DECOIT

Cybernetics and Information Technologies, Systems and Applications (CITSA) 2008

CITSA 2008

VoIP Security

regarding the Open Source Software Asterisk

Prof. Dr.-Ing. Kai-Oliver Detken
Company: DECOIT GmbH
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

DECOIT

Table of content

- State-of-the-art: Scenarios and standards
- Open Source Software Asterisk
- Protocol risks
- Potential threats and attacks
- Assessment and impacts
- Conclusions

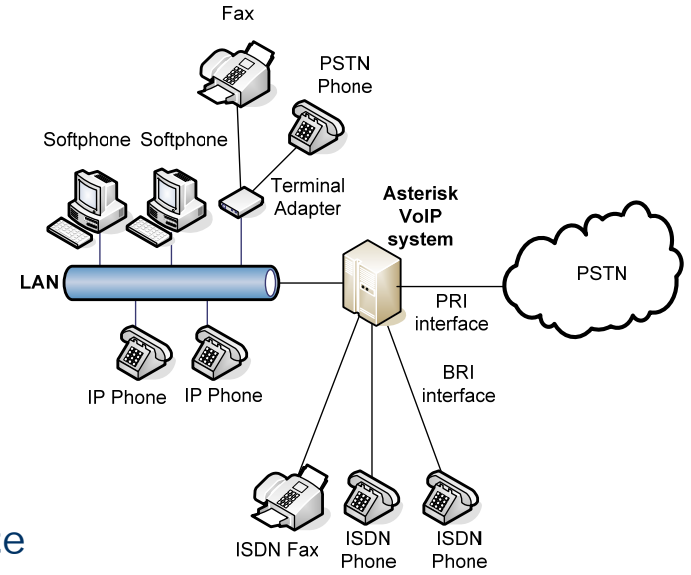
DECOIT

VoIP security introduction

- A VoIP system can be deployed in different ways (next slide)
- 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)
- The media stream has to be encrypted in order to avoid sniffing and manipulation
- Authentication and encryption requires a solid key management
- Interfaces for device configuration should be secured as well, e.g. by means of HTTPS
- An important issue of VoIP security is the protection of the network against attacks (hacking) and malware (viruses, worms, Trojan horses, etc.)
- VoIP software implementation has to checked against security holes

VoIP deployment scenarios

- **Campus VoIP:** Campus VoIP uses an IP PBX (Private Branch eXchange), which is most common, or IP-enabled PBX. IP phones and/or softphones are connected to the IP PBX. Calls initiated from these phones are routed through a gateway to the PSTN.
- **IP Centrex/Hosted IP:** This type requires the involvement of a VoIP service provider hosting the IP PBX and providing VoIP services from this network. The enterprise only needs IP phones, no other VoIP customer premises equipment is necessary.
- **VoIP Trunks:** VoIP trunks increasingly replace circuit-switched connections, e.g. T1 and PRI.



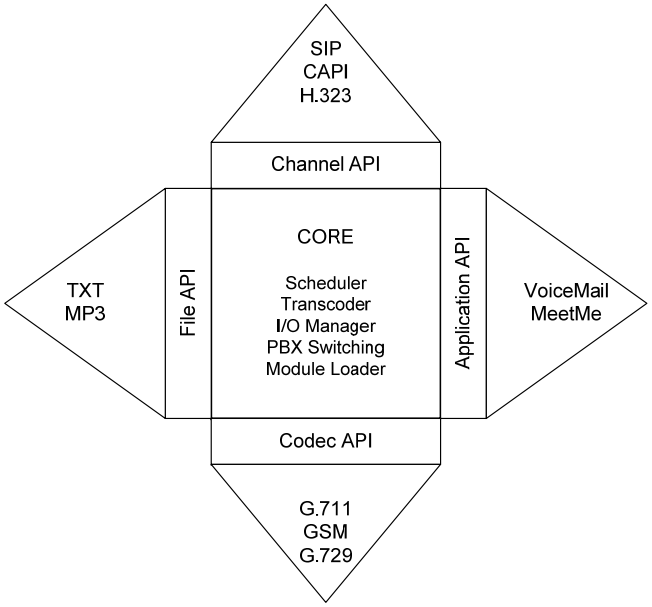
Protocols and standards of VoIP

<table>
<tr><td>Audio applications</td><td>Video applications</td><td colspan="4">Terminal control and management</td><td>Data</td></tr>
<tr><td rowspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.261
H.263</td><td rowspan="3">RTCP</td><td rowspan="3">Terminal to Gatekeeper signaling

RAS</td><td rowspan="3">H.255.0
Q.931
connection signaling (call setup)</td><td rowspan="3">H.245 Control Channel</td><td>T.124</td></tr>
<tr><td rowspan="2">T.125</td></tr>
<tr><td colspan="2">RTP</td></tr>
<tr><td colspan="4">Unreliable Transport (UDP)</td><td colspan="2">Reliable Transport (TCP)</td><td rowspan="3">T.123</td></tr>
<tr><td colspan="6">Network security (IP)</td></tr>
<tr><td colspan="6">Security Layer (IEEE 802.3)</td></tr>
<tr><td colspan="7">Physical Layer (IEEE 802.3)</td></tr>
</table>

Open Source Software Asterisk (1)

- Asterisk 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. 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 deployment
- Many manufacturer of VoIP software PBX systems use Asterisk today and do not invest more time into own development



Open Source Software Asterisk (2)

- 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).

Open Source Sofware Asterisk (3)

- Supported protocols & codecs
  - Protocols
    - SIP
    - H.323
    - MGCP
    - SCCP/Skinny
    - IAX/IAX2
  - Codecs:
    - G.723.1
    - G.711 (μ-Law, A-Law),
    - GSM
    - ADPCM
    - optional G.729

Inter-Asterisk eXchange (IAX)

- IAX now most commonly refers to IAX2, 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
  - IAX2 supports trunking, which means multiplexing channels over a single link on a very efficient way (overhead and quality)
  - As a positive result, the IP overhead is smaller than by other signaling protocols and no additional latency will produce

Protocol risks (1)

- SIP
  - SIP messages are mostly not authenticated and most of the devices do not check the source of the message
  - Attackers can infiltrate messages to manipulate or disturb SIP services
  - Typical threats are SIP-Spam (identity forgery), manipulation, redirecting and sniffing of connections, flooding of mailboxes with Spam and modification of messages
- H.323
  - Wrong identities and Man-in-the-Middle (MitM) attacks make the H.323 protocol suite assailable
  - The identification of a caller is managed by an authentication password, which is communicated unencrypted via the network

Protocol risks (2)

- RTP
  - With information of particular sequence number, time stamp, media type etc., a high number of data packets of a connection can be decoded in correct order and can be played at the output device
  - This easy decoding mechanism enables an attacker to eavesdrop and manipulate speech data stream as soon as he has gained access to the data
- IAX
  - Attackers can carry out Denial of Service (DoS) attacks against Asterisk servers and are able to spy on accounts for which no or only weak passwords exist

Potential threats and attacks (1)

- Network Layer
  - Denial-of-Service (DoS)
  - ARP, MAC, IP, UDP, IRDP spoofing
  - SYN-, PING- oder MAC- Flooding
  - TCP-Session-Hijacking
  - RST-Attack
  - Data Injection through ISN-Guessing
  - Sniffing
  - Replay

Potential threats and attacks (2)

- Application Layer
  - Toll interception: malware such as Trojans are sufficient to sniff and copy speech packets and to even send them to someone else
  - Manipulation of calls: By means of a MitM attack speech packets of a call can be selectively modified
  - Unauthorised usage/phreaking/toll fraud: If an attacker is able to compromise user credentials (VoIP provider access credentials) he can set up calls at the expense of the user (toll fraud)
  - Dialer: Softphones are exposed to a particular risk, since Trojans or worms are able to autonomously establish calls without any user notice
  - Violation of Privacy: Credentials and other user (subscriber) information can be collected with the aim to monitor and analyse communication profiles
  - SPIT (Spam over IP Telephony): Comparable to Spam-Mails, SPIT massively sends VoIP messages

Potential threats and attacks (3)

- Further **security risks** can be named as dynamic port usage, configuration of network devices etc.:
  - Dynamic port usage
  - Configuration of network devices
    - Default Ports
    - Passwords
    - Administration
  - Faulty implementation of VoIP protocols
  - Attacks against IP PBX
  - Attacks against operating systems in VoIP systems

Assessment and impacts: 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

DECOIT

Assessment and impacts: SIP

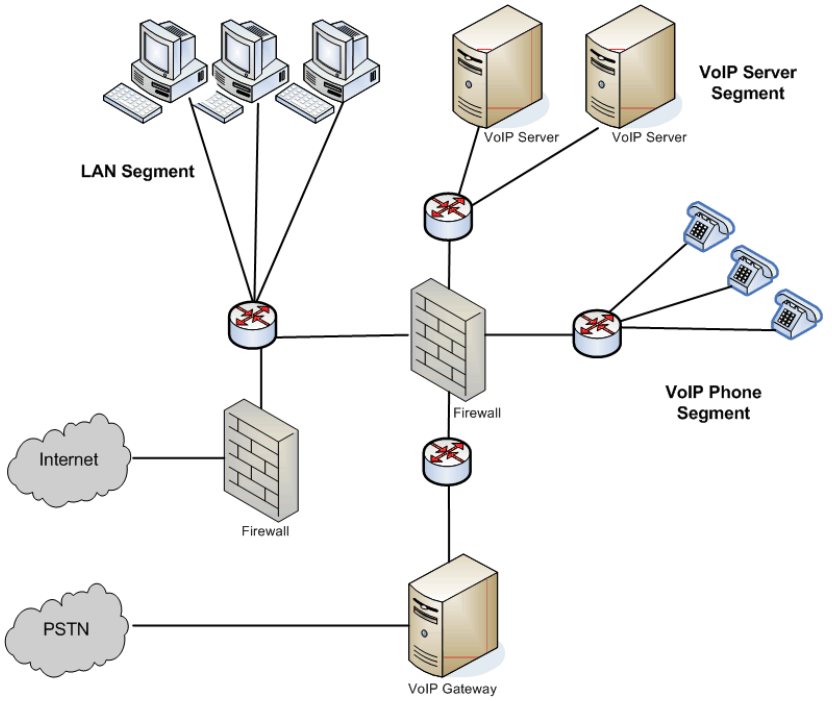
- SIP has been extended with TLS, HTTP Digest, IPsec with IKE, and S/MIME
- Also end-to-end-security and hop-by-hop-communications are optional available
- However, as Asterisk deploys SIP signaling over UDP, TLS protection is not possible since it requires TCP
- Although, there have been efforts to 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) , which have been under development in the Pineapple project.
- Because of the stronger impact on the Asterisk architecture, there will be no backwards compatibility

Assessment and impacts: IAX2

- 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
  - With MD5 the peers have plaintext access to the secret key
  - RSA restricts the access in one direction via the public/private key pairs
  - It is recommended to secure the private key using 3DES encryption
- 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
- Using a single well-known port alleviates Denial-of-Service (DoS) attacks, which have significant impacts of real-time applications
- IAX2 URI scheme (iax2:) does not provide any security mechanism such as the SIPS URI scheme within the SIP protocol

Segmentation and VLANs

- 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)
- A separation of networks at layer 2 has to be realized with VLANs, so that data and speech can be separated logically while the same physical network is used.



Conclusions

- At present, secure VoIP should be operated using the campus scenario which establishes calls via PSTN.
- 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.

Thank you!

...for your attention.

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies