Interworking 2006

Voice-over-IP Security Mechanisms

State-of-the-art, risks assessment, concepts and recommendations

Interworking Conference, 15th - 17th of January 2007

Dr.-Ing. Kai-Oliver Detken
Business URL: http://www.decoit.de
Private URL: http://www.detken.net

Consultancy & Internet Technologies

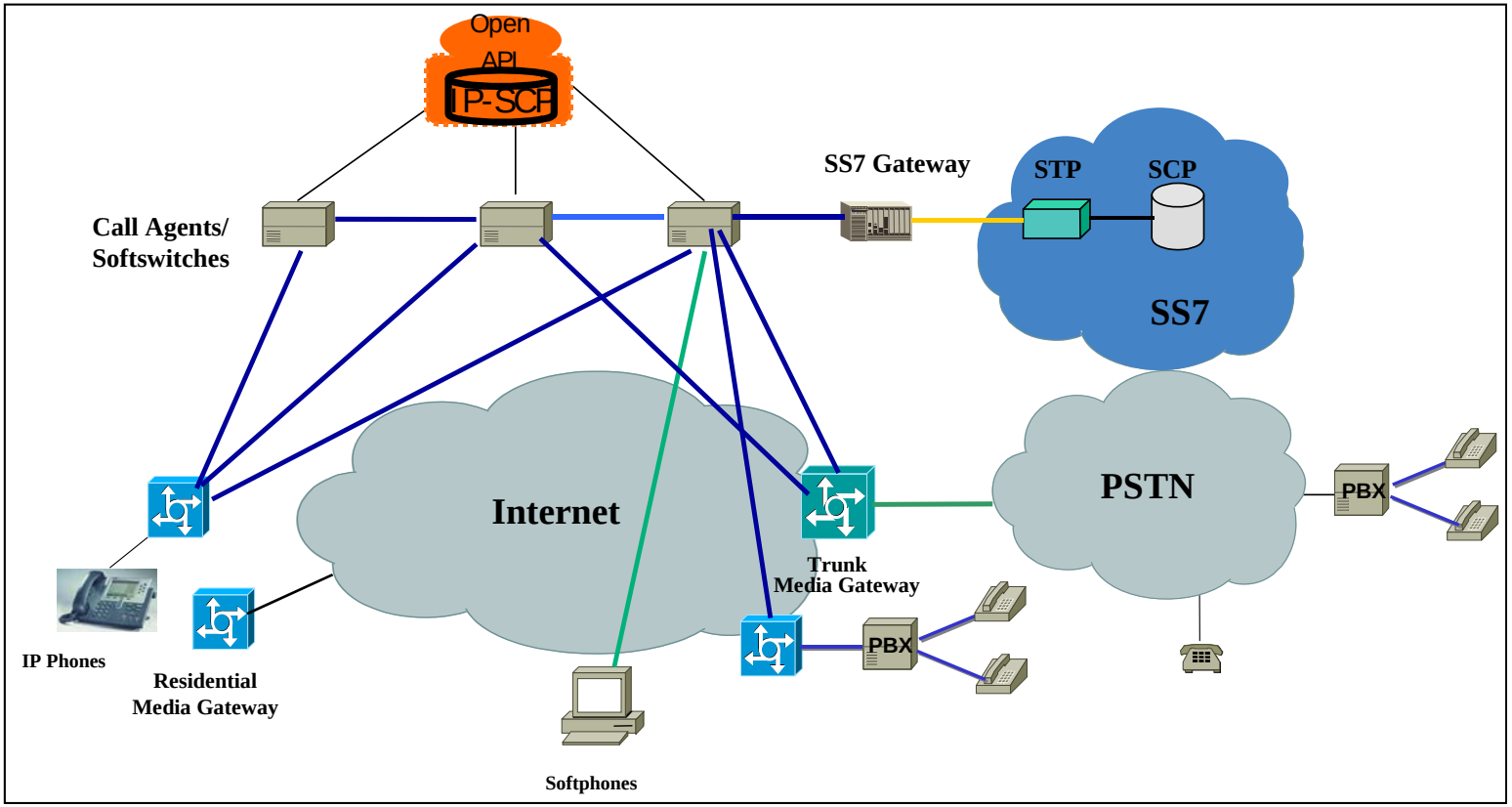
VoIP security

- This presentation addresses the issues in five steps:
  - Identifying typical VoIP communication and application profiles in enterprises
  - Analysing security risks and possible attacks and their implications on the overall security
  - Assessing risks
  - Presenting security mechanisms and standards
  - Presenting security concepts and recommendations

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. Thus, this topology is not prone to attacks since the VoIP network does not extend to the Internet or any other non-trusted network. Potential attacks must originate from within the intranet.
- 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. In this case – as with Campus VoIP – internal attacks exist; additionally, attacks are possible from the service provider's network, since it is a shared one.
- VoIP Trunks: VoIP trunks increasingly substitute circuit-switched connections, e.g. T1 and PRI on the basis of non-trusted networks. Especially, attacks coming from the Internet make the enterprise network vulnerable

VoIP architecture



Risks in VoIP-based communications

- 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
- 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

Attacking tools for VoIP (1)

- Cain & Abel: uses ARP spoofing and ARP poisoning. This tool enables sniffing and recording of VoIP conversations. It supports a big amount of different password formats.
- Vomit: converts a Cisco IP conversation into a Wave-File. It requires a tcpdump output file Vomit only supports G.711 coding.
- VoIPong: VoIPong finds all conversations in a network, which are coded in G.711. It supports SIP, H.323, Cisco skinny protocol, RTP and RTCP. Like Vomit, it converts conversation to a wave-file.
- SiVuS: is a vulnerability scanner for VoIP networks. It comprises three components (message generator, component discovery, vulnerability scanner)
- SIPcrack: is a SIP protocol login cracker (identify logged in SIP users and crack the passwords of the SIP users by means of bruteforce attacks)
- RingAll: This simple mechanism allows for a DoS-attack against unsecured SIP clients. It sets the field “User-Agents” with the value “RingAll” and thus forces a broadcast call

Attacking tools for VoIP (2)

- Wireshark: This is a network packet analyser which monitors and records transmitted packets for analysing purposes. It can be misused for attacks such as sniffing of user credentials during connection establishment. It supports SIP and H.323 and records conversations in the ".au" file format.
- Sipsak: Sipsak is a small command line program for SIP developers and SIP administrators. It can be used for simple tests of SIP applications.
- Nmap: This port scanner is normally used for port validation of hosts. It is possible to identify active hosts and open ports in an operating system. With this tool an attacker can easily make use of weaknesses within an operating system.
- THC-Hydra: THC-Hydra is a logon cracker which supports numerous protocols such as SIP. It is a proof-of-concept-tool which cracks the password of a specific protocol.

Risk assessment (1)

- This table shows general threats and their implication of the main security requirements integrity, authenticity, confidentiality, and availability
- The most attacks want to destroy the availability of VoIP systems and are not spying tools regarding recording or evaluation of voice and data streams
- But there are many more attacks possible by using standard networks and protocols as in PSTN networks before

Attacks	Integrity	Authenticity	Confidentiality	Availability
Disturbing the normal course of operations	√			
Subscriber unreachable	√			
Eavesdropping conversation data*		√	√	
Sniffing registration data on VoIP servers or gateways*		√	√	
Manipulating modifying data*		√	√	√
Hijacking connections or sessions*		√		√
Identity fraud*		√		√
Circumventing communications*	√			
Toll fraud*				√
Interfering the QoS*				√
Malfunction of devices*	√			

* = Redirecting data streams

Risk assessment (2)

- This table shows named attacks directly
- The majority of consumer VoIP solutions do not support encryption yet
- There are several open source solutions that facilitate sniffing of VoIP conversations
- Real security requires encryption and cryptographic authentication which are not widely available at a consumer level

Attacks	Integrity	Authenticity	Confidentiality	Availability
DoS /DDos				√
MAC, Ping, SYN, LAND Flooding				√
TLS Connection Reset				√
Replay Attack	√	√	√	√
DHCP Starvation Attack				√
MAC-Spoofing		√	√	
ARP-Spoofing	√	√	√	√
IP-Spoofing		√	√	√
DNS-Spoofing	√	√	√	√
Password Sniffing	√	√	√	√
SPIT				√

Security mechanisms and standards

- SIP Digest (RFC-2617): it allows authentication of SIP subscribers (user agent, proxy-server or registrar server) and based of the transmission of shared secrets
- SIPS (SIP over SSL/TLS): protects sensitive data such as SIP URI, IP addresses from sniffing or message manipulation
- SRTP (RFC-3711): encrypts data symmetrically with AES and authenticate the sender; replay protection and integrity is also supported
- S/MIME: offers „end-to-end"-encryption
- H.235: Authentication by means of certified public keys; also key exchange methods are implemented (Diffie-Hellmann)
- ZRTP: ZRTP is an extension of RTP and describes a key agreement/establishment protocol for use with SIP and SRTP without the need for a shared secret or PKI infrastructure
- SPIT filtering: A countermeasure to SPIT attacks is SPIT filtering with different mechanisms like buddylists/whitelists and blacklists

Assessment (1)

- SIP Digest features several major weaknesses which can be easily exploited
- SIPS does not provide end-to-end-security, but secure hop-by-hop-communications
- S/MIME secured connections take to long to establish a session. Also, there is no organisation that manages worldwide distribution of certificates
- SRTP enables secure RTP sessions during connection establishment phase, but also plain text is communicated
- H.235 has a high complexity and different vendor implementations

Security mechanism	Confidentiality	Integrity	Authentication	Access Control	Liability	Anonymity
SIP Digest	-	-	+	+	+	-
SIPS	+	+	(+)	-	-	-
S/MIME (Message Body)	(+)	(+)	(+)	(+)	(+)	(+)
SRTP	(+)	(+)	(+)	-	-	-
H.235	+	+	+	-	-	-
ZRTP	(+)	(+)	(+)	-	-	-
IAX	+	+	+	-	-	(+)
Skype	(+)	(+)	-	-	-	-

Assessment (2)

- Given normal conditions ZRTP is cryptographically secure. However, this protocol is vulnerable to adversaries with strong capabilities
- IAX in version 2 can use encryption mechanisms to hide signalling and voice data on a secure way and is a very robust protocol
- The main difference between Skype and other VoIP clients is that Skype operates on a peer-to-peer model. All Skype traffic is encrypted by default and the user cannot turn it off. Skype reportedly uses openly available, strong encryption algorithms. The user is not involved in the encryption process and therefore does not have to deal with the issues of PKI infrastructure

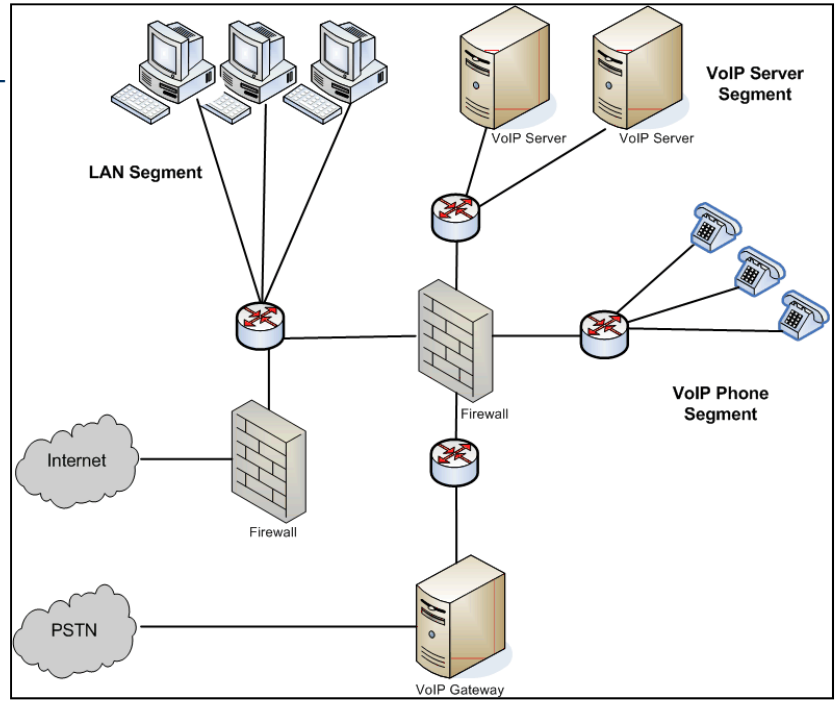
Security mechanism	Confidentiality	Integrity	Authentication	Access Control	Liability	Anonymity
SIP Digest	-	-	+	+	+	-
SIPS	+	+	(+)	-	-	-
S/MIME (Message Body)	(+)	(+)	(+)	(+)	(+)	(+)
SRTP	(+)	(+)	(+)	-	-	-
H.235	+	+	+	-	-	-
ZRTP	(+)	(+)	(+)	-	-	-
IAX	+	+	+	-	-	(+)
Skype	(+)	(+)	-	-	-	-

Security measurements and concepts (1)

- Standard network security
  - Protection of a VoIP network has to start with standard network security measures applied for data networking
  - Additionally, new techniques are necessary due to special and emerging risks associated with VoIP
  - A prerequisite and essential preparation is an in-depth planning to insure reliable service with a satisfactory quality-of-service (QoS)
- Encryption
  - Encryption allows privacy and authentication in phone communications
  - Securing call streams are possible through SRTP, encrypting RTP content, and call signalling with TLS
  - TLS is an alternative to IPsec and provides effective security against hijacking attacks whereas SRTP preventing eavesdropping attacks
  - But, the majority of consumer VoIP solutions do not support encryption yet

Security measurements and concepts (2)

- Virtual LAN (VLAN)
  - It is highly recommended to establish two separate VLANs – one for data and one for voice traffic
  - The logical separation ensures that both data network and VoIP network can not be compromised
  - A providing of priority classes for quality-of-service management is possible
  - Two firewalls are necessary, one for the communication to/from the Internet and one firewall via PSTN



Security measurements and concepts (3)

- Authentication: privacy between users communicating (talking) on a VoIP network is of major concern. Appropriate encryption and authentication of conversation are required.
- Firewalls: UDP and incoming TCP connections are dropped in the most cases from the firewall. Dynamic port assignments throughout the call is an additional problem with filtering VoIP traffic.
- IDS/IPS: VoIP traffic can be detected as attack.
- NAT/STUN: routing problems can be appear. STUN works similar to dynDNS and is able to resolve the different IP addresses. But that can be a security risk depending on the VoIP scenario.
- QoS: should be guaranteed by the provider or the own network

Best-practice approaches

- The main open issues of VoIP are quality-of-service (QoS) and security
- SIP and RTP are improved regarding encryption and authentication and also H.323 can provide a secure communication
- It is a question of implementation into the VoIP equipment and the knowledge about it
- Additionally, there are further developments on work which will improve the VoIP technology in the next future

Risk	Best-Practice Approach
Application-level attacks	• ALGs, firewalls and application-aware IDS/IPS
DoS/DDoS	• Application-aware IDS/IPS • Maintain current patch levels • Antivirus system • Policy-based security zones • VLAN
Eavesdropping	• VPN to isolate VoIP traffic • Selective encryption
Attacks against protocols	• ALGs and IDS/IPS
SPIT	• Strong authentication, authorisation and IPsec
Unauthorized SIP monitoring, spoofing	• Strong authentication, authorisation and IPsec
Viruses and worms	• Current patch levels • Antivirus system • Application-aware IDS/IPS • Policy-based security zones • VLAN

Thank you for your attention

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Germany
Phone: +49-421-596064-01
Fax: +49-421-596064-09
E-Mail: detken@decoit.de

Consultancy & Internet Technologies