Securing VoIP Networks using graded Protection Levels

Andreas C. Schmidt

Bundesamt für Sicherheit in der Informationstechnik,
Godesberger Allee 185-189, D-53175 Bonn
Andreas.Schmidt@bsi.bund.de

Abstract This contribution evaluates the security of VoIP networks. Potential threats to VoIP networks lead to unbearable risks which need to be eliminated by suitable countermeasures. However, cost and complexity of countermeasures should be adapted to the practical situation. Therefore the protection requirements are assessed. In this contribution the range of possible protection requirements is divided into three graded protection levels to allow for an adaptation of the cost of the countermeasures to the required protection level. VoIP-specific threats, countermeasures and implementation problems are disussed. It is derived at which protection level encryption of VoIP is necessary and which problems currently have to be considered with VoIP encryption.

1 Introduction

Voice over IP (VoIP) is a technology which uses the Internet Protocol (IP) to implement voice services for data networks. It is generally expected, that in the near future a domination of data over voice will occur. This is a key driver for the convergence of voice and data. An important motivation to use VoIP is Computer Telephony Integration (CTI) which enables the implementation of many new applications. The IP protocol relies on packets of varying size and can therefore not guarantee a quality of service (QoS) as it is the case for classical telephony or ATM (Asynchronous Transfer Mode). For the QoS problem several solutions exist which are complex an require a careful network design. However, more critical is the secure use of VoIP services and is therefore treated in this paper. A threat analysis conducted in [TIPHON] shows that considerable risks exist for VoIP. In this contribution a different approach is described, where risks and countermeasures depend on the protection requirements resulting from the processed information. The protection requirements are divided into graded protection levels. This has the advantage that for lower protection requirements simpler countermeasures at a reduced cost can be used.

2 VoIP Network Model

Practical networks are normally very different in size and structure. Due to this a reference model is used as shown in Figure 1 and taken as a basis for the analysis of threats and risks. This reference model consists of the following basic elements:

1. PCs implementing IP-Soft-Phones
2. IP-Phones

3. Call Server (to process the calls)
4. Physical links
5. VoIP-Provider (here: interconnects two sites)
6. Logical configuration connections (see broken lines in Figure 1)
7. Switches
8. Router (voice-enabled)
9. Network Management
10. Interfaces of terminal devices and network components.

Hereby the switches in Figure 1 represent a switched Ethernet Local Area Network (LAN) consisting of Layer 2 and possibly Layer 3 switches. Switched Ethernet is a prerequisite for the reasonable use of VoIP technology for business quality voice service. VoIP over shared media or the Internet, although interesting applications may exist, is not considered here.

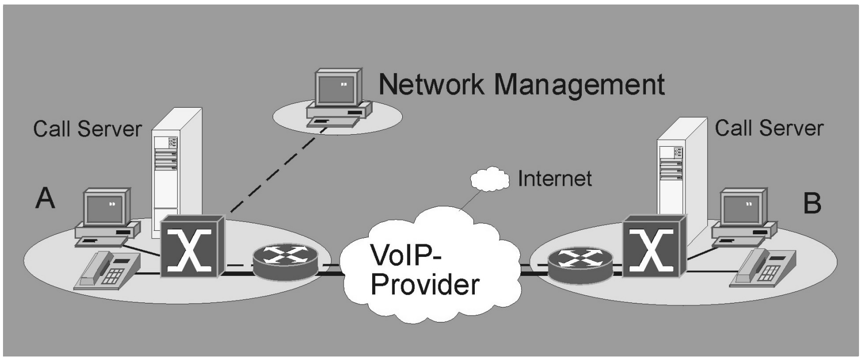

Figure 1: Network reference model

3 Assessment of Protection Requirements

The assessment of protection requirements in this contribution is based on three basic security properties: availability, integrity and confidentiality. Hereby integrity is defined to comprise also authenticity.

The required protection with regard to the three basic security properties depends on the practical situation and is divided into three graded protection levels. They cover a range from low to moderate up to very high protection requirements as depicted in Table 1.

Using the criteria listed in Table 1 it is possible to derive the protection level for any given network. The protection level of the network is the maximum level resulting from the criteria when applied to the network.

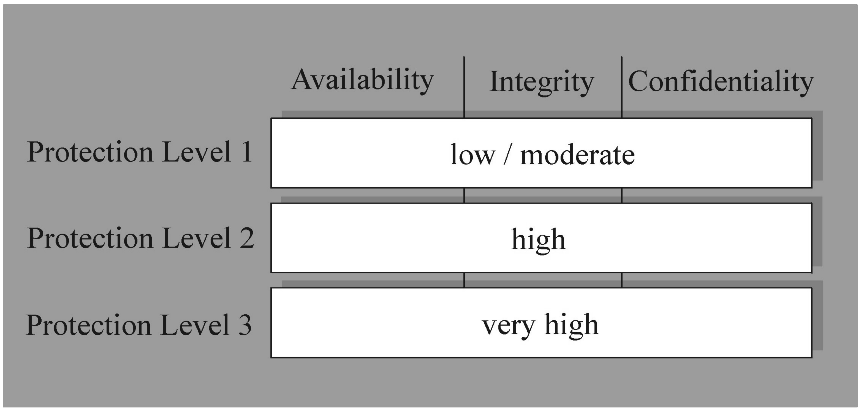

Figure 2: The protection levels comprise the three basic security properties: availability, integrity (including authenticity) and confidentiality

Criterion	**Protection Level 1**	**Protection Level 2**	**Protection Level 3**
Max. duration of failure/ cumul. downtime per year	1 day per failure/ 10 days	1 hour per failure/ 10 hours	10 minutes per failure/ 20 minutes
Strength of attacks	Attack by simple means	Attack by qualified means	Attack by sophisticated means
Degree of secrecy	Unrestricted to restricted	Confidential	Secret and higher
Financial consequences	Uncritical	Critical	Highly critical
Personal and organisation related data	Damage with little consequences	Damage with serious consequences	Damage of vital significance

Table 1: Criteria for selection of a protection level

4 Generic Threats to the VoIP-Service and Risk Analysis

VoIP services and the underlying technology can be subject of a multitude of threats. In the following major generic threats are described, which can occur in the network reference model shown in Figure 1. The specific threat scenario for a practical network can be derived by mapping the generic threats onto that network.

Denial of Service (DoS): the attacker impairs the availability of information and VoIP services by using one or more of the following attack methods:

- Flooding the call server, network or terminal devices
- Injecting of Disconnect or Connect messages
- Sending forged error messages.

Eavesdropping of User Information: the attacker eavesdrops user data and information exchanged during VoIP calls. Note, that the VoIP-provider network shown in Figure 1 is assumed uncontrollable for the customer and includes a connection to the Internet. An attacker could use the following means:

- Attaching a protocol analyser to the network
- Establishing a conference session imperceptible for the other parties
- Using system weaknesses or logical access to the call server or other system components.

Unauthorized Access: the attacker can obtain access to the VoIP service without being authorized for this service. This means that the attacker cannot be charged for the service or gets unauthorized access to information.

Network Manipulation: the attacker is able to change the configuration of the VoIP network. He can manipulate the network, eavesdrop and manipulate information. He can perform denial of service and man in the middle attacks by using one or more of the following attack methods:

- Physical or logical access to configuration ports of system components
- Access to the call server enables denial of service, man in the middle attacks, change of user related registration data and assignments

Spoofing: the attacker uses authentication information which has not been assigned to him by:

- Gaining the information by eavesdropping or other means
- Hijacking a link after successful authentication

Alteration of User Information: the attacker modifies voice mails or messages or impairs the integrity of user information by:

Deletion of information

Modification of stored or transmitted information.

Other relevant threats, which can occur in VoIP networks, but are not detailed here are e.g.:

Repudiation, forgery, viruses and traffic analysis.

In Table 2 a simplified evaluation of the risks resulting from the identified threats is given. In order to determine the risks the estimated cost for an attacker is related to motivating factors like benefit or the potential damage the attacker could cause.

5 Countermeasures

The concept of graded protection levels is characterized by the important property, that cost and complexity of the countermeasures depend on the protection level. The countermeasures e.g. for protection level 1 need to withstand attacks based on simple means only. Graded protection levels allow for a more cost effective, simpler implementation of countermeasures, depending on the required protection level.

Level	Threat	Remarks	Risk
1	DoS Eavesdropping Unauthorized Access Network Manipulation Spoofing	Without a suitable network design and countermeasures an attacker can implement threats by simple means. The risk for the given threats is therefore assumed unbearable.	Unbearable
	Alteration	The low protection level and the fact that qualified means would be needed for an attack leads to a bearable risk.	Bearable
2	See class 1.	The protection level of the information and the possibility of qualified attacks leads to an unbearable risk.	Unbearable
3	See class 1.	The protection level of the information and the possibility of highly qualified attacks leads to an unbearable risk.	Unbearable

Table 2: : Risk evaluation

5.1 Protection Level 1

The two sites A and B shown in Figure 3 are assumed to be secured infrastructures where physical access to all network elements is controlled. It is assumed that a baseline protection comparable with the baseline protection manual [BPM] is implemented. The countermeasures given below address VoIP specific Problems.

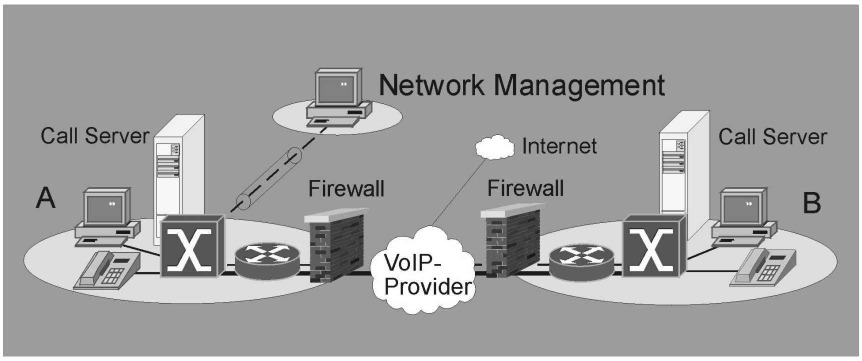

Figure 3: Countermeasure for protection level 1: firewall implementation

Access Control: For prevention of unauthorized use of VoIP resources including the transmission of curruptive data from DoS attacks, several activities are necessary:

- Assignment of access rights according to an access control policy
- Verification of the access rights for each user or terminal before a VoIP service is granted

- A VoIP-enabled firewall should be used to allow for authorized access from external devices. DoS attacks are filtered as far as possible. A problem are dynamically allocated port numbers and the latency requirements of VoIP traffic. A dynamic firewall is needed which introduces only a small latency
- Use of an Intrusion Detection System for detection of internal and external intruders.

Authentication: It is verified that a user or entity has the claimed identity:

- A password or pin mechanism should be used during logon to the VoIP network
- Passwords and pins should be sent encrypted
- The identity of terminal devices is verified before a call is proceeded by the VoIP network.

Prevention of eavesdropping: It is assumed that an attacker uses only simple means. This can be exploited to identify cost effective countermeasures:

- Each network port receives only VoIP packets destined for this port and the attached terminal device according to a given ID
- A reasonable network partitioning for security reasons should be introduced
- All external connections should make use of dedicated lines or VPN solutions
- VoIP calls over the Internet are not considered here, due to limited quality and security
- A trustworthy VoIP provider should be selected.

Secure Configuration: One important task of secure configuration is the prevention of network modification and the resulting consequences. As standardized countermeasures are described in the literature (e.g. [BPM]), specific countermeasures for VoIP are adressed here:

- Control and protection of inband access to network components. The network management system is protected against physical and logical access of other persons than the administrator in charge
- Secure Call Server: All unnecessary applications should be removed from the call server. Only the administrator should be able to make changes to the call server. The same holds for VoIP-Gateways. The call server is protected against unauthorized access of internal or external attackers
- Secure Configuration of all terminal devices
- Secure connection between network management and the networks A and B
- Implementation of standard countermeasures according to e.g. [BPM].

5.2 Protection Level 2

Countermeasures for protection level 2 are designed to withstand qualified attacks. The two sites A and B are assumed to be secured infrastructures where physical access to all network devices is strictly controlled. However, when information is carried over long distances and otherwise uncontrollable networks suitable physical protection is in most cases not feasible or too expensive. In Figure 4 IP encryptors are used to protect VoIP user data against eavesdropping during transmission over the provider network. Combined with the encryptor is an access control function depicted as firewall in Figure 4. This is done because encryption provides only some kind of implicit access control. Furthermore, it is assumed that IT baseline protection and relevant countermeasures for protection level 1 are already implemented.

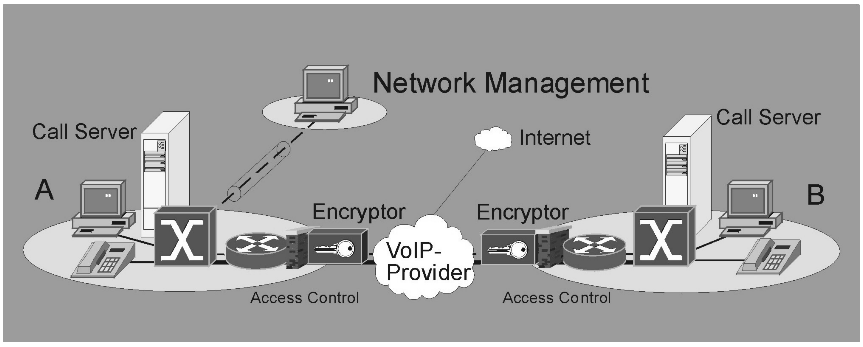

Figure 4: Countermeasure for protection level 2

Further countermeasures for protection level 2 are:

- remote logical configuration connections are protected by cryptographic means in case physical protection is not feasible or too expensive
- configuration ports are protected
- security clearance for personnel possibly obtaining knowledge of sensitive information is conducted
- only accredited security hardware is used
- an audit programme for countermeasures is designed and managed.

To obtain a comprehensive set of countermeasures it is important to perform a detailed security concept taking into acount all known threats and risks for the given VoIP-Network.

5.3 Protection Level 3

Countermeasures for protection level 3 should withstand highly qualified attacks and are therefore difficult to implement. VoIP technology and its security features are not yet stable and mature. Suitable countermeasures remain to be defined.

6 Implementation Problems

The encryption of VoIP traffic leads to several difficulties. At first a suitable standard needs to be selected. One approach is to implement encryption as an IP layer service according to the IPSEC standard [RFC2401]. However, IPSEC does not integrate well with VoIP and leads to a considerable overhead, because VoIP packets are typically small. In addition

QoS is not easy to guarantee in IP networks. Furthermore, encrypted signalling leads to problems when combined with firewalls or NAT devices [M.Shore].

In [RFC1889] and [H.235] the encryption of RTP payload is described. This could avoid a significant overhead and firewall problems as far as only the RTP payload is encrypted. However, it does not seem clear yet what would be the generally accepted VoIP encryption method.

7 Conclusion

The use of graded protection levels can help to reduce the effort of countermeasures for securing VoIP networks for lower protection levels. When encryption and firewalls are combined with VoIP several problems should be taken into account.

References

[1] ETSI, DTR/TIPHON-08002: ”Telecommunications and Internet Protocol Harmonisation over Networks (TIPHON) Security; Threat Analysis”, V0.1.10, February 2001

[2] German Information Security Agency (BSI): ”IT Baseline Protection Manual”

[3] S. Kent, R. Atkinson: “Security Architecture for the Internet Protocol”, November 1998

[4] M. Shore, ”H.323 and Firewalls: Problem Statement and Solution Framework”, July 2000

[5] Schulzrinne et. al.: ”RTP: A Transport Protocol for Real-Time Applications”, January 1996

[6] ITU-T Rec. H.235: ”Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals”