Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

On the detection of desynchronisation attacks against security protocols that use dynamic shared secrets

Ioana Lasc, Reiner Dojen*, Tom Coffey

Department of Electronic & Computer Engineering, University of Limerick, Plassey Park, Limerick, Ireland

ARTICLE INFO

Article history:
Received 21 December 2011
Received in revised form
6 September 2012
Accepted 5 October 2012

Keywords:
Authentication
Protocol verification
Wireless communication
Mobile communication systems
Denial of service

ABSTRACT

Many peer-to-peer security protocols in mobile communications utilise shared secrets. Synchronous storage of shared secrets is imperative for the successful operation of security protocols, as asynchronous storage of shared secrets may lead to service unavailability. Hence, update mechanisms must not only guarantee the secrecy of shared secrets, but also their synchrony.

This paper addresses synchronisation weaknesses in security protocols for wireless communications. It is demonstrated that a wide range of protocols contain such weaknesses. A new class of attack, called suppress-and-desynchronise attack, is introduced that exploit these weaknesses. These new attacks desynchronise the shared secrets of principals by suppressing messages, resulting in a permanent denial of service condition.

A verification system to model update mechanisms for shared secrets is introduced. Based on this verification system detection rules are developed that are able to detect synchronisation weaknesses that can be exploited by suppress-and-desynchronise attacks. Application of the detection rules to three security protocols results in the detection of hitherto unknown weaknesses. Consequently, these security protocols are susceptible to suppress-and-desynchronise attacks and details of mounting the attacks are presented. Finally, amendments to one of these protocols are proposed and application of the introduced formal system establishes the immunity of the amended protocol against suppress-and-desynchronise attacks.

1. Introduction

The security of electronic networks and information systems is nowadays a critical issue for the growth of information and communication technologies. This is particularly the case in the wireless environment, where the data is broadcasted over open airwaves. As these networks are often trusted with highly sensitive information, the security of both the infrastructure itself and the information that runs through it must be guaranteed. Security protocols are used to provide such protection by offering services such as authentication, key establishment, confidentiality, integrity and non-repudiation. Such security protocols need to be able to withstand threats such as replay attacks, type-flaw attacks and denial of service attacks.

In addition to security requirements, security protocols for wireless communications have to consider the restricted computational abilities and the limited power resources of the wireless/mobile devices (Ravi et al., 2004; Coffey et al., 2003). Thus, many peer-to-peer security protocols in the mobile

* *Corresponding author*. Tel.: +353 61 213442; fax: +353 61 338176.
E-mail addresses: ioana.lasc@ul.ie (I. Lasc), reiner.dojen@ul.ie (R. Dojen), tom.coffey@ul.ie (T. Coffey).

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.10.004

environment utilise shared secrets to minimise the computational burden on mobile devices (Aziz and Diffie, 1994; Bargh et al., 2004; Lee and Yeh, 2005; Nan and Jian, 2008; Lee et al., 2009; Li and Sandrasegaran, 2009). However, there are security concerns raised by the long-term storage of shared secrets (Shim and Denget al, 2002). Therefore, modern security protocols utilise dynamic shared secrets, which are updated to new values in each session by an underlying update mechanism (Lasc et al., 2011a,b; Hwang et al., 2003; Chang and Chang, 2005; Tseng, 2007; H. Chen et al., 2009). For most applications an off-line update via smart cards or other security tokens is not feasible. Therefore, an online update mechanism is employed, where the new shared secret value is established through message exchanges between the involved principals.

Mutual authentication based on such dynamic shared secrets is performed by proving ownership of the current instance of the shared secret (Lee et al., 2009; Chang and Chang, 2005). Additionally, these dynamic shared secrets may also be used:

- as fresh components to protect against replay attacks and in the generation of session keys (Aziz and Diffie, 1994; Li and Sandrasegaran, 2009; Hwang et al., 2003; Tseng, 2007).
- to act as non-related aliases to mobile users while roaming in foreign domains with the purpose of preserving user privacy (H. Chen et al., 2009; TZ. Chen et al., 2009).
- in the creation of evidence of service access to provide non-repudiation in billing protocols (Lee and Yeh, 2005; Tseng et al., 2004).

Online update mechanisms for dynamic shared secrets must not only ensure the secrecy of the shared secrets, but must also guarantee their synchrony.

1.1. *Original contribution of this work*

In this paper we reveal a new weakness in the update mechanisms of current security protocols that utilise dynamic shared secrets. It will be demonstrated that this weakness is inherent in a wide range of protocols such as Aziz and Diffie (1994) (AD), Hwang et al. (2003) (HYS), Chang and Chang (2005) (CC), Tseng (2007) and TZ. Chen et al. (2009) (CLC) protocols.

Further, a new form of attack – termed in this paper as suppress-and-desynchronise attack (SD attack) – that exploits this weakness is presented. In an SD attack, the intruder interferes with the delivery or integrity of messages to cause failure of the update mechanism. In many cases, the SD attack is mounted by suppressing a single message between the communicating parties. As a result, the attacked security protocol is compromised and further communication between the involved parties is no longer possible. Thus, if the security protocol is not designed to deal with the possibility of a failed update mechanism, a permanent denial of service condition is reached.

This paper also proposes a new verification system that is able to model update mechanisms for shared secrets. Further, the verification system is able to detect update mechanisms that are susceptible to SD attacks.

To demonstrate the effectiveness of the verification system, it is used to establish the presence of hitherto unknown weaknesses in AD (Aziz and Diffie, 1994), HYS (Hwang et al., 2003) and Tseng (Tseng, 2007) security protocols. It is demonstrated how an attacker can exploit the detected weaknesses by mounting SD attacks against these protocols. In each case, executing the SD attack results in a permanent DoS condition. Finally, amendments to the AD protocol are proposed and the formal system is used to prove the immunity of the amended AD protocol against SD attacks.

2. New attacks against security protocols implementing update mechanisms

Providing mutual authentication based on shared secrets is a common feature in security protocols. The communicating parties involved in a protocol session prove their identity by showing possession of the shared secrets as follows: Two principals initially establish a shared secret θ and store it in their memory. During one protocol run (we use the terms “protocol run”, “protocol session” and “protocol iteration” synonymously) the communicating parties challenge each other to prove possession of the shared secret θ by sending a message based on θ. If both principals are able to formulate the expected messages, mutual authentication is successful. If either principal is incapable of producing the correct message, mutual authentication fails.

Authentication based on static shared secrets, which are not updated online during a session, implies their long term usage. However, there are potential vulnerabilities associated with the long term storage of static shared secrets (Shim and Denget al, 2002), such as disclosure of past and current session keys and identity disclosure (H. Chen et al., 2009). Dynamic shared secrets, which are updated online, can be used to avoid potential vulnerabilities associated with static shared secrets (Chang and Chang, 2005; TZ. Chen et al., 2009).

2.1. *Authentication based on dynamic shared secrets*

Security protocols that implement dynamic shared secrets employ an underlying online mechanism to update these shared secrets to new values. Thus, a sequence of shared secrets θ_1 to θ_n is used, where a successful run of a protocol ensures mutual authentication of both principals by proving possession of the current shared secret θ_i (see Fig. 1).

The initial shared secret θ_1 is usually established in an offline process. In the first protocol run, principals mutually authenticate each other using θ_1. At the same time, the update phase of the protocol provides the principals with θ_2, the next instance of the shared secret. In general, the protocol run that uses θ_i also establishes the next shared secret θ_{i+1}. This new shared secret θ_{i+1} will be used in the subsequent protocol run, which also updates to the next shared secret θ_{i+2} and so on. Subsequent shared secrets can be either unrelated, i.e. be generated randomly (TZ. Chen et al., 2009), or can be created from the same seed (Tseng et al., 2004). In the latter case there is a functional relationship between consecutive values and perfect forward secrecy needs to be addressed (Chang and