“FAST & AUTOMATIC VERIFICATION OF AUTHENTICATION & KEY EXCHANGE PROTOCOL “

Naresh Chetwani, Javed A khan

Dean CSE/IT**,** Takshshila Institute Of Engineering & Technology, Jabalpur
Email: NareshChetwani@takshshila.org

Abstract

In this paper we introduce the automatic verification of authentication & key exchange protocol its name suggest/show the paper summery now It is preferable for authentication and key exchange protocols to be verified automatically and rapidly in accordance with security requirements. In order to meet these requirements, we proposed the automatic security verification method for the protocols based on Bellaire et al.'s model and showed the verification points of security properties to verify their security efficiently. We show the novel verification points for each security property in the authentication and key exchange protocols in accordance with the aforementioned revisions. In addition, we describe the relations among the six verification points, explain how the proposed method verifies the aforementioned protocols by providing one example and show the validity of the proposed method by verifying the security challenges .

Keyword: Protocol , verification ,authentication , key exchanging startges . Security Verification Method,

Introduction

Authentication is the process[1] of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten

Authentication is one of the core security properties that many cryptographic protocols aim to provide: one party wishes to be convinced of the identity of another party. But in many contexts, the opposite property, anonymity is equally important: one party wishes for no one to be able to determine her identity.1 Anonymity is an enabling technology for privacy, whether for normal citizens going about their day-to-day lives or for dissidents and whistleblowers putting themselves in danger because of the information they transmit.[2]

Literature survey

In this paper I introduce the fast and automatic verification of authentication &key Exchange protocol for this I am read some the latest research paper its
conclusition include in this literature survey [3] this paper proposed the The IKE also
provides mutual authentication by authenticating both of the parties to each other; Both of the parties need to provide a digital signature in the key exchange protocol that the other party will verify. A successful verification means that the other party is authenticated. In order to be able to verify the signature also the public key (certificate) needs to be trusted, and verified. If certificates are not available, this IKE paper used the concept of modes which define how the actual key exchange procedure is to be done. Two of the most common modes are Main Mode and Aggressive Mode. There are also other modes like Base Mode and New Group Mode, but they are seldom used, and vendors usually does not support them at all. The difference of Main Mode (MM) and Aggressive Mode (AM) is in length of the procedure. Second paper is for password authentication key [4] .
A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide

authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DHEKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Other paper is[5] The Extensible Authentication

Protocol (EAP) describes a framework that allows the use of multiple authentication mechanisms. This document defines an authentication mechanism for EAP called EAP-EKE, based on the Encrypted Key Exchange (EKE) protocol. This method provides mutual authentication through the use of a short, easy to remember password. Compared with other common authentication methods, EAP-EKE is not susceptible to dictionary attacks. Neither does it require the availability of public-key certificates.

[6] according this paper research literature a typical protocol in the public-key setting aims for key secrecy and mutual authentication. However, there are many important practical scenarios where mutual authentication is undesirable, such as in anonymity networks like Tor, or is di_cult to achieve due to insu_cient public-key infrastructure at the user level, as is the case on the Internet today. In this work author are concerned with the scenario where two parties establish a private shared session key, but only one party authenticates to the other; in fact, the unauthenticated party may wish to have strong anonymity guar- antees. In this paper author present a desirable set of security, authentication, and anonymity goals for this setting and develop a model which captures these properties. Our approach allows for clients to choose among di_erent levels of authentication. We also describe an attack on a previous protocol of _verlier and Syverson, and present a new, e_cient key exchange protocol that provides one-way authentication and anonymity. Authenticated key agreement. Key agreement is an important cryptographic primitive that has been extensively studied, especially in the two-party authen- ticated setting [7,8,9,10 11] However, only a few protocols have considered the problem of one-way authentication. Goldberg [12] gave a specialized one-way AKE security de_nition for the Tor authentication protocol. _verlier and Syverson proposed some alternative protocols for circuit establishment in Tor but without any security arguments. We analyze one of their protocols in Section 3 and demonstrate it does not prevent server impersonation. Kate et al. [13] describe an identity-based anonymous authenticated key exchange protocol but with a limited session key secrecy de_nition based on key recov- ery, not indistinguishability. Morrissey, Smart, and Warinschi [14] analyzed Other key exchange protocols [15] aim to give anonymity, in which even the peer does not learn the long-term identity of the party. This is an important goal for practical

applications such as the Tor anonymity network [15]. Most of the references above do not analyze the anonymity prop- erties of their protocols in a formal manner, although a few do. Shoup [34] de- _nes anonymity in the context of the simulation framework for key exchange security, as opposed to the indistinguishability framework of, for example, Canetti-Krawczyk , which has now become more commonplace for analyz- ing key agreement protocols. Kate et al.authenticated key exchange protocol with formal anonymity goals, although their de_nition is specialized for the protocol in question. In this paper, we present a generic anonymity de_nition, suitable for analyzing a wide variety of protocols, in a framework similar to the key exchange security framework of Canetti-Krawczyk Some protocols] provide deniability, where it cannot be conclusively proven that a party participated in a key exchange session. This di_ers from anonymity in that a deniable protocol may still leak information about the parties involved in its normal operation Two different types of methods have been proposed as ways of verifying the security of authentication and key exchange protocols: those based on a computational complexity approach and those based on formal verification. As one example based on the computational complexity approach, Bellare, Pointcheval and Rogaway introduced the first in distinguish ability-based formal model of security for authentication and key exchange protocols .

Problem definition - For a considerable period, existing authentication and key exchange protocols were designed by trial and error, based on the designer's understanding of security and cryptographic techniques. Therefore, it is vital to be able to deal with compromised protocols quickly. However, the process of specialists designing authentication and key exchange protocols is a time-consuming one. Furthermore, designing a new protocol or modifying an existing protocol and then verifying its security are a lengthy process. As a result, there were neither the methods to evaluate the authentication and key exchange protocols formally nor the mechanisms to deal with compromised protocols quickly.

Proposed solution

We make special note of the di_erence between one-way AKE and one-ow AKE. One-ow AKE protocols are designed to establish a session key using a single message from the client to the server. It can provide mutual authentication by using two static keys (one each from the client and the server) and one ephemeral key (from the client). In contrast, one-way AKE can use one static key (from the server) and two ephemeral keys (one each from the client and the server), but provides no authentication to the server. Although one can try to view a one-way AKE protocol as the complement of a one-ow AKE protocol, switching ephemeral and static keys, the security properties are substantially di_erent. Key con_rmation is an integral part of many authenticated key exchange pro- tocols. The TLS protocol [16], for exa]mple, uses Finished messages in both directions, which are computed as a MAC, under the master secret key, of the text \client _nished" or \server _nished" and the _ngerprint of the transcript. Key con_rmation enhances the security properties of the basic schemes. NIST SP800-56A [17] states: Key agreement, accompanied by key con_rmation can be used to provide the recipient with assurance of either the provider's current or prior possession of the static private key that is associated with a particular static public key. Moreover, in SP800-56A key con_rmation is associated with the use of a static key pair: a party provides a key con_rmation message only if that party contributed a static key pair in the key agreement protocol. In the previous section we gave examples where parties not authenticating their peers do not alter their behaviour based on the presence of encryption. From the point of view that key con_rmation enhances session-key secrecy

PDF to Word