A Novel Key Management Scheme for Next Generation Internet: An Attack Resistant and Scalable Approach

Vinod Vijaykumar Kimbahune, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India
Arvind V. Deshpande, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India
Parikshit N. Mahalle, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT

The computational complexity of the next generation internet (NGI) is increasing at a faster rate. Due to the large scale of ubiquitous devices, effective and secure communication and addressing mechanism is vulnerable to several threats. Apart from resource constraints of the devices, the unknown topology of the network and the higher risk of device capture make the key management a more challenging task in NGI. In this context, a novel attack resistant and salable key management scheme must be in place to enable end-to-end secure communication. In the first part of the article, is a detailed analysis of various threats along with behavioral modeling of attack. Further, this article presents comprehensive literature survey and the gap analysis. The proposed key management scheme has been evaluated in two scenarios viz. centralized and decentralized and its formal security analysis also proves that it is safe from replay attack. The proposed key management scheme has been evaluated with a performance metric like delay and the results shows that it is salable in nature.

KEYWORDS

Key Management, Next Generation Internet, Replay Attacks, Threats

INTRODUCTION

Today’s Internet suffers from its own success. Fortunately, researchers believe that new technologies, protocols, and standards can be developed to meet tomorrow’s demands. These advances will start to put us on track to a Next Generation Internet (NGI) offering reliable, affordable, secure information delivery at rates thousands of times faster than today’s rate. Achieving this goal will require research and testing. It is appropriate that the research community is participating in this research activity to achieve all the vision of NGI technology. The emergence of the NGI is mainly oriented toward a series of serious challenges that cannot be solved through limited improvement under the current network architecture.

Figure 1 shows that many mobile devices located within radio range of each other. Few of them can be access points which provide connectivity to the other devices. This paper discusses two addressing schemes: IP addresses which have global acceptance, and MAC addresses used at the local level. These addresses are assigned to all the devices uniquely.

DOI: 10.4018/IJISMD.2018010105

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
In this scenario, a particular device advertises its information using Neighbor Advertisement message and can request information about its neighbors by a Neighbor Solicitation. In this example, we have to make sure that no two devices use the same addresses for avoiding the duplication of address. IP can be assigned manually or by using local authority.

Assume an attacking device has compromised a legitimate device of the local network. An attacker can either gain control of the relevant device to cause more chaos in the network or creates Denial-of-Service attacks (DoS). It can also try to combine these two attacks to organize and initiate flooding DoS attack. Enemy device redirects as many traffic flow as possible towards a given victim device, in such a way that the latter is overwhelmed.

In Figure 1 devices which are shown in dark colors are the Sybil devices. When these devices want to communicate to their neighboring device they use any one of the identities. When packets transfer at the time these multiple identities will respond as a result it will confuse and collapse the network.

There are several ways by which an attacker can initiate these attacks. An attacking device can spoof a Neighbor Advertisement message; it can cause packets to the legitimate device to be sent to some other link-layer address. Another attack possible is to interrupt Duplicate Address Detection protocol in which the attacking device responds to every Duplicate Address Detection message attempt made by an entering device so that the device is unable to obtain an address.

As mentioned above each device is assigned a unique address, to avoid ambiguity. An attacker can try to break address ownership and uniqueness by initiating a Sybil attack. (Zhang & Shen, 2014) Many networks, like a peer-to-peer network, rely on assumptions of identity, where each device represents one identity. A Sybil attack happens when an insecure device is hacked to claim multiple identities. An attacker with many identities can use them to act maliciously, by either stealing information or disrupting communication. In the case of wireless networks, Sybil attacks are a crucial concern, as the attacker can hack the device and initiate the replication attack.

Outstanding research has been done in the area of addressing to avoid such attacks. Cryptographically Generated Address (CGA) is a Public Key Cryptographic method. It is created by replacing the least-significant 64 bits of the 128-bit IPv6 address with the cryptographic hash of the public key (Kimbahune, Mahalle & Deshpade, 2017). Host identification protocol (HIP) is a public key cryptographic method. It is a host identification technology for use on Internet Protocol (IP). HIP separates the end user identifier and locator roles of IP addresses. IPv6 addresses are computed by the host identifier using cryptographic Hash Function. IPv6 addressing comes into existence because...
Channel Optimization for On Field Sales Force by Integration of Business Software on Mobile Platforms
www.igi-global.com/chapter/channel-optimization-field-sales-force/29523?camid=4v1a

Improving Novice Programmers' Skills through Playability and Pattern Discovery: A Descriptive Study of a Game Building Workshop
www.igi-global.com/chapter/improving-novice-programmers-skills-through-playability-and-pattern-discovery/117300?camid=4v1a