Examining the DoS Resistance of HIP

Suratose Tritilanunt, Colin Boyd,
Ernest Foo, and Juan Manuel González Nieto

Information Security Institute
Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia
s.tritilanunt@student.qut.edu.au,
{c.boyd, e.foo, j.gonzaleznieto}@qut.edu.au

Abstract. We examine DoS resistance of the Host Identity Protocol (HIP) and discuss a technique to deny legitimate services. To demonstrate the experiment, we implement a formal model of HIP based on Timed Petri Nets and use a simulation approach provided in CPN Tools to achieve a formal analysis. By integrating adjustable puzzle difficulty, HIP can mitigate the effect of DoS attacks. However, the inability to protect against coordinated adversaries on a hash-based puzzle causes the responder to be susceptible to DoS attacks at the identity verification phase. As a result, we propose an enhanced approach by employing a time-lock puzzle instead of a hash-based scheme. Once the time-lock puzzle is adopted, the effect of coordinated attacks will be removed and the throughput from legitimate users will return to the desirable level.

1 Introduction

Many key exchange protocols have been developed for dealing with denial-of-service (DoS) attacks, especially resource exhaustion attacks. Host Identity Protocol (HIP) [14] is an interesting example of a DoS-resistant protocol which has been developed to deal with this kind of DoS attack. The concept behind this implementation is that HIP does not commit the responder's resource before the responder ensures the identity of the initiator. HIP achieves this concept by adopting stateless connection [3] and reachability testing by using a *client puzzle* [4, 12] incorporated via a cookie [16] to protect the responder from SYN flooding attacks [7] at the beginning phase. Moreover, the responder can authenticate the initiator by starting with the cheap computation using a client puzzle and then increase the level of authentication to the expensive computation using a digital signature for ensuring the identity of the initiator.

HIP is a promising key exchange protocol which includes DoS-resistant mechanisms for protecting the responder. However, lack of formal analysis in the design phase of HIP might introduce other kinds of vulnerability. Moreover, the instruction on how to adjust the client puzzle difficulty is not clearly specified and examined in the HIP specification [14]. In this paper, we implement a formal model of HIP using the formal specification language of Timed Petri Nets.

R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops 2006, LNCS 4277, pp. 616–625, 2006.

In order to achieve a formal analysis, we use a simulation technique provided in CPN Tools for analysing HIP model. The purpose of the simulation in the cryptographic protocol is to identify vulnerabilities in the system that might be difficult to explore in the design phase.

Simulation approaches are well-known not only for exploring vulnerabilities in cryptographic protocols, but guaranteeing security services of such protocols as well. Using simulation approaches has several benefits over mathematical analysis. For instance, they can provide *flexibility* and *visualization* during protocol analysis and verification. In our experiment, we set up the simulation of HIP for exploring unbalanced computational steps that cause a responder to spend more computations than an initiator does. In addition, our experimental result provides a measurement of successful legitimate traffic as proposed by Beal and Shepard [6] in different situations under DoS attacks. This factor can be used as a parameter for justifying the effectiveness of HIP to resist DoS attacks. In order to set up an experiment, we allow four kinds of adversary and the honest client to participate with the same responder during the protocol run. We set up two experiments; 1) the responder can choose only a fixed value of a puzzle difficulty no matter what the workload is, and 2) the responder has an ability to flexibly adjust puzzle difficulty by using the workload condition as criterion.

The main contributions of this paper are:

1. A simulation and analysis of HIP in Timed Coloured Petri Nets.
2. Identification of four scenarios of resource exhaustion attack on HIP.
3. A proposed technique to deal with adversaries who try to overwhelm the responder's resource by computing a puzzle solution in parallel.

1.1 Host Identity Protocol (HIP)

HIP has been developed by Moskowitz [14]. Later, Aura et al. [2] found some vulnerabilities and proposed guidelines to strengthen its security. HIP is a four-packet exchange protocol which allows the initiator I and responder R to establish an authenticated communication. Both I and R hold long-term keys to generate signatures $Sig_I(\cdot)$ and $Sig_R(\cdot)$ respectively. It is assumed that both principals know the public key PK_I of the initiator and PK_R of the responder represented in the form of host identifiers (HI) in advance. HIT represents the host identity tag created by taking a cryptographic hash H over a host identifier.

H_{K_s} represents a keyed hash function using session key K_s to generate a hashed-MAC ($HMAC$). The value s is a periodically changing secret only known to the responder. LSB takes as input a string t and a parameter k and returns the k least significant bits of t. 0^k is a string consisting of k zero bits. $E_{K_e}(\cdot)$ and $D_{K_e}(\cdot)$ denotes a symmetric encryption and decryption respectively under session key K_e. In order to generate session keys K_e and K_s, HIP employs Diffie-Hellman key agreement. Diffie-Hellman parameters used to generate these keys consist of large prime numbers p and q, a generator g, a responder's secret value r, and an initiator's secret value i.

HIP adopts a proof-of-work scheme [11] for countering resource exhaustion attacks. In a proof-of-work, HIP extends the concept of a *client puzzle* [4, 12]