and it is a point-to-point protocol which does not scale as the number of users increases. Other solutions propose the use of a Key Distribution Server (KDS), which pre-distributes symmetric keys to every user. Although this solution can be optimized with respect to the scalability, e.g. by using the Blom's