Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Design guidelines for security protocols to prevent replay & parallel session attacks

Anca D. Jurcut, Tom Coffey, Reiner Dojen *

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

ARTICLE INFO

Article history:
Received 26 September 2013
Received in revised form
28 February 2014
Accepted 27 May 2014
Available online 12 June 2014

Keywords:
Security protocols
Design guidelines
Attack detection
Replay attacks
Parallel session attacks
Freshness of messages
Symmetry of messages
Signed messages
Challenge-response handshake

ABSTRACT

This work is concerned with the design of security protocols. These protocols are susceptible to intruder attacks and their security compromised if weaknesses in the protocols' design are evident. In this paper a new analysis is presented on the reasons why security protocols are vulnerable to replay and parallel session attack and based on this analysis a new set of design guidelines to ensure resistance to these attacks is proposed. The guidelines are general purpose so as to encompass a wide spectrum of security protocols.

Further, an empirical study on the effectiveness of the proposed guidelines is carried out on a set of protocols, incorporating those that are known to be vulnerable to replay or parallel session attacks as well as some amended versions that are known to be free of these weaknesses. The goal of this study is to establish conformance of the set of protocols with the proposed design guidelines. The results of the study show that any protocol following the design guidelines can be considered free of weaknesses exploitable by replay or parallel session attacks. On the other hand, if non-conformance of a protocol with the design guidelines is determined, then the protocol is vulnerable to replay or parallel session attacks.

1. Introduction

Cryptographic protocols play an important role in today's communications environment, where they are used to provide a wide variety of security services, such as: key distribution, data confidentiality, authentication and non-repudiation.

The design of provably secure protocols is complex and prone to error, where the main difficulty is to address the vast possibilities of an adversary to gain information (Dojen and Coffey, 2005). These protocols can be vulnerable to a host of subtle attacks that compromise the services they provide; so designing them to be impervious to such attacks has proved to be extremely challenging. Many published security protocols have subsequently been found to contain security weaknesses that are exploitable by attacks. The public key authentication of Needham and Schroeder (Needham and Schroeder, 1978), for example, was considered secure for over a decade. Other protocol weaknesses exploitable by attacks can be found in: (Denning and Sacco, 1981; Burrows et al., 1990; Syverson, June 1994; Lowe, 1996; Abadi, March 1997; Heather et al., 2000). The difficulty of designing security protocols that are free of mountable attacks continues today, as highlighted by many

* *Corresponding author.*
E-mail addresses: anca.jurcut@ul.ie (A.D. Jurcut), tom.coffey@ul.ie (T. Coffey), reiner.dojen@ul.ie (R. Dojen).

http://dx.doi.org/10.1016/j.cose.2014.05.010

recently found instances of replay and parallel session attacks:

- attacks found in 2003 (Coffey et al., December 2003) on several authentication and key agreement protocols for mobile communications (Beller et al., 1993; Carlsen, 1994; Mu & Varadharajan, 1996)
- attacks found in 2006 (Xu & Huang, September, 2006) and 2008 (Altaf et al., 2008) on privacy and key management IEEE Std. 802.16e-2005 protocol, (IEEE Std. 802.16e/D12, 2005)
- attacks (Nam et al., Jan 2007) found in 2007 on an authentication protocol introduced in 2005 (Lee et al., 2005)
- attack found in 2008 (Espelid et al., 2008) on Norway national security for e-commerce protocol BankID introduced in 2006 (The Norwegian Banks' Payment and Clearing Centre, 2006)
- attack found in 2008 (Xu et al., July, 2008) on a fingerprint-based authentication scheme with smart cards introduced in 2006 (Khan and Zhang, 2006)
- attacks found in 2008 (Dojen et al., 2008b) on a Key Management Protocol for Wireless Sensor Networks (Shen et al., 2008)
- attack found in 2008 (Dojen et al., 2008c)on a key distribution protocol (Lowe, 1997)
- attack found in 2009 (Hsiang and Shih, 2009) on a remote user authentication scheme using smart cards introduced in 2005 (Yoon and Yoo, 2005)
- attacks found in 2009 (Dojen et al., 2009) on an end-to-end authentication and secrecy protocol introduced in 2003 (Lee et al., 2003)
- attacks found in 2012 (Yoo et al., 2012) on an authentication scheme introduced in 2009 (Das, 2009) and its derivatives (Nyang and Lee, 2009; Huang et al., October 2010; Chen and Shih, 2010; Khan and Alghathbar, 2010)
- attacks found in 2013 (Wang and Ma, 2013) on ID-based scheme for mobile client–server environment introduced in 2012 (He et al., 2012)
- attacks found in 2013 (Fu and Guo, 2013) on lightweight RFID mutual authentication protocol introduced in 2011 (Jin et al., 2011)
- attack found in 2013 (Zhuang et al., July 2013) on RAPP ultra-lightweight RFID protocol introduced in 2012 (Tian et al., 2012)

1.1. *Original contribution of this work*

The research work presented in this paper is concerned with the design of security protocols, in particular the prevention of design weaknesses that may be subsequently exploited by replay or parallel session attacks.

A new analysis on the reasons why freshness and parallel session attacks against security protocols succeed is presented. This analysis discovers the vulnerabilities in the structure of the protocol message exchanges that can be exploited by these attacks. Specifically, the analysis seeks answers to the questions:

- Why are freshness and parallel session attacks successful?
- Can the reasons be represented by a finite set of data patterns representing the message exchanges?
- Is it possible to develop a finite set of protocol design rules or guidelines that will prevent the effectiveness of these attacks?

A new comprehensive set of guidelines for security protocols to prevent design weaknesses that are exploitable by replay or parallel session attacks is proposed. The guidelines are general purpose so as to encompass a wide spectrum of security protocols. The effectiveness of the guidelines is also established in a presented case study which shows that: (i) protocols with known weaknesses violate some of the guidelines, (ii) protocols without weaknesses do not violate any guidelines.

These guidelines are intended to be used at the design stage of security protocols. Any protocol following these guidelines can be considered to be free of any weaknesses exploitable by replay or parallel session attacks. On the other hand, if non-conformance of a protocol with the design guidelines is established, then the protocol is vulnerable to replay or parallel session attacks.

1.2. *Paper structure*

The remainder of this paper has the following structure. Section 2 gives an overview of related work and Section 3 outlines the analysed methodology used in this work. Section 4 introduces the language and definitions used through the paper. Each defined weakness type is then separately analysed and corresponding design guidelines are proposed: Section 5 addresses the issue of freshness of messages, Section 6 addresses the issue of symmetry of messages, Section 7 addresses the issue of signed messages and Section 8 addresses the issue of challenge-response handshake construction. In Section 9, the effectiveness of the proposed guidelines is evaluated by way of an empirical study on a set of protocols with known weaknesses and those that are known to be secure. The conformance of one protocol (and its amended version) is analysed in detail and the conformance of a range of protocols is presented in summary form. Finally, Section 10 concludes the paper. A summary of the proposed design guidelines is included in Appendix A.

2. Related work

The design of reliable and trustworthy security protocols has been addressed by a series of publications over the past two decades. Bird et al. (Bird et al., 1992) introduced in 1992 a two-way authentication protocol using symmetric key cryptography and gave a set of considerations to avoid weaknesses in the design of these types of protocols. This work was extended in 1993 (Bird et al., June 1993) in the form of a methodology to systematically build a family of cryptographic two-way authentication protocols that are resistant to a number of attacks. In order to protect protocol messages from being vulnerable to replay attacks, Carlsen (Carlsen, June 1994) provided a list (list included: protocol identifier, step identifier, message subcomponents identifier, primitive types of data items and protocol run identifier) of information that should be attached to cyphertexts. Gong and Syverson (Gong &