Secure VoIP – Don't end up speechless

Whitepaper

Voice-over-IP has been on the market for years but with the continuing rollout in the mass market it attracts more and more attention of attackers. This could affect your organization too. With new drivers such as fiber-to-the-home, VoIP spreads into many households – along with that, attackers become more aware of the underlying technology. Attack tools get easier to use and there are some easily exploitable targets which offer a convenient business case for the fraudster.

This white paper addresses security managers, VoIP engineers and CIOs with a technical background. It provides a good overview of possible threats, including some that you might not have thought about yet. Whether it is a new deployment or an existing VoIP platform in your organization, if you use an IP Centrex, IMS or cloud solution, even if you are a service provider, it is now time to reflect if your VoIP environment is ready for the next level of professionalized attacks. Allow your mind to grasp the variety of possible threats by combining the threats from classical TDM voice and everything you have ever seen in IT security popping up on your screen.

The author of this paper, Marco Schnüriger, has been working in the field of Voice over IP for several years. His work as a security consultant for service providers allows him to get an insight of the most commonly used technologies as well as forthcoming attack patterns.

Special thanks go to Oezguer Akkaya, an experienced VoIP engineer and manager whose critical review helped to greatly improve the quality of this paper.

Zürich, 09.01.2012

Contents

Version History

Date	Version	Author	Changes
09.01.2012	1.0	Marco Schnüriger, Protect7 GmbH	Initial version

Learn & Understand

The basis of security lies in the ability to understand how a system works. To secure VoIP, you need to identify and understand the ins and outs of this technology to decide where you need to focus on.

- Identify relevant functions – such as different types of phones (hard-phones, ATA, ITA etc.), protocols in use (e.g. SIP, H.323, MGCP, Diameter), proxies, media gateways, upstream providers, conferencing servers and many more.
- Get to know your platform's communication patterns – how do functions communicate with each other? How do the usual patterns change if a user makes a call, if he forwards a call to another destination, if a call is routed to the PSTN? Testing and sometimes reverse engineering is the key to understand how your deployment works.
- Which protocols and configuration parameters can be set – many security features are optional, such as signaling over TLS. Before you focus on securing specific protocols, see what vendors have to offer for example in an RfP.
- Complexity – The more complicated the system the more potential security vulnerabilities could be introduced due to missing configuration options. A secure VoIP platform is only feasible if the relevant features are identified and configured properly.
- Software changes – IT is not just about hardware, each software update hopefully results in improved functions or enhancements for your system. Unfortunately it sometimes also leads to undesirable changes of existing features, which might not be visible at first sight. Therefore it's recommended you test your system regularly (also in respect to security).
- Customization – If you develop your own software around VoIP, your software department needs to be aware of security issues that come along with the technology.
- Education – Organize security trainings for your key project and engineering employees. Allow them to think like an attacker and provide a test environment which can also be used for security testing.
- Specialize in VoIP features – There's a set of common VoIP features such as call forwarding which are common to every platform, but many systems provide advanced versions of these features. The more you know about these features, the better you understand how an attacker may misuse these features.
- State-of-the-art – Take a closer look at your vendor's software especially the aspects that do not correlate directly with the core VoIP system. Your vendor might be a Telco "pro" and give you all the tools to mitigate fraud, but they might be less skilled if it comes to IT-Security.
- Share Experience – Exchange your knowledge with others in workshops, courses as well as national and international conferences.
- Security Audit – A profound analysis of your system architecture and an assessment of the current risk situation can give you a better overview of your VoIP platform and is a good starting point to identify and reduce primary risks.

Privacy & Safety

Whenever you read something about VoIP or voice security in general, privacy related subjects quickly arise. It is still common for VoIP environments to use protocols that don't provide any means of privacy protection. Depending on your environment and the threat potential, you can take that risk, but for many organizations, this might not be acceptable.

- Protection of data – Protect signaling and media especially when you're outside of your trusted network. Inspect your solution's possibilities. Does it provide secure protocols such as SRTP and SIP over TLS or IPSec?
- Internal eavesdropping – Find out why privacy is important within your company, especially when you plan to implement secure protocols internally. This helps to justify if additional costs are generated. Consider the options an attacker has if he installs a Trojan somewhere in your network and the impact it causes for your company.

- Internal Competition – Are the users of your VoIP platform in some kind of internal competition? This might be the case for outbound call centers where agents try to sell products and get a provision. They could be tempted to listen to what co-workers offer to their customers.
- Think about the upstream traffic – Don't forget to secure the connection to your Telco company, wiretapping may also happen outside of your building.
- Protect company data – if you provide additional information or functions such as corporate address books, SMS, mailbox integration and so on - you should also implement proper access control for these features. Protect your peripheral systems too.
- Educate road warriors – Instruct users about added risks with nomadic usage such as eavesdropping and integrity concerns. This might be especially important if you use a cloud service and thus cannot provide confidentiality and integrity protection for network communication.
- Confidential data – Hide your network topology to protect your core or private network.
- Route emergency calls – make sure emergency calls are signaled correctly and routed via an appropriate gateway. Place a test call to find out if it would work in a real emergency situation.

Authentication & Device Security

After identifying VoIP components, you should go ahead and protect them from internal and external threats. Most of the usual IT security lifecycle topics such as vulnerability & patch management also apply here.

- Isolation – limit the attack surface of your VoIP servers. Place them in a network segment which only allows the necessary traffic to get through. Don't expose your interfaces on public networks. If possible, implement a separate Voice VLAN.
- Application hardening – regularly check the configuration settings of your VoIP software for updates which might have an effect on security. As a rule of thumb, everything which contains the words "maximum" or "minimum" in it might be interesting. Do this both for server and client!
- Internal authentication – Closely inspect the provisioning and authentication process of your devices. Make sure devices must also authenticate against internal VoIP servers.
- Dynamic organizations – provide guidance for temporary offices and keep solutions ready such as properly tested softphone configurations. The natural order of things brings security in people's mind only after an incident occurred.
- External exposure – if your solution must be reachable from public networks, take special care for these interfaces. Monitor traffic closely and implement a session border controller ("VoIP Firewall") if it is a large deployment.
- Decommissioning – check uninstall routines of softphones to make sure VoIP credentials are really deleted.
- VoIP compliancy – Check compliancy in signaling for wanted and unwanted cases (positive and negative testing). This is especially important if you ship and introduce user equipment to your customers or end users. A self-inflicted denial-of-service attack is one thing you definitely never want.
- Software updates – Changes in the software running on user equipment might change the signaling chain behavior and create situations which may allow an attacker to get access to that equipment.
- Physical and logical access – Protect your gateway and directly connected network equipment from physical access.

Fraud & Abuse

Think about the money your platform costs. Now think the other way round and imagine that (almost) everything that costs you money could result in a fraud case. Attackers may also just hack for fun, which makes bad press. But probably the worst case for many companies is espionage.

- Call forwarding – Take precautions to avoid call forwarding fraud schemes such as limiting to a set of valid destination numbers.

- Counters – always implement reasonable upper limits (e.g. max. number of concurrent calls). Set maximum counters to limit the maximum damage possible.
- Number screening – displayed phone numbers are a trusting element. Take the necessary steps to prevent displaying illicit numbers and names.
- Collect and analyze CDRs – this can be a simple Excel file up to a complete fraud analysis engine. This also helps you to detect low-level internal fraud.
- Post-billing – As a service provider you want to make sure that in post-billing cases, your customers are trustworthy. A deposit is no guarantee for a later payment, especially if the fraudster can generate large revenue within a short timeframe. Implement fraud detection systems and monitor them closely.
- Outbound dial plan – Define a simple set of rules of what users are allowed to do. Does everybody really need to call abroad? Is there a need for value-added numbers for every back office employee?
- Unexpected destinations – VoIP allows to dial non-digit destinations. Check the need for this feature and decide whether you need to allow this. User-generated destinations will be logged in your VoIP systems and might harm for example your accounting engines and billing systems.
- React upon fraud – If you detect fraud, your customer might be the victim. Don't just interrupt the connection, it's better to set a reasonable barring set (e.g. limit to local calls).
- Alternative interfaces – most solutions allow configuring settings using a variety of different ways (*-codes, Web-based interfaces). Attackers love these often unknown and thus not protected ways to configure sensitive settings.
- Customization – are your specifically for your needs developed applications secure enough? Do they provide security-sensitive functions? What about an API to an electrical door opener or the dial-up line for the elevator? What about access control for auto responding private video surveillance systems?
- Educate users – make your users think before they blindly follow a social engineer that asks them to press some *-code on their phone. If you haven't limited your maximum counters, one single line can generate a loss of thousands a day.
- Number display – some Telco companies offer possibilities to display any chosen number on the PSTN – make sure your company users cannot directly access this functionality from their workplace.
- Black vs. white lists – Allow users to black list unsolicited numbers. Although not a big problem yet, SPIT (Spam over IP telephony) could gain much attention in the next few years and needs to be on the security radar.
- Criminal call centers – Businessmen in many countries might as well use hacked accounts for their call centers instead of achieving a low cost for international calls only through intelligent routing.

Availability & Business Continuity

Man-made or natural threats limit the availability of your VoIP environment. Classical availability and BCP patterns also apply in the VoIP environment, but the real-time nature of this service makes this a very important point. If your organization has a lot of voice-based customer interaction, you might quickly loose business opportunities.

- Requirements – Define the necessary level of availability for the different components. Don't overlook end devices.
- Protection against DoS Attacks – There's DoS potential everywhere in VoIP. Intruders could attack devices, interrupt RTP streams, generate fake SIP responses, start a DoS attack for voice boxes, block lines and much more. Even your own distributed user equipment can cause harm. A reboot of remotely managed devices or the restart of a gateway could generate an avalanche of requests. Many of these threats can be reduced by implementing secure protocols as well as configuring and operating your VoIP environment with a sense of security.
- Failover techniques – are the VoIP phones able to select another gateway in case of a failure? Will calls be interrupted and is this acceptable for your business? Don't forget other technologies such as DNS which are important parts in the delivery chain.

- Disaster Tolerance – is there a need for geographical redundancy to provide the required availability level of the platform?
- Billing – if you have internal billing requirements or if you are a service provider, you want to make sure that calls are correctly billed. Make sure the billing works properly even if there is a partial or complete outage of the platform.
- Testing – Perform a failover test at least after the initial deployment or with every new major software release.
- Shared components – If you are a service provider, shared components may have an impact to all services in case of a failure as a result of an attack. Be aware of potential service impact and damage.

Glossary

- API – Application programming interface
- ATA – Analog telephone adapter
- BCP – Business continuity planning
- CDR – Call detail record
- DNS – Domain name system
- DoS – Denial of Service
- H.323 – Signaling protocol
- IMS – IP Multimedia Subsystem
- ITA – ISDN telephone adapter
- MGCP – Media Gateway Control Protocol
- PSTN – Public switched telephone network
- RfP – Request for proposal
- RTP – Real-time transport protocol
- SIP – Session Initiation Protocol
- SPIT – Spam over Internet Telephony
- SRTP – Secure Real-Time Transport Protocol
- TDM – Time-division multiplexing
- Telco – Telecommunications company
- TLS – Transport Layer Security
- VLAN – Virtual LAN
- VoIP – Voice over IP