A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications

Ioana Lasc, University of Limerick, Ireland
Reiner Dojen, University of Limerick, Ireland
Tom Coffey, University of Limerick, Ireland

ABSTRACT

Many peer-to-peer security protocols proposed for wireless communications use one-time shared secrets for authentication purposes. This paper analyses online update mechanisms for one-time shared secrets. A new type of attack against update mechanisms, called desynchronisation attack, is introduced. This type of attack may lead to a permanent denial of service condition. A case study demonstrates the effectiveness of desynchronisation attacks against a security protocol for mobile satellite communications. A new mutual authentication protocol for satellite communications, incorporating a resynchronisation capability, is proposed to counter the disruptive effects of desynchronisation attacks. The new protocol has an synchronisation phase that is initiated whenever desynchronisation is suspected. Thus, the possibility of causing permanent denial of service conditions by mounting desynchronisation attacks is eliminated. A security analysis of the proposed protocol establishes its resistance against attacks like replay attacks, dictionary attacks, and desynchronisation attacks.

Keywords: Authentication, Denial of Service, Desynchronisation Attacks, Security Protocols, Wireless Communications

INTRODUCTION

Wireless communications are being driven by the need to provide network access for mobile or nomadic computing devices. The increase of available services using these wireless devices requires users to trust the employed communication networks with highly sensitive information. Security protocols are one of the most critical elements in enabling the secure communication and processing of information. Basic security protocols allow agents to authenticate each other, to establish fresh session keys for confidential communication and to ensure the authenticity of data and services (Dojen, Lasc, & Coffey, 2008). Building on such basic security protocols, more advanced services like non-repudiation, fairness, electronic payment...
and electronic contract signing are achieved. The design of such security protocols should be robust enough to resist attacks, such as replay attacks, parallel session attacks or type-flaw attacks. Additionally, the possibility of interfering with communication on physical channels by jamming needs to be considered as it can affect the security at the application layer (Gansler & Binnendijk, 2005). Denial of Service (DoS) attacks are a common form of cross-layer attacks (Radosavac, Benammar, & Baras, 2004), which can be achieved in two ways (Peng, Leckie, & Ramamohanarao, 2007): Firstly, an attacker can interact continuously with the targeted system to prevent service availability. In this case, the DoS condition disappears when the malicious interaction ends. Secondly, an attacker can interact with the targeted system for only a limited time to achieve a permanent denial of service condition. In this case the DoS condition remains until some corrective measures are taken.

Many peer-to-peer security protocols proposed for wireless communications use one-time shared secrets for authentication purposes (Lee, Chang, Hwang, & Chong, 2009; Chen, Lee, & Chen, 2008; Tseng, 2007; Chang & Chang, 2005; Lee & Yeh, 2005). These secrets are used by the owning principals to prove their identity in a protocol session. Additionally, the same protocol run establishes a new instance of the shared secret that will be used in the next session. The messages of the protocol that establish the new shared secret are referred to as the update mechanism. These update mechanisms serve two purposes: Firstly, the generation of a new instance of the shared secret and, secondly, agreement on the same new shared secret by all communicating parties. Thus, update mechanisms aim to ensure synchronous storage of the shared secret by all principals at the end of each protocol run.

In this paper, online update mechanisms for shared secrets are analysed. This analysis reveals a new form of attack against security protocols employing update mechanisms. As these new attacks aim to desynchronise the communicating parties on their stored shared secret, we term them desynchronisation attacks. A successful desynchronisation attack disables the affected parties from authenticating each other in future protocol runs. Thus, by mounting a desynchronisation attack, the intruder can cause a permanent DoS condition. As an example, a case study is performed on a protocol for mobile satellite communications that aims at providing mutual authentication between a mobile user and the Network Control Centre (NCC). This case study reveals two desynchronisation attacks that exploit the weaknesses in the update mechanism employed by the protocol. Subsequently, the targeted users are denied access to the communication service and a permanent denial of service condition is reached that persists even after the jamming ends.

To counter the disruptive effects of desynchronisation attacks, a new mutual authentication protocol with resynchronisation capability is proposed that confirms synchrony of the stored shared secrets. If desynchronisation is detected a resynchronisation phase is initiated that re-establishes synchrony between the communicating parties. Thus, the possibility of affecting the security at application layer by interfering with the communication on physical channels is eliminated. A security analysis of the proposed protocol establishes its resistance against attacks such as replay attacks, dictionary attacks and desynchronisation attacks.

**ONLINE UPDATE MECHANISMS OF SHARED SECRETS**

Providing mutual authentication based on shared secrets is a common feature in security protocols (Bargh et al., 2004), where the communicating parties involved prove their identity by showing possession of the shared secrets. To avoid freshness issues, such as compromise of long-term session keys, replay attacks etc., security protocols use dynamic shared secrets, where the secrets are renewed in an online update mechanism.

Online update mechanisms have two goals: Firstly, the generation of new instance of the
An Efficient Intrusion Alerts Miner for Forensics Readiness in High Speed Networks
www.igi-global.com/article/an-efficient-intrusion-alerts-miner-for-forensics-readiness-in-high-speed-networks/111286?camid=4v1a

Securing Multiple Biometric Data Using SVD and Curvelet-Based Watermarking
www.igi-global.com/article/securing-multiple-biometric-data-using-svd-and-curvelet-based-watermarking/216848?camid=4v1a