Overview of SIP Attacks and Countermeasures

Fadi El-moussa[1], Parmindher Mudhar[2], and Andy Jones[1,3]

[1] Centre for Information & Security Research
[2] Security Design and Operate
[3] Edith Cowan University
BT
Adastral Park, Ipswich IP5 3RE
Fadiali.el-moussa@bt.com,
parminder.mudhar@bt.com,
Andrew.28.jones@bt.com

Abstract. The Security threats to current circuit switched networks dedicated to a single voice application such as the Public Switched Telephone Network *(*PSTN*)* are considered minimal. However, in open environments such as the Internet, conducting an attack on voice applications such as Voice over IP (VoIP) is much simpler. This is because VoIP services such as Session Initiation Protocol (SIP) are using servers that are reachable through the Internet. The aim of SIP is to provide the same functionality as traditional PSTN over the Internet. SIP service is implemented in either software or hardware and can suffer similar security threats as HTTP or any publicly available service on the Internet such as buffer overflow, injection attack, hijacking, etc. These attacks are simple to mount, with minimal charges or no cost to the attacker. This paper describes various possible security threats that a VoIP provider could encounter and the impact of these threats on the VoIP infrastructure. In addition, this paper investigates current solutions and mitigation techniques for VoIP attacks in order to provide more reliable VoIP services. The SIP taxonomy presented in the paper can be used as a baseline model to evaluate a SIP product against current and future vulnerabilities and gives a number of possible countermeasures that can be used to mitigate the threats.

Keywords: SIP, Denial of Service, Authentication, Buffer overflow, SIP Injection, SPIT, Internet Telephony.

1 Introduction

Session Initiation Protocol (SIP) [11] is an application layer control protocol that is used for creating, modifying and terminating sessions with one or more participants. The SIP protocol is a signalling protocol used for establishing sessions in an IP network. A session could be a simple two-way telephone call, the distribution of multi-media, multi-media conference sessions, the distributed computer games, etc. The aim of SIP is to provide the same functionality as a traditional PSTN over the Internet.

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 82–91, 2010.

The SIP network infrastructure consists of the following:

- The SIP end-point device: a user agent that is responsible for generating and terminating SIP requests. This could be a soft-phone, an instant messenger, an IP phone or even a cellular phone.
- SIP Proxy: an application that enables SIP devices to locate and communicate with one another.
- SIP Registrar: an application with which the SIP devices need to register in order to make and receive calls.
- SIP Redirect Server: an application that receives a request from another SIP device or proxy and returns a redirection response indicating where the request should be directed.
- Usually the SIP proxy, SIP registrar and SIP redirect server are implemented on one system.

Figure 1 illustrates a typical SIP call between two user agents [4]. In the SIP infrastructure the user is defined as a SIP Uniform Resource Identifier (URI) in the form of sip:user@domain. The SIP agent needs to register the URI and the corresponding IP address with the SIP registrar responsible for the domain in order to identify the SIP device location. In order for the SIP agent to register it needs to send a SIP REGISTER message request which informs the SIP registrar that a SIP device is available to place or receive calls and associate a device's IP address with the SIP URI. Registration is performed via UDP protocol.

2 SIP Security Measures

This Section discusses possible attacks on the SIP infrastructure [1] [2] [8]. The SIP infrastructure consists of a number of components dealing with signalling messages, user management, address resolution, packet transfer and services. It is crucial that each component of the SIP infrastructure is secured in order to secure the SIP environment.

2.1 Denial of Service Attack

Flooding attacks occur when an attacker sends a high volume of traffic that causes the target system to consume all of its resources and renders it unable to serve legitimate customers. Flooding in the SIP network infrastructure can easily occur since there is no separation of the channels for signalling and data transfer. It is difficult to trace the source call and a single device can simultaneously generate a high number of calls.

In the following sub-sections the different types of flooding attacks are discussed.

2.1.1 SIP Register Flooding

SIP devices need to send REGISTER requests in order to register with the SIP registrar as they start up. The SIP Register flooding attack occurs when an attacking source sends a stream of SIP REGISTER messages to the SIP registrar to deplete its

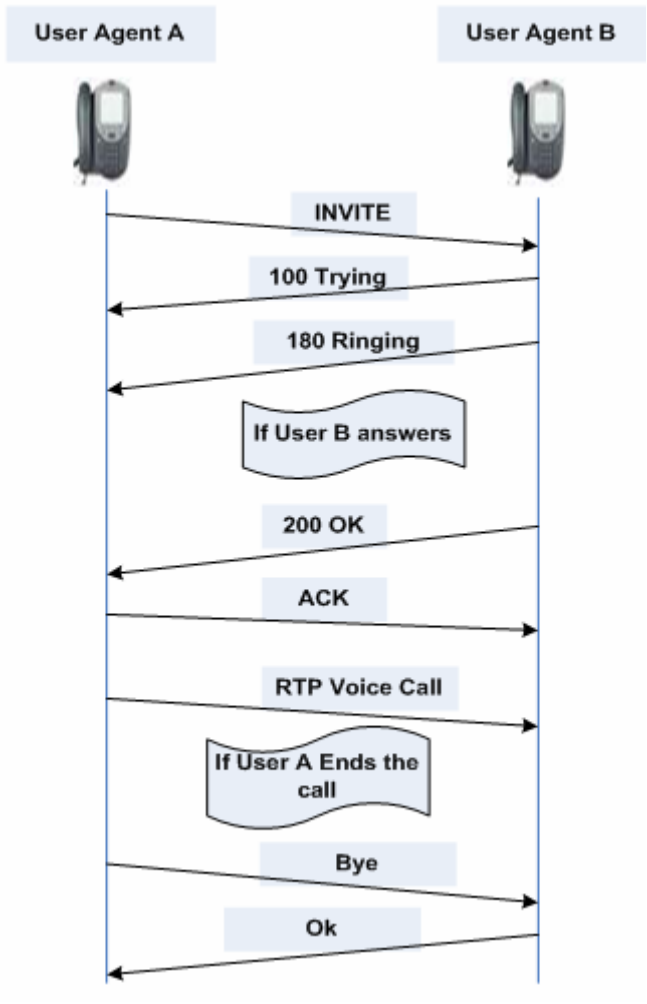

Fig. 1. SIP Signalling Protocol

resources and force it to a point where it cannot handle legitimate new calls. The attacker can use a tool to craft a REGISTER request with multiple user names in order to create a unique spoofed request and flood the application server. The SIP registrar will spend time looking into the database and sending back "Not Found" error messages which will be ignored by the attacker.

2.1.2 Call Flooding Attack

This type of attack occurs when a malicious attacker sends a stream of SIP INVITE requests to an end SIP device. The attacker keeps sending SIP INVITE requests and hangs up once it receives the Ringing or 100 OK messages from the end-device. As a result, the end device will not be able to make any calls or receive any legitimate calls.

There are several ways of defending against the attacks mentioned above if an organization adopts the following countermeasures:

- The use of ingress filtering at the network border: Implementing ingress filtering at the network border will allow spoofed IP packets to be dropped. However, an attacker can still perform DDoS attack by spoofing addresses within the network.
- Deploying a VoIP rate limiting device that can monitor and limit the number of SIP messages accepted at the border gateway.
- The use of a separate VLAN for VoIP signaling and data.
- Enabling authentication for various type of requests.

2.2 SIP Injection Attack

SIP is a complex protocol with many different messages. Attackers may exploit the SIP application layer or network layer by injecting malicious code [5] or traffic to either trigger a failure in the SIP server, leave it in unstable state or to gain full control over the system. There are several different types of SIP injection attacks and two of these are described below.

2.2.1 Buffer Overflow Attack

A buffer overflow attack [13] exploits a vulnerability in the SIP implementation which allows an attacker to inject malicious code into the victim's machine and gain full control. For example, Cisco Unified IP Phone series [3] was vulnerable to buffer overflow that allow an attacker to execute a malicious code at the system. Keeping in mind that VoIP software will inherit any vulnerability from the operating system or firmware that it is running at. The consequences of buffer overflow can be serious given that the attacker can run malicious code and gain control of the target system.

2.2.2 RTP Injection Attack

SIP is a call management protocol that carries voice or video data in its payload. The voice or video data is carried via the Real-Time Transport Protocol (RTP) protocol. The RTP runs on top of the UDP or TCP protocol in order to transmit media such as audio or video via the Internet. The RTP protocol does not provide an encryption or authentication mechanism to the transmitted media. Therefore, an attacker would be able to monitor the INVITE message request between the two end SIP devices to determine the IP address and the port number that the RTP call stream is being sent to. Once these details are known, the attacker can start sending streams of RTP packets to the appropriate IP address and port number. This results in one of the callers receiving the injected RTP stream rather than the actual conversation.

Possible countermeasures to SIP injection attacks are:

- Enforcing audio encryption to prevent RTP injection/mixing.
- Adopting authentication where possible.
- Keeping operating system and application patches up-to-date.
- Deploying a VoIP Intruder Detection Systems (IDS)/Intrusion Prevention Systems (IPS) system for detecting malicious code and vulnerabilities

targeting the VoIP devices. The IDS should be able to learn the SIP message grammar of the deployed SIP devices within the network in order to detect any SIP traffic that deviates from the stored ones.

2.3 SIP Spoofing Attack

As SIP control messages are text based and in most cases are sent in clear text, they are prone to spoofing, modification or interception. Basically, SIP allows any request to be processed without authentication and does not enforce SIP source message validation mechanisms. The SIP authentication service is optional and the system allows a SIP request to be processed without authentication. Most of the attacks in this section can be easily mitigated by the use of a SIP authentication mechanism.

2.3.1 De-registration Attack

This type of attack is based on an attacker sending a REGISTER message with the *Expire* field set to zero. This type of message is normally sent by a soft phone to indicate that it is shutting down and that no more calls can be sent. An attacker can generate a crafted REGISTER request message that spoofs a user identity with an *Expire* field set to zero as shown in Figure 2. The illustration shows the attacker spoofing the identity of user 100 by sending a SIP REGISTER request message with the *Expire* field set to zero. As a result, user 100 will not be able to receive any calls, will not have a dial-tone and will not be able to make outbound calls.

Implementing a strong authentication mechanism before processing the REGISTER request can mitigate such attacks. Both the SIP device and SIP registrar should use a strong authentication mechanism for registration in order to prevent this type of attack.

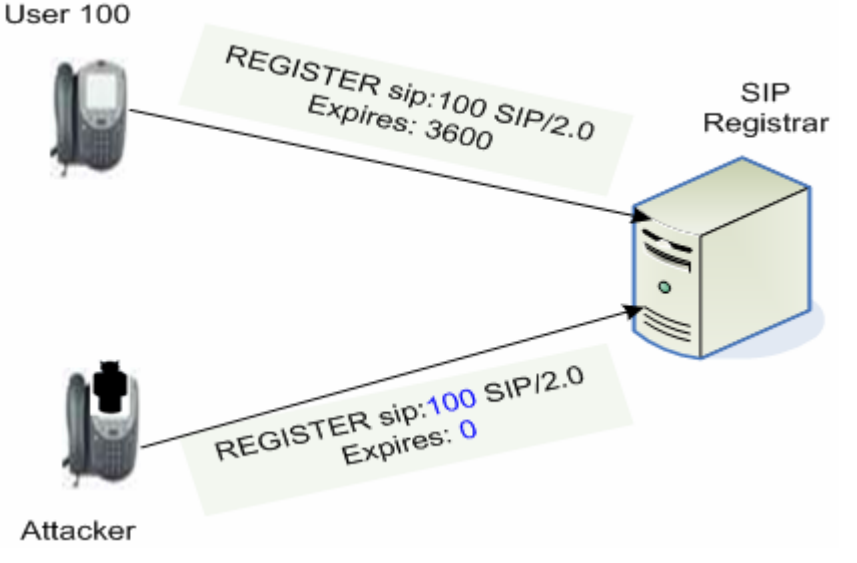

Fig. 2. De-Registration Attack

2.3.2 SIP Spoofing BYE Attack (Call Tear Down Attack)

The BYE request is used to terminate a SIP connection. An attacker can construct a BYE request and send it to the end device to terminate calls between participants. An attacker has to be able to intercept the calls between the participants and spoof a BYE request message with the Call-ID, To and From tag number fields and user SIP URI in order to achieve his attack.

If an attacker manages to listen to an organizations call centre and capture all the required fields then the attacker could launch a devastating attack and close down all the established calls.

2.3.3 SIP Re-Send Attack

An attacker can resend a SIP request message to an already established session in order to modify one or more of the parameters of the existing dialog session. For example, an attacker can resend a spoofed INVITE message to modify dialog parameters such as the To or From fields and this can cause a DoS attack to occur against the end system.

2.3.4 SIP Call Hijacking

SIP call hijacking is based on the attacker hijacking a call and re-directing it to his device. A call hijack attack is a combination of a de-registration attack and a registration attack. In order for an attacker to perform a call hijacking attack, the attacker needs to de-register one of the end SIP devices and then register the attacker's own device, masquerading as the user's identity in order to redirect the calls to the attacker's phone. A stealthier call hijacking might involve skipping the de-registration attack phase and simply sending a spoofed INVITE message with the victims identity to another SIP proxy. Depending on the SIP device, some systems will direct calls to both the original device and to the attacker's device. As a result the attacker may be able to passively listen and record any confidential conversation.

In order to reduce the likelihood of successful SIP spoofing attacks, the following measured should be enforced:

- A strong authentication mechanism to authenticate SIP request messages.
- The SIP proxy should ignore any SIP CANCEL request that follows any other message type than INVITE request.
- The challenge/response mechanism should be used to protect against replay attack. This method can be adopted by a SIP gateway solution to challenge SIP terminals before passing their SIP request.
- To prevent spoofing, an organization can modify the soft phone client software to embed the user's information into the application, thus making it unique to that user.
- Encrypt the SIP communications. By encrypting SIP messages, an attacker will not be able to gather information about the call itself in order to determine how to inject the attacker's control messages.
- Enable ingress filtering at the edges to drop packets that have a spoofed IP source address.

2.4 SIP Authentication Attack

SIP authentication [12] [7] does not provide a high level of security as it is based on the MD5 digest algorithm rather than using a public key algorithm. In addition, SIP authentication is based on a challenge/response where a trust is built based on a server sending a challenge to the client and then the client responding to the server. The challenge/response is based on MD5 hash (where the server needs to check the client response by repeating the MD5 calculation using a stored value of the username and password. Calculating the response is a computationally expensive task for the server, since it has to look for the username and password stored in the server database and combine it with the original challenge to compute the MD5 hash. The following subsections describes some of the SIP authentication attacks.

2.4.1 SIP DoS Authentication Attack

An attacker can exploit the SIP authentication mechanisms by generating a large number of requests and response messages to each challenge with a randomized or fixed response. The attack does not need to go through the expensive MD5 calculation and can just send a random response. All responses will fail but that will still keep the server busy checking the bogus requests and it will therefore have less time/resource to serve or handle legitimate calls.

2.4.2 Dictionary and Enumeration Attack

The SIP authentication mechanism is only as strong as the user password and as a result, a user's password could be vulnerable to a dictionary attack. An attacker might use a dictionary attack to discover a weak password of an end user. A dictionary attack can be detected as the result of multiple authentication failures. However, a much stealthier attack can be executed by monitoring the challenge and response session, which is sent in clear text, in order to predict the user's password.

In order to mitigate SIP authentication attacks:

- The SIP proxy should verify the client identity before going through the expensive SIP message verifications.
- Users should use a strong password to protect against dictionary attacks.

2.5 SIP Traffic Capturing

The SIP protocol does not provide encryption or authentication to the transmitted media. Therefore, an attacker can simply capture and record the SIP traffic using tool such as Wireshark [14]. SIP traffic capturing is the basic method for recording a conversation without the consent of the participants. For example, an attacker can eavesdrop on the current call, extract the RTP stream from the traffic and then convert the stream to a WAV file for unauthorized recording or to listen to it. By capturing and recording the media stream, an attacker may gain access to unauthorized material such as user's confidential information, passwords or personal information.

2.6 SIP Messages Modification Attack

As mentioned earlier, SIP consists of an envelope and a payload which are sent in clear text. The SIP envelope and payload contain various parameters that can be read and modified by an attacker. If an attacker intercepts a call message between the participants then he may be able to manipulate those parameters and affect the whole communication. For example an attacker can simply alter the Content-Length field from 450 to 200 in the SIP envelope. This would result of loss of 250 bytes and as a result the content would be truncated and the full contents will not be interpreted by the server. An attacker could also alter any other fields such as Content-Encoding, Content-Type field to disrupt the conversation.

Possible countermeasures for call eavesdropping are:

- Encrypt the SIP header and payload using the Secure Real-Time Transport Protocol (SRTP). Both media and signalling should be encrypted. If the signalling protocols contain encryption keys or if the identity of call participants is sensitive then it should be encrypted. Encrypting the media content prevents eavesdropping.
- Send the SIP messages over a secure channel such as Transport Layer Security (TLS)[4].

2.7 VoIP SPAM (SPIT)

Spam over Internet Telephony (SPIT) [6] is similar in nature to email SPAM where hundreds or thousands of unsolicited voice mail messages arrive at the end device. However, it would be very disruptive and time consuming to listen to and delete every voice mail message. When the VoIP service is free or cheap, users will be tempted to use it for spamming. Therefore, VoIP SPAM can be much more disruptive to a VoIP system than e-mail SPAM. A simple attack is to create a script that initiates calls to a range of numbers or IP addresses with a recorded voice message.

Countermeasures for voice SPAM include the deployment of a SPAM controller such as the White List/Blacklist technique, speech segmentation, speaker classification, automated verification, and content/header filtering [9]. Other solutions including voice prompts, for example “press 45 if you are real person” can be used [1].

3 Conclusions

Most organizations today are deploying VoIP in their infrastructure or providing VoIP as a service to their customers. While it has become increasingly attractive to deploy VoIP, many organizations still need to understand how VoIP can be deployed without placing their information and the continuity of their business at risk. Determining VoIP security threats and mitigation techniques is the first step in securing an organization’s information from the increasing number of threats in this area. Once the security threats and mitigation processes are understood and identified an organization can

then map out the type of features a vendor product must have in order to secure the VoIP network.

The vendor product should implement as many mitigation features as possible and make it easy for an organization to manage those features. Defence-in-depth is essential as there are no single mechanism that can ensure total security and as a result, multiple layers of security are recommended. For example, besides the security mitigation mechanisms proposed, a virtual separation of data and control information is essential. Virtual separation, for example by using VLANs, makes managing the security of the network easier and isolates different services into different network zones.

Most of the VoIP threats can be mitigated by having strong authentication, authorization and encryption in place. Implementing these security measures in the VoIP infrastructure will make spoofing, impersonation, and eavesdropping difficult to carry out. In order to prevent buffer overflow and application level exploitation, each device needs to be updated, patched and all unnecessary services and applications must be disabled.

In general, adopting best practice in the design and deployment of VoIP will ensure that the existing effectiveness of network security for an organization is not negatively impacted.

References

[1] Amber Group, VoIP Security Considerations for Service Providers, Centre for the protection of national Infrastructure (2007), http://209.85.229.132/search?q=cache:fDKtkHCdsUoJ:csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf+Amber+Group+%2B+VoIP+Security+Considerations&cd=1&hl=en&ct=clnk&client=firefox-a

[2] Collier, M.: Basic Vulnerability Issues for SIP Security, SecureLogix Corporation (2005)

[3] Cisco, Cisco Security Advisory: Cisco Unified IP Phone Overflow and Denial of Service Vulnerabilities (2008), http://www.cisco.com/warp/public/707/cisco-sa-20080213-phone.shtml

[4] Dierks, T., Rescorla, E.: The Transport layer Security (TLS) Protocol, RFC 4346 (2006)

[5] Endler, D., Collier, M.: Hacking VoIP Exposed: Voice Over IP Security Secrets & Solutions. McGraw-Hill, London (2007)

[6] Kaplan, H., Packet, A., Wing, D.: The SIP Identity Baiting Attack. Cisco Systems, Internet Draft paper (2008), https://datatracker.ietf.org/drafts/draft-kaplan-sip-baiting-attack

[7] Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998)

[8] META Group, IP Telephony Security: Deploying Secure IP Telephony in the Enterprise network, META Group White Paper (2005), http://seclab.cs.ucdavis.edu/seminars/ReynoldsSeminar.ppt

[9] Pantridge, M.: VoIP SPAM Counter Measure. MSc Thesis, Informatics and Mathematical Modelling department, Technical University of Denmark (2006)

[10] Rivest, R.: The MD Message-digest Algorithm, RFC 1321 (1992)
[11] Rosenberg, J., Schulzrinne, H.: SIP: Session Initiation Protocol, RFC3261 (2002)
[12] Stefano, S., Luca, V., Donald, P.: SIP security issues: the SIP authentication procedure and its processing load. IEEE Network 16(6), 38–44 (2002)
[13] Thermos, P., Takanen, A.: Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures. Addison Wesley, London (2008)
[14] Wireshark (2008), http://www.wireshark.org/