Petri net Based Model of Internet Key Exchange Protocol
Harshwardhan Mittal & Abhishek Sharma

Abstract
In this paper we present the process language based model of the Internet Key Exchange (IKE) Protocol which is represented by the Petri nets. This protocol is used to create and maintain Internet Protocol Security (IPSec) associations and secure tunnels in the IP layer. Secure tunnels are used to construct virtual private networks (VPNs) over the Internet. The denotation of the process is a set of events and each event specifies a set of preconditions and postconditions, this denotation is best represented by a Petri net. The Petrinet based model leads to reduction of the complexity associated with the implementations of IKE. The proposed model helps in the validation of the security properties of the IKE. The model is graphical which facilitates better visualization of the protocol. We have modeled the IKE Phase-1 Main and Aggressive modes for preshared key, public key signature, public key encryption, and revised public key encryption and various security features like identity protection and perfect forward secrecy has been validated.

Key words – IKE, Petrinets, Modeling, Formal Methods, Validation

INTRODUCTION
IKE[1] is the primary protocol to generate and maintain IPSec[2] security associations, which are the basic building blocks of virtual private networks (VPNs) over the Internet. IKE uses cryptography[3] extensively. This is a complex protocol and complexity is the worst enemy of security. The formal specifications of this protocol are rather abstruse Schneier, Radia Perlman et al.[4,5], which leads to the need of formal analysis of this protocol in order to validate the various security properties. Like all other security protocols IKE is also concerned with exchanging messages between agents via an untrusted medium i.e. the Internet. IKE guarantees an extensive number of security features such as authentication of interacting parties, anonymity etc as required by the ISAKMP framework[6]. The IKE protocols accomplishes its work in two phases ( Phase I and Phase II ). Phase I consists of Main and Aggressive modes while Phase II has Quick mode. There is one supplementary mode also called New Group mode. The IKE standard 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 use is determined by the parameter negotiation.

The message exchange sequence for IKE phase I main mode preshared key authentication is as shown below:

A --- B  C_a,SA  C_a,C_b are the Cookies.
B --- A  (C_a, C_b), SA’  N_a,N_b are the Nonces.
A --- B  (C_a, C_b, N_a, G_a)  G_a’, G_b’ Diffie Hellman key’s public part.
B --- A  (C_a, C_b, N_b, G_b’)  ID_a, ID_b are Identities.
A --- B  (ID_a, HASH_a) key(a,b)  HASH_a , HASH_b are the authenticating codes.
B --- A  (ID_b, HASH_b) key(a,b)  Key(a,b) is the encryption key derived from preshared key and Diffie Hellman keys.

The first two messages are used for negotiating the security policy for the exchange and also use Anti clogging token for prevention of Denial of service attack. The next two messages are used for the Diffie–Hellman keying material exchange. The last two messages are used for authenticating the peers with hashes. Last two authentication messages are encrypted with the previously negotiated key.
The process language on which our model is based is inspired by Crazzolara & Winskel[7] and Paulson[8,9]. In our approach we follow the assumptions of the Dolev–Yao model [10]. To summarise, this whole semantics describes a process by its set of events giving rise to a Petri net and supports the local reasoning that appears to be useful in analysing cryptographic protocols like IKE.

### Proposed Model

**Init(A,B)**

- `Out{ (IP_b)^0(a), C_a, G^x(a), x }`
- `In X`
- `[X>C_a, SA']`
- `New x`
- `Out { (IP_b)^0(a), C_b, G^x(a), x }`
- `In X'
- `[(X')^0(a)] > (IP_b)^0(a), (C_a, G^x(b), y)`
- `Out { (G^{(a,b)}[C_a]C_b|SA|ID_a)^{1} (a,b), ID_a }`
- `In X''`
- `{ (X'')^{k(a,b)} > (G^{(a,b)}[C_a]C_b|SA|ID_a)^{1} (a,b), ID_a ) }`

**Resp(A,B)**

- `In X`
- `[X>C_a, SA']`
- `Out{ (IP_a)^0(b), ID_b, (G^{(a,b)}[C_a]C_b|SA|ID_b)^{1} (a,b), ID_b, k_4(a,b) }`
- `In X'
- `[X' >C_a, (IP_a)^0(b), (G^{(a,b)}(y)]`
- `New x`
- `Out { C_a,(IP_a)^0(b),G^{(b)}, x }`
- `In X''`
- `{ (X'')^{k(a,b)} < (G^{(a,b)}[C_a]C_b|SA|ID_a)^{1} (a,b), ID_a ) }`
- `Out { (G^{(a,b)}[C_a]C_b|SA|ID_b)^{1} (a,b), ID_b, k_4(a,b) }`

**Spy**

- `Spy1= In X.In X'.Out(X,X').nil (composing).`
- `Spy2= In(X,X').Out X.Out X'.nil (decomposing)`
- `Spy3= BAB K.nil (leaked keys)`
- `Spy= \{ i \in \{1..3\} \} Spy_i`

The keys are defined as follows:

- `k_{(a,b)}` is the preshared key between A and B.
- `k^0(a), k^0(b)` are the local secrets of A and B used for driving cookies.
- `k^{1}(a,b)=Na*Nb^{i}k_{(a,b)}` is the key for calculating hashes.
- `k^{2}_{(a,b)} = (G^{x}_{ab}|C_a[C_b][0])^{1}(a,b),` is the session key used to drive other keys.
- `k^{3}_{(a,b)} = (k^{2}_{(a,b)}|G^{x}_{ab}|C_a[C_b][1])^{1}(a,b),` is the authentication key.
- `k^{4}_{(a,b)} = (k^{3}_{(a,b)}|G^{x}_{ab}|C_a[C_b][2])^{1}(a,b),` is the encryption key.

All the functions except (M)^i which is used for keyed hash are taken from [7]. The superscripts like k^i are used for names related to same process. And the subscripts like C_a,C_b are taken for denoting the entities associated.

**Conclusion:**

We have developed a formal Petri net based model of Internet Key Exchange Protocol and analysed various security properties of it. We have modeled all the phases of IKE and model of Phase I main mode with preshared key has been presented to illustrate this approach. This model helps in better visualization and validation of the IKE thus reducing the complexity associated with its implementations.
Init(A,B)

...
The figure shows Initiator’s Petri–net based graphical model, the similar type of models are also drawn for Responder and Spies for the various modes of IKE.

REFERENCES

1. D. Harkins, D. Carrel "The Internet Key Exchange (IKE) " *RFC 2409* November 1998
7. Federico Crazzolara and Glynn Winskel" *Petri nets in cryptographic protocols*” 0–7695–0990–8/01/$10.00 (C) 2001 IEEE

Author’s Affiliation

**Harshwardhan Mittal** is with the Department of Computer Engineering Institute of Technology Banaras Hindu University Varanasi–221005 INDIA(91)

**Abhishek Sharma** is with the Department of Electronics & Communication Engineering Institute of Technology Banaras Hindu University Varanasi–221005 INDIA(91)