VoIP Security regarding the Open Source Software Asterisk

Prof. Dr. -Ing. Kai-Oliver DETKEN
DECOIT GmbH, Fahrenheitstraße 9
D-28359 Bremen, Germany

and

Prof. Dr. -Ing. Evren EREN
University of Applied Sciences Dortmund, Emil-Figge-Str. 42
D-44227 Dortmund, Germany

ABSTRACT

Enterprises and organizations improve their business processes and drop their infrastructure cost by using Voice-over-IP (VoIP) technology. However, security aspects are often neglected. With the increasing merge of application data and speech data within IP networks new challenges arise for overall network and system security.

VoIP packets are being transmitted over a „shared medium“, i.e., via a network which is shared by numerous subscribers with different profiles and for different services. Under certain conditions attackers can sniff data on the communication path and record VoIP conversations.

This article will demonstrate existing security risks regarding the VoIP technology and present viable solutions and concepts. In this context VoIP standards will be analyzed with respect to their security mechanisms. Because of its growing prevalence especially the open source VoIP solution „Asterisk“ will be analyzed and evaluated against typical security requirements.

Keywords: VoIP, VoIP Security, risks, attacks, Asterisk, H.323, SIP, RTP, SCCP, MGCP, MEGACO, IAX, SIMCO.

1. STATE-OF-THE-ART

IP telephony behaves similar to classical telephony, i.e., the subscriber does not experience a difference. Like in conventional telephony, the telephone conversation comprises three processes: establishment of the connection, transmission of speech, and termination of the connection. However, in contrast to classical telephony VoIP is not connection-orientated. Speech data is transported within IP packets.

Connection establishment and termination is often controlled by a protocol separate from speech communication. This is different in IAX2 – the signaling protocol for Asterisk. A differentiation is given depending on the packet type. Also negotiation and exchange of parameters for speech transmission is dispatched by dedicated protocols.

In an IP network the IP address of the caller device has to be known, however not necessarily the caller’s. There are no fixed subscriber links as it is the case in Public Switched Telephone Network (PSTN). Caller reachability is provided, similar to cellular networks such as GSM and UMTS, by means of a preceding authentication of the caller and associated notification of his actual location (i.e., the IP address).

A fixed assignment of telephone number and IP address is not possible since the subscriber could change his location or different subscribers could use a PC or a terminal, or due to dynamical addressing using Dynamic Host Configuration Protocol (DHCP). This problem is solved by using a registration service the subscriber notifies his actual IP address at. The calling entity (gateway, host or end device of the caller) retrieves the actual IP address of the communication partner via the user name and can establish the connection.

If application and speech data use the same network, the latter is exposed to typical data network attacks. Though, speech data can be encrypted, only few users deploy encryption for specific reasons. E.g., some products do not support encryption, or some users do not know how to configure their equipment appropriately. But one should also consider that encrypting speech data can negatively affect speech quality, which for many users has a higher priority than security.

A VoIP system can be deployed in different ways. There are competing protocols with specific advantages and disadvantages. Securing VoIP systems begins with securing connection establishment in order to guarantee authenticity of the subscriber and avoid/prevent redirecting or sniffing data traffic (media stream). Furthermore, the media stream has to be encrypted in order to avoid sniffing and manipulation. Authentication and encryption requires solid key management.
Interfaces for device configuration should be secured as well, e.g. by means of HTTPS. Additionally, it has to be assured that the arising fees (calls between a VoIP network and a classical telephone network such as ISDN) can be captured properly and that they cannot be manipulated.

Another important issue is the protection of the network against attacks (hacking) and malware (viruses, worms, Trojan horses, etc.), which can be managed with suitable firewalls, intrusion detection systems (IDS), and virus scanners. Furthermore, attention should be paid to defective implementation in VoIP applications software (code), which is responsible for numerous security holes and vulnerabilities.

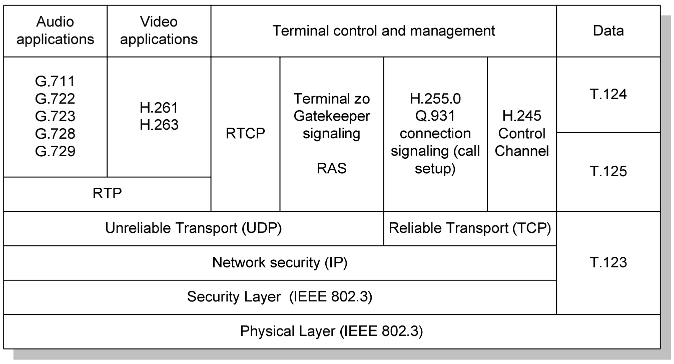
Most common signaling protocols for VoIP are:

- Session Initiation Protocol (SIP), IETF RFC-3261
- Session Description Protocol (SDP), IETF RFC-4566
- H.323 – Packet-based multimedia communications systems, ITU-T-Standard
- Inter-Asterisk eXchange Protocol (IAX)
- ISDN over IP – ISDN/CAPI-based protocol
- MGCP and Megaco – Media Gateway Control Protocol H.248, common specification of ITU-T and IETF
- MiNET – from Mitel
- Skinny Client Control Protocol – from Cisco

Usually, all end devices send speech data directly via the network to the IP address of the communication partner. These data do not traverse the server of a VoIP provider. They are exchanged directly between subscriber end devices.

Real-time data are transported via RTP (Real-Time Transport Protocol) and controlled by RTCP (Real-Time Control Protocol). For transmission RTP normally uses UDP (User Datagram Protocol), because it is a minimal, connectionless network protocol, which does not (unlike TCP (Transmission Control Protocol) provides reliability. This means, that the reception of speech packets is not acknowledged; there is no guarantee for delivery of packets. Compared to TCP, UDP has less packet latency, since erroneous or lost packets are not retransmitted and the sender does not wait for any acknowledgement of receipt leading to a continuous data flow without delays. A total error free transmission is not necessary because speech has a high redundancy and today’s codecs are able to compensate a certain number of errors. For a continues conversation low latency is of higher importance.

Figure 1 depicts the VoIP protocol stack giving a rough orientation according to the ISO-OSI layer model. The focus of this figure is the use of ITU-T signaling protocol standard H.323.



Audio applications	Video applications	Terminal control and management				Data
G.711 G.722 G.723 G.728 G.729	H.261 H.263	RTCP	Terminal zo Gatekeeper signaling RAS	H.255.0 Q.931 connection signaling (call setup)	H.245 Control Channel	T.124
						T.125
RTP						
Unreliable Transport (UDP)				Reliable Transport (TCP)		T.123
Network security (IP)						
Security Layer (IEEE 802.3)						
Physical Layer (IEEE 802.3)						

Figure 1: VoIP protocol stack [DEER06]

Data networks and IP telephony networks have different requirements. In addition to data bandwidth (approx. 64 kbps for an uncompressed speech data stream), quality of service (QoS) parameters such as latency, jitter, and packet loss impose considerable impact on speech quality. Through prioritization and suitable network scaling, it is possible to control QoS.

2. ASTERISK

Asterisk [ASTE07] is an open source software product, which provides all functions of a conventional PBX. It runs on Linux, BSD, Windows (emulated) and OS X. It supports different VoIP protocols and can be interconnected with PSTN, ISDN (BRI, PRI, E1 or T1) by means of relatively low priced hardware. Asterisk has been developed by Mark Spencer from Digium[1]. However, important extensions and applications originate also from other developers. The Asterisk software has been published under the GNU General Public License, which pushes its rapid worldwide development and distribution. That means many manufacturer of VoIP software PBX systems use Asterisk today and do not invest more time into own development.

Figure 2 illustrates the modules and protocols implemented in Asterisk.

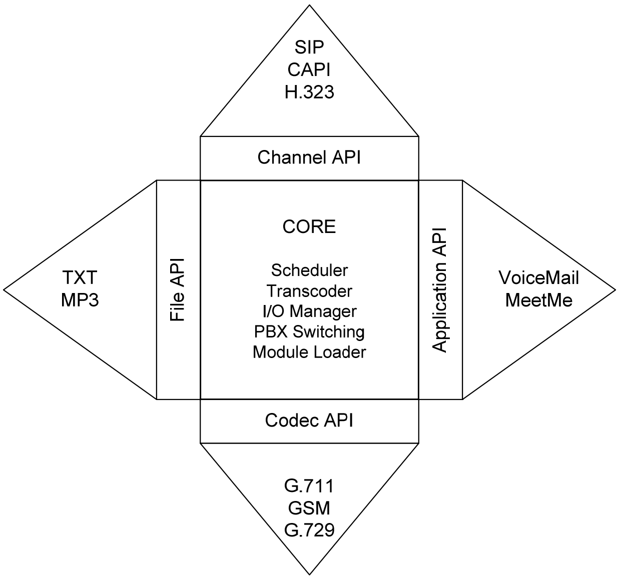


Figure 2: Asterisk modules and protocols [KESS06]

Some of the basic functions of Asterisk are:

- Dial plan, which can be individually configured and extended by additional applications. Herewith, it is possible to decide how an incoming call is handled.
- Interactive Voice Response (IVR) menu guiding the caller.
- Time, accounting, and billing for each subscriber / number.
- Voicemail with a complete caller response system by password access and forwarding of the call records via e-mail.
- Conferencing for support caller groups, to establish a telephone call between more than one participant.
- Call forwarding if „unreachable“ or „busy“.
- Blacklists to block undesired callers (provided that the subscriber number is transmitted).

Furthermore, Asterisk supports packet based protocols such as IAX/IAX2, H.323, SIP, MGCP, and SCCP. Since not only packet based systems shall be interconnected, conventional telephony protocols such as E-DSS1 (Euro-ISDN), National ISDN2, DMS100, BRI (ISDN4Linux), and 4ESS are also supported. Hence, all packet based protocols have to be analyzed with respect to security. [KESS06]

For interconnection with digital and analog telephony equipment, Asterisk supports a number of hardware devices. Other vendors' cards than from Digium can be used for BRI

[1] www.digium.com

(ISDN2) or quad- and octo- port BRI based upon CAPI compatible cards or HFC chipset cards.

The native protocol of Asterisk is the Inter-Asterisk eXchange (IAX) protocol, which is also supported by a number of other soft-switches and PBXs. It is used to enable VoIP connections between servers as well as client-server communication. IAX now most commonly refers to IAX2, the second version of the IAX protocol, because of no available security mechanisms.

IAX2 is able to carries signaling and data on the same path. The commands and parameters are sent binary and any extension has to have a new numeric code allocated. IAX2 uses a single UDP data stream (usually on port 4569 for IAX2, 5036 for IAX) to communicate between endpoints, both for signaling and data. The voice traffic is transmitted in-band. That makes it for IAX2 easier to get through firewalls and other security equipments by using a single port. Additionally the work behind network address translation (NAT) will be better supported. This is in contrast to SIP, H.323 and Media Gateway Control Protocol (MGCP) which are using an out-of-band RTP stream to deliver information.

IAX2 supports trunking, which means multiplexing channels over a single link. That is necessary by the use of one single port for communication. If trunking is used, data from multiple calls will be merged into a single set of packets by the use of a 15 bit call number. That means that one IP datagram can deliver information for more than one call. As a positive result, the IP overhead is smaller than by other signaling protocols and no additional latency will produce.

Figure 3 shows a Full Frame of an IAX message. The Full Frame can be used to send signaling, audio, or video information reliably. Full Frames are the only frame type which can be transmitted reliably.

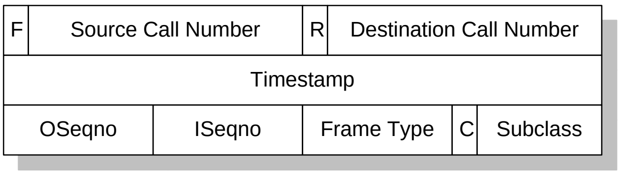


Figure 3: IAX full frame header [SPMI05]

There are several basic frame types define for IAX2 to transport voice, control frames, or information frames. Each of these frame types are described in the Internet draft [SPMI05] in detail. Here we describe only the Full Frame which consists of:

- F (1 bit): An F bit is used in indicate whether a frame is a Full Frame or not.
- Source Call Number (15 bit): A call number is a 15-bit unsigned integer that is used to track a media stream endpoint on a host. The value zero is a special call number that indicates the call number is unknown.
- R (1 bit): The R bit shows if the frame is being retransmitted. Retransmission occurs after some timeout period and retransmissions are retried several times, depending on the context.
- Destination Call Number (15 bit): A phone call actually has two call numbers associated with it, one for either direction.
- Timestamp (32 bit): A Timestamp can be a full 32- or an abridged 16-bit value. In the case of a 16-bit field, the value is actually the lower 16 bits of a full 32-bit timestamp that is maintained by the endpoint host.
- OSeqno (8 bit): This outbound stream sequence number always begins with 0 and increases monotonically. OSeqno is used by the recipient to track the ordering of media frames.
- ISeqno (8 bit): ISeqno is similar to OSeqno, except that it is used to track the ordering of inbound media frames. Specifically, ISeqno is the next expected inbound stream sequence number for the incoming media frames.
- Frame Type (8 bit): Frame Type identifies the class of message as defined in Table 1.
- C (1 bit): The C bit determines how the subclass value should be interpreted.
- Subclass (7 bit): If C is set to 1, the subclass value is interpreted as a power of two. If C is set to 0, subclass is interpreted as a simple 7-bit unsigned integer value.

Type	Description
0x01	DTMF
0x02	Voice Data
0x03	Video
0x04	Control
0x05	Null
0x06	IAX Control
0x07	Text
0x08	Image
0x09	HTML

Table 1: IAX2 Full Frame Types [SPMI05]

Figure 4 describes how a call set-up works by IAX. At first the IP Phone 1 starts to send the message NEW to the second IP Phone. The receiver confirms this call with ACCEPT to allow further setup procedures. After the messages ACK and RINGING the sender also confirms with an ACK message the telephone call. If the participant of IP Phone 2 starts the phone call a last ANSWER and ACK message will be sent. After all acknowledgements a full-duplex phone call can be used.

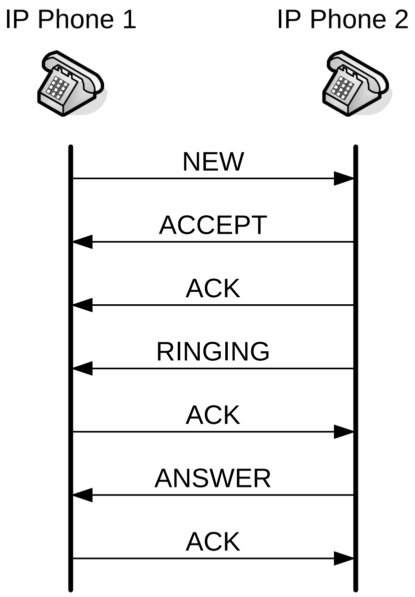


Figure 4: Call setup via IAX protocol [KESS06]

The current release versions of Asterisk are 1.2.27, 1.4.19.2 and 1.6.0-beta9 (State: May 2008).

3. PROTOCOL RISKS

Because speech data is transmitted via standardized and open data networks, various threats exist. Moreover, VoIP systems are composed of numerous components and each component is a complex system with potential weaknesses.

The magnitude of threats at the peerings between networks depends on the protocols used. RTP is used almost exclusively for media streams (speech data), whereas H.323, SIP, MGCP, and MEGACO are for signaling. Depending on the infrastructure and scenario, proprietary protocols can be used as well.

H.323

Most essential attacks against the H.323 protocol suite are identity forgery on the caller side and message manipulation by means of Man-in-the-Middle attacks. If a subscriber succeeds in establishing a connection via a gateway with a forged identity, not only toll fraud would be possible. The caller can be identified by means of the IP address, the H.323 identification, or the caller's number. Often, only one of these criteria – namely H.323 identification – is used for authentication in combination with a password. Data is being transmitted in an unencrypted way. An attacker only has to sniff the signaling stream in order to access the data. Subsequently he can decode the binary data stream using a usual ASN.1 parser (e.g., with the tool Wireshark).

Furthermore, it is possible to manipulate addresses of media streams during connection establishment. This allows an attacker to forward streams to any IP address, recording and modification and further forwarding. These threats affect both devices and gateways.

SESSION INITIATION PROTOCOL (SIP)

Session Initiation Protocol (SIP) secures messages by means of cryptographic hashes and encryption, allowing a reliable authentication and integrity check of signaling messages. However, not all message headers can be covered by hashing. Thus, manipulation of sender information is still possible. In case SIP messages are not secured by hashes it is even possible to apply H.323 specific attacks with easier means, since messages are coded with ASCII, i.e. plaintext. A short script is sufficient to modify and forward certain message headers. This can affect end devices and gateways.

The prevalent SIP protocol can not be regarded as secure. Though it has security mechanisms such as Caller-IDs based on hashes, it is vulnerable for DoS attacks.
In addition, phreaking could have a revival. Here, signaling (for instance via SIP) is decoupled from speech data (payload, e.g. RTP). Two specifically primed clients establish a call via the SIP proxy and obey standards. After connection establishment the SIP proxy receives a connection termination signal. Thus, the SIP proxy interprets the session as terminated. Only the RTP data stream is still maintained by the clients. The communication partners keep their conversation at no charge.

REAL-TIME TRANSPORT PROTOCOL (RTP)

Real-time Transport Protocol (RTP) serves to transmit media streams of real-time applications. For this, necessary information is transmitted in each data packet in order to reconstruct the data. This includes in particular sequence number, time stamp, media type (audio/video), and RTP header length. With these information, a high number of data packets of a connection can be decoded in correct order with the appropriate codec and can be played at the output device, without any access to the signaling information of the connection. This easy decoding mechanism enables an attacker to eavesdrop and manipulate speech data stream as soon as he has gained access to the data. In this scenario the order of received data packets is negligible. Even in the case of lost data packets, both ends will remain synchronized.

MGCP and MEGACO

Also the protocols MGCP and MEGACO do not directly stipulate security mechanisms. A potential attacker can eavesdrop, decode, and manipulate data streams. In case that data is encoded with ASN.1 or ASCII, he solely needs an ASN.1 parser. These protocols are only applied between VoIP servers and gateways or as an inter-gateway protocol. Thus, only gateways are affected by such manipulations.

SKINNY CLIENT CONTROL PROTOCOL (SCCP)

Skinny Client Control Protocol (SCCP) is a proprietary communication protocol which is used for communication control between IP phones and a gatekeeper (e.g. the Cisco Call Manager). There is no public documentation available and the protocol can be modified by the manufacturer at any time.

The workflow of the protocol is simple. Link control is managed by a single TCP connection, in which binary coded, parameterized commands are transmitted. In older protocol versions which are still in use in many end devices, only the MAC address is transmitted as authentication parameter. This communication can be easily reproduced (approx. 300 lines of Perl code is needed) in order to feign an IP phone (rogue phone). By this, identity spoofing and hence toll fraud, but also denial-of-service-attacks against VoIP servers are possible.

New versions of SCCP-based IP phones use SCCPS for authentication by means of X.509 certificates and encrypt TCP signaling stream through TLS.[2] This prevents identity spoofing and decoding of data on the connection path between IP phones and the gatekeeper.

INTERASTERISK EXCHANGE PROTOCOL (IAX)

InterAsterisk eXchange Protocol (IAX) is an open source product. It is suitable for interconnecting Asterisk servers and also a means for end device communication (transmission of media such as audio, video, text, and image). Main features of the IAX protocol can be shortly summarized as follows:

- It is proprietary, but open.
- Signaling and media transport are dispatched via a single Port (IAX2: UDP 4569). Thus, IAX2 can be easily transported in NAT environments and firewall rules are less complex.
- It is a lean protocol due to its binary coding and small protocol overhead. It has only four bytes.
- It is eligible for communications in private networks using NAT (Network Address Translation) and also through firewalls.
- Bundling of multiple IAX connections between two Asterisk servers into one trunk.

The original IAX protocol has no built-in security mechanisms. These have been added in IAX2. Furthermore, IAX end devices do not have a high market penetration so that this protocol is only relevant in scenarios with Asterisk servers. [DEER07a]

[2] Note: Similar to HTTPS (port 443) TCP port 2443 is used. SCCP uses TCP port 2000.

4. ASSESSMENT AND IMPACTS

Compared to conventional telephony VoIP basically offers a broader attack spectrum since open network protocols are used in an unsecured way and due to shared usage of speech and data in a single network. However, the weaknesses have to be assessed depending on the VoIP scenario and implementation profile:

- **Campus VoIP:** In a campus VoIP environment an IP based PBX (Private Branch eXchange) is used. IP phones and/or softphones are connected with this PBX. Connection to the public telephone network is established via gateways. It can be realized both by software (server system with VoIP software) or hardware (extended PBX with VoIP interface). Both options are hard to attack since telephone conversations are not routed via the Internet or other unsecured networks. Potential attacks have to be initiated mainly from the intranet or from outside through the firewall.
- **IP Centrex / Hosted IP:** This option consists of a virtual, IP based PBX which is provided by a VoIP provider. Through this, he is able to provide his own speech services without the need of client-side gateways or PBX systems. The user simply requires an adequate internet access and has to acquire IP phones and/or soft phones. Attacks against the VoIP system can only take place from the Intranet or via the internet (from the provider network).
- **VoIP-Trunks:** VoIP trunk connections increasingly replace connection-orientated telephone links because of the growing convergence of networks and resulting cost savings. Furthermore, companies gain flexibility when T1 or PRI interfaces do not have to be used any longer. However, the probability for attacks increases if data is transmitted via unsecured networks. Specifically attacks from the internet jeopardize corporate networks.

To seal off insecure internet connections a Campus VoIP solution should be used for Asterisk (Figure 5). The VoIP system is protected since the corporate network is safeguarded against outbound attacks. In addition, quality-of-service (QoS) for keeping speech quality on a high level is possible. In this scenario VoIP is conceived as a further IP service having high requirements on network and security.

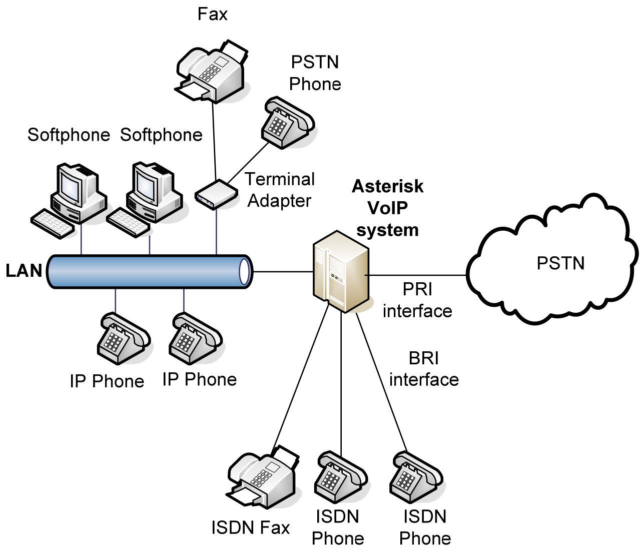


Figure 5: VoIP scenario with Asterisk

VoIP networks comprise many different components such as IP phones, gateways, server (gatekeeper or SIP proxy), router, etc., having specific requirements with regards to security. In this context both the network and application part have to be considered. On the network side this includes classical network security, virtual LAN (VLAN), encryption, authentication, firewalling, intrusion detection / intrusion prevention (IDS/IPS), network address translation (NAT) and Simple Traversal of UDP through NAT (STUN), softphones and hardphones, network equipment, operating systems, QoS, remote management, and patch management. Here, we do not further focus on network security issues, as they have to be adressed by elementary security mechanisms anyway. This is different for signaling protocols. As we focus on Asterisk, protocols with security extensions are relevant. These are SRTP, IAX2, and security mechanisms for SIP.

SRTP

SRTP encrypts the media stream. For this purpose, key exchange has to take place. Because of the encryption method AES it is guaranteed that the content (speech data) of a conversation can not be recorded. Communication partners are authenticated by means of SHA-1 hashing. However, the key used for data encryption is transmitted via SIP (using signaling path keying), which is exposed to sniffing attacks in case that SIP is not sufficiently secured[3].

ZRTP

ZRTP is a protocol for the media path session key exchange based on Diffie-Hellman, and parameters for establishing SRTP sessions. The ZRTP protocol is multiplexed on the same port as RTP and does not require support in the signaling protocol. A key advantage of ZRTP is, that it does not assume a Public Key Infrastructure (PKI) or certificates in end devices.

The Zfone Project [ZFON08] allows ZRTP support for Asterisk so that SIP/RTP calls in Asterisk can be encrypted. To add support for ZRTP, the libZRTP SDK is needed together with the Asterisk patch file for ZRTP support.

A patch is mandatory since an unmodified (unpatched) Asterisk would cause problems because of P2P key negotiation and encryption. It would reject ZRTP protocol packets.

SIP

SIP has been extended with TLS, HTTP Digest, IPsec with IKE, and S/MIME. Also end-to-end-security and hop-by-hop-communications are optionally available[4]. However, as Asterisk deploys SIP signaling over UDP, TLS protection is not possible since it requires TCP. Although, there have been efforts to implement other security mechanisms for SIP, Asterisk only provides SIP Digest authentication with MD5. Missing security features for SIP shall be implemented in the next generation of the SIP channels (Version 3)[5], which have been under development in the Pineapple project. [PINE07] Because of the stronger impact on the Asterisk architecture, there will be no backwards compatibility.

[3] The key is transmitted within the SIP body via SDP parameters

[4] For Hop-by-Hop security TLS and IPsec are used. End-to-end security are realized by SIP Digest authentication, and S/MIME. In RFC-3261 S/MIME is optional.

[5] The current version is still version 1. Version 2 had ony patch level status and development efforts have been postponed.

IAX2

In contrast to SIP, IAX2 is a binary protocol and not text based. Originally, the IAX protocol has been developed in order to realize a communication between Asterisk servers. However, IAX allows to initialize conversations and to transmit speech data. For this, some security mechanisms are provided. Asterisk servers are able to authenticate each other using a public key infrastructure (PKI) based on a RSA or alternatively Diffie-Hellman key exchange. Messages are encrypted using AES with 128 bit keys. Since IAX2 only uses one port (UDP port 4569) for connection establishment only this port has to be opened in a firewall to pass IAX2 traffic through.

Since very few IP end devices support IAX2, SIP security features or SRTP have to be implemented respectively. IAX2 should be used for interconnecting Asterisk servers between different locations. Besides increased security, improvements in speech quality and better exploitation of bandwidth argue for IAX2.

Regarding security we can summarize the following key aspects:

- IAX2 supports authentication via Public Key Infrastructure (PKI), e.g. between two Asterisk servers using RSA key pairs.
- IAX2 allows user authentication via RSA or MD5. However, with MD5 the peers have plaintext access to the secret key whereas RSA restricts the access in one direction via the public/private key pairs. Thus, it is recommended to secure the private key using 3DES-encryption.
- Also, IAX2 offers mutual peer registration with address and credentials, so that caller can reach the peer. The respective registration protocol can be deployed in parts.

One of the strengths of the design of IAX2 constitutes a potential security problem. Using a single well-known port alleviates Denial-of-Service (DoS) attacks, which have significant impacts of real-time applications such as VoIP as they are extremely sensible to. Furthermore, the IAX2 URI scheme (iax2:) does not provide any security mechanism such as the SIPS URI scheme within the SIP protocol.

SIMCO

A further way to secure Asterisk (for the „VoIP trunk scenario“) is via the SIMCO (SImple Middlebox COnfiguration, RFC-4540) protocol. SIMCO is fully compliant to the MIDCOM protocol (MIDdlebox COMmunication, RFC-3303 and RFC-3304). End of January 2006 Digium Partner Ranch Networks provided the developer community with the source code. This is developed under the Asterisk-Netsec development branch. Through the implementation of these protocols into Asterisk through a software library called libcom[6], firewall ports (in particular for RTP) are dynamically[7] controlled by „Policy Rule Control Messages“. Communication between the Asterisk server and the middlebox device[8] is secured by means of OpenSSL. Although, this is a generic method, it is only supported by Ranch Networks devices.

Segmentation and VLAN

Furthermore, a separation of data and VoIP segments is mandatory in order to avoid collisions and bottlenecks. The VoIP segment should be isolated by a firewall which provides additional protection. Also IP phones should be positioned in different subnets or network segments. This enables a better network partitioning and efficient deployment of prioritization (Q-Tag, DiffServ). Also a separation of networks at layer 2 can be realized with VLANs, so that data and speech can be separated logically while the same physical network is used. [DEER07b]

Current information about security risks in Asterisk can be found in the security advisories in [ASTE08] and Asterisk security discussion from Digium. [DIGI08]

5. CONCLUSIONS

At present, secure VoIP should be operated using the Campus scenario which establishes calls via ISDN. VoIP should be regarded as a further IP service which is separated from the remaining networks. In the future an interconnection to public VoIP providers or operators can be realized if signaling standards have reached a sufficient and comprehensive security level. Authentication and encryption have to be implemented by the providers. This is an essential prerequisite.

6. REFERENCES

[ASTE07] www.asterisk.org

[ASTE08] www.asteriskpbx.org

[DEER07a] Kai-Oliver Detken, Evren Eren: Voice-over-IP Security Mechanisms - State-of-the-art, risks assessment, concepts and recommendations. 8th International Symposium on Communications Interworking, Santiago de Chile 2007

[DEER07b] Detken, Eren: VoIP Security - Konzepte und Lösungen für sichere VoIP-Kommunikation; 310 Seiten; Hardcover; hanser Verlag; ISBN: 3-4464-1086-4; München 2007

[DIGI08] lists.digium.com/mailman/listinfo/asterisk-security

[KESS06] Lars Kessner: VoIP-Standards und Migration verschiedener Unternehmensszenarien. Diplomarbeit, Hochschule Bremen, Studiengang: Technische Informatik, Bremen Januar 2006

[PINE07] Pineapple-Projekt: www.codename-pineapple.org/start.shtml

[RSC+02] Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, Handley, Schooler: SIP – Session Initiation Protocol. RFC-3261. Network Working Group. Category: Standards Track. IETF 2002

[SMS+02] Swale, Mart, Sijben, Brim, Shore: Middlebox Communications (midcom) Proto-col Requirements. RFC-3304. Network Working Group. Category: Informa-tional. IETF 2002

[SPMI05] M. Spencer, F. Miller: Inter-Asterisk EXchange (IAX) Version 2. Internet-Draft, Network Working Group, IETF 2005

[SQC06] Stiemerling, Quittek, Cadar: NEC's Simple Middlebox Configuration (SIMCO) Protocol Version 3.0. RFC-4540. Network Working Group. Category: Experi-mental. IETF 2006

[ZFON08] www.zfoneproject.com

[6] Only available for Asterisk 1.2 and not yet available for 1.4

[7] Only if during a call

[8] E.g. NAT device, firewall, Ranch Network device or combinations