# VoIP Security Methodology and Results

NGS Software Ltd

*Barrie Dempster – Senior Security Consultant* *barrie@ngssoftware.com*

# Agenda

- VoIP Security Issues
- Assessment Methodology
- Case Study: Asterisk

# VoIP Security Issues

## Why is VoIP such a problem ?

- If you take a systematic approach to it, it isn't

- Assessing VoIP systems is quite different from the “probe and parse” technique commonly used on databases and web applications.

- It appears this way as it's multi-discipline -

  Data networks, voice networks and security knowledge

# Convergence!

- One of the major selling points but one of the biggest issues

  Goes against current network security best practise.

  Firewalls, VPNs, VLANS etc.. are focused on separation of traffic, often to separate into security boundaries

- Convergence not only makes administration easier, it makes hacking easier too

  Voice traffic on a data network is open to attacks using tools and techniques that have been used in the past on data networks

# A convergence quote

**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.”*

# The Main Threats

- Toll Fraud
- Eavesdropping
- Caller ID Spoofing
- Denial of Service
- Another Entry Point

# Toll Fraud

- It's easy
  - The slightest misconfiguration can lead to toll fraud - Misconfiguration of DISA, Default passwords and simple social engineering.
- It's profitable
  - Free use of services
  - Services can be resold
  - Overheads are low
- It's happening (and has been for a long time)

# Eavesdropping

- VoIP doesn't introduce threats like this, it does make them more likely
  - Traditional/non-VoIP/PSTN networks are not immune to eavesdropping
- VoIP adds more peers to the conversation
  - Coffee Shop, ISP, VoIP provider
  - Misconfiguration and vulnerabilities in any of these can expose you
- Encryption is not used across the board in-fact, very few providers offer it as an option
- VoIP services are becoming fragmented and incompatible
  - Skype/Standard protocols/Supermarkets
  - The solutions to this involve more software and more data manipulation.

    Data manipulation is a common source of vulnerabilities.

# Caller-ID Spoofing

- There are a number of ways to do this
- This is another threat that existed before VoIP but just got easier
- It's still not an attack method that the general public are aware of
  - Many companies still use it as part of an authentication mechanism
- You now need no technical knowledge to spoof Caller-ID.
  - A number of companies sell these services

# Denial of Service

- Uptime on traditional telephony networks is generally very high
  - It's not easy to DoS someone
  - It's not easy to hide your tracks when performing an attack
  - Only a few companies control the access points
- Service Levels for telephony are more important than most IP protocols
  - Emergency services
  - Customers/Users are used to high service levels
- VoIP brings IP's problems to voice
  - IP has suffered many DoS vulnerabilities
  - DdoS is expensive and difficult to combat

## Another Entry Point

- VoIP brings problems to the IP network as well
- It's as bad as email, IM clients and web browsers (which is bad!)
- Complicated/Numerous protocols
- Lots of vulnerabilities already found
- Attackers are finding more

# Methodology

# How we look at it

The issues brought up in VoIP security and throughout this presentation are not new and are not a surprise. Telephony experience and IP experience combined with a security focused mindset are enough to combat these issues.

There is a lot of public coverage of VoIP issues, however the approach to understanding and tackling the problem of VoIP security is similar in concept to database, application, network infrastructure and other areas where security is an issue.

# Focusing Efforts

- The majority of research focus at present is on the protocols and encryption.
- This doesn't address all of the major threats
- Attackers have a different focus and security assessments should have this same focus

# So we break it down into components

VoIP is made up of a number of components, many of these are covered by existing testing methodologies.

- The Operating Platform
- Configuration
- VoIP Protocols
- Support Protocols

# Operating Platform

- Network infrastructure
  - VoIP is supported by a number of devices
  - Firewalls and IDS's for example must be configured for VoIP
- Operating Systems
  - VoIP products often run on their own self contained OS
  - Some are based on general purpose OS's (Linux/Windows)
- Databases/Webservices/CRM
  - VoIP systems depend on these for additional functions
  - Used for call logging, user information, customer management etc...
- Vulnerabilities in the VoIP product itself!

# Configuration

How to assess configuration ?

- Scanning with war diallers and similar software is not enough
- The configuration also has to be manually reviewed, by checking the configuration file/database.
- Charting IVR's and call dialing plans makes vulnerabilities obvious

# Configuration

- Default passwords

  still rampant in PBX's

- Bad dial plan logic

  Users/Callers allowed to acces features/numbers/extensions they shouldn't be able to

- Call Control and monitoring

  Can monitoring and recording functions be abused

  Can forwarding support be abused

- Accounting and Billing

  Sometimes integrated, sometimes external support system, but often have easily guessable account and access code as well as vulnerabilities of their own

# VoIP Protocols

SIP/RTP/RTCP/MGCP/IAX/Skinny etc.....

The basic approach to assessing a protocol implementation:

- Authentication Methods
- Unauthenticated Attacks
- Authenticated Attacks
- Encryption/Signing options

# Support Protocols

- The “IP” component in VoIP is slightly more than IP, it extends to TCP, UDP and supporting protocols like DHCP,DNS, TFTP etc...
- These protocols all have their own issues
- These protocols also have some ideas for solutions (eg.. IPsec,VPN's, IDS/IPS, firewalls etc....)
- Combined with VoIP increase the risk of some of the attacks that can occur
- A VoIP assessment can be done as part of an infrastructure assessment or standalone but standalone assessments should caveat that validity is dependent on infrastructure assessments being performed independantly.

# Case Study: Asterisk

# Why Asterisk as a study subject ?

- It's popular
- It's freely available
- No additional hardware required
- It's open source

# Asterisk: Operating Platform

- Network infrastructure
  - Firewalls will have to be configured to support Asterisk
  - Mail server configuration
  - Basic networking DNS, TCP, UDP, IP etc...
- Operating Systems
  - Runs on Linux so security issues relating to Linux apply to Asterisk.
  - Patching of the OS/Asterisk and other components, file permissions, iptables etc...
- Databases/Webservices/CRM
  - Can have a database backend
  - Commonly integrated with SugarCRM
  - Has a number of web front ends (AsteriskNOW, FreePBX/TrixBox, FOP, MeetMe)

# Asterisk: Vulnerabilities – Denial of Service

- 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

# Asterisk: Vulnerabilities – Code Execution

- 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

# Asterisk: Vulnerabilities – Code Execution

Asterisk T.38 SDP Parser chan_sip.c process_sdp Function Overflows

```
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;
```

---

```
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);
```

# Asterisk: Configuration

- Default passwords

  Very common on Asterisk, as are easily guessable SIP passwords

- Bad dial plan logic

  Dial plan logic in Asterisk can become fairly complex and the flat file format makes it hard to follow, if the dial plan isn't documented (and updated) it can make it easy to make mistakes. Common mistakes in Asterisk include giving access to too many contexts or too many options in a public context.

- Call Control and monitoring

  Asterisk can be configured (MixMonitor) to record calls to a file and these can often be left with lax permissions. Asterisk also has Intrude/Barge functionality with ChanSpy. A misconfigured dial plan can unintentionaly give call monitoring abilities.

- Accounting and Billing

  There are a variety of options for billing with Asterisk, they generally plug in to Asterisk using it's Call Detail Record files. Each of these has their own security considerations.

# Asterisk: VoIP Protocols

- Encryption options ?
- We've already seen simple vulnerabilities in the implementations
- Fairly complicated to configure
- Assumptions made by the developers

# Conclusion

# Configuration

- Practise safe convergence
- Apply traditional network security logic to VoIP.
- Check the VoIP products for vulnerabilities.
- Don't just scan, audit as well!

# Where else can I get more information?

http://www.voipsa.org - The VoIP security alliance released a voip threat taxonomy and have an active mailing list covering VoIP issues

http:/www.nist.gov - US centric but have excellent telephony security references

http://www.voip-info.org - Not particularly security related but a good source of VoIP information.

http://www.osstmm.org - The Open Source Security Testing Methodology Manual. The VoIP component is currently under development.

# Thank You

*http://www.ngssoftware.com/*

# Comments/Questions ?

**Barrie Dempster - barrie@ngssoftware.com**