Computer Communications 31 (2008) 2443–2456

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Two layer Denial of Service prevention on SIP VoIP infrastructures

Sven Ehlert [a,*], Ge Zhang [a], Dimitris Geneiatakis [b], Georgios Kambourakis [b], Tasos Dagiuklas [c], Jiří Markl [d], Dorgham Sisalem [e]

[a] Fraunhofer Institute FOKUS, Next Generation Network Infrastructures, Kaiserin-Augusta-Allee 31, Berlin 10589, Germany
[b] University of the Aegean, Greece
[c] TEI of Mesolonghi, Greece
[d] Nextsoft, Prague, Czech Republic
[e] Tekelec, Berlin, Germany

ARTICLE INFO

Article history:
Received 11 April 2007
Received in revised form 10 March 2008
Accepted 10 March 2008
Available online 28 March 2008

Keywords:
VoIP
SIP
Denial of Service
Flooding protection
Security
Malformed messages
DNS cache

ABSTRACT

The emergence of Voice over IP (VoIP) has offered numerous advantages for end users and providers alike, but simultaneously has introduced security threats, vulnerabilities and attacks not previously encountered in networks with a closed architecture like the Public Switch Telephone Network (PSTN). In this paper we propose a two layer architecture to prevent Denial of Service attacks on VoIP systems based on the Session Initiation Protocol (SIP). The architecture is designed to handle different types of attacks, including request flooding, malformed message sending, and attacks on the underlying DNS system. The effectiveness of the prevention mechanisms have been tested both in the laboratory and on a real live VoIP provider network.

1. Introduction

Security threats are considered minimal in current circuit-switched networks as it is the case in the current Public Swithced Telephone Network (PSTN). This is achieved by using a closed networking environment dedicated to a single service (Voice). However, in an open environment such as the Internet, launching an attack on a telephony server is much simpler. This is due to the fact that Voice over IP (VoIP) services are based on standardized and open technologies (i.e., SIP, H.323, MEGACO) using servers reachable through the Internet, implemented in software and relied often on general purpose computing hardware. Therefore, such services can suffer from similar security threats as any other Internet service.

The Session Initiation Protocol (SIP) [1] has been adopted as the dominant signaling protocol to handle multimedia sessions at both the Internet and the 3G Realms [2]. In this paper we present an architecture to mitigate Denial of Service attacks on a SIP-based VoIP infrastructure. The proposed architecture is designed to detect effectively different SIP vulnerabilities (message flooding, malformed message sending, DNS blocking) through specialized detection modules without requiring modification in the core of the SIP architecture. Those modules have been implemented and assessed under various tests in laboratory and in a real-life VoIP network.

Flooding a server with malicious messages or even high-rate regular messages can have serious consequences on any service. The server is busy processing useless messages while lacking the processing power to reply to authentic user requests. In the worst case, a malformed message that exploits know security holes in an implementation might crash the whole system with a single packet (aka the infamous *Ping of Death* [3]).

We counter such attacks by providing a double-level security architecture. A first line *Bastion host* provides essential security checks against well-known TCP/IP related attacks and detects and prevents SIP message flooding against the host. In the second line of defence, we enhance the SIP proxy with additional security modules that provide specialized SIP related security features. We achieve this by providing a signature-based malformed message detection module that checks incoming messages and a specialized SIP-based DNS cache that is guaranteed to be non-blocking even under time-consuming operation requests.

* Corresponding author. Tel.: +49 30 3463 7378; fax: +49 30 3463 8000.
E-mail addresses: sven.ehlert@fokus.fraunhofer.de (S. Ehlert), ge.zhang@fokus.fraunhofer.de (G. Zhang), dgen@aegean.gr (D. Geneiatakis), gkamb@aegean.gr (G. Kambourakis), ntan@teimes.gr (T. Dagiuklas), jiri.markl@nextsoft.cz (J. Markl), dorgham.sisalem@tekelec.com (D. Sisalem).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.03.016

Laboratory and real-life testbed measurements prove the effectiveness of the modules for these kinds of attacks. Furthermore, we show that these modules introduce only a slight processing overhead, which does not affect service operation negatively.

The remaining of the paper is structured as follows. The next section provides some elemental information about SIP in VoIP environments, necessary for the analysis to follow. Section 3 exhibits major security threats concerning SIP in the context of this paper. Section 4 introduces our defence architecture to repel and thwart attacks discussed in the previous section, while Section 5 presents and analyses the experimental results. The last section concludes the paper and gives pointers to future work.

1.1. Related works

Several researchers have proposed VoIP security solutions to detect and prevent VoIP-related attacks. Most of these solution focus on different detection strategies.

Sengar et al. [4] propose a detection framework based on Hellinger distance calculation. Another flooding detection algorithm based on Cumulative Sums is presented by Rebahi [5]. Both solutions are able to detect message flooding, but do not provide a mitigation solution.

Wu et al. [6] propose a cross-platform detection framework. Based on the correlation of SIP and RTP traces they detect misbehavioural patterns, e.g., malicious session termination.

Chen [7] proposes a concept for detecting DoS Attacks on SIP systems using a SIP state machine model. The system is outlined to detect unauthorized invalid message flooding.

Another online detection mechanism based on a Bayesian Model for SIP is proposed by Nassar et al. [8]. The system is able to detect different kinds of threats towards VoIP applications besides DoS, including SPIT and password cracking.

2. Background information

2.1. Voice over IP using the Session Initiation Protocol

SIP is an application-layer signaling protocol for creating, modifying, and terminating multimedia sessions among one or more participants [1]. It is a text based protocol designed to establish or terminate a session among two or more partners. The message format is similar to the HTTP protocol, with message headers and corresponding values, e.g., "From: user@sip.org" to denote the sender of a message. The destination of a SIP messages (Request-URI) is provided in the first line of the message, the *request line*. Fig. 2 illustrates a sample SIP-INVITE message. Additionally, several other message headers are dedicated to routing purposes in the network:

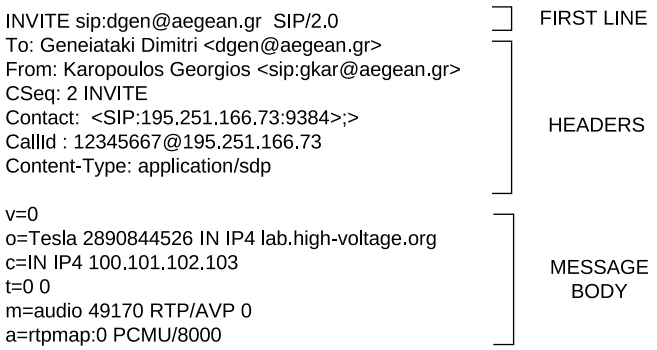

Fig. 2. A typical well-formed SIP-INVITE message.

To	Denotes the receiver of this SIP message. This is generally the public available address of the user (Address of Record).
From	Denotes the sender of the message.
Contact	The actual location where a user can be reached. This location can be different from the *From* URI.
Record-Route	Indicates that an intermediate proxy wants to receive further signalling traffic.
Route	Indicates a route that a new request is going to take.
Via	A list of all intermediate SIP entities that this messages has passed so far.

Further, various network entities compose a SIP network (see Fig. 1), such as *User Agents* (UAs) that generate or terminate SIP requests, *Registrars*, where users log in and announce their availability in the SIP network and *Proxies* that forward requests in the appropriate SIP networks. Several proxies can be deployed in a SIP infrastructure, e.g., outbound proxies that regulate routing outgoing traffic from one network to a foreign network and incoming proxies that handle all incoming SIP requests possibly enforcing additional security checks.

3. SIP security threats

3.1. Resources susceptible to DoS in SIP servers

Denial of Service (DoS) attacks aim at denying or degrading a legitimate user's access to a service or network resource, or at bringing down the servers offering such services. According to a 2004 CSI/FBI survey report 17% of respondents detected DoS attacks directed against them, with the respondents indicating that DoS was the most costly cyberattack for them, even before theft of proprietary information [9]. To make things worse, attackers have developed tools to coordinate distributed attacks simultaneously

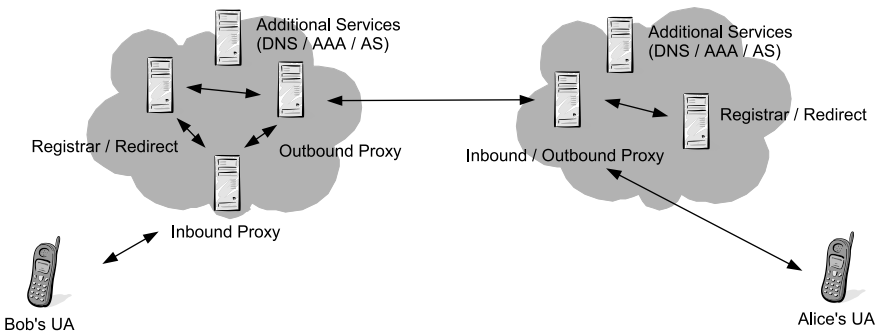

Fig. 1. SIP architecture schematic overview.