Attack Analysis & Bio-Inspired Security Framework for IP Multimedia Subsystem

Aliya Awais, Muddassar Farooq, M Younus Javed
College of Electrical & Mechanical Engineering
National University of Sciences & Technology
Rawalpindi, Pakistan
aliya.awais@gmail.com, muddassar.farooq@udo.edu ,myjaved@ceme.edu.pk

ABSTRACT

This paper analyzes the security vulnerabilities and requirements of IP Multimedia Subsystem (IMS), particularly the impact of Denial-of-Service (DoS) and Distributed DoS(DDoS) attacks on the IMS. We propose and develop an intelligent Bio-inspired, self-defending security framework for the IMS and Next Generation all-IP Networks. Our proposed framework will complement the existing authentication and encryption mechanisms to protect infrastructure nodes and subscribers against the attacks launched by the malicious nodes in the network. This framework is expected to become a cardinal component which can be integrated into any IMS converged network infrastructure to provide defense against wide variety of attacks particularly DoS and DDoS attacks.

Categories and Subject Descriptors

C.2.2 [**Computer Systems Organization**]: Computer Communication Networks—*Network Protocols*[Applications]; C.2.0 [**Computer Systems Organization**]: Computer Communication Networks—*Security and protection*

General Terms

Experimentation, Security

Keywords

Artificial Immune Systems, IP Multimedia Subsystem, Network Security

1. INTRODUCTION

IMS can be defined as a global, access independent, standards based IP connectivity and service control architecture that enables various types of multimedia services to end-users, using common internet-based protocols [1]. IMS architecture makes it possible to establish peer-to-peer IP communications with all types of clients with the requisite quality of service. In addition to the session management, IMS architecture also addresses functionalities that are necessary for complete service delivery, for example, registration, security, billing, media control and roaming. IMS is still being defined and there are still many open issues within the IMS architecture. The 3GPP IMS standardization is ongoing, and yet there is no commercial deployment of IMS within the operators' networks [1].

GECCO'08, July 12–16, 2008, Atlanta, Georgia, USA.
ACM 978-1-60558-130-9/08/07.

2. IMS SECURITY REQUIREMENT

Most of the issues regarding the security for IMS, like authentication, encryption, confidentiality and reliability, are standardized by the 3GPP release 5 that provide security at the first level in IMS networks [2]. In this study, we show that attackers can penetrate into the network through security trap doors by breaking the first level of security to misuse network resources and services. IMS network is not only open for known IP-based vulnerabilities but also to a completely new set of IMS applications based vulnerabilities. In typical DoS and DDoS attacks on an IMS network, large number of random or control messages are simultaneously sent from a single or multiple malicious nodes to overwhelm network's resource.

Generally, malicious node(s) in DoS or DDoS attacks abuse or exploit vulnerabilities in the networking protocols. Relevant examples are ICMP SMURF attack, TCP-SYN flood, and UDP flood. SIP floods such as *register request floods* and *presence update floods* are also possible. These attacks can be easily launched using publicly available tools.

3. SECURITY FRAMEWORK FOR IMS

Now we propose our Bio-inspired, Artificial Immune System (AIS) based self-defending framework, AIS-IDP (Intrusion Detection & Prevention system) for IMS and Next Generation all-IP networks. Our goal is to design a generic security framework which is based on the principles of AIS. The proposed solution will be deployed at the Home Subscriber Server (HSS), IMS Core (Proxy/Interrogating/Serving Call State Control Functions (P/I/S-CSCF)), applications and media servers to monitor the network traffic in real-time. Figure 1 shows the framework for the proposed AIS-IDP.

Components of AIS-IDP A secure IMS framework must be able to counter the malicious attacks originated by the nodes within the network or being launched by the external network entities. The security module must be able to analyze both packet's header and payload in real-time and maintain service transparency and at the same time must not degrade the performance of the IMS network. We now briefly provide an overview of our proposed AIS-IDP and discuss its components. Figure 2 shows the functionality of our proposed system. AIS based solution needs to learn the normal behavior of a network host by analyzing the network traffic passing through it. During the learning phase, AIS-IDP collects "self-antigens", which define the *normal* state of the system. By the end of learning phase, a detector database is populated to be used in the protection phase. The detectors in the detector database only match to the

Table 1: Mapping of Attacks to IMS domains and streams

Attack name	*IMS Layer Mapping*	*IMS Component Affected*	*Information Stream*	*Attack Type OSI Layer Mapping*	*Protocol*
IMS Register Request Flood	Application, Session	I/S-CSCF,HSS	Control, Management	Application Layer	SIP
UDP Flood	Session	P-CSCF,I/S-CSCF	Control, Management	Transport Layer	UDP
TCP SYN Flood based DDoS attack	Session	P-CSCF,I/S-CSCF	Control, Management	Transport Layer	TCP
ICMP Flood	Session	P-CSCF,I/S-CSCF	Control, Management	Network Layer	ICMP

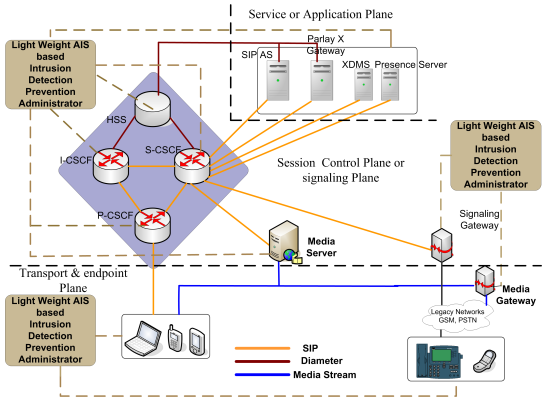

Figure 1: Framework of AIS-IDP

"non-self" antigens. Due to stringent complexity and memory constraints, the size of the detector database must be small. The small detector database size would also reduce the search time during the protection phase because we need to match the network traffic with the detector database during the protection phase. The size of the database is variable and is mostly of the order of a few kilobytes. The detector database is shown at the top of Figure 2.

1-Network Layer 3 learning/detection module: The IMS network must be able to thwart flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against IP, ICMP, IGMP protocols at the network layer of OSI reference model. If no anomaly is detected at this layer then the packet is handed over to the upper layer (i.e. Transport layer 4) for further processing (see Figure 2).

2-Transport Layer 4 learning/detection module: The IMS network must be able to prevent flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against the UDP and TCP protocols. TCP-SYN flood based DDoS attacks are launched in the session layer of the IMS layered architecture and are mapped to the transport-layer of the OSI reference model (see Table 1). The Transport layer AIS-IDP module detects these different types of attacks at the transport layer of the OSI reference model and accordingly secures different components of the IMS network. If the packet is not detected as anomalous at this layer, then the packet is handed over to the application layer for further processing (see Figure 2).

3-Application Layer learning/detection module: This module detects all such types of attacks including DoS/DDoS, sweep, scan, malformed packets, spoofing, and fragmentation attacks against SIP protocol by matching it with the detector database. If this filter also does not detect any anomaly, then the packet is allowed to propagate further to upper layer or respective application (see Figure 2).

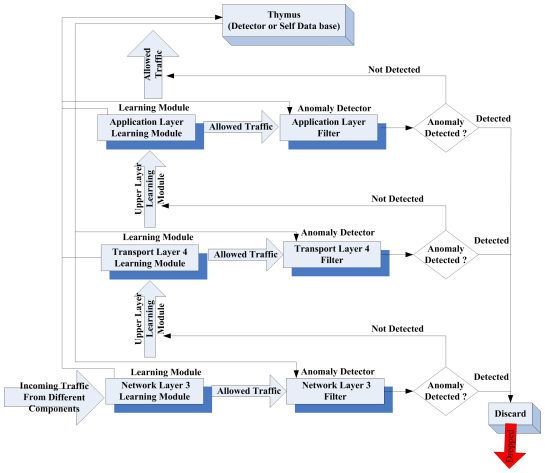

Figure 2: Packet processing in the protection phase of AIS-IDP

4. CLASSIFICATION TECHNIQUES FOR DOS AND DDOS ATTACK DETECTION

In this paper, we present the security framework for IMS and implement two security systems. The first system is a Bio-inspired Artificial Immune System (AIS) [3] and the second system is a signature based cryptology algorithm [4]. Our results show that AIS based solution provides good detection accuracy which low overheads. Although, crypto-based solution gives 100% detection rate but has high memory and computational overhead which makes it unsuitable for IMS users.

5. REFERENCES

[1] Poikeselka, Mayer, Khartabil, Niemi, "The IMS IP Multimedia Concepts and Services",Second Edition, 2006 Jhon Wiley & Sons, LTD.

[2] M.Sher, T.Magedanz, "Secure Service Provisioning Framework (SSPF) for IMS and Next Generation Mobile Networks",3rd IWWST, London, U.K., IWWST'05 Proceeding (101-106), April 2005.

[3] Steven A. Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation Journal, pp. 443-473, 2000.

[4] Juels and Brainard, "A Cryptographic Defense Against Connection Depletion Attacks", RSA Laboratories.