An Internet Key Exchange Protocol Based on Public Key Infrastructure

ZHU Jian-min(朱健明)\(^1\), MA Jian-fen(马建峰)\(^1\)
1. School of Computer, Xidian University, Xi'an 710071, P.R. China
2. State Key Laboratory for Information Security, Chinese Academy of Sciences, Beijing 100039, P.R. China

Abstract Internet key exchange (IKE) is an automated key exchange mechanism that is used to facilitate the transfer of IPSec security associations (SAs). Public key infrastructure (PKI) is considered as a key element for providing security to new distributed communication networks and services. In this paper, we concentrate on the properties of the protocol of Phase 1 IKE. After investigating IKE protocol and PKI technology, we combine IKE protocol and PKI and present an implementation scheme of the IKE based on PKI. Then, we give a logic analysis of the proposed protocol with the BAN-logic and discuss the security of the protocol. The result indicates that the protocol is correct and satisfies the security requirements of Internet key exchange.

Key words authentication, encryption, Internet key exchange (IKE), public key infrastructure (PKI).

1 Introduction

With the development of Internet, the security of IP has become increasingly important. As one of the most important technologies of IPSec, Internet key exchange (IKE) has received significant interests from the research community\(^{[1,4]}\). A protocol that allows two parties to agree on a shared secret key is commonly known as a key exchange protocol. IKE is the default automated key management protocol selected for using with Internet protocol security protocol (IPSec). The IKE protocol is the answer from the IPSec group to protocol negotiation and key exchange through the Internet. It provides a way to agree on which protocols, algorithms and keys to be used. Secondly, it provides a way to ensure from the beginning of exchange that you are talking to whom you think you are talking to.

The IKE protocol\(^{[3]}\) can be thought of as a combination of two protocols, Internet Security Association and Key Management Protocol (ISAKMP)\(^{[6]}\) and Oakley. ISAKMP specifies only a framework for key management protocols but does not prescribe any particular authentication mechanism. Oakley is a suit of key agreement protocols in which two parties generate a key jointly. The IKE document describes how Oakley can be used to provide an instantiation.

The IKE protocol has two phases: in the first phase a secure channel between the two key management daemons can be established, while in the second IPSec SAs can be directly negotiated. In the first phase, two entities use master keys to agree, not only on keying material, but also on the various mechanisms (e.g. cryptographic algorithms, hash functions, etc.), which will be used in the second phase. The keying material and set of mechanisms thus agreed upon is called phase I security association (Phase I SA). Using this information, the peers authenticate each other and compute key material to be used for protecting Phase II.

The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange. They all use Diffie-Hellman key agreement technique (DH) to generate shared secrets. RFC 2409\(^{[3]}\) defines four different authentication methods for Phase I protocols: preshared key, public key signature, public key encryption, and revised public key encryption. Which method to be used is determined by the parameter negotiation.

The phase II is commonly called "quick mode" and results in an IPSec SA tuple. As quick mode is protected by Phase I ISA, it does not need to provide its
own authentication protection, allowing a fast negotiation.

Using public keys for authentication, the Phase I exchange can be accomplished either by using signatures or by using public key encryption. Public key cryptography is suitable for distributed and dynamic environments with a medium or big number of communicating parties sending data through insecure channels. In this article, we focus on the authentication and key generation mechanisms of IKE using public key, then we propose an authentication method based on public key infrastructure (PKI).

In this paper, we assume that we have a network in which the nodes inherently distrust each other, and in which a global or centralized PKI or KDC (key distribution center) is available. In our network, both parties (initiator and responder) possess X.509 public key certificates issued by hierarchies of certification authorities (CAs). We make use of the advantages of PKI and propose the Phase I protocols of IKE based on PKI.

The remainder of this paper is organized as follows. Section 2 gives an introduction to IKE. This shows basic design principles of the Phase I protocols of IKE. Section 3 proposes our IKE protocols based on PKI. In Sections 4, we prove correctness of our protocol using BAN-type logical and discuss the security of the proposed protocol. Finally, conclusions are presented in Section 5.

2 The Rationales of IKE Protocol

IKE is a complex protocol, and a detailed description of it is outside the scope of this paper. We only introduce it with enough details to put the description of our design and implementation in context and interested readers should refer to RFC 2409[3] for details.

There are two basic methods used to establish an authenticated key exchange: main mode and aggressive mode. Main mode is an instantiation of the ISAKMP identity protect exchange. In main mode there are three pairs of messages. The first negotiates policy; the second consists of a Diffie-Hellman exchange; in the third pair, messages is encrypted with the Diffie-Hellman value agreed upon in the second pair of messages and each side reveals its identity and proves that it knows the relevant secret (for example, private key or pre-shared secret key). The authentication method negotiated as part of the initial ISAKMP exchange influences the composition of the payloads but not their purpose. Similarly, aggressive mode is an instantiation of the ISAKMP aggressive exchange. In aggressive mode there are only three messages. The first two messages consist of a Diffie-Hellman exchange to establish a session key, and in the second and third messages each side proves they know both the Diffie-Hellman value and their secret. The price paid for fewer messages is that identities generally cannot be encrypted and the room for negotiation is constrained.

Fig. 1 shows the basic mode in Phase I with ISAKMP security associations, nonces and authentication. The four different authentication methods for Phase I protocols in RFC 2409 can do different authentication as this mode.

Fig. 1 Phase 1 with ISAKMP security associations, nonces and authentication

Messages (1) and (2) carry out the parameter negotiation. In message (1), the Initiator generates a random number, cookie-I (CI), such that < Responder, CI > is unique with respect to the Initiator, and sends the CI in the first message to the responder. Usually, CI is generated from some local secret, some unique information about the Responder (e. g., IP address), and possibly other local state information. The [SA]_prop includes a list of proposals to the responder that the Initiator sends, for example encrypt arithmetic (e. g., DES, 3DES) and authentication arithmetic (e. g., MD5, SHA-1). In message (2), the Responder generates a request for confirmation, < C1, C_R >, and sends the request to the supposed Initiator. The C_R is a random number generated from