

Voice over IP Security

Matthew Tanase 2004-03-12

Introduction

As information technology professionals, we are constantly bombarded with new products and ideas claiming to be revolutionary. And for a brief amount of time, a few of these technologies seem to grab all the headlines, in trade magazines, on tech sites and at industry conferences. The technology darling of late is VoIP. Short for Voice over IP, you've likely come across it, probably considered it and possibly deployed it. The hype, deservedly so, is reaching a crescendo as excess bandwidth, improved software and better hardware drive this technology forward. For the right situations, it's a truly wonderful solution. Lower phone bills, virtual offices, centralized management and rapid deployment are just a few of the benefits. And the success of companies such as Vonage and Skype, combined with the growth of wireless networks will move this technology from enterprises to smaller businesses and the SOHO market. Unfortunately, new technologies bring new security concerns. Suddenly, you have the burden of protecting two infrastructures - voice and data. This article will introduce voice over IP concepts and the new security concerns they raise.

Is it better?

Before jumping into the security factors of a voice over IP network, let's examine the rationale behind it. The traditional telephone network, known as POTS (plain old telephone service) or the PSTN (public switched telephone network), served us well for many years. Unfortunately, it was costly, managed by only a few companies and inefficient. Each voice call over POTS uses a unique connection, allotted 64K of bandwidth. We're all familiar with a T1 connection, which has 24 channels and 1.5M of bandwidth (64K * 24). In reality, a quality voice call on one of these channels requires a fraction of the 64K granted to it by POTS. Moreover, a silent moment, or lapses in speech still consume the 64K. VoIP deployments capitalize on the inefficiency of this design. The analog voice signal is digitized, compressed, chunked into packets and sent over a data network. Advanced compression algorithms reduce the bandwidth necessary for a quality voice call to a fraction of the 64K required by POTS. The silence and background noise transmission of POTS can be eliminated as well (although some deployments build this feature in to comfort end users!). As if the bandwidth savings weren't enough, VoIP deployments also reduce cost and enhance scalability by employing standard data networking components (routers, network switches), instead of expensive, complicated telephone switches. Now the

same team handling the data network can manage a voice network - great news for all of you overworked IT staffers.

How does it work?

The process of VoIP is dependent on signaling and media transport. A signaling protocol, such as SIP (session initiation protocol), performs the legwork: locating users, call parameters, modifications and building or ending a session. Media transport protocols, like RTP (real time transport protocol) handle the voice portion of a call: digitizing, encoding and ordering. Networking protocols, such as IP, are wrapped around the VoIP packets when they are transmitted to the proper servers.

VoIP calls can take place between LANs or on WANs, as is the case with internal calls on a corporate network. If a VoIP user wishes to call a destination on POTS, a special gateway is used. These devices act as connectors between the data network and the SS7 network used by POTS. They translate the incoming data into a format the recipient, be it IP or SS7, can understand.

Onto security

With an understanding of VoIP technology and its benefits in place, let's consider the security ramifications. In the process of saving money and increasing efficiency, two crucial portions of any infrastructure, voice and data, were combined. Suddenly, an IT staff is not responsible for securing only standard servers (database, mail, web), workstations and routers. As if these data security concerns weren't enough, VoIP servers acting as gateways, special routers, phones, new protocols and operating systems are now thrown into the mix. The burden of voice and telecommunications security has been shifted from the carrier to the IT team. It has moved from an obscure PSTN, to an IP network every cracker is familiar with. Let's examine the risks and how you can mitigate them.

What are the threats?

Unfortunately, there are numerous threats to a VoIP network, many of which aren't obvious to newcomers. The networking devices, the servers and their operating systems, the protocols, the phones and their software are all vulnerable.

Information about a call is almost as valuable as the voice content. For instance, a

compromised signaling server used to setup and manage calls, might yield the following: a list of incoming and outgoing calls, their durations and parameters. Using just this information, an attacker could map all of the calls on your network, creating complex conversation records and user tracking.

The conversation itself is also at risk and the most obvious target of a VoIP network. By breaching a key part of the infrastructure, such as a VoIP gateway, an attacker could capture and reassemble packets in order to eavesdrop on the conversation. Or even more nefariously, record everything, and replay all conversations occurring on your network. On the PSTN, this would be an impressive feat, since few are skilled enough on or have access to the huge switches managing calls. That's obviously not the case on a data network, as legions of script kiddies prove every day. And if your VoIP packets traverse the Internet to reach a destination, a number of attackers have a shot at your voice data.

The calls are also vulnerable to hijacking or a man in the middle attack. In such a scenario, an attacker would intercept a connection and modify call parameters. This is an especially scary attack, since the participants likely wouldn't notice a change. The ramifications include spoofing or identity theft and call redirection, making data integrity a major risk.

The availability of the VoIP network is also a major concern. On the PSTN, availability is rarely a problem. Attackers would need to overload some very large circuits or cut a connection. It's much easier to thwart a VoIP network. All of us are familiar with the crippling effects of distributed denial of service attacks. If directed at key points of your network, it would disrupt your ability to communicate via voice or data.

The phones and servers are targets themselves. Although as a whole they mimic phones, they are, at the core, computers with software. Obviously, this software is vulnerable to the same types of bugs and exploits that hamper every operating system and application available today. Code could be inserted to perform any number of malicious actions.

VoIP security and defense

How anticlimactic. I point out the wonders of voice over IP and follow them up with major security problems! Fortunately, the situation is not without remedy. The risks outlined above, while specific to VoIP, are all issues we deal with on regular IP networks. Unfortunately, in the initial rollouts and designs of voice related hardware, software and protocols, security was not a

major concern. But that's usually the case with every new technology, a fact that we are all working to change. Let's examine some of the tried and true workarounds that can alleviate the threats outlined above.

The first thing that should come to mind reading about VoIP is encryption. While it's not easy to capture, reassemble and decode voice packets, it can definitely be done. Encryption is the only way to prevent such an attack. Unfortunately, it adds overhead, eating up or eliminating altogether the bandwidth reductions from traditional voice calls. This, in turn, affects throughput and performance - which can introduce dreaded jitter into the call. So what can you do? There are multiple encryption options - VPN setups, the IPSec protocol and other protocols such as SRTP (secure RTP- though it does not offer any authentication features like VPNs, it does encrypt voice packet payloads). The key however, is to choose a fast, efficient encryption algorithm and employ a dedicated encryption processor. This should alleviate any performance concerns. Another option would be strict QoS standards for VoIP packets on your network and powerful hardware. Such QoS requirements will ensure that voice is always handled in a timely manner, reducing the chance of degraded quality.

Next, as should be expected, would be the process of securing all elements of a VoIP network. You'll be dealing with call servers, routers, switches (you're not still using a hub that can be sniffed!), workstations and phones. You need to perform regular assessments on each of these devices to ensure they are in line with your security demands. The servers should have minimal jobs running and only the necessary ports open. The routers and switches should be configured properly, with access control lists and filters in place. All of the devices should be up to date in terms of patches and upgrades. These are the same types of precautions you would take when adding new elements to your existing data network, just extend the process to the VoIP portion as well.

As mentioned, the availability of your VoIP network is a concern as well. Unlike POTS, a power loss will bring your network down -- so make sure prolonged redundancy options are in place. DDoS attacks are always difficult to defend against. Aside from proper router configurations, make sure you have an escalation process in place with your IP carrier, since many times they are needed to assist. Remember, such an attack would not only halt your data services, but voice as well.

Lastly, you can employ a firewall and an IDS to help protect your voice network. A VoIP firewall is a difficult beast to manage due to the ever-changing requirements. Call servers are

constantly opening and closing ports for new connections. This dynamic element makes rule management difficult, even on stateful devices. But the costs are far outweighed by the benefits, so spend some time perfecting your access controls. An IDS can assist in monitoring the network for any anomalies or potential abuses. Early warnings are key to preventing larger attacks.

Conclusion

As evidenced by the explosive growth of the voice over IP market, this technology will work its way into your businesses and networks. It carries with it however, the new burden of voice security. Careful planning and architecture, borrowed from our data security experiences, can help mitigate the risks and amplify the returns.

About the author

[Matthew Tanase](#) is President of Qaddisin (www.qaddisin.com). He and his company provide nationwide security consulting services. Additionally, he writes for the [Security Blog](#), a daily weblog dedicated to network security.

View [more articles](#) by Matthew Tanase on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus