Misuse Patterns in VoIP

Juan C. Pelaez
U.S. Army Research Lab.
Networking Security Branch
Aberdeen, Maryland, USA
+1 410 278-0014
jpelaez@ieee.org

Eduardo B. Fernandez
Florida Atlantic University
Dept of CEECS
Boca Raton, Florida, USA
+1 561 297-3466
ed@cse.fau.edu

M. M. Larrondo-Petrie
Florida Atlantic University
College of Engineering
Boca Raton, Florida, USA
+1 561 297-3899
petrie@fau.edu

Christian Wieser
University of Oulu
Electrical & Info. Eng. Dept.
Oulu, Finland
+358 8 553-1011
chweiser@ee.oulu.fi

ABSTRACT

In VoIP, in order to avoid attacks and discover security vulnerabilities, it is necessary to be aware of typical risks and to have a good understanding of how vulnerabilities can be exploited. In a previous paper we presented the concept of misuse patterns. Attack patterns describe from the point of view of the attacker, how a type of attack is performed (what system units it uses and how), analyzes the ways of stopping the attack by enumerating possible security patterns that can be applied for this purpose, and describes how to trace the attack once it has happened by appropriate collection and observation of forensics data. We present a set of misuse patterns for VoIP: Denial of Service (DoS), Call Interception, and Theft of Service on VoIP.

Categories and Subject Descriptors

D.2.11 [**Software Architectures]**: Patterns

General Terms

Design, Security.

Keywords

Security Patterns, Voice over IP, software architecture, network architecture.

1. INTRODUCTION

In order to design a secure system developers first need to understand what the possible threats to the system are. Without this understanding they may produce a system that is more expensive than necessary and that has a large performance overhead. On the other hand security novices need to understand the enemy in order to implement successful countermeasures (e.g. security patterns). To successfully defend a system against attacks, they must understand the characteristics of such attacks. Discovering vulnerabilities in VoIP networks is complex and as an aid we have proposed in [1] a new type of pattern, the attack pattern. This pattern describes, from the point of view of the attacker, how a type of attack is performed (what system units it uses and how), proposes ways of stopping the attack by enumerating possible security patterns that can be applied for this purpose, and helps analyzing the attack once it has happened by indicating where we can find forensics data as well as what type of data.

In VoIP network forensics a systematic approach is needed to detect vulnerabilities and the resulting attacks. Misuse patterns as an investigative method help to provide an understanding of the attacker's point of view, his or her goals and methods are the main focus in almost all forensic investigations. Therefore, misuse patterns should be integrated in the VoIP network forensic process.

Misuse patterns enable us to focus on the vulnerable parts of a specific VoIP network and allow us to be better able to secure them. There are various threats to a VoIP deployment from external domains and internal sources. The goal is to prevent those attacks that have the potential to affect a VoIP environment.

We describe this type of patterns using a template based on the one used in [2], which is commonly used for architectural patterns as well as security patterns [3]. We have reinterpreted the *problem* and *solution* sections to fit the new viewpoint of attack instead of defense. Likewise, we included two new (compared to the template for standard security patterns) sections: *Countermeasures and forensics* and *Where to look for forensic evidence.*

Misuse patterns can guide forensic examiners in the process of searching for evidence. They could also serve as a structured method for obtaining and representing relevant network forensics information. Misuse patterns are particularly useful in cases where criminals break into a VoIP network segment that is not monitored by network security devices. Therefore, investigators should look for evidence in other network components (e.g. terminal devices) considered as secondary data sources. An misuse pattern is also an important technique that helps examiners to ensure that they have considered all possible contexts and evidence sources by using the proposed template.

The value of the proposed approach comes from the fact that the attack, described dynamically in a sequence diagram, makes direct reference to the components of the system, described in turn by the class diagram. The sequence diagram uses objects from classes in the class diagram and we can then relate messages to the components where they are sent (classes represent the components of the system). The parameters in these messages are data that can be found in the corresponding component. In other words, the combination of sequence and class diagrams tells us where to look and what information we can find after some attack.

Preliminary versions of these papers were workshopped at Pattern Languages of Programming (PLoP) '07 September 5-8, 2007, Monticello IL, USA. ISBN:978-1-60558-411-9.

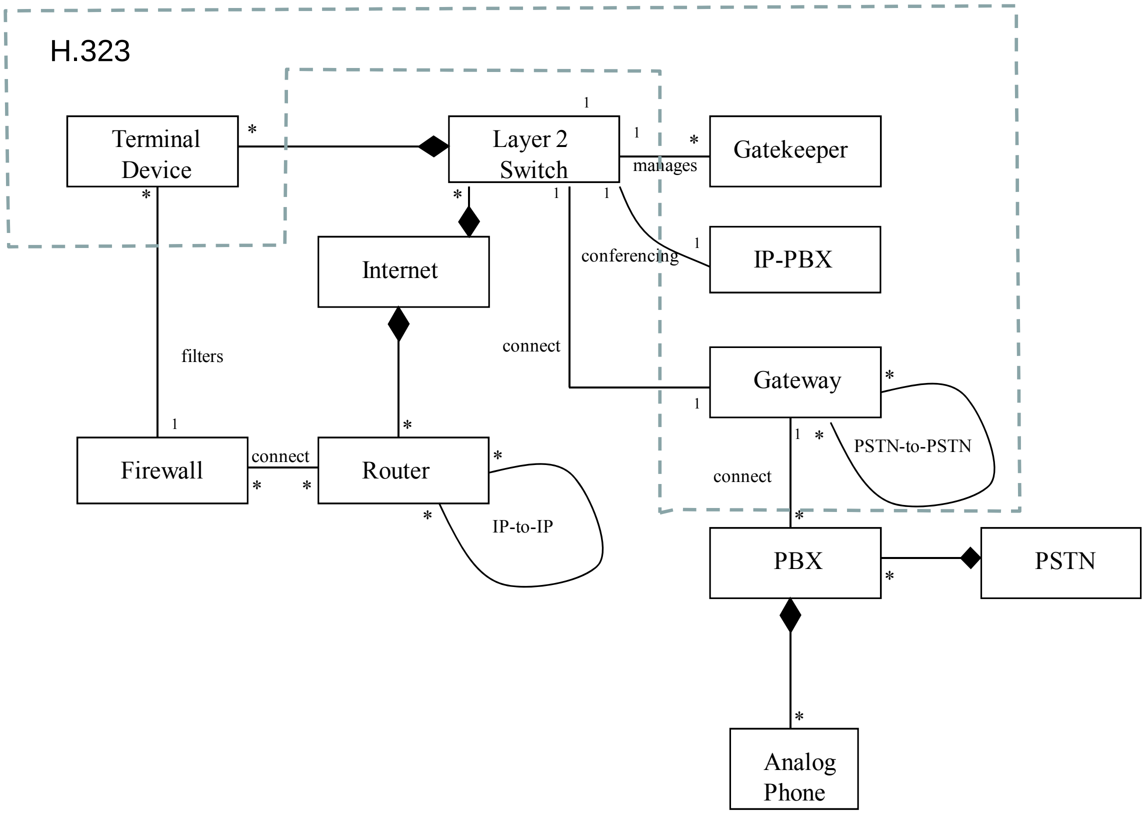

Figure 1 Class Diagram for an H.323 architecture

In this paper we illustrate this type of pattern by presenting specific misuse patterns for DoS, VoIP Call Interception, and Theft of Service attacks on VoIP.

Two common signaling standards are used for VoIP systems: H.323 and SIP. We consider here attacks in an H.323 environment (See [4] for details of a SIP attack). SIP attacks can be considered a variant of these patterns or a separate pattern.

Figure 1 shows the class diagram of the structure of an H.323 system. The **Layer 2 Switch** provides connectivity between H.323 components. The **Gateway** takes a voice call from a circuit-switched Public Switched Telephone Network (**PSTN**) and places it on the IP network. The PSTN uses **PBX** switches and **Analog Phones**. The Internet (IP network) contains **Routers** and **Firewalls** to filter traffic to the **Terminal Devices**. The gateway also queries the **Gatekeeper** via the Internet with caller/callee numbers and the gatekeeper translates them into routing numbers based upon service logic. The **IP-PBX** Server acts like a call processing manager providing call setup and routing the calls throughout the network to other voice devices. Softphones are applications installed in Terminal Devices (e.g. PCs or wireless devices).

This paper is divided into four parts. In the following section we discuss the DoS misuse pattern. In Section 3 we analyze the VoIP Call Interception misuse pattern, a commonly used method for intercepting calls in VoIP. Further in Section 4 we analyze the Theft of Service misuse pattern. We end with some conclusions and possible directions of future work in Section 5.

2. MISUSE PATTERN: DENIAL-OF-SERVICE (DOS) IN VOIP

Intent

The VoIP DoS attack is intended to overwhelm limited resources to disrupt VoIP operations through a flood of messages; this leads to degrading the quality of messages, thus preventing subscribers from effectively using the service.

Context

We must take into account two different scenarios when studying DoS attacks: those where end systems are targets and those that target gateways. In the former, subscribers trying to establish a call over a VoIP channel. VoIP services should be available to subscribers when requested. In the latter, some VoIP systems use control protocols (e.g. MGCP and Megaco/H.248) and security mechanisms, in order to manage the Media gateways deployed across the infrastructure. In general, the VoIP system should have adequate capability (i.e. routing, bandwidth, and QoS) to meet the peak communication load. The system may have a minimum set of perimeter defenses, e.g. firewalls. More complex VoIP implementations may have an intrusion detection system (IDS), firewall on the phone itself to check the media packet flow, or perform authentication.

Problem

IP telephony subscribers need to be blocked from using VoIP services. The attack can be carried out taking advantage of the following **vulnerabilities**:

- VoIP security is in an incipient phase at the moment, there is lack of expertise and security standards. Users might inadvertently expose the system. While there exist some basic countermeasures such as IDSs and firewalls, administrators may not configure them appropriately due to a lack of training and time.
- Until now VoIP has been developed and deployed focusing on functionality with less thought for security [5]. That means that not very advanced defenses are in place. For example, strong authentication is not common in VoIP.
- All Internet building blocks – and thus VoIP- are vulnerable to DoS attacks which have not previously been a security issue with the circuit-switched telephony system because of its analog nature.
- With the rush to implement new VoIP systems, features and standards, implementation flaws are common. IP PBXs include many layers of software that may contain vulnerabilities. Programming mistakes, such as not properly checking the size of the parameters of a protocol request, when exploited, can result in the following issues:
    - **Remote access**. An attacker obtaining remote (often administrator level) access.
    - **Malformed request DoS**. A carefully crafted protocol request (a packet) exploiting a vulnerability which results in a partial or complete loss of function.
    - **Load-based DoS**. A "flood" of legitimate requests overwhelming a system [6].
- As with any network-based service, enterprise VoIP must communicate with other components on a LAN and possibly over an untrusted network such as the Internet, where packets are easy to intercept.
- Because RTP carries media, which must be delivered in real-time to be usable for an acceptable conversation, VoIP is vulnerable to DoS attacks that impact the quality delivery of audio such as those that affect jitter and delay.
- VoIP traffic can offer very good cover for DoS attacks because VoIP runs continuous media over IP packets [7].

Solution

One method to launch a DoS attack is to flood a VoIP server (e.g. Gatekeeper) with repeated requests for legal service in an attempt to overload it. This may cause severe degradation or complete unavailability of the voice service. A flooding attack can also be launched against IP phones, Gateways or any VoIP network components that accept signaling (e.g. a flood of "register" or "invite" events). With this form of DoS attack, the target system is so busy processing packets from the attack that it will be unable to process legitimate packets which will either be ignored or processed so slowly that the VoIP service is unusable. Attackers can also use the TCP SYN Flood attack (also known as resource starvation attack) to obtain similar results. This attack floods the port with synchronization packets, normally used to start a connection.

In a Distributed DoS, multiple systems are used to generate a massive flood of packets. To launch a massive DDoS attack the hacker previously installs malicious software on compromised terminal devices (infected with a Trojan) that can be triggered at a later time (a.k.a. "zombies") to send fake traffic to targeted VoIP components. Targeted DoS attacks are also possible where the attacker disrupts specific connections.

The class diagram of Figure 2 shows the structure for a DDoS attack in an H.323 architecture where any VoIP component can be a target for DoS. Classes Attack Control Mechanism and Zombie describe the software introduced by the attacker. Note that the zombie is just a terminal device in a different role.

The sequence diagram of Figure 3 shows the sequence of steps necessary to perform an instance of a DoS attack of the first type mentioned above. An attacker (internal or remote), with knowledge of a valid user name on a VoIP system, could generate enough call requests to over-whelm the IP-PBX server. An attacker may disrupt a subscriber's call attempt by sending specially crafted messages to his ISP server or IP PBX component, causing it to over allocate resources such that the Caller receives a "service not available" (busy tone) message. This is an example of a targeted attack. Similarly, out-of-sequence voice packets (such as receiving media packets before a session is accepted) or a very large phone number could open the way to Application Layer attacks (a.k.a. Attacks against Network Services). Buffer Overflow attacks might paralyze a VoIP number using repeated calling. For example, an attacker intermittently sends garbage (i.e. both the header and the payload are filled with random bytes corrupting the Callee's jitter buffer voice packets) to the Callee's phone in between those of the Caller's voice packets. Therefore the Callee's phone is so busy trying to process the increased packet flow that the jitter (delay variation) causes any conversation to be incomprehensible [4].

DoS attacks against gateways are analyzed from the supporting Megaco/H.248 protocol viewpoint. Figure 4 shows the class diagram of the media gateway control protocol structure. Megaco/H.248 is a master-slave, transaction-oriented protocol in which **Media Gateway Controllers (MGC)** control the operation of **Media Gateways (MG)** [8]. VoIP media gateways are vulnerable to DoS because they accept signaling messages.

In this setting, a DoS attack would occur at a MGC when the attacker send large amount of UDP packets to the protocol's default port 2944 or 2945**,** which keeps the MGC busy handling illegal messages, and finally block the normal service. An attacker can keep sending Service change or Audit capabilities command to a MG and thereby bring down the MG [9]. Therefore, VoIP Gateways will not be able to initiate calls or maintain a voice call during a DoS attack. The audio quality will be affected as well. An alternative to launch DoS attacks is when an attacker redirects media sessions to a media gateway. The attack will overwhelm this voice component and prevent it from processing legitimate requests.

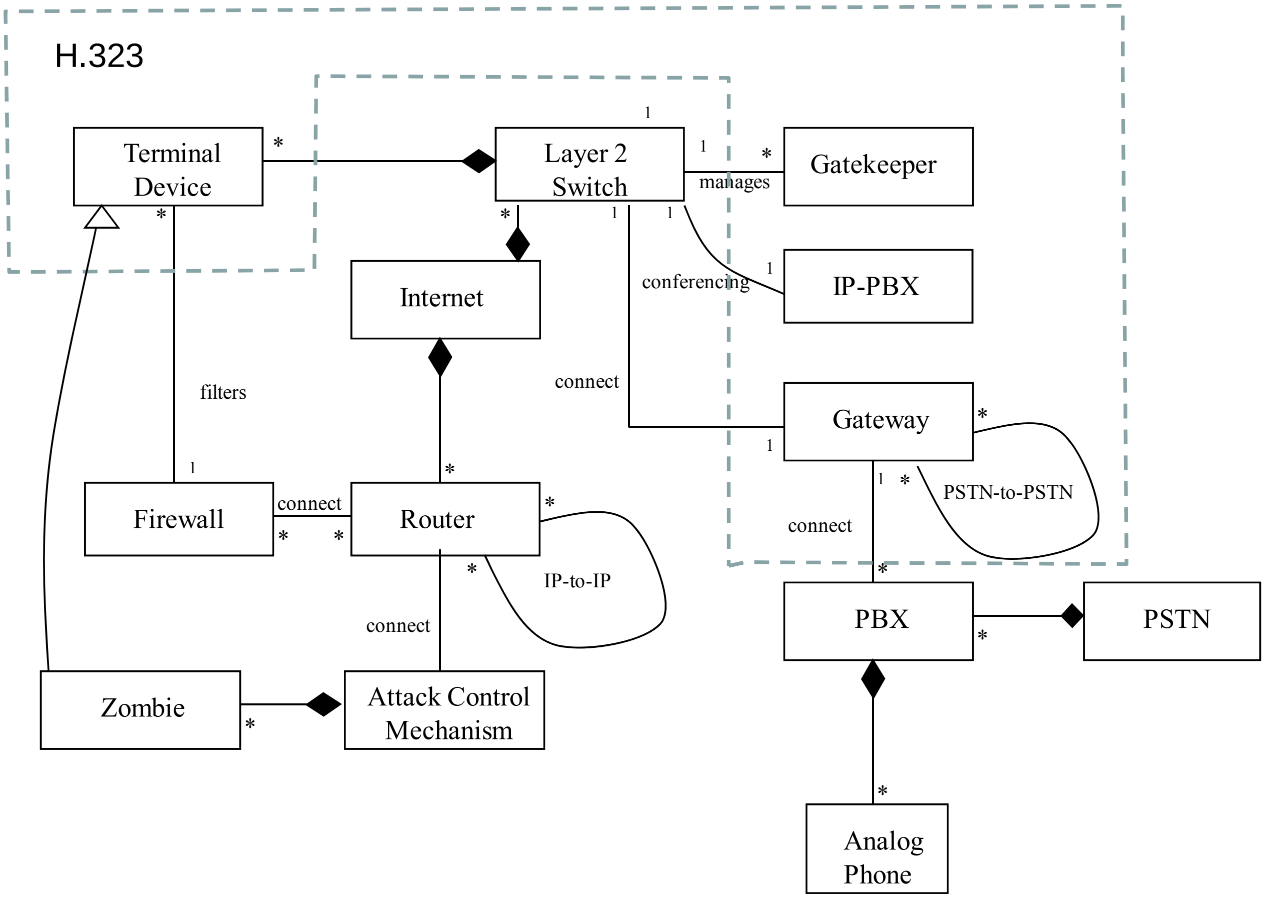

Figure 2 Class Diagram for DoS attacks in H.323

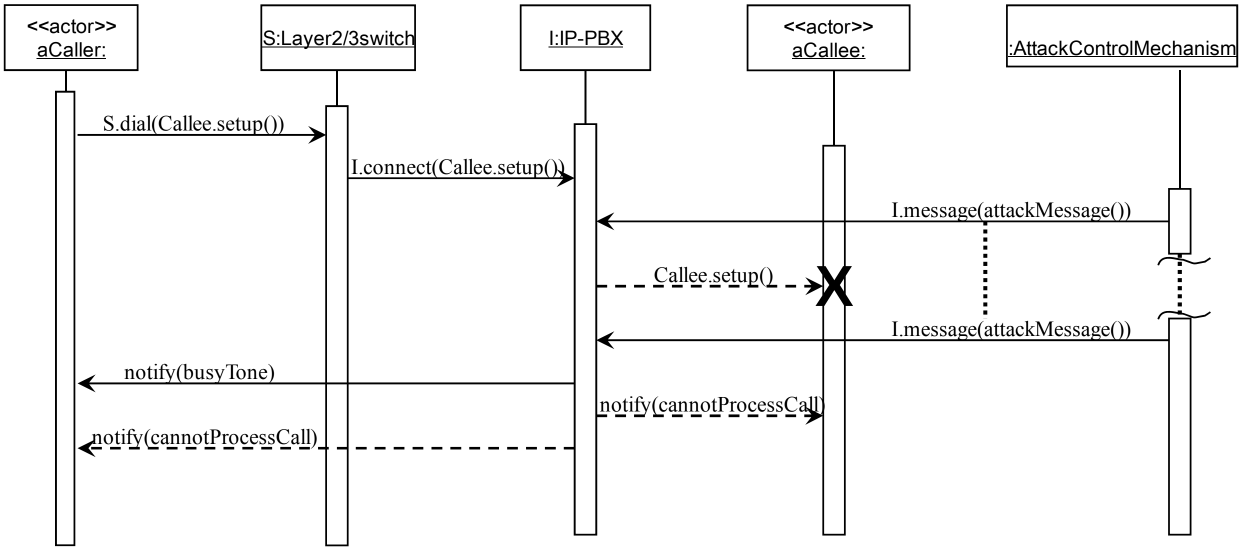

Figure 3 Sequence diagram for a DoS attack in H.323

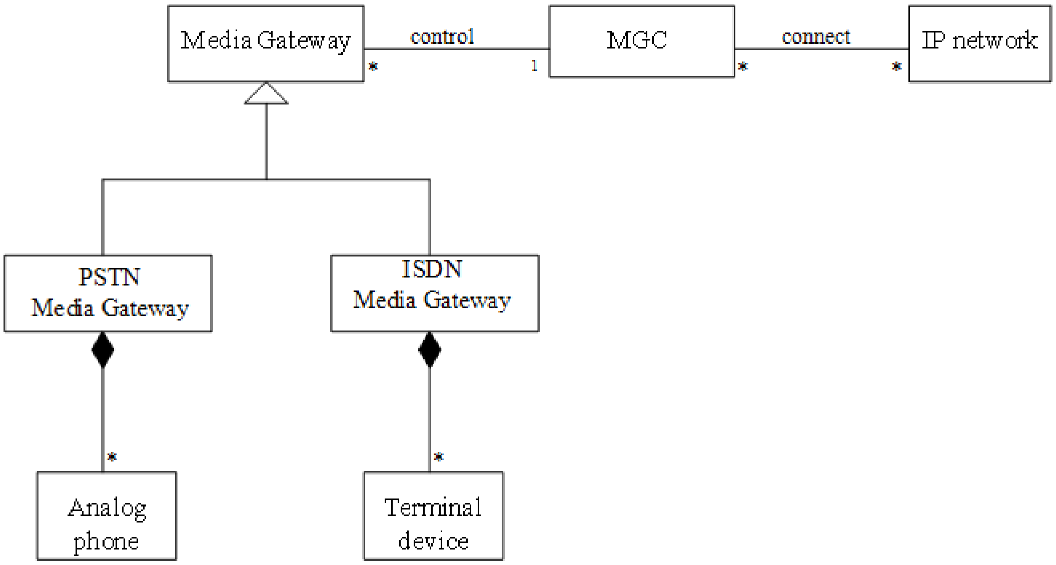

Figure 4. Class Diagram for a Megaco/H.248 environment

Signaling DoS attacks on media gateways can consume all available TDM bandwidth, preventing other outbound and inbound calls and affecting other sites that use TDM. On the other hand, due to the fact that VoIP media sessions are very sensitive to latency and jitter, DoS on media is a serious problem. VoIP media, which is normally carried with RTP, is vulnerable to any attack that congests the network or slows the ability of an end device (phone or gateway) to process the packets in real time. An attacker with access to the portion of the network where media is present simply needs to inject large numbers of either RTP packets or high QoS packets, which will contend with the legitimate RTP packets [6].

Consequences

The success of this attack implies:

- DoS can be especially damaging if key resources are targeted (e.g., media gateways); leading to cascading effects if a server is impacted.
- Flooding of the firewall can prevent it from properly managing ports for legitimate calls.
- VoIP QoS can be degraded by jitter and delay and may become totally unusable.
- The zombies in the targeted network can also be used as DoS launching points to perform attacks on another network.

Possible sources of failure include:

- Threats and attacks can be defined but are difficult to carry out in practice, mainly due to the lack of knowledge and testing opportunities for attackers.

Countermeasures and Forensics

The attack can be stopped or mitigated by the following **countermeasures**:

- DoS is mitigated by disabling and removing unnecessary network services, reinforcing the operating system, and using host-based intrusion detection systems (IDS pattern in [10]). This makes it harder to introduce Trojan horses that may make the terminal device to become a zombie.
- IDSs and firewalls ensure that packets with very large sequence numbers and garbage packets are discarded. Again the IDS pattern is relevant as well as the Firewalls patterns [3].
- Use of Stateful-Inspection Firewalls (See [3] for a pattern) with Deep Packet Inspection technology in order to look inside the voice packet, and analyze the contents of the packet as well as the headers to decide if the information is safe or not (Proxy Firewall pattern [3]).
- Use the Authenticated Call pattern [11] which performs both device and user authentication before deciding access to VoIP services. Although this takes longer it can protect from targeted attacks that do not possess authentication tokens.

Likewise, the following **network forensics mechanisms** are possible:

- Logs in the terminal devices not only provide call details (e.g. start/end times and dates of each call) but they can also reveal the presence of Trojan Horses. As we indicated, some attacks come from compromised devices that become zombies.
- Network analysis procedures such as the examination of router logs (e.g. denied connection attempts, connectionless packets) and firewall logs, provide information about the location (i.e. where the attack entered the network) and the way that attackers performed their exploits.

- Selective use of events sent to the ISP or IP PBX was shown to produce another range of attacks. Those could be traced through logs on these devices.

- Network forensic analysis techniques such as IP Traceback and Packet Marking are useful for attack attribution. During a denial of service attack the victim will receive sufficient traceback packets to reconstruct the attack path [Sha03]. Locating attackers with the IP trace back technology is also a potential security mechanism to counter DoS attacks. The deployment of a traceback mechanism on a single router would provide minimal benefit. This process requires the cooperation of all network operators along the attack path in order to trace it back to the source. IP trace back works even when criminals conceal their geographic locations by spoofing source addresses.

- Comparing traffic patterns against predefined thresholds (as done by some IDSs) is an effective method of detecting DDoS attacks. Such a method can produce an alert, helping network examiners to detect malicious traffic (e.g. observing congestion in a router's buffer) from entering or leaving their networks.

- Event logging allows network administrators to collect important information (e.g. date, time and result of each action) during the setup and execution of the attack. For example, logs may identify the type of DDoS attack used against a targeted system.

- The use of Honeypots placed on selected VoIP components (see Figure 2) and other network forensics tools can help in the event of a successful attack.

- In VoIP, the misuse pattern technique may be complemented with the use of a network forensics analysis tool (NFAT) to offer a better view (interpretation) of the collected voice packets.

Where to look for evidence

Based on Figure 2, the following may be considered secondary sources of forensic information in a VoIP environment: Terminal devices (i.e. softphones, hardphones and wireless VoIP phones), gatekeepers, gateways, and IP-PBXs.

Known Uses

DoS attacks are performed on different systems in the Internet every day on all protocol layers. Some of those attacks affect VoIP systems.

Related Patterns

Several security patterns for defending against these (and related) attacks are listed in [4], [Pel04], and [11]. Some general security patterns such as firewalls [3], IDS [10], and authentication [3] can be used to control these attacks as discussed earlier. An misuse pattern can be developed to describe similar attacks on SIP networks.

3. MISUSE PATTERN: CALL INTERCEPTION IN VOIP

Intent

The VoIP Call Interception pattern provides a way of monitoring voice packets or RTCP transmissions. This kind of attack is the equivalent of wiretapping in a circuit-switched telephone system.

Context

Two or more subscribers are participating in a voice call conversation over a VoIP channel. In public IP networks such as the Internet, anyone can capture the packets meant for another user. In order to achieve confidentiality, enterprises may use encryption and decryption techniques when using VoIP. Since cryptographic algorithms are typically implemented in hardware they are difficult to implement in VoIP which is software-based. In VoIP networks, transport-protocol-based threats rely upon a non-encrypted RTP stream [12]. On the other hand, enterprises may route voice traffic over a private network using either point-to-point connections or a carrier-based IP VPN service. Two basic common signaling protocols are used for VoIP systems: H.323 and SIP. We consider here an attack in an H.323 environment. The SIP attack can be considered a variant of this pattern or a separate pattern.

Problem

A call that traverses in a converged network needs to be intercepted. The attack can be carried out taking advantage of the following **vulnerabilities**:

- The Real Time Protocol (RTP) is not a complete protocol but rather a framework where vendors are provided implementation freedom according to their specific application profiles [12]. This means that specific implementations may have no default security mechanisms.

- In RTP, information on the used codec is available in the header of every RTP packet, via the PT header field [12].

- PC-based IP Phones (a.k.a. Softphones) are applications installed on user systems (e.g. desktops) with speakers and microphones that reside in the data segment. It is possible for worms, viruses and other malicious software common on PCs to infect the voice segment in VoIP.

- In wireless VoIP (i.e. VoIPoW), publicly available software can be used to crack Wired Equivalent Privacy (WEP) products.

- As VoIP in a wireless environment operates on a converged (voice, data, and video) network, voice and video packets are subject to the same threats than those associated with data networks. Likewise, all the vulnerabilities that exist in a VoIP wired network apply to VoIPoW technologies plus the new risks introduced by weaknesses in wireless protocols.

- The tools used for call interception purposes (packet sniffers) can be downloaded freely from the Internet, greatly increasing the potential of this type of attack.

- VoIP security is in an incipient phase at the moment, there is lack of expertise and security standards. Users might inadvertently expose the system. While there exist some basic countermeasures such as IDSs and firewalls, administrators may not configure them appropriately.

- Until now VoIP has been developed and deployed focusing on functionality with less thought for security [5]. That means that not very advanced defenses are in place. For example, strong authentication is not common in VoIP.
- Because VoIP traffic traverses several hops, call interception can be applied in many places.
- Hardware endpoints typically possess remote administration capabilities, which are sometimes not well protected, giving a further attack vector.
- The transport of voice data over public networks (i.e. the Internet), facilitates the possibility of attacks on this technology.
- It is much easier to hack VoIP network hubs than traditional phone switches. Although hackers cannot intercept voice calls, they can have access to packets traversing the converged network.
- Anyone can record, duplicate and distribute to unintended parties voice calls over IP
- IP Phones have become available for software developers. The increase in features and complexity comes however with a security cost: more applications equal more avenues of attack [13].
- VoIP is vulnerable to call interception attacks which have not previously been a security issue with circuit-switched networks where tapping requires physical access to the system. Therefore tapping is a serious concern in IP telephony when compared with the traditional telephony environment.

Solution

VoIP Call Interception gives attackers the ability to listen and record private phone conversations by intercepting both the signaling and the media stream.

The attacker is also able to modify the content of the packets being intercepted acting as a man in the middle. In principle this threat affects both the signaling and the data depending on the ability of the attacker of intercepting both [13].

Due to the fact that voice travels in packets over the data network, hackers can use data-sniffing and other hacking tools to identify, modify, store and play back unprotected voice communications traversing the network, thus violating confidentiality and integrity. A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a particular collision domain. This packet sniffer application can reside in a general-purpose computer attached, for example, in a local area network [10]. For example, the tool "voice over misconfigured Internet telephones" (a.k.a. “vomit”), takes an IP phone conversation trace captured by the UNIX tool tcpdump, and reassembles it into a wave file which makes listening easy [14, 15], using MP3 or alternative audio files. The reassembled files can be collected later, emailed or otherwise sent on to the eavesdropper.

Figure 5 shows the sequence of the steps necessary to monitor a VoIP conversation (Figure 1 shows the units involved). With tcpdump, hackers can identify the IP and MAC addresses of the phone to be attacked By using an Address Resolution Protocol (ARP) spoofing tool, the attacker could impersonate the local gateway and the IP phone on the network, creating a default gateway [14]. This allows RTP streams to and from the target IP phone to be monitored by the attacker.

The communication between the Gateway and Gatekeeper is equally vulnerable to call interception using the same techniques described for terminals devices. The RTP streams can be intercepted between the IP end-stations or between the Gateway and Gatekeeper (IP Trunk) [16].

Likewise, the FragRouter tool would have to be enabled on the attacking machine so the data packets would reach their ultimate destination. If the hacker has access to the local switched segment, he may be able to intercept a call by inserting a phone into the voice segment with a spoofed Media Access Control (MAC) address, and assuming the target phone's identity.

Consequences

The success of this attack implies:

- It is possible to listen in on a conversation by intercepting the unencrypted media stream between the two terminal devices.
- Attackers may use telephone systems for divulging crucial information such as Social Security numbers, Credit Card numbers or other confidential information. Inside a company, eavesdropping could allow access to confidential business information.
- Hackers could capture the packets and decode their voice packet payload between two or more VoIP terminal devices.
- Due to the fact that voice travels in packets over the data network, hackers can use data-sniffing and other hacking tools to identify, modify, store and play back unprotected voice communications traversing the network, thus violating confidentiality and integrity.
- A hacker breaking into a VoIP trunk has access to many more calls than he would with traditional telephone tapping. Consequently, he has a much greater opportunity of obtaining useful information from tapping a VoIP data stream than from monitoring traditional phone systems.
- Call interception attacks result in the attacker being able to use the intercepted data for other malicious intents, such as: call pattern tracking, number harvesting, and conversation reconstruction [13].
- The interception and modification threat results in the attacker being able to modify the packets for malicious actions, examples are:
  - *Call blackholing* - the attacker intentionally drops essential packets (e.g. INVITE) of the VoIP protocol resulting the call initiation to fail;

- *Call rerouting* - the attacker redirects the packets on a different path in order to include unauthorized nodes in the path or to exclude authorized ones from it;
- *Conversation alteration* - the attacker alters the packets in order to modify the conversation between two users;
- *Conversation degrading* - the attacker intentionally drops a selection of packets or modify the content of them with the objective of degrading the overall quality of the conversation [13].

Possible sources of failure include:

- Call Interception is somewhat limited because it would require physical access to the local network or remote access to a compromised host on the local network.
- Intercepting voice traffic as it crosses the Internet is more difficult because once the packetized voice hits the carrier, it becomes much harder to single out among other traffic.
- It is more difficult to intercept calls on VoIP networks than capturing and reading text messages on public networks.

Countermeasures and Forensics

The attack can be stopped or mitigated by the following **countermeasures**:

- Call interception is mitigated by encrypting the sensitive data being transferred using an encryption technique such as secure sockets layer (SSL), IPSec, or secure shell (SSH).
- In order to improve performance, it is better to use encryption at routers or other gateways instead of at terminal devices.
- Use the Secure Real-time Protocol, a profile of the Real-time Transport Protocol (RTP) which offers confidentiality, message authentication, and replay protection for the RTP and RTCP traffic [12]. This end-to-end encryption is performed at the media level.
- Use the Secure VoIP Channel pattern [11] which hides the meaning of messages by performing encryption of calls in a VoIP environment.

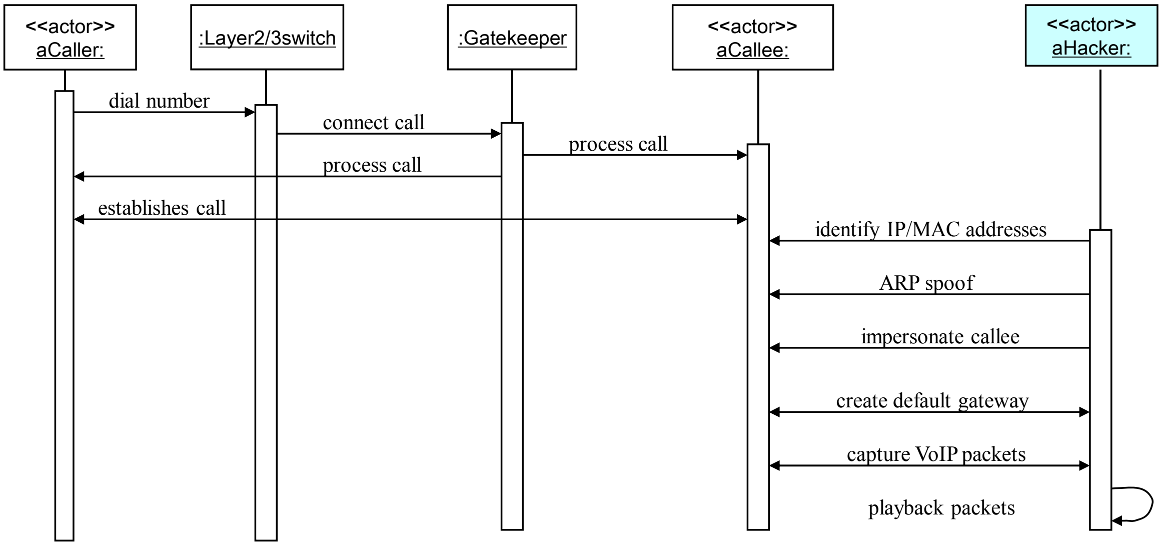

Figure 5 Sequence diagram for a call interception

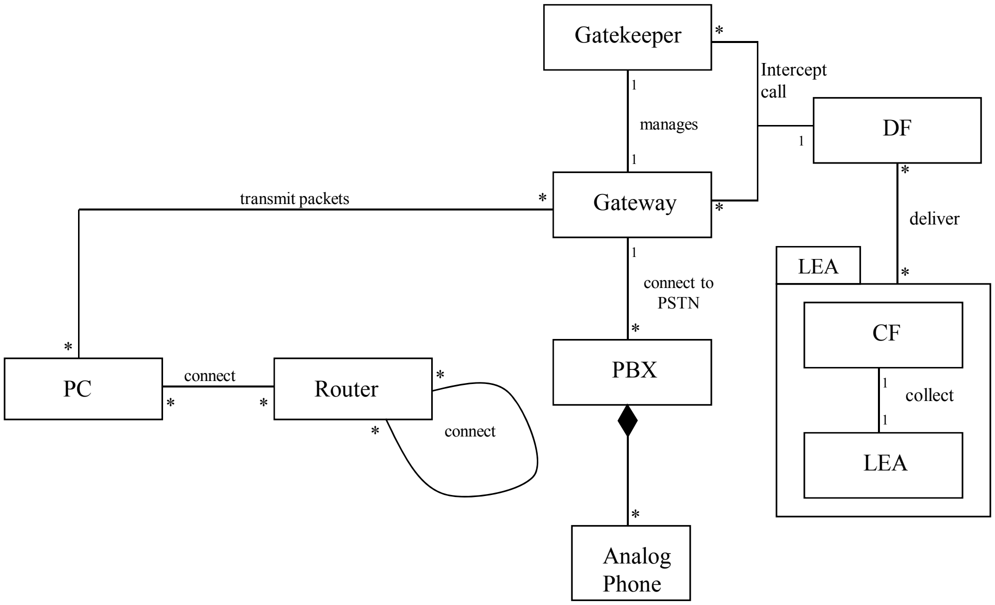

Figure 6 Class Diagram for CALEA Model

- Use the Network Segmentation pattern [11] which performs separation of the voice and data services to counter possible attacks against the voice VLAN by an attacker in the data VLAN. Using network segmentation, an attack aimed at the data network (i.e. against softphones) won't impact critical voice traffic and vice versa.
- Use the VoIP Tunneling pattern [11] which provides a way of guaranteeing the confidentiality and integrity of calls in IP telephony by the encapsulation of data from one protocol into the protocol stream of another.

Likewise, the following **network forensics** mechanisms are possible:

- Use packet sniffers (also referred to as network monitors or packet analyzers). A packet sniffer may be installed on any VoIP component or inter-network link to monitor VoIP traffic. Packet sniffers are good tools for network investigators who want to monitor the information that enters and leaves the system.
- Use Network Forensic Analysis Tools (NFAT), which typically provide the same functionality as packet sniffers and protocol analyzers. NFAT software is primarily focused on collecting and analyzing network traffic [17].
- The collection of data in real time and the use of automatic mechanisms are also useful when conducting network forensics investigations in a VoIP environment.
- With the appropriate tools, investigators could capture the packets and decode their voice packet payloads in order to analyze VoIP calls.

Where to look for evidence

Based on Figure 4, the following may be considered secondary sources of forensic information in a VoIP environment: Terminal devices (i.e. softphones, hardphones and wireless VoIP phones), gatekeepers, and gateways.

Known Uses

Government Surveillance is a special case of call interception. Communications Assistance for Law Enforcement Act (CALEA) is another term for this electronic surveillance. It means that the legal enforcement agent taps into a communication channel to intercept, but not alter, the information [15]. The wiretap facility is based on the MAC address of the cable modem so it can be used for either data or digitized voice connections. This feature is controlled by the interface command, cable intercept, which requires a MAC address, an IP address, and a UDP port number as its parameters. When activated, the router examines each packet for the desired MAC address; when a matching MAC address is found (for either the origination or destination terminal device), a copy of the packet is encapsulated into a UDP packet which is then sent to the server at the specified IP address and port.

Figure 6 shows how the CALEA model components (i.e. Delivery Function, Collection Function and Law Enforcement Agency) integrate with a VoIP system providing a transparent lawful interception. Calls are routed via an access gateway that hides any intercepts in place.

Wiretaps fall into two categories. *Call detail* is a tap in which the details of the calls made and received by a subscriber are passed to LEA. Call records generated from signaling messages can be very valuable in criminal investigations. Signaling messages provide data about phone calls - not the content of phone conversations. Therefore, collecting and analyzing signaling messages may not be subject to the same legal restrictions as recording voice conversations [18]. In the second kind of tap *Call content,* the actual contents of a call are passed to LEA. The suspect must not detect the tap, so the tap must occur within the network and not at the subscriber gateway. Also, the tap may not be detectable by any change in timing, feature availability or operation.

In order for LEA to tap the content of calls without the subscriber noticing any change, all calls must be routed via a device competent in duplicating the content and passing it to that agency.

Hepting v. AT&T is a United States class action filed in January 2006 y the Electronic Frontier Foundation (EFF) against the telcom company AT&T, in which the EFF alleges that AT&T permitted and assisted the United States Government in unlawfully monitoring the communications of a large part of the USA, including AT&T customers, businesses and third parties whose communications were routed through AT&T's network, as well as VoIP telephone calls routed via the internet [19]

Lawful interception requirements in many countries could prevent a public carrier from allowing direct connection between IP phones [20]. With regard to fighting terrorism, support for CALEA over IP is a matter of special concern because many terrorist activities have taken place by using the Internet. VoIP services that cannot be monitored and lawfully intercepted may be used to perform criminal or terrorist activity. Thus, lawful interception in VoIP is vital for national security but because it threatens user's privacy it must be performed only in authorized cases.

Related Patterns

Several patterns for defending against these (and related) attacks are listed in [4], [11]. A pattern can be developed to describe similar attacks on SIP networks.

4. MISUSE PATTERN: THEFT OF SERVICE IN VOIP

Intent

The Theft of Service pattern provides an opportunity for hackers to gain access to the VoIP network by imitating subscribers and/or seizing control of terminal devices and performing free calls.

Context

The VoIP system should have adequate capability (i.e. routing, bandwidth, and QoS) to meet the peak communication load. The system may have a minimum set of perimeter defenses, e.g. a firewall. Some VoIP systems use control protocols (e.g. MGCP and Megaco/H.248) and security mechanisms, in order to manage the Media gateways deployed across the infrastructure as well as to make it difficult for an attacker to overcome system resources. In a converged network both the signaling and media traffic must be monitored. Similarly, secure VoIP implementations use cryptographic algorithms to protect the media packets. Theft of service attack (a.k.a. IP telephony fraud) is intended against service providers.

Problem

An unauthorized user wants to make expensive phone calls without paying for them. The attack can be carried out taking advantage of the following **vulnerabilities**:

- Theft of service attacks may be caused by inadequate security mechanisms in VoIP, the insertion of malicious software that modifies the normal behavior of terminal devices, and the unauthorized connection of devices to the network.
- It is possible to charge calls to another user's account by using stolen user identification details.
- Phone usage and billing systems can be manipulated by fraudulent telephone users in order to make profit.
- The benefits of portability and accessibility introduced by IP Telephony have a downside of an increased risk of service theft [16].
- When using "Hoteling," the primary protection against theft of service in the traditional telephony environment, the physical security of the handset, is no longer enough [16].
- Unattended IP telephone.
- Rogue telephones can be installed.
- MAC addresses are easy to spoof.
- Authentication data is disclosed by the legitimate user.

Solution

This attack could be accomplished using several techniques. An attacker may just simply want to place calls using an unattended IP phone or assuming the identity of the legitimate user of a terminal device. The attacker uses the identity of the owner (i.e. identity theft) without the owner's consent. She then charges the call to the owner's account. A more complex method is when the attacker place a rogue IP phone on the network or use a breached VoIP gateway to make fraudulent calls.

In a service volume fraud, the attacker injects in the network more traffic than what declared in the session request in order to avoid paying for the used resources [13].

Theft of service can also be perpetrated using falsified authentication credentials. A number of IP Telephony vendors authenticate their end points via Ethernet media access control addresses (MACs). MAC addresses are notoriously easy to spoof. [16]. An attacker might impersonate as an IP Telephony signaling server and "request" an end-device to perform authentication before dealing with its call request. Using the end-point's IP Telephony network credentials the malicious party will be able to authenticate to any IP Telephony based server as well as to place free of charge phone calls.

Figure 7 shows the sequence of the steps necessary to commit theft of service in VoIP (Figure 1 shows the units involved). First, the attacker uses a brute force attack to find the special prefixes that Internet phone companies use to identify authorized calls to be routed over their networks. The attacker then looks for vulnerable ports and routers in private companies and gets their IP addresses. On finding vulnerable ports, she hacks into the network to get administrator names and passwords. The attacker then reprograms the routers to allow them to handle VoIP calls, and to masquerade the true source of the traffic. The attacker then routes her calls to the targeted network via the routers she has hacked, and then sends the calls from the targeted network to Internet phone service providers. She may also attach the access codes to the calls, so that the Internet phone providers believe they are legitimate calls. Finally, unauthorized calls will go through successfully and will be completed over the Internet phone provider networks.

Another method of attack is by receiving an application in a spam email, or accidentally downloaded from the Internet. This application can direct the phone to call premium rate numbers by installing itself on a softphone (i.e. applications installed on user systems with speakers and microphones). Finally, the reduction in costs for Moves, Adds, and Changes (MAC) in an IP Telephony environment has led to the addition of daemons/services on many vendors IP Telephones. Some of the more popular services include HTTP, SNMP, and Telnet. [16]. Attackers may take advantage of the benefits of portability and accessibility introduced by VoIP to perform theft of service. “Hoteling” is one of the most popular features of VoIP, it consist of moving all the features, including address book, access abilities and personalized speed dial from one phone to another [16]. When using hoteling, the physical security of the IP phone is no longer enough.

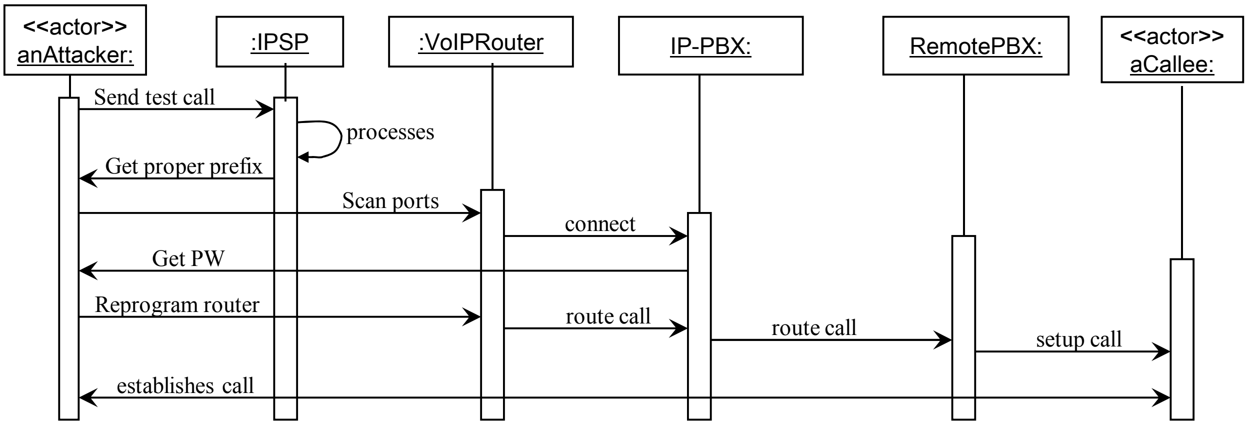

Figure 7 Sequence diagram for a Theft of Service attack

Consequences

The success of this attack implies:

- In order to make expensive calls to premium rate numbers, rogue devices could be attached to an organization's network without the user's knowledge.
- Weaknesses in wireless security policies could also be exploited by rogue devices.
- Unauthorized phone calls will seem to originate from subscribers inside the attacked VoIP network.
- Attackers could also steal minutes from VoIP service providers and resell them on the black market.
- Attackers will be able to register for unauthorized services taking advantage of the virtual communication paths in IP networks.
- In IP telephony, premium rate numbers will be dialed automatically.

Possible sources of failure include:

- Threats and attacks can be defined and theorized but are difficult to carry out in practice, mainly due to the lack of knowledge and testing opportunities for attackers.

Countermeasures and Forensics

The attack can be stopped or mitigated by the following **countermeasures**:

- Authentication of terminal devices and users to the VoIP system. Use of the Authenticated Call pattern [11] coupled with device identification measures will help prevent unauthorized access.
- The IP-PBX will prevent unknown terminal devices from being configured protecting the VoIP system from theft of service
- Limited administrative access to IP-PBXs and VoIP gateways
- VoIP call servers should be configured to reduce the opportunity for dial-through fraud.
- Guard log-on details and install anti-virus solutions to stop malware infecting IP phones.
- When signaling message is being used to generate billing information, a good user authentication is necessary in order to provide non-repudiation mechanisms for service providers.
- Repudiation attacks can take place when two parties talk over the phone and later on one party denies that the conversation occurred. This type of attack is not common and it can be easily mitigated with Challenge-response based client authentication – a cryptographic process that proves the identity of a user logging onto the network – can also ensure that only authorized personnel are able to use the phone system.

Likewise, the following **network forensics** mechanisms are possible:

- Comparing traffic patterns against predefined thresholds (Threshold-based analysis) is a method used to compare how much data is sent to the user and how much he actually pays for it [21]. Such information can be obtained from primary evidence sources like routers or IDS systems.
- In order to reconstruct and analyze the inappropriate VoIP network usage, examiners can use data from network traffic collectors.
- NFAT tools to monitor call patterns and events to ensure that vulnerabilities in VoIP are not being exploited and to identify those that are.

Known uses

Edwin Andres Pena of Miami, FL, USA hacked into the networks of Internet telephone providers and fraudulently sold more than 10 million minutes of VoIP calls in June 2006 [22]. Likewise, a Panamanian telecom lost $110,000 due to phreakers [23].

Related patterns

The Theft of Service in VoIP pattern has direct relationships to the following misuse patterns:

- The Call Hijacking in VoIP pattern which will be presented next.
- The IP Spoofing in VoIP pattern.
- The Call Interception pattern which was previously introduced.

CONCLUSIONS AND FUTURE WORK

Misuse patterns can guide forensic examiners in the process of searching for evidence. They could also serve as a structured method for obtaining and representing relevant network forensics information. They are particularly useful in cases where criminals break into a VoIP network segment that is not monitored by network security devices. Therefore, investigators should look for evidence in other network components (e.g. terminal devices) considered as secondary data sources. An misuse pattern is also an important technique that helps examiners to ensure that they have considered all possible contexts and evidence sources by using the proposed template.

We consider the context or environment as part of the pattern, a pattern for VoIP using the SIP protocol or using a fixed network would be a different pattern. This is because we want to relate specific events or data with specific parts of the network. Preconditions for an attack would be part of the context. Because of the association with system components, we think that our approach is useful to define where defenses are needed and where to look for evidence of attacks. Developers are familiar with patterns and using this type of patterns should be easy for them when looking for ways to correct the security of the system. The fact that each pattern corresponds to a specific attack would make easy the selection of which security pattern to use once the possible attacks to the system are determined using a method such as [24] or similar. Their value for forensics comes from having an indication of where to look for attack data, which components of the network may be more useful to find evidence, and which parts of the network should have additional capabilities to collect forensic data. The systematic structure provided by the template is useful to organize information and compare the effects of different attacks. Some of the methods described in this section can be complementary and it is worthwhile to look for possible combinations.

4. Acknowledgements

We thank our shepherd Sami Lehtonen for valuable comments and suggestions that significantly improved this paper.

5. References

[1] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie. “Attack patterns: A new forensic and design tool.” Proceedings of the Third Annual IFIP WG 11.9 International. Conference on Digital Forensics, Orlando, FL, Jan. 29-31, 2007.

[2] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal. Pattern-Oriented Software Architecture: A System of Patterns, Volume 1, West Sussex, England: John Wiley & Sons, 1996.

[3] M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating Security and Systems Engineering, Wiley 2006.

[4] Z. Anwar, W. Yurcik, R. Johnson, M. Hafiz and R. Campbell. “Multiple design patterns for Voice over IP (VoIP) security”, Procs. of the IEEE Workshop on Information Assurance (WIA 2006), Phoenix, AZ, April 2006.

[5] Wieser C., Röning J., Takanen A. "Security analysis and experiments for Voice over IP RTP media streams". Proceedings of the 8th International Symposium on Systems and Information Security (SSI'2006). Sao Jose dos Campos, Sao Paulo, Brazil. November 08-10, 2006.

[6] M. Collier.“The Value of VoIP Security”, July 2004. Online at http://www.callcentermagazine.com/shared/printableArticle.jhtml?articleID=22103933 (last accessed 10 June 2007).

[7] The Communications Research Network (CRN). “VoIP loophole aids service deniers?” February 2006.

[8] Ellis, J. “Voice, Video and Data Network” Academic Press, Amsterdam, 2003

[9] S. Vuong, Y. Bai. “A survey of VoIP intrusions and intrusion detection systems.” Proceedings of the 6th International Conference on Advanced Communication Technology, August 2004.

[10] E.B. Fernandez and A.Kumar, “A security pattern for rule-based intrusion detection”, Procs. of the Nordic Pattern Languages of Programs Conference (VikingPLoP 2005)

[11] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie 2007. Security patterns for Voice over IP Networks. Journal of Software 2, 2 (August 2007), 19-29.

[12] A. Mihai. “Voice over IP Security: A layered approach.” March 2006. Online at http://www.xmcopartners.com/whitepapers/voip-security-layered-approach.pdf (last 25 May 2007).

[13] S. Niccolini. ‘VoIP Security Threats.” Internet-Draft, NEC SPEERMINT Working Group. March 1, 2007.

[14] N. Pogar. “Data Security in a Converged Network” July 23, 2003. Online at http://www.computerworld.com/printthis/2003/0,4814,83624,00.html (last accessed 18 June 2007).

[15] S. Scoggins. “Security Challenges for CALEA in Voice over Packet Networks”. April 16, 2004. Online at http://www.interesting-people.org/archives/ interesting-people/200412/msg00044.html (last accessed 7 June 2007).

[16] A. Klein. “Security Analysis: Traditional Telephony and IP Telephony.” Assignment: v.1.4b. SANS Inst., Apr.2003.

[17] National Institute of Standards and Technology, “Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response”, August 2005.

[18] T. Moore, A. Meehan, G. Manes, and S. Shenoi. “Using Signaling Information in Telecom Network forensics.” Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005

[19] Wikipedia, the free encyclopedia. Online at http://en.wikipedia.org/wiki/Hepting_vs._AT&T (last accessed 17 June 2007).

[20] P. Drew. “Next-Generation VoIP Network Architecture” March, 2003. Online at http://www.msforum.org/YaBB.pl?num=1077906803/0 (last accessed 24 May 2007).

[21] The International Engineering Consortium. “Fraud analysis in IP and Next Generation Networks.” Web ProForum Tutorials. Online at http://www.iec.org/tutorials/fraud_analysis/ (last accessed 16 May 2007).

[22] D. Searcey, S. Young. “Arrests Reveal Vulnerability Of Web Phone Service to Fraud.” The Wall Street Journal, June 8, 2006.

[23] B. Sutherland. “Stealing Minutes.” Newsweek International, March 19, 2007.

[24] E.B. Fernandez, M.M. Larrondo-Petrie, T. Sorgente, and M. Van-Hilst, “A methodology to develop secure systems using patterns”, Ch. 5 in “Integrating security and software engineering: Advances and future vision”, H. Mouratidis and P. Giorgini (Eds.), IDEA Press, 2006, 107-126