Security threats in VoIP

Now that VoIP is widely accepted and becoming one of the mainstream communications technologies, security has become a major concern. Let's take a look at the threats faced by VoIP users today.

In the early stages of VoIP, there was no major concern about the security issues associated with its use. People are primarily concerned with the cost, functionality and reliability of VoIP. Now that VoIP is widely accepted and becoming one of the mainstream communications technologies, security has become a major concern.

Security threats are even more worrisome when we think that VoIP is replacing the oldest and safest communications system the world has ever known - POTS (Plain Old Telephone System). Let's take a look at the threats faced by VoIP users today.

Identity and service theft

Phreaking is a type of hack that steals a service from a provider or uses the service but transfers the cost to others. Encryption is not common in SIP (assuming the role of authenticating VoIP calls), so user credentials are easily stolen.

Identity and service theft
Eavesdropping is the way most hackers use to steal information. Through eavesdropping, third parties can obtain names, passwords and phone numbers, allowing them to gain control over voicemail, call forwarding and payment information. This leads to what is known as service theft.

Stealing login information to make calls without paying is not the only reason behind identity theft. Thieves do it to gain valuable information such as business data, access to secret elements such as voicemail and do personal things like changing call forwarding numbers, etc.

Vishing

Vishing is another way of writing Phishing, which involves a party pretending to be a trusted organization (e.g. a bank), calling you and requesting confidential, important information.

Virus and malware

VoIP is just as vulnerable to malware as any other program
The use of VoIP involves smartphones and software, being susceptible to worms, viruses and malware, just like any Internet application. Running on user systems such as PCs and PDAs makes mobile applications vulnerable to malicious attacks.

DoS (Denial of Service)

A DoS attack is an attack on a network or device, denying service or connecting. An attacker consumes bandwidth or overloads the device's internal network or resources.

In VoIP, DoS attacks overwhelm the target with unnecessary SIP call messages, thereby reducing service quality.

When the service is down, an attacker can gain remote control of the system's administrative facilities.

SPIT (Spamming over Internet Telephony)

If you use email regularly, you probably know what spam is. Put simply, spam is emailing people against their will. These emails are mainly related to online sales. Spam in VoIP is becoming more common.

Each VoIP account has an associated IP address. Spammers can easily send messages (voicemail) to thousands of IP addresses. Spam clogs up your voicemail box, so better voicemail management tools become necessary. Spam messages can also carry viruses and spyware.

This brings us to another variation of SPIT, phishing over VoIP. These phishing attacks include sending a voicemail to a person, forging information from a trusted party to the recipient, such as a bank or online payment service, making the target think they are safe. This voicemail usually requires confidential data such as passwords or credit card numbers.

Call tampering

Call tampering is an attack involving ongoing phone call spoofing
Call tampering is an attack involving ongoing phone call spoofing. For example, an attacker could only ruin call quality by transmitting jamming packets into the communication stream. He can also handle the distribution of packets so that communications become abnormal and the participants spend extended periods of silence during the call.

Man-in-the-Middle attack

VoIP is particularly vulnerable to man-in-the-middle attacks, where an attacker blocks the SIP message traffic that signals the call and spoofs as the calling party to the called party or vice versa. When the attacker does this, he can hijack the call through a redirect server.