VoIP Security – Methodology and Results

Barrie Dempster - *barrie@ngssoftware.com*

An NGSSoftware Insight Security Research (NISR) Publication

http://www.ngssoftware.com

Abstract

As VoIP products and services increase in popularity and as the "convergence" buzzword is used as the major selling point, it's time that the impact of such convergence and other VoIP security issues underwent a thorough security review. This presentation will discuss the current issues in VoIP security, explain why the current focus is slightly wrong, then detail how to effectively test the security of VoIP products and services. With examples of real life vulnerabilities found, how to find these vulnerabilities and why many of them shouldn't be there in the first place.

Table of Contents

VoIP Security Issues

Introduction to VoIP Security

VoIP has become an integral part of most networks and has brought with it some security issues, these issues however, are not entirely new. In order to effectively secure a network with VoIP, the efforts involved are not significantly different to securing any other suite of protocols. For example, databases have vulnerabilities in their implementation, their configuration and their operating platform. VoIP is no different in this respect, if we take a systematic look at any networks security configuration we can assess and respond to security threats effectively.

VoIP is given extra attention and breeds an element of fear, uncertainty and doubt. Being in a position of fear and uncertainty is rarely warranted with VoIP, it's security issues can be addressed in much the same way as we address other security issues. In this paper we will cover some of the issues relating to VoIP, explain how to direct focus in assessing VoIP products and networks.

Why is VoIP such a big problem ?

It's not. It's just perceived that way as it is a slightly different problem. For example when looking for vulnerabilities in a Web application server or a database server a certain amount of probing and parsing the output can be effective. You can for example find issues such as SQL injection, cross site scripting, command execution etc... There are a variety of techniques for finding these issues there are relatively few issues that database and web application scanners don't have some method of identifying. With telephony there is a lot of manual verification involved. It's quite likely that a VoIP system that has a clear vulnerability will go unnoticed with current VoIP assessment tools.

It's also an area of the industry where experience in multiple disciplines is generally required. In order to understand a VoIP system there are a number of components to understand. For example, in order to complete an effective VoIP security assessment, knowledge of data networks, voice/telephony networking and an overall security background is required.

Convergence

big selling point - big security risk

Convergence, VoIPs favourite buzzword. The selling points of convergence have been presented time and time again. However, from a security point of view and even from a stability point of view convergence is bad!

From the NIST Security considerations for Voice over IP systems:

> *“The flexibility of VOIP comes at a price: added complexity in securing voice and data. Because VOIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VOIP system than a conventional voice telephone system or PBX.”*

When designing a network with security in mind, one of the most common protection mechanisms is to physically and logically segregate the network. For most businesses network stability, service level and security are amongst the most important factors. Converging networks can be bad for each of these. This adds to the perceived complexity of VoIP deployments, where it shouldn't.

Dealing with VoIP within the network is no different with dealing with mail routing, web access and databases. The components have to be setup in a manner that is logically and physically in keeping with the organisations requirements. The simplest way to do this with VoIP is to keep it separate from from data components, configure products appropriately, document and assess regularly. It's the assessment portion that we will cover in this paper, but the point of safe convergence is worth noting.

The Threats

Toll Fraud:

The threat most likely to make the news, is that of toll fraud. A very high dollar value can be placed on toll fraud, the cost of the services used and resource allocation for clean up can add up. It's fairly common for toll fraud to be reported as costing hundreds of thousands or millions of dollars. This threat is often the most important in the eyes of a large organisation. A successful theft of service from a large organisation can go unnoticed for quite sometime, allowing the attacker to rack up a large bill at the organisations expense. However, toll fraud is also quite easy to accomplish, simple configuration problems in a dial plan can allow this and lines left open for test purposes and remote access can be abused by an attacker. These issues are often difficult to identify as it can be quite time consuming and inconvenient to scan for them.

It's very profitable from the point of view of the attacker to commit toll fraud as once the attack is complete there are no real costs involved and the attacker can abuse the services quite rapidly, by reselling them for example.

Eavesdropping:

Eavesdropping is not limited to VoIP services, it's not even limited to voice it's a general communications problem. It is given a lot of attention when it comes to VoIP for a number of reasons. Firstly, VoIP calls are not encrypted, in general. There are plenty of encryption options from PKI to using add-ons such as zfone, however there is a layer of incompatibility. If you want to communicate with a web server, you're web client could negotiate a TLS/SSL encryption method fairly easily and use an appropriate algorithm. This issue isn't entirely solved when it comes to VoIP. The fragmented nature of VoIP implementations means that encryption is very difficult to implement. There's also no easy solution to ensure end to end encryption, with end points as diverse as traditional telephones, Skype and zfone before we even consider the multitude of other VoIP protocols in use, this isn't a simple problem. Even with the encryption options available not all VoIP providers offer them in an attempt to keep resource usage on their services low.

Another issue that enhances the threat of eavesdropping is the number of peers in the conversation. In order for VoIP to reach it's potential as a useful piece of technology for the user it has to be mobile. This leads to the user requiring VoIP access at locations such as coffee shops, which introduces more peers to the conversation. The security of the VoIP conversation is also dependant on the security of the coffee shop, their ISP and the other peers in between.

Caller-ID spoofing

There are now so many options for spoofing caller-ID that it has become a fairly easy thing to do, you can do it with no technical knowledge as many providers sell this as a service. Like many of the threats related to VoIP this problem was present prior to VoIPs popularity. With VoIP however caller ID spoofing has got a lot easier and a lot more anonymous than it ever was before. Sadly it's still not an issue that the general public are aware of, even though it is now decades old.

Denial of Service

Uptime on telephone networks is generally very high. Telecommunications providers give us a fairly impressive uptime, when compared to ISPs and content providers. When it comes to communications using the telephone we are accustomed to always being able to pick up the phone and get a line. This has meant that VoIP customers have high expectations from their providers and therefore VoIP providers have high expectations when it comes to their infrastructure. The trouble with this, is that, the traffic is using the Internet as it's transport. This can be extremely problematic as it exposes the VoIP infrastructure to all the denial of service issues associated with being Internet connected. It's expensive and can be quite difficult to combat attacks such as distributed denial of services and this can have a knock on effect to the price of VoIP communications, which is already a business with a decreasing profit margin.

This also affects how VoIP is used, as many providers will not allow use of VoIP for calling emergency services.

Another Entry point.

This issue is the one that we will focus on in the next section as we discuss a method for effectively assessing VoIP infrastructure and products for security. This is where VoIP is currently moving as more vulnerabilities are being discovered in VoIP products and as researchers take on VoIP both as a tool and as a target.

So we've heard that the IP network causes problem for VoIP services, but what issues does using VoIP itself bring ?

The foremost issue when it comes to adding VoIP to any infrastructure is it's impact on the infrastructure. When functionality is added to a network it often brings with it extra complexity, which is not always beneficial to the security posture.

Taking even the simplest VoIP deployment of a single server with a few clients. The network has to incorporate :-

More services exposed externally – The public face of an organisation needs at the very least, some email contact and a website. Some organisations offer more, but these are arguably the two most common communication methods for an organisation. The threats involved with these are pretty well understood and there are all sorts of vulnerabilities in web servers, web browsers, email servers and email clients. These pieces of software are attacked very often and have all undergone a variety of upgrades and rethinks on features in order to protect them. These minimal services provided by most organisations (hosted or otherwise) have historically been a major focus for vulnerability research and as the initial attack vector. The reasoning behind this from the attackers point of view, is that an exploit in popular software will be very valuable. Exposing services such as VoIP along side these increases the administrative overhead and increases the attack surface and as VoIP itself becomes more popular it becomes another target for the attacker to focus on in order to gain the important first step in to the network in order to complete their attack.

More clients in use – Going hand-in-hand with the HTTP and SMTP services, we have the web browsers and email clients, which have evolved to incorporate all sorts of added complexity and these clients became a focus for attackers and were again used as an initial attack vector. VoIP clients are as complicated, sometimes more so, than email clients and there is fierce competition in this market.

This has led to a large number of buggy clients being available which could be quite a risk to an organisation. Many of these clients will fall over with not much more than gentle prodding from the most naïve of fuzzing tools. VoIP vendors could and should learn from the mistakes of the vendors of web/email software, but as it stands they haven't. The push is “features, features, features” with less emphasis on security. This is why we need third party add-ons to help with security.

Complicated and numerous Protocols – Just taking two of the most common protocols (SIP and H.323) we find very complicated, wide in scope RFCs, some of which are not very easy to understand for the software developer. This leads to one of security's biggest enemy, the assumption. When software developers start assuming something will work a certain way, or messages will be sent in a certain order then the scope for vulnerability increases.

Assessing VoIP

Where the current focus is

The current focus of publicly available VoIP security research and publications focuses quite heavily on the protocols and how they are implemented. In order to address some of the issues we are faced with when it comes to VoIP this has to change. There is a lot more to VoIP security than encryption, which takes much of the focus in this arena just now. The encryption problem isn't universally solved as we have seen, but it is receiving proportionate attention. In order to fully address VoIP security we must also address the other relevant threats.

Where more focus is needed

We will focus on the issues that VoIP really does bring to a network and how we can address them. There is also a little bit of focus on identifying vulnerabilities based on software versions, however this is still in it's infancy. Comparing the availability of tools that scan general purpose operating systems, databases and web applications to those that scan VoIP, there is an extreme difference in quantity and quality. In order to properly assess a VoIP network or a VoIP product a well thought out methodology is required. In the next section we will have a look at a way to assess VoIP, allowing us to understand the security posture of the network and remove some of the fear, uncertainty and doubt.

Breaking it down into it's components

VoIP, like any sufficiently complicated service, can be broken down into a number of components. These components can then be assessed fairly easily using established techniques, tools and methods. It is then quite easy to identify where there is a lack of research in a particular area. This presentation is the result of just such an approach and reinforces the point that whilst VoIP is not a trivial problem, it's far from the headache it is perceived as. When looking at a VoIP deployment and assessing it's security posture, we can identify clear key areas and decide upon the best approach for these. We will look at each component and discuss techniques for assessment.

Operating Platform

The definition we will be using for “Operating Platform” is the surrounding infrastructure relating to the VoIP system and the VoIP system itself. For example VoIP services will have a reliance on other networking components such as switches, routers, basic TCP/IP services such as DNS, DHCP and so on. We can look at these as separate issues, but since our VoIP network will be segregated for security purposes, as will it's infrastructure. Therefore, we must address the infrastructure as part of a VoIP assessment, while treating it as a sub-component of the network.

What exactly does our VoIP system run on ?

This is information which would come from general footprinting of a network. In any assessment there will generally be a footprinting stage, this isn't very specialised when it comes to VoIP and standard tools can be used. There are also a few VoIP specific tools, which are out of scope for this paper.

Once we have identified what sort of VoIP setup we have then we can look further at the details and what's involved.

The architecture of the VoIP system

Generally, VoIP services are provided by a dedicated device or a piece of software running on a general purpose OS.

In the case of the general purpose OS our approach is fairly simple, we assess it as we would during any infrastructure assessment. So if it's a Windows host we consider configuration of shares and patch levels. Following our standard procedures for identifying services, additional applications etc.. It's at this point we will identify any VoIP services present and prepare to work on these later.

The dedicated devices get a bit more interesting and they bring up my first point about focusing VoIP research. What we find with these devices is that they are based on an architecture that has expanded from traditional telephony systems to incorporate VoIP functionality. Taking a Siemens Hicom system as an example, the PBX would be a traditional PBX until a VoIP telephony card is added and it becomes VoIP enabled.

With these devices there are a number of issues to be covered and a number of access points. They can be assessed much like a traditional OS, however a vulnerability scanner for these OS's is unlikely to pick up many vulnerabilities, firstly as few have been reported and secondly because the signatures just aren't there for these devices. This is the first area that has been neglected with VoIP security research up until now. To address this, security research could be more focused on finding vulnerabilities in these systems.

Previous VoIP security discussion and presentation has quite neglected this area and there are a number of good reasons. It's difficult and expensive to test these systems as you can't just download the software and install it, you're going to need the hardware and a good understanding of how it's configured within an organisation.

There is now a fair bit of competition in this market, so the price has fallen and the barrier to buying equipment for research purposes has lowered. There is also an increased understanding, in general, amongst those with an interest in organisational security, when it comes to VoIP telephony and it's integration into a network.

The current state of VoIP revolves around protocol implementations, encryption and standards. The future however is going to (or at least should!) involve more focus on the architecture itself with vulnerabilities being identified in VoIP products. This focus is slowly shifting and we are seeing research on VoIP products come through as they mature. We will look at VoIP vulnerabilities found in a particular product later and see how these relate to other aspects of network security.

Surrounding Infrastructure

VoIP assessments should be accompanied by a thorough infrastructure security assessment. It's essential when auditing VoIP that we also look at the infrastructure that supports the VoIP deployment. If the VoIP network is separated from the data network, then a lot of it's infrastructure will be separated. In this configuration it's important to keep in mind that whilst the infrastructure assessment doesn't differ much from infrastructure to support other services, we still have to carefully examine it with VoIP in mind.

There are a number of support protocols and services for VoIP deployments, these include

- TCP/UDP/IP
- DNS
- TFTP
- HTTP
- DHCP
- STUN
- SDP
- SNMP
- etc....

There is a variety of different ways these protocols are used and they can be used and abused within the network. When analysing the infrastructure supporting VoIP we will come across these protocols and this is why a VoIP assessment must allow scope for assessing related infrastructure. The best example I can give for this is remote access. VoIP systems have remote access from a few different angles, most commonly dial-in and over another Internet connection. If this is configured incorrectly, it could mean that a compromise of a VoIP PBX over a dial-in connection would lead an attacker in to the core of the internal network. It's very common to have a front-end/back-end configuration with web/database/email servers but less common when it comes to telephony implementations. When it comes to security, partitioning the infrastructure like this, makes it much easier to control access and security boundaries. This approach has been adopted by those designing networks, quite fully, but telephony systems are neglected all too often.

A solution to this problem is to bring telephony systems in-line with an organisations current security requirements and ensure that they apply the same logic to all entry points.

Proprietary Protocols

Although we have some extensive research going on when it comes to SIP and H.323 there is very little attention being paid to the other lesser known protocols involved.
Many of the VoIP vendors have protocols in use with their software and hardware.
Examples being Nortel's UNISTIM and Mitels MiNet among others.

Protocols other than SIP or H.323 are often seen as the fringe protocols with no notoriety attached to them, therefore unimportant. However not paying attention to the other protocols and their implementations seriously hinders a security assessment. When assessing VoIP infrastructure and coming across these protocols there is little in the way of tools and previously identified vulnerabilities – this does not mean these vulnerabilities don't exist, it means researchers are not currently paying attention to them and specific tools such as fuzzers aren't publicly available.

The VOIPSA threat taxonomy which exists to give details of the threats to look out for in a VoIP network, ignores many of the proprietary protocols, yet does include protocols such as HTTP. While VoIP systems do have a reliance on standard protocols such as HTTP, there is also a need to mention, link to and advise on the other protocols involved and how to deal with them in such a taxonomy.

Databases/Web Services/CRM

A VoIP system will often rely on a database for storage of configuration and calling information. There are also web interfaces for managing the VoIP software or for end user access. Call centres will often have a web based customer contact system which performs functions such as “screen popping” of customer details for incoming and outgoing calls. These additional applications which are installed to support the VoIP infrastructure also require attention during an assessment. Where a client has considered scope for assessing the VoIP application they often neglect the back end systems supporting the application. These applications will often have a number of vulnerabilities.

Configuration

Current documentation and discussion on VoIP security, as we have discussed, focuses on protocols. However one of the most important aspects of a secure telephony system, VoIP or otherwise, is a robust configuration. There is little point in having a well segregated, well protected network infrastructure if with the touch of a few buttons an attacker can make international calls at the expense of the organisation.

When it comes to auditing the configuration of a VoIP system it's not often feasible to exclusively use war diallers and scanning software. The most effective way to assess the configuration is to look directly at the configuration. By this we mean, viewing the configuration files/database directly. Most VoIP systems have a feature allowing you to download and view the configuration. At this point a detailed understanding of the particular VoIP equipment is required. This configuration should also be compared to any written policy on telephony use, so that policies such as “call centre agents aren't allowed to make outgoing calls” can be checked. An automated scanner will not pick up this information as it won't be aware of the relationship between extensions, users and what they should or should not be allowed to do.

An effective technique for analysing the configuration is to draw out the relationships between the objects in the dial plan. This helps visualise the relationships within the system and quite often will help identify some basic vulnerable configurations, especially if the vulnerability appears due to multiple levels in a hierarchy.

Default Passwords

Are we still banging on about default passwords in 2007? Yes, sadly we are. Telephony systems are the worst offenders when it comes to this issue. Of the telephony systems I've used and assessed around 50% of them have a default password issue when it comes to the management interfaces and if we include default and easily guessable passwords on voicemail this figure is near to 100%. Administrators and users of telephony systems just do not want to use complex passwords.

Bad Dial Plan Logic

This issue has to be addressed differently based on the specific system. Generally the more options a PBX has for controlling dialling logic, the more issues there are to find. This is also the area where a diagram of the configuration comes in handy. Configuration issues and breaches of policy can be seen quite easily. Eg.. Inbound Agent is a member of Agents group, Agents group is a member of Inbound and Outbound callers, but Inbound Agent isn't supposed to be allowed to make outbound calls. This example, contrived as it may seem, is actually quite common.

Call Control and Monitoring

There are a number of different issues to identify when it comes to call control and monitoring. Call forwarding is an ongoing issue in telephony.
Can users forward an incoming call to an outside line?
What happens if a user asks to be forwarded to extension 011/00 (International dialling digits)
Can the system be brought down with call forwarding loops?

Call monitoring, which should only be accessible on privileged lines or to privileged users can be configured incorrectly allow all users access to the feature or even external callers if they hit the right key combination!

Accounting and Billing

Alongside a PBX there are also commonly accounting and billing systems which are most often web based with a database back end These add more databases and web servers to the infrastructure. The nature of the accounting and billing system means that they are accessed by systems and users who may not be direct users of the PBX itself. This means that these systems can't be entirely separated from the rest of the infrastructure and can be a cross over point between the infrastructure supporting the PBX and the rest of the internal network.

Exploiting VoIP

The VOIPSA threat taxonomy details numerous threats to VoIP, from the relatively mundane denial of service attack, to physical intrusion and extortion! Neglecting to mention the simplest and most likely threat presented to an organisation with their VoIP infrastructure

It's another entry point in to the data network. This is an extremely important aspect is not only worth mentioning in the threat taxonomy but worth covering in extreme detail. So if we take a look at what the VoIP service brings to our network.

Looking at Asterisk as an example of a VoIP PBX and the vulnerabilities that it has we see the following vulnerabilities.

The Vulnerabilities

Source - Open Source Vulnerability Database (http://www.osvdb.org)

Denial of Service vulnerabilities

- Asterisk SIP Channel Driver (chan_sip) SIP Malformed UDP Packet DoS
- Asterisk Manager Interface Passwordless User MD5 Authentication DoS
- Asterisk Malformed SIP INVITE Request DoS
- Asterisk Crafted SIP Response Code handle_response Function DoS
- Asterisk Malformed SIP Register Packet Remote DoS
- Asterisk SIP Channel Driver Unspecified Remote DoS
- Asterisk IAX2 Call Request Flood Remote DoS
- Asterisk chan_iax2 IAX2 Channel Driver Unspecified DoS

Code execution vulnerabilities

- Asterisk T.38 SDP Parser chan_sip.c process_sdp Function Overflows
- Asterisk pbx/pbx_ael.c Extension Language (AEL) Generation Weakness Arbitrary Extension Execution
- Asterisk Skinny Channel Driver get_input Function Remote Overflow
- Asterisk MGCP Malformed AUEP Response Handling Remote Overflow
- Asterisk Record() Application Remote Format String
- Asterisk JPEG Image Processing Overflow
- Asterisk Manager CLI Command Overflow

These vulnerabilities are almost exclusively within the protocol implementations of Asterisk and it;s very obvious that SIP has received a lot of attention by researchers. A number of vulnerabilities have been found through a combination of fuzzing and source code analysis.

This highlights the importance of analyzing the implementations of the protocols and checking the PBX software for common vulnerability classes. It's worth noting here the number of simple overflow type vulnerabilities found in Asterisk. This shows that these well known vulnerability classes are still present in modern day PBX systems and that VoIP vendors have not learnt from the mistakes of other vendors.

Using the recent chan_sip overflows as an example:

Two closely related stack based buffer overflows exist in the SIP/SDP handler of Asterisk, the vulnerabilities are very similar but exist as two separate unsafe function calls. The T38FaxRateManagement and T38FaxUdpEC SDP parameters can be exploited remotely leading to arbitrary code execution without authentication. In order for these overflows to occur, t38 fax over SIP must be enabled in sip.conf. Examples of SIP INVITE packets are shown below, however these vulnerabilities can be triggered with a number of different SIP messages affecting calls received by Asterisk, or in response to calls made by Asterisk.
Remote Unauthenticated stack overflow in Asterisk SIP/SDP T38FaxRateManagement parameter
A remote unauthenticated stack overflow exists in the SIP/SDP handler of Asterisk. By sending a SIP packet with SDP data which includes an overly long T38 parameter it is possible to overflow a stack based buffer and execute arbitrary code.
The process_sdp function of chan_sip.c in Asterisk contains the following vulnerable call to sscanf.

```
else if ((sscanf(a, "T38FaxRateManagement:%s", s) == 1)) {
found = 1;
if (option_debug > 2)
ast_log(LOG_DEBUG, "RateMangement: %s\n", s);
if (!strcasecmp(s, "localTCF"))
peert38capability |= T38FAX_RATE_MANAGEMENT_LOCAL_TCF;
else if (!strcasecmp(s, "transferredTCF"))
peert38capability |= T38FAX_RATE_MANAGEMENT_TRANSFERED_TCF;
```

and...

```
else if ((sscanf(a, "T38FaxUdpEC:%s", s) == 1)) {
found = 1;
if (option_debug > 2)
ast_log(LOG_DEBUG, "UDP EC: %s\n", s);
if (!strcasecmp(s, "t38UDPRedundancy")) {
peert38capability |= T38FAX_UDP_EC_REDUNDANCY;
ast_udptl_set_error_correction_scheme(p->udptl,
UDPTL_ERROR_CORRECTION_REDUNDANCY);
```

This shows a classic buffer overflow in possibly it's simplest form. This vulnerability was only recently disclosed! Even though multiple vulnerabilities have been discovered in Asterisk over the past few years, this simple bug persisted for a few years without being identified. these have been identified and publicly exposed.

There are many more to find

Asterisk being an open source project and being fairly accessible means that it has received a fair amount of security researcher intelligence. The closed source products have similar vulnerabilities and very few of them have been found and reported as yet. Attackers and researchers should and will be focusing more on these PBX systems in order to identify and report these vulnerabilities.

Summary

Practise safe convergence
Ensure that the convergence associated with VoIP applications does not negatively impact on the rest of the unfrastructure.

Apply traditional network security logic to VoIP
The problem of VoIP security can be tackled in much the same way as security in other areas. However particular attention has to be paid to auditing configurations to identify vulnerabilities that vulnerability scanners are unlikely to pick up.

VoIP clients and servers are an important entry point
The public face of an organisation needs at the very least, some email contact and a website. Some organisations offer more, but these are arguably the two most common communication methods for an organisation. The threats involved with these are pretty well understood and there are all sorts of vulnerabilities in web servers, web browsers, email servers and email clients. These pieces of software are attacked very often and have all undergone a variety of upgrades and rethinks on features in order to protect them. For example email clients are more wary about HTML and external linking, handling file types appropriately and so on.

So how does this relate to VoIP ?

VoIP brings to the network, VoIP services and VoIP clients. Much the same as HTTP, even so far as SIP being very HTTP like in basic design.

VoIP vendors haven't learned from other vendors mistakes
It could be argued that VoIP vendors will have learnt from the mistakes of the software of the past and is designed using more secure coding practises. Therefore we don't need to cover these basic issues and should focus more so on other VoIP issues such as eavesdropping, man in the middle attacks and so on. This isn't the case however as evidenced by some of the simple vulnerabilities present in VoIP clients and services.