**Milestone 1.2**

**VoIP Vulnerabilities**



1. **Confidentiality threats**

Confidentiality means that the information cannot be accessed by unauthorized parties. The confidential information of end users includes private documentation, financial information, security information like password, conversion content, conversion history or pattern, etc. The confidential information for network components includes operation systems, IP addresses, protocols used, address mapping, user records, etc. Leak of this information might make attackers’ jobs easier.

**Eavesdropping of phone conversation**

Conventional telephone eavesdropping requires either physical access to tap a line, or penetration of a switch. With VoIP, opportunities for eavesdroppers increase dramatically because of the large number of nodes in the path between two conservation entities. If the attacker compromises any of these nodes, he can access the IP packets flowing through that node. There are many free network analyzers and packet capture tools that can convert VoIP traffic to wave files. These tools allow the attackers to save the conversation into the files and play them back on a computer. VoMIT (Voice over Misconfigured Internet Telephones) is an example of such a tool. Ethreal can also be used to record SIP packets and retrieve voice message in wav file format.

**Unauthorized access attack**

Unauthorized access means that the attacker(s) can access resources on a network that they do not have the authority. Shawn Merdinger reported multiple undocumented ports and services in certain VoIP phones. There are also vulnerabilities due to implementation issues. There are systems for call control, administration, billing and other voice telephone functions. Repositories in these systems may contain passwords, user identities, phone numbers, and private personal information. Lots of gateways and switches are shipped with default well-known passwords. If these passwords are left without changes, the attackers can easily break in. Some switches still use TELNET for remote access. The clear-text protocol exposes everything to anyone who can sniff the network traffic. Some of the gateways or switches might have a web server interfaces for remote control. The attacker might sniff the HTTP traffic in local network to steal sensitive information. Attackers can also use ARP cache poisoning to forward all traffic through their machines to capture network traffic.

1. **Integrity threats**

Integrity of information means that information remains unaltered by unauthorized users. A legitimate user may perform an incorrect or unauthorized operations function and may cause delirious modification, destruction, deletion or disclosure of switch software and data. An intruder may masquerade as a legitimate user and access an operation port of the switch.

**Registration Hijacking**

Registration hijacking happens when an attacker replace the legitimate registration of the victim with his address. The attack causes all incoming calls for the victim to be sent to the attacker’s address. Registration is normally performed using UDP, which make it easy to spoof registration requests. For example, Alice wants to register her address at registrar using SIP protocol. The “REGISTER” message looks like the following:

REGISTER sip:alice@atlanta.com SIP/2.0

Via: SIP/2.0/UDP 192.168.2.10; branch=z9hG4bK776asdhds

Max-Forwards: 70

To: Alice

From: Alice;

Call-ID: [a84b4c76e66710@192.168.2.3](mailto:a84b4c76e66710@192.168.2.3)

CSeq: 314159 INVITE

Contact: Alice; expire=60

Content-Type: application/sdp

Content-Length: 142

**Proxy impersonation**

Proxy impersonation attack tricks the victim into communicating with a rogue proxy set up by the attacker. Once an attacker impersonates a proxy, he has complete control of the call. Figure 8 illustrates proxy impersonation. The attacker tricks Alice to communicate with the rogue proxy server instead of the legitimate proxy server. The UAs and proxies normally communicate using UDP and do not require strong authentication to communicate with another proxy. The attack can work by several means, including DNS (Domain Name Service) spoofing, ARP (Address Resolution Protocol) cache spoofing, DHCP spoofing, or changing proxy address for a SIP phone.

**Call redirection or hijacking**

Call redirection occurs when a call is intercepted and rerouted through a different path before reaching the destination. Possible methods include proxy impersonation and registration spoofing. The attacker can also spoof the response from the recipient and trick the requestor to talk with the attacker.

1. **Availability threats**

**VoIP signaling DoS attacks**

The attackers can abuse signaling protocol to conduct denial of service attacks. In first case, the attackers can create large number of call setup requests that consume the processing power of proxy server or terminal. One example is shown in Figure 10(a) where Tim sends way too many “invite” requests to Bob and Bob cannot take request from Alice. This type of DoS attack does not have same LAN requirement. It only needs large volumes of requests to flood the victim. The attackers can also launch distributed DoS to cover trace and aggregate requests. In the second case, the attackers use cancellation of pending call set up signals including sending a CANCEL, GOODBYE or PORT UNREQACHABLE message. This causes the phone not being able to complete calls or hang up. This type of attacks is aided by the complexity of the signal protocols. University of Oulu in Finland has developed simple SIP and H.323 protocol test suites and run them against several implementations. The results were “alarming”, indicating that virtually all of the testbed components failed [20]. Figure 10(b) shows an example where CANCEL message is spoofed by the attacker to prevent call setup. Figure 10(c) gives an example where spoofed GOODBYE message tear down the established connections. One correctly crafted packet can tear down the call. However, this attack does require the attacker to be able to fill certain headers of the message correctly. The attacker can gather network data to extract this information.

**VoIP media DoS attacks**

Attackers can flood gateway, IP phone and other media processing VoIP components with large number of RTP packets. If the target is forced to drop RTP packets, the voice quality will degrade. Furthermore, the attacker might knock key components like gateway offline. A failure in one of these devices could bring the entire voice network to a halt. Since RTP is encapsulated in UDP, it is easy to craft.

**Physical DoS attacks**

These attacks include power outrage and physical damage to network components. Traditional telephone operate on 48 volts supplied by the telephone line itself and can operate smoothly during a power failure. VoIP cannot operate without power supply. Also, an attacker with physical access to any key components of VoIP network can disrupt its normal operations easily. He can plug out the power cord or network cable.

References:

1. <https://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701>
2. https://www.sans.org/reading-room/whitepapers/voip/voip-security-vulnerabilities-2036