Chapter 7
Securing Next Generation Internet Services

Asoke K. Talukder
ABV Indian Institute of Information Technology & Management, India & Geschickten Solutions, India

ABSTRACT

In Next Generation Internet (NGI), internet will graduate from being just a network of networks to network of interoperable services. Security in NGI must cover all 7 layers of the OSI model instead of just 3 bottom layers as in the past. This chapter discusses the security issues in NGI and proposes a methodology for security countermeasures in NGI.

1. INTRODUCTION

First Generation Internet was the data communication protocol for researchers – it was born on 1969 with RFC1 (Crocker S. 1969) which was entitled "Host Software" and dealt with Interface Message Processor (IMP) and Host-to-Host protocols. The IMP was the packet-switching node used to interconnect participant networks to the ARPANET from the late 1960s to 1989. IMP was the first generation of gateways, which are known today as routers. Some literatures state though – Internet was born on 1972 when Larry Roberts and Bob Kahn demonstrated the ARPANET at the International Conference on Computer Communication (ICCC) held in Washington, DC, in October 1972. This generation of Interne was used by the research community. These days, people in the industry were using their own proprietary protocols like System Network Architecture (SNA), DECnet etcetera. Second generation Internet was the generic data communication protocol; it can be timed at 1989 when inter-domain routing was included in the Internet with specifications like Open Shortest Path First (OSPF) protocol (RFC1131), the Border Gateway Protocol (BGP) (RFC1105), with IP Multicasting (RFC1112). These protocols helped quick acceptance of Internet – Australia, Germany, Israel, Italy, Japan, Mexico, Netherlands, New Zealand and the United Kingdom joined the Internet (Internet History 2010). The number of hosts increases from 80,000 in January

DOI: 10.4018/978-1-60960-123-2.ch007

1989 to over 160,000 in November of that year. Then was the emergence of Third Generation Internet with voice being integrated in Internet on 1995. This was through Voice over IP (VoIP) protocols – that made Internet the protocol for generic communication – be it data, voice, image, or multimedia.

By the turn of the century, the domain of Internet started expanding – it graduated from the protocol for communication to a media for services; emergence of Next Generation Internet (NGI) became apparent. In NGI, consumers became the innovators. We saw large software slowly fading out; task based thin services started emerging. Also, applications and services started moving from private data centers and servers to the internet. Services, platforms, infrastructures will be agnostic to each other. Like energy, consumers will not worry where the server is, how to access it – they will get the service as and when they need, on-demand, using any device – be it a desktop computer or a mobile phone. Users will access these solutions or services through simple user-agents on these devices. All these thin services will hide behind the cloud and interoperate to offer a rich set of services and rich user experience. NGI will offer subscription based services that will be dynamically scalable and mobile. As services in the NGI will move from private space (intranet) to a public space (Internet), NGI services will become more vulnerable to security attacks. Therefore, in the NGI security must cover all 7 layers – network security at Layer 1 to 3; Transport and Platform security at layer 4; and, Application security at layer 5 to 7. This chapter will discuss security issues in the Next Generation Internet – how they synergize.

2. NEXT GENERATION INTERNET (NGI)

The current internet – IPv4 has many problems; major ones are,

- **Addressing space:** the current address space of internet is 32 bits. With the growth of internet users this is not sufficient
- **Quality of Service:** it is a major challenge to guarantee quality of service
- **Mobility:** IP inherently does not include mobility by design
- **Security:** IP inherently does not include security by design

According to some researchers NGI is Internet2 (Internet2), according to some thinkers NGI is Internet 3.0 (Jain, 2009); according to many thinkers, IPv6 (Deering, 1998) is the NGI. However, in our analysis, NGI is combination of all of these and many more (Talukder & Prahalad, 2009c) features that can be listed as,

- **Multi-user-agent:** Smartphones and Computers (Portable & Desktops)
- **Multi-service:** Voice (telephony), TV (consumer entertainment), and multimedia (computer communication) over IP
- Multi-access (Wireless, & Wired Broadband)
- Multi-provider
- Multi-protocol networks
- Web 2.0 and Web 3.0
- Services deployed in Cloud-computing paradigm
- Services availability anywhere anytime through universal user-agents
- Trust (Opinion, Emotions, and Intent)
- IPv6 with IPsec
- Support seamless mobility at vehicular state
- Intelligent and programmable networks
- Definable service quality
- Definable security level
- On demand scalability
- API in the network to obtain context information (spatial, environmental, and temporal attributes)