Chapter 17
Necessary Standard for Providing Privacy and Security in IPv6 Networks

Hosnieh Rafiee
University of Potsdam, Germany

Christoph Meinel
University of Potsdam, Germany

ABSTRACT

Security and privacy have become important issues when dealing with Internet Protocol version 6 (IPv6) networks. On one hand, anonymity, which is related to privacy, makes it hard for current security systems to differentiate between legitimate users and illegitimate users, especially when the users need to be authenticated by those systems whose services they require. On the other hand, a lack of privacy exposes legitimate users to abuse, which can result from the information gained from privacy-related attacks. The current problems inherent within IPv6-enabled networks are due, in part, to the fact that there is no standard available telling companies about the current deficiencies that exist within IPv6 networks. The purpose of this chapter is to show a balance between the use of privacy and security, and to describe a framework that can offer the minimum standard requirement needed for providing security and privacy to IPv6 networks.

INTRODUCTION

IPv6 (Deering & Hinden, 1998) is the successor version of Internet Protocol version 4 (IPv4). These protocols are what makes communication possible across the Internet. Without the use of an IP address, it would not be possible to access the information located on many distributed repositories in many different locations across the world.

When the Internet Engineering Task Force (IETF) first proposed IPv6, the main assumption was to have a highly secure protocol which could support Internet Protocol Security (IPsec) (Kent, & Seo,

DOI: 10.4018/978-1-5225-8897-9.ch017

2005) natively, thus solving any problems dealing with end-to-end communications. However, this assumption proved to be unsupported. Unfortunately many implementers, and vendors alike, have not supported or have not activated IPsec. One reason for this is because of the complexity that is involved in configuring IPsec and also the key management involved. This protocol thus remains with only the basic protection mechanisms in play so companies and governments are thus unwilling to widely deploy IPv6 or to replace their current IPv6 backbones with one making use of the IPsec protocol.

But the story does not end here. The development of a new address scheme for IPv6, which was necessitated by the IPv4 address space exhaustion, has led to new technology waves in which several volunteer experts and companies have become involved in looking for the flaws in IPv6. They are doing this in order to provide new security protocols to the users' of IPv6-enabled networks so that they can have the same security that exists when using IPv4, or maybe even higher.

The increased use of clouds and other repositories on the internet, in order to service and support many users at the same time, exposes this data to the vulnerabilities exploited by several types of privacy and security attacks. Today, we are living in an information technology world where governments and companies try to collect as much information as possible about their competitors. They do this so that they can overcome any possible threats from other governments or companies. Along with the risk of competitors, there are also individual/groups of attackers who are interested in obtaining the information available in those repositories so that they can misuse this information for their own criminal purposes. This is why, today, cyber attacks (attacks that are accomplished using cyber methods) are one of the main concerns of both societies and governments. Over the past 10 to 15 years multiple cyber attacks have occurred targeting both governmental agencies and private companies. The damage estimates are placed at more than $1 billion. Based on an official report from the United States Homeland Security Agency, in 2011 there were more than 106,000 incidents reported of which 5000 needed an urgent response.

Unfortunately, nobody knows yet, whether or not through the use of all security protocols, if IPv6 nodes will have the security level that is necessary to prevent several types of attacks or whether there are still many uncoverd flaws that might prevent the current services from being available to users or that can leak confidential information. What if there is a system that helps to show the current flaws in IPv6 networks and enables the user to do further tests to discover uncovered flaws in order to find a solution before these vulnerabilities can be used, like a tool in the hand of criminals? The remaining sections of this chapter are organized as follows:

Section 2: Introduce different meanings for privacy, anonymity and security in general and survey the current approaches in use in the application and network layers by explaining their issues and by introducing any available solutions.
Section 3: Explains some of the possible attacks in use across the internet.
Section 4: Surveys the currently available tools
Section 5: Introduces a system which can be used as a basic consultant system
Section 6: Explains the security recommendations for use in IPv6 networks and gives a basic security requirement.
Section 7: Summarizes this chapter.