VoIP Security - Does it exist?

by Sheran Gunasekera

VoIP is becoming one of the hottest services being offered by start up providers and adopted even by large telecommunications corporations in order to lower their operating costs. But how secure is VoIP really? Scanit R&D Labs conducted extensive research on VoIP security and found the truth to be a little startling.

The pace at which technology has developed and the reduction in price of computer and network equipment has contributed significantly to the evolution and advancement of home networks. The recent penetration of broadband connectivity to the household has grown rapidly and it has become progressively easier to "get connected". With broadband on the rise, the requirements for bandwidth hungry implementations such as Video or Voice over IP have been easily met. This has meant that concepts such as video blogging, podcasting, streaming internet video and VoIP have managed to gain a strong foot-hold in present day online services.

What is VoIP?

VoIP or Voice over Internet Protocol is the term used for voice conversations that are routed over the Internet or via an IP based network. While the fundamentals between VoIP and PSTN (Public Switched Telephone Network) remain more or less the same, the protocols used in each implementation differ. VoIP relies on protocols such as H323 or SIP for the purpose of signalling and RTP (Real-time Transport Protocol) for Media transmission.

RTP is a UDP protocol where a stream of voice data is sent from one IP to another. The voice data is encoded in one of several existing codecs depending on voice quality or bandwidth required in the implementation. Some of the more popular codecs are: GSM, G723 and G729. The codecs that take up a little extra bandwidth offer call quality that far exceeds a standard telephone line.

Signalling: Signalling protocols handle all aspects of setting up a call initiating media delivery and tearing down a call after it is complete. SIP has a very similar HTTP style "Request" and "Response" system complete with SIP response codes such as 403 – Forbidden or 404 – Not found.

VoIP presents significant advantages to the end-user in terms of being extremely cost-effective and easy to setup. Several VoIP providers have popped up all over the place offering international call rates at least 6 to 10 time cheaper than regular PSTN IDD calls. All an end-user would have to do is to download a softphone client, install it on their PC, charge their account online through their credit card and start dialling their relatives in far away countries. The simplicity involved is far too tempting to resist and by this, the number of VoIP users is on a sharp increase. VoIP is not without its flaws by any means. Users also have to put up with bad call quality, network congestion and billing issues, but the disadvantages are far outweighed by the advantages. One more disadvantage of VoIP is its security.

The team at Scanit R&D Labs have conducted a significant amount of research into VoIP and it's inherent vulnerabilities. Broadly, VoIP attacks can be divided into two groups: Signalling attacks and Media stream attacks. We tested the most popular SIP routers that are being used by the majority of VoIP providers and uncovered some startling results.

Signalling attacks can be used to eavesdrop on conversations and re-route or hijack calls. Due to the fact that the SIP protocol presently does not support message integrity, it is extremely easy to re-play or re-send SIP messages to the SIP registrar or proxy and have it perform functions such as adding another client to a conversation or re-routing of a call. Since SIP messages are also sent over a clear-text channel, it becomes a trivial task for an attacker to perform ARP poisoning and inspect, intercept and modify all SIP messages on the local network.

An example of Registration Hijacking

A typical SIP REGISTER Message will have fields similar to the following

REGISTER: rdlabs.scanit.net: 5061 SIP/2.0	FROM: 01-141337 <sip:01141337@ rdlabs.scanit.net>	TO: 01-141337 <sip:01141337@ rdlabs.scanit.net>	CONTACT: 01-141337 <sip:01141337@ 192.168.133.7:5061>

A message similar to this will always be used by a client to announce itself to a SIP registrar. Once announced, the SIP registrar is aware of the client's location and the fact that it is ready to accept calls.

The Contact field is the important field here as it contains the location or IP address of the client being registered. When a call to the above user is placed, the SIP proxy will perform a lookup to ascertain the location of the client. In this particular instance, the user with the phone number 01-141337 can be reached at IP address 192.168.133.7.

An attacker can easily sniff this information, modify it and re-send it to the SIP registrar. Consider the scenario where the above packet is sniffed by an attacker, then modified to look like this:

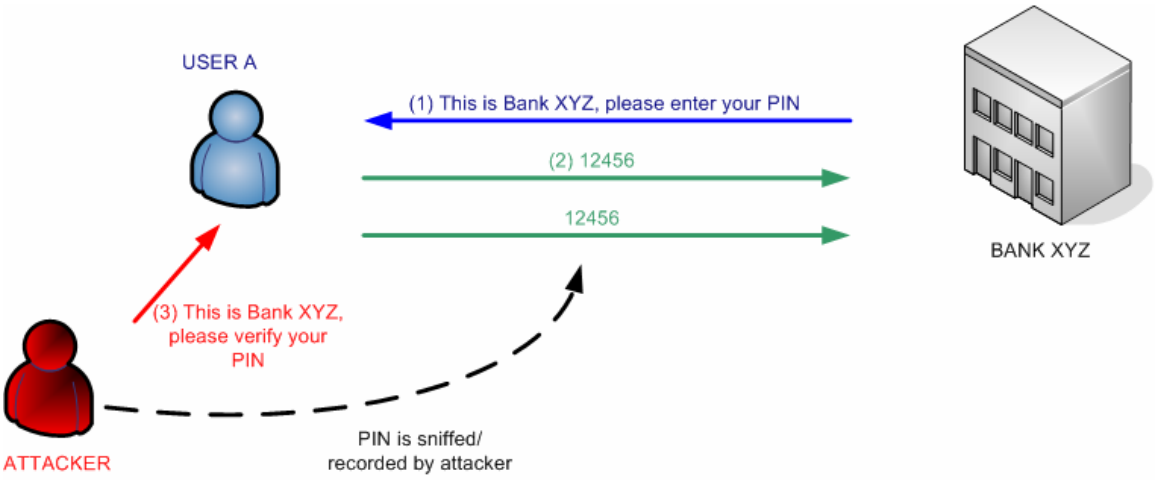
REGISTER: rdlabs.scanit.net: 5061 SIP/2.0	FROM: 01-141337 <sip:01141337@ rdlabs.scanit.net>	TO: 01-141337 <sip:01141337@ rdlabs.scanit.net>	CONTACT: 01-141337 <sip:01141337@ 192.168.39.69:5061>

The packet is re-sent to the Registrar and now any calls made to the number 01-141337 will be routed to IP Address 192.168.39.69 rather than the original IP Address of 192.168.133.7.

Media Stream attacks

Media Stream attacks are as easy to perform in a typical VoIP implementation. As stated previously, voice data is sent over the Real-time Transport Protocol. This is a UDP based protocol which streams voice data from one IP to another. The voice data that traverses an RTP stream is generally encoded by a specific audio codec and not encrypted. This means that any RTP streams intercepted by an attacker can easily be decoded with the relevant audio codec and the actual voice call can be recorded or listened to.

Media stream attacks bring with them their own high risk threats such as injection of data. An instance where data injection can be used effectively could be in a situation where an attacker replays a message to enter a PIN code and then captures the subsequent touch tones which he can use later on.



VoIP is definitely here to stay. However, the rapid deployment of VoIP has seen it progress with little or no attention given to security. While the technological advancements of VoIP have grown by leaps and bounds, security is still left behind to catch up. The vulnerabilities listed in this article are merely a small percentage. Several more vulnerabilities have presented themselves during internal tests and a large number of Proof of Concept attacks have been developed in-house.

This does not mean that larger organizations should abandon the idea of a VoIP implementation. VoIP implementations can be secured with a little effort placed during the design and implementations phases. Being fully aware of the risks involved with VoIP implementations goes a long way into understanding how to secure it.