Identification Protocols

C

Sattar J. Aboud
Department of Computer Science and Technology, University of Bedfordshire, UK

INTRODUCTION

The identification protocol is the scheme that checks an identity of the user that sent the message on open channel. The trusted authority validates an identity of a user that aims to send messages, or generates a new identity and certifies a user has a denoted identity. The only aim of an identification protocol is to check that a trusted authority is satisfied of an identity of that user. The identification protocol should convince a requirement that no hacker can impersonate the user assigned identity. In this regards this simple password is not acceptable since a hacker can eavesdrop and steal a password (Meier et al., 2013). The authorized receiver can become a hacker and use a password. To prevent this, identification code should be calculated from the private identity key that is not exposed. The user then creates its identity by proving the identity key. It should be computationally difficult to extract an identity key from an identification code. In result, an identity key plays a role of a password that is kept secret by the user and is never sent or exposed.

The identification protocol checks an identity of a user, called the claimant, by checking a user have possession the private key or password that only the user know. The claimant identifies itself to a verifier by proving it knows a private key without revealing it. The zero-knowledge protocol is one that a clamant proves it have a private key without revealing other information to a verifier or to the trusted authority intercepting the messages.

The identification scheme is secure if it is not disclose any information that subsequently allows another participant to falsely identify itself as a holder of an identity private. The identification scheme is sound if information of a private is enough for identification (Nikande et al., 2010). The community should bind a possession of a private to the general consensus regarding an identity of that user. This needs an existence of the trusted certification authority authenticated by a community. The trusted certification authority publicly published statement connecting an identity of a holder of a private. The identification protocol is carried out on the open channel, but must not disclose any information that will allow the following impersonation by a hacker that has intercepted a message. The identification protocol use time-variant parameters to build every example of its use unique. This is to stop replay attacks and interleaving attacks, to prevent some selected attacks and to guarantee uniqueness.

The identification scheme executes its job using the so-called challenge-response sequence. This sequence starts with the claim message from a claimant to a verifier, where a clamant needs verification. The verifier then responds with a challenge message to a claimant. The claimant posts the response message to a verifier and a verifier verifies for consistency of a claim message. If a claimant is a device, then a procedure checks an identity of a device not a user of a device. There still remains a possibility that a rightful possessor of a device is not the one using it. Therefore, a possessor of the device must participate in an identification protocol (Polikarpova et al., 2012).

The identification protocol should not vulnerable to the man-in-the-middle attack. The man in the middle is a hidden relay that intercepts, understands, alters and retransmits a message of the purpose of deception. The goal of the man in the middle is to steal an identity of the claimant by deceiving the protocol rather by breaking the scheme.

BACKGROUND

We will concentrate on simple cryptography identification protocol, by which the productive claimant wants to know certain private key. There are many cryptography buildings of identification protocol. The typical objective is to reduce a computational effort for a claimant and a verifier. The security choices from a

DOI: 10.4018/978-1-4666-5888-2.ch136

weak for password-typed protocols to a robust for zero knowledge protocol. We observe that the difficulty adopted by identification protocol is connected to message authentication, digital signature and an authenticated key exchange. Compared with message authentication, the major difference is that there is certain idea of novelty to be satisfied. Whereas, compared with digital signature, there is nothing like undeniable, it is not needed that a verifier is able to satisfy the outsider at the later use; eventually the claimant certainly must identified it to a verifier. However, it is not must that a claimant obtains the defense from involving in the identification protocol. Compared with authenticated key exchange, a difficulty is easier because there is no condition for creating the secure session key.

Each identification scheme includes mainly two protocols, registration and identification protocols, between two participants so-called a claimant and a verifier. In public key cryptography identification scheme registration will finish with both participants sharing the public key pair, by which just a claimant knows a secret key. The main gain of public key cryptography scheme is that a claimant can utilize its public key with many verifiers (Blahut, 2014). We will study the attacks on an identification protocols only in this article. Thus, we suppose that a registration protocol is done in the secure setting. Also, we will study cryptography attacks only. The essential security need for the identification protocol is that it prevents impersonation attacks; it must be difficult for a hacker to positively classify it as another participant. We distinguish some passive and active impersonation attacks. The main form of passive impersonation attack is spying on communication between the claimant and the verifier in authorized implementations of an identification protocol. Another form of passive attack is a key-only attack for asymmetric scheme, by which a hacker attempts to compute a private key from a public key. But, we will not be concerned with key-only attacks. The easy type of active impersonation attack is the guessing attack, by which a hacker impersonates as a claimant and dreams to reach a right guesses, without knowing a claimant private key. The success percentage of the guessing attack can be improved greatly by combining it with the fraud verifier attack.

Finally, a hacker might act as the man-in-the-middle attack, when the claimant P implements an identification protocol with verifier V^* the verifier posts all messages to the verifier V who trusts it, since implements a protocol with P. The man-in-the-middle attack is evocative with a master chess attack, by which the chess player attempts to increase its rating by playing communication chess with two masters at the same time. The chess player will involve in the chess game with both masters, playing white in one game and black in the other one. Once began, the chess player easily copies all moves from one master to the other. Therefore, the chess player will win one game and lose other game. In any event, a chess player rating will increase greatly. We will concern mostly on cheating verifier attacks.

MAIN FOCUS OF THE ARTICLE

In this section, we are going to describe the traditional methods, the solution protocols, then the discussions and finally the conclusions and remarks.

Traditional Methods

In this section, we describe the related methods which are as follows.

Password-Typed Scheme

The traditional method to login to the computer is to supply the user-id and the password. Upon registration it is confirmed that a claimant obtains the unique user-id. A claimant is also permitted to choice the password. Through identification, a claimant posts a user-id and password to a verifier. The password scheme is asymmetric identification scheme, assumed to resist guessing attacks. One might consider of a password as the arbitrary bit string in $(0,1)^k$. When a password is human-memorable, a security parameter k is typically small $k \leq 20$. We will not consider dictionary attacks. Obviously, it is potential to resist guessing attacks by choosing $k = 80$, but then a password will be difficult to memorize. The password scheme is not resist eavesdropping attacks. Once a scheme is intercepted, a password is broken.

The fairly simple method to prevent eavesdropping attacks is to utilize a hash chains. The hash chain of size ℓ is the sequence of integers $x_i, 0 \leq i \leq \ell$, con-