ETSI TR 101 771 V1.1.1 (2001-04)

Technical Report

TIPHON Release 4; Service Independent requirements definition; Threat Analysis

Reference

DTR/TIPHON-08002

Keywords

IP, network, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2001.
All rights reserved.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1 Scope

The present document provides a comprehensive analysis of security threats to the TIPHON environment as described in principle in TS 101 313 [9]. It includes a definition of the security objectives, a description of the assets within the TIPHON environment, a list of threats to the TIPHON environment, a risk assessment, and a recommendation of the necessary security countermeasures.

TIPHON compliant systems bring together IP-based and SCN-based communications. Therefore it is recommended to comply with a certain level of security. Because of the well-known threats and counter-measures in the SCN, the present document focuses primarily on the IP-internal, IP-to-SCN functions.

The following network elements form the simplified TIPHON architecture as described in principle in TS 101 313 [9] for ITU-T Recommendation H.323 [12] to SCN interworking, which is used as basis for the present document:

- Terminals;
- Call control element, e.g. Gatekeeper;
- Admission control element, e.g. User Profile;
- Decomposed Inter-technology gateway consisting of:
  - Media Gateway Controller;
  - Media Gateway;
  - Signalling Gateway.

Where appropriate the guidelines for conduct of a threat analysis described in ETR 332 [1] are followed.

It is intended to expand the present document to cover additional functions and services in a future edition to cover the extended TIPHON environment described by TS 101 314 ed1 (for TIPHON release 2), for TS 101 314 ed2 (TIPHON release 3) and also in TS 101 882 [17] (TIPHON release 3) as an examination of threats against meta-protocols.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[2] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[3] ETSI TR 101 750: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception".

[4] ITU-T Recommendation X.811 (1995): "Information technology - Open System Interconnection - Security framework for open systems: Authentication framework".

[5] ETSI ETR 237 (1996): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[6] ETSI EN 301 261-3 (1998): "Telecommunications Management Network (TMN); Security; Part 3: Security services; Authentication of users and entities in a TMN environment".

[7] ISO/IEC 13335 (parts 1 to 5): "Information technology - Guidelines for the Management of IT Security (GMITS)".

[8] ISO/IEC 10181-4: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework".

[9] ETSI TS 101 313:"Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Phase II: Scenario 1 + Scenario 2".

[10] ISO/IEC 10181-3:"Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework".

[11] ETSI TS 101 323: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable security profiles".

[12] ITU-T Recommendation H.323: "Packet based multimedia communication systems".

[13] ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[14] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[15] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; TIPHON Release 2".

[16] RFC 2194 (1997): "Review of Roaming implementations".

[17] ETSI TR 101 882: "TIPHON Release 3; Protocol Framework Definition; General".

[18] RFC 2828: "Internet Security Glossary".

[19] RFC 2644: "Changing the Default for Directed Broadcasts in Routers".

[20] RFC 2267: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing ".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETR 232 [2] and the following apply.

NOTE: TIPHON is used in the following as synonym for "TIPHON compliant systems".

federation: collection of networked systems that can interact (interoperate) without being part of a single management domain

hijack attack: form of active wiretapping in which the attacker seizes control of a previously established communication association [18]

security policy: set of rules and practices that specify or regulate how a system or organization provides security to protect sensitive and critical system resources and the offered services

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BE	Back End
BER	Back End Routing function
CH	ClearingHouse
DoS	Denial of Service
GK	GateKeeper
GW	GateWay
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITSP	IP-Telephony Service Provider
MGC	Media Gateway Controller
MGW	Media Gateway
MMI	Man-Machine-Interface

NE	Network Element
OSP	Open Settlement Protocol
PIN	Personal Identification Number
PRS	Premium Rate Service
PSTN	Public Switched Telephony Network
RAS	Request Admission Status
RFC	Request For Comments
RS	Resolution Service
SAP	Service Access Point
SCN	Switched Circuit Network
SGW	Signalling Gateway
TCP	Transport Control Protocol
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks
TR	Technical Report
UP	User Profile
UPT	Universal Personal Telecommunications
VoIP	Voice over IP

4 Overview

The present document follows the methodology generally described in ETR 332 [1] and is therefore structured in the following way.

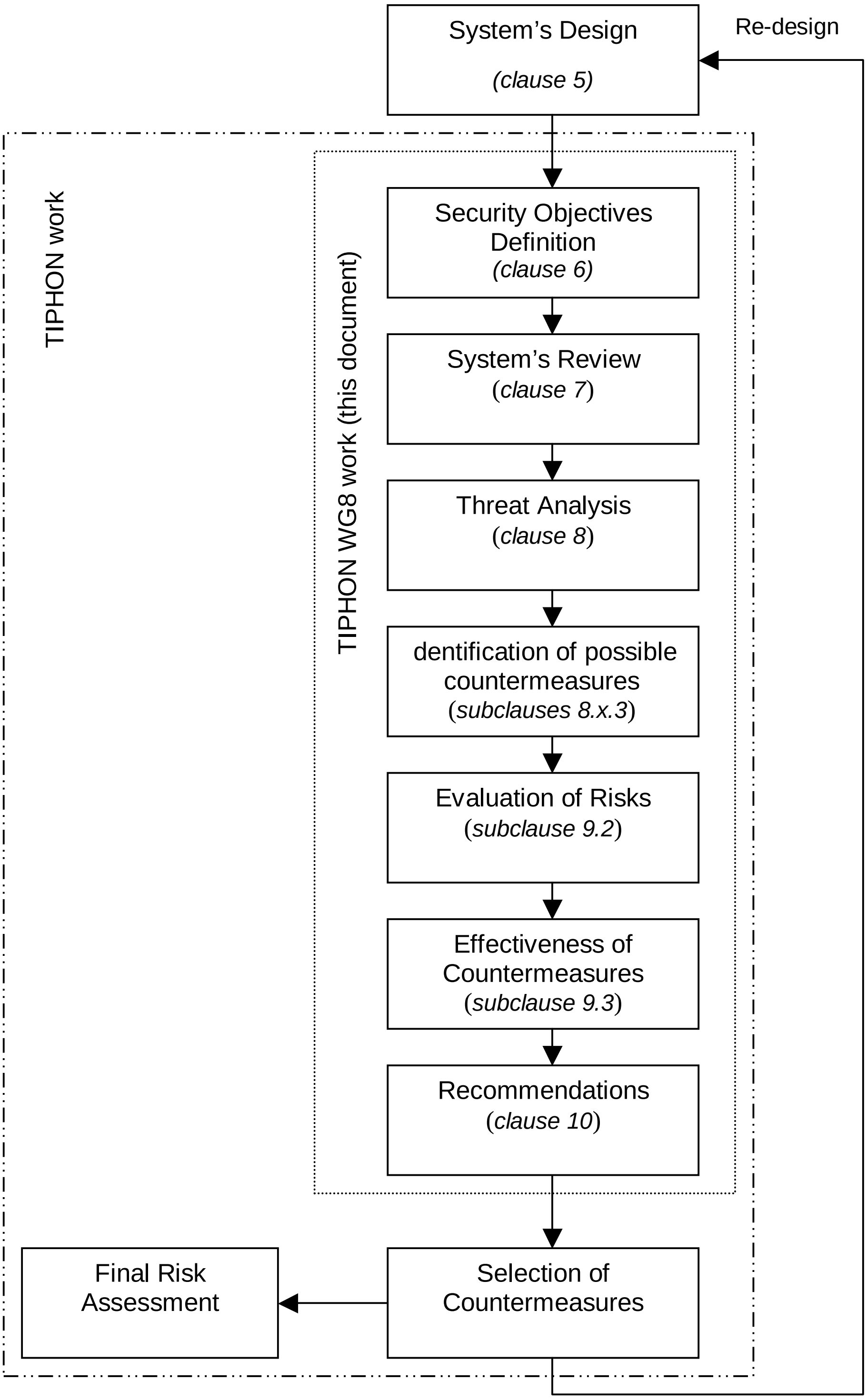


Figure 1: Structure of analysis

The present document is structured in the following way:

Clause 5 reflects the TIPHON architecture by using a simplified model as described in [17] according to the scope of the present document. The definition of the Security Objectives can be found in clause 6. A System's Review for a complete understanding of the system, its properties, boundaries and relationships to the external world is given in clause 7 based on a simplified architectural model. Clause 8 describes the threats identified to the network elements, their impact and lists possible countermeasures in clauses 8.1.3 to 8.7.3. The methodology of the risk assessment and the risk assessment itself is outlined in clause 9, covering the Evaluation of risks in clause 9.2 and the Effectiveness of countermeasures in clause 9.3. Clause 10 draws conclusions of the steps described in clauses 5 to 9 in listing a number of recommendations.

The following annexes are informative. Annex A deals with the Legislation Issues. Annex B provides a comprehensive description of the identified threats and gives examples. Annex C lists a number of countermeasures and possible implementations. Annex D contains a checklist for countermeasures against major threats.

5 System's Design

5.1 Network Architecture

This clause describes the general TIPHON network architecture in order to provide a basis to perform a complete threat analysis as outlined in clause 4. It covers the step "System's Review".

5.2 General Design

In this clause the mapping of the functional to the physical architecture and the network procedures are shortly described.

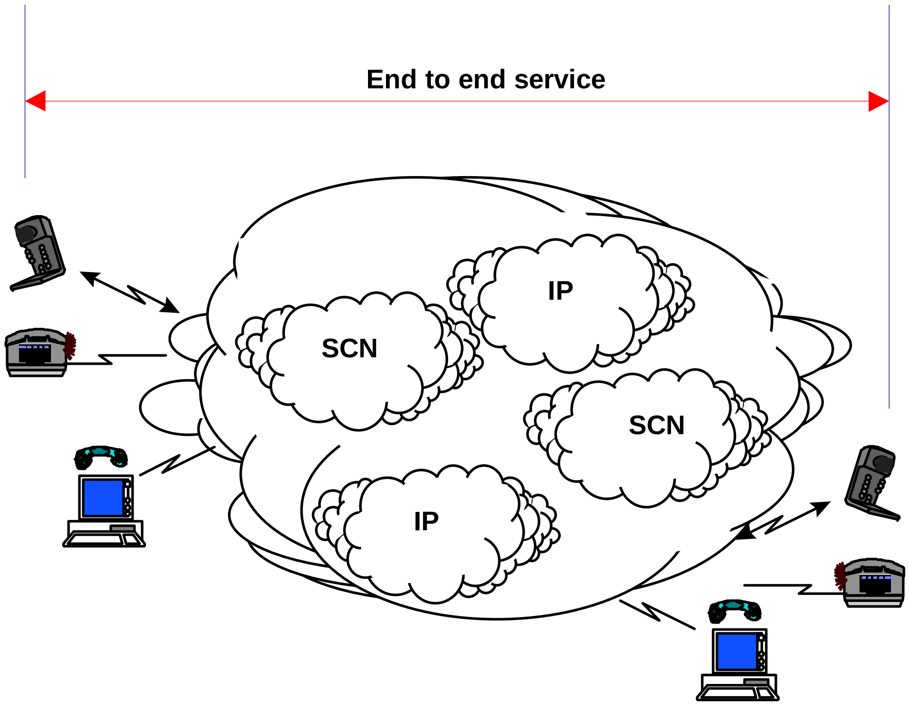


Figure 2: Overview of a general TIPHON domain

TIPHON can be drawn as a network of networks where the constituent networks may be based upon IP or Circuit Switching technologies. In addition TIPHON ensures that service users and providers are able to call upon standardized inter-domain settlement protocols.

The following assumptions shall apply as guiding principles for TIPHON:

- TIPHON terminals may be PC-like or telephone-like;
- the MMI of the terminal shall tend towards that of a telephone;
- operation of a TIPHON terminal shall tend towards that of a telephone (and shall therefore encompass single stage dialling, network type abstraction).

5.3 TIPHON Connectivity Scenarios

The TIPHON architecture is defined with respect to the support of a number of reference scenarios outlined below:

- the delivery of telephone calls which originate in an IP network and are delivered to Switched Circuit Networks (SCN), such as Public Switched Telephone Network (PSTN), Integrated Services Digital Networks (ISDN) and Global System for Mobile communication (GSM) networks (according to TIPHON Scenario 1);
- the delivery of telephone calls which originate in SCNs and are delivered in an IP network (according to TIPHON Scenario 2);
- the delivery of telephone calls which originate in SCNs, routed through an IP network and finally delivered to an SCN (according to TIPHON Scenario 3);
- the delivery of telephone calls which originate and terminate in IP networks. Such calls may be routed using an SCN (according to TIPHON Scenario 4).

NOTE: In each of the above cases the IP network hosted user is assumed to be using a TIPHON compliant terminal.

5.3.1 Scenario 1

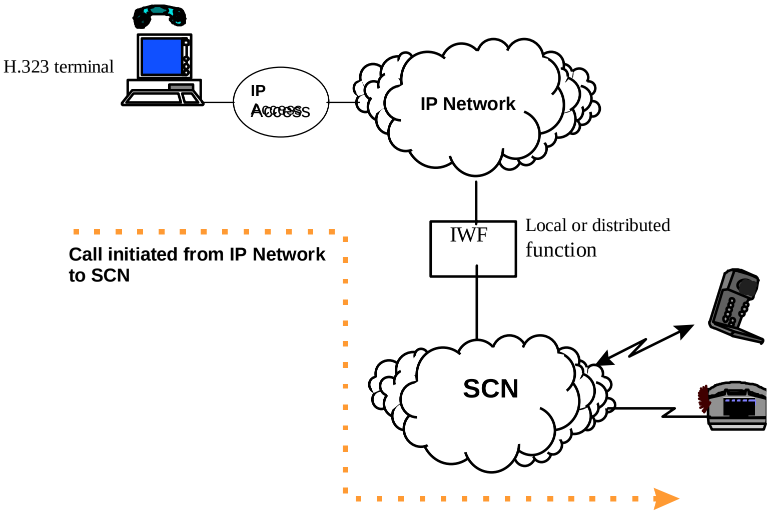

H.323 terminal
IP Access
IP Network
IWF
Local or distributed function
Call initiated from IP Network to SCN
SCN

Figure 3: Scenario 1, Source on IP network to destination on SCN network

5.3.2 Scenario 2

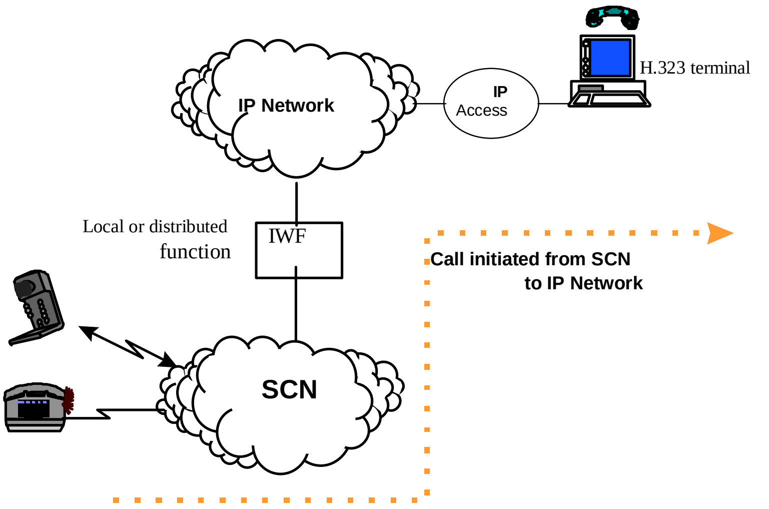


Figure 4: Scenario 2, Source on SCN network to destination on IP network

5.3.3 Scenario 3

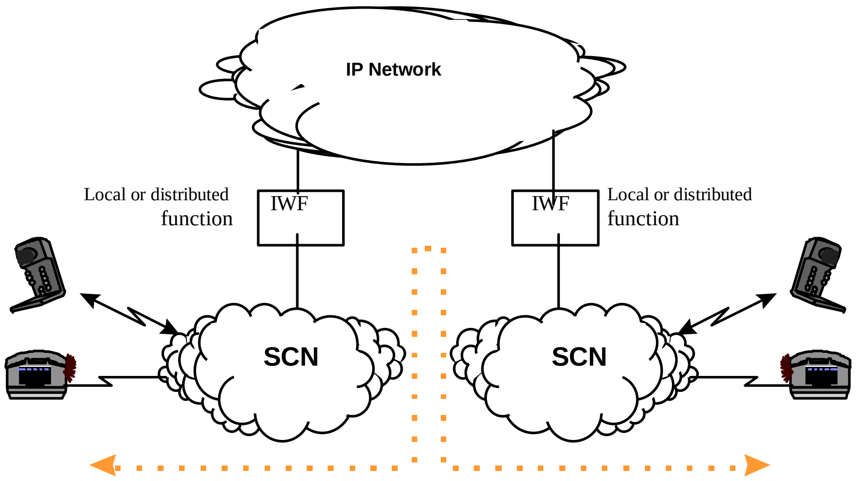


Figure 5: Scenario 3, Source and destination on SCN network using an IP transit network

5.3.4 Scenario 4

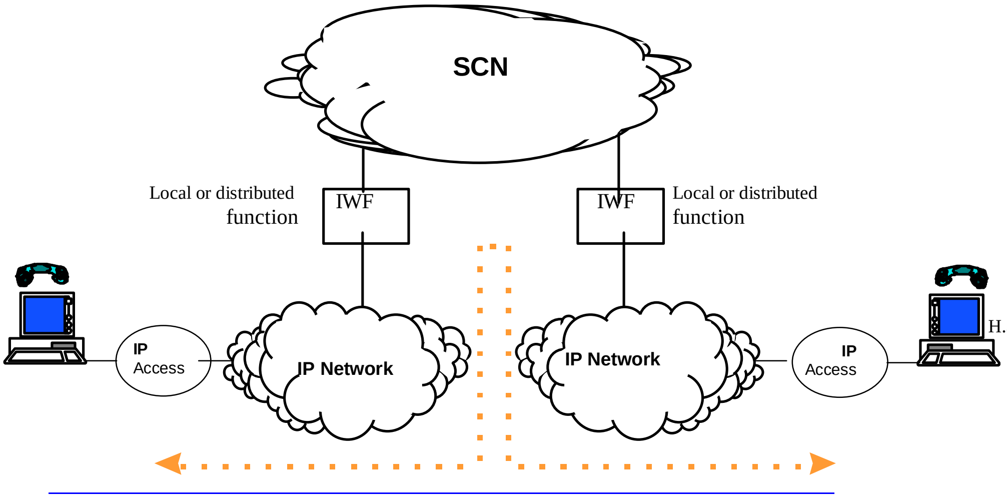


Figure 6: Scenario 4, Source and destination on IP network (maybe using an SCN transit network)

5.4 Services

For further study.

6 Security Objectives

The requirements for TIPHON security originate from different sources:

- Customers/Subscribers need confidence in services relying on EP TIPHON specifications, e.g. correct billing. In addition Customers/Subscribers demand availability of services, fair competition and privacy protection;
- Network Operators/Service Providers/Access Providers themselves need security to safeguard their operation and business interests, to meet their obligations to the customers and the public;
- The Authorities demand security by Directives and Legislation in order to ensure availability of services.

The reason why these parties are increasingly aware of security requirements is the fact that there are growing threats and risks caused by changes in the overall regulatory and technological environment. The purpose of this clause is to describe the aim of the security measures taken in a network and management for TIPHON compliant systems. Focus is on what security will achieve rather than how it is done. These generic security objectives form, together with the system's design (see clause 5: System's Design), a basis for threat analysis and risk assessment. The listed objectives do not contain general constraints like performance, cost, user friendliness etc.

6.1 Main Security Objectives

The general security objectives of the present document can be summarized to the following main security objectives (with appropriate definitions from ETR 332 [1]):

- **confidentiality**
  The avoidance of the disclosure of information without the permission of its owner.
- **integrity**
  The property that data has not been altered or destroyed in an unauthorized manner.

- **accountability**
  The principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation.

- **availability**
  The property of being accessible and usable upon demand by an authorized entity.

- **non-repudiation**
  A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

Therefore, threat analysis, risk assessment and proposed countermeasures will be based on these objectives. However, the following specific objectives may also be considered.

6.2 Customers' (Subscribers') Objectives

The objectives of customers are not uniform. An enterprise does not always require the same as a private person. The following list gives examples of possible objectives which may have implications on security:

- availability and correct functionality of service subscription (including reachability, availability and correct functionality);
- correct and verifiable billing;
- data integrity;
- data confidentiality/privacy;
- capability to use a service anonymously;
- location confidentiality (is probably part of service anonymousity).

6.3 Objectives of (TIPHON) Service and Network Providers

The following list gives examples of objectives that may have implications on security:

- availability and correct functionality of network procedures for TIPHON;
- availability and correct functionality of service, network and element management for TIPHON;
- correct and verifiable billing and accounting, above all no possibility of fraud;
- non-repudiation for all network procedures and for all management activities;
- preservation of reputation (above all preservation of customers' and investors' trust).

6.4 Manufacturers' Objectives

The following list gives examples of objectives that may have implications on security:

- fulfilling market objectives;
- preservation of reputation.

7 System's Review

In this first edition of the Threat Analysis the following architecture, which is derived from annex B of [15] forms the basis for evaluation and assessment. It has to be recognized that the architecture is subject to change as a result of the present document and thus may lead to revisions of the present document.

However, it should be noted that for the purpose of this generic threat analysis it is not necessary to look at the internal operations of the functional entities and therefore the following simplified architectural model can be used for all TIPHON scenarios.

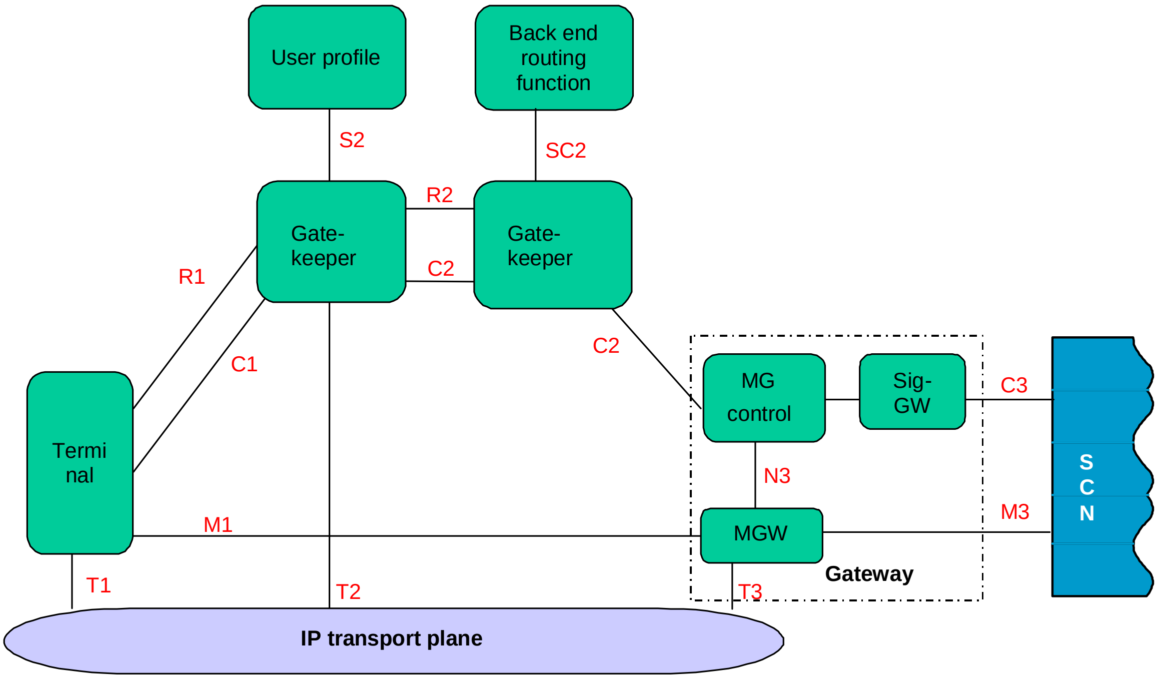


Figure 7: Network Elements and Interfaces

The primary investigations will be for reference points C1, C2, Mx, N3, Rx, S2, SC2 with all other reference points being investigated only where significant risks are identified. Physical access points are used to access logical reference points. This threat analysis concentrates on logical reference points to allow a finer granularity with the respect to threats.

Reference point C3 is out of scope of the present document, because it is part of an SS7 network, which should be based on an SS7 threat analysis.

For reference points Tx the IP transport plane is likely to also support non-TIPHON services. Generally a network provider for a large number of IP-based services will provide the IP transport plane. The IP transport plane is therefore out of scope of the present document. However, it is strongly recommended to IP network providers to perform an individual risk analysis and implement appropriate countermeasures to secure their network.

NOTE: After having read the TR 101 882 [17] we consider the present document as very useful. However, due to the urging demand for a first edition of the threat analysis, it was decided to go on with the simplified architecture model shown in the figure above.

8 Threat Analysis and possible Countermeasures

In this clause a description of common threats concerning the network and service architecture of TIPHON is given, in order to evaluate risks. Sophisticated application services based on generic TIPHON services are not taken into account. The likelihood of the threats is different and will be covered in clause 9. These major categories of threats are described below:

- Denial of service.
- Eavesdropping.
- Masquerade.
- Unauthorized access.

- Loss of information.
- Corruption of information.
- Repudiation.

8.1 Denial of service

An entity fails to perform its function or prevents other entities from performing their functions. More comprehensive descriptions and functions can be found in clause B.1.

8.1.1 Possible Attack Methods

- Flooding the target.
- Modifying stored information (e.g. user profile, routing information).
- Physical removing of resources (e.g. theft of equipment).
- Cutting off network connections.

8.1.2 Impact

- Inability to provide the service.
- Service failure.
- Degradation of service.
- Loss of revenue.
- Reduction of customer satisfaction (may lead to loss of customers).

8.1.3 Possible Countermeasures

- Authentication (see clause C.1).
- Access Control (see clause C.3).
- Secure Configuration of Operating Systems (see clause C.5).
- Physical Protection (see clause C.8).

8.2 Eavesdropping

A breach of confidentiality by unauthorized monitoring of communication, see clause B.2.

8.2.1 Possible Attack Methods

- Attaching a protocol analyser to any accessible link.
- Illegal use of lawful interception facilities.
- Illegal activation of optional features/tools (e.g. conference features).

8.2.2 Impact

- Loss of confidentiality of customer data.
- Loss of confidentiality of service information data.
- Loss of confidentiality of management information.
- Loss of confidentiality of charging information.
- Loss of confidentiality of authentication data.

8.2.3 Possible Countermeasures

- Virtual Private Network (see clause C.4).
- Access Control (see clause C.3).
- Secure Configuration of Operating Systems (see clause C.5).
- Secure Configuration of Network Elements (see clause C.6).
- Physical Protection (see clause C.8).
- Encryption (see clause C.9).

8.3 Masquerade

The pretence of an entity to be a different entity, see clause B.3. This may be the bases for other threats like unauthorized access or forgery.

8.3.1 Possible Attack Methods

- Hijack attack on a link after authentication has been performed.
- Using authentication information which has been obtained by eavesdropping, e.g. replay attack.

8.3.2 Impact

- Illegal access to the service/network.
- Loss of revenue.
- Financial disadvantage for individual legal subscribers.
- Loss of confidentiality.
- Loss of confidence in the system.

8.3.3 Possible Countermeasures

- Authentication by strong methods like one-time password, challenge response (see clause C.1).
- Digital Signature (see clause C.2).
- Virtual Private Network (see clause C.4).
- Access Control (see clause C.3).
- Physical Protection (see clause C.8).

- Encryption (see clause C.9).

8.4 Unauthorized access

An attacker gains access to a system or application without permission, see clause B.5.

8.4.1 Possible Attack Methods

- Exploiting system weaknesses.
- Masquerading as an entity with higher access permission.

8.4.2 Impact

- Loss of revenue.
- Illegal use of service.
- Loss of confidentiality.
- Loss or corruption of information.
- Forgery.
- Denial of service.

8.4.3 Possible Countermeasures

- Authentication (see clause C.1).
- Access Control (see clause C.3).
- Secure Configuration of Operating Systems (see clause C.5).
- Secure Configuration of Network Elements (see clause C.6).
- Virtual Private Network (see clause C.4).
- Digital Signature (see clause C.2).

8.5 Loss of information

The destruction of information, which may be stored or in transit along a path of communication. There is a difference in the impact of this threat to the users and the service providers. More information can be found in clause B.4.

8.5.1 Possible Attack Methods

- Deletion of data.
- Modification of access rights of other parties (as a consequence of an unauthorized access attack).

8.5.2 Impact

- Incorrect routing and addressing of messages.
- Loss of availability (e.g. denial of service).
- Loss of charging information.

- Loss of call content.
- Loss of revenue.

8.5.3 Possible Countermeasures

- Access Control (see clause C.3).
- Secure Configuration of Network Elements (see clause C.6).
- Secure Configuration of Operating Systems (see clause C.5).
- Physical Protection (see clause C.8).

8.6 Corruption of information

The compromise of data integrity by unauthorized insertion, modification or reordering. More information can be found in clause B.4.

8.6.1 Possible Attack Methods

- Modifying transmitted information.
- Modifying stored information (e.g. by masquerading or bypassing access control).

8.6.2 Impact

- Incorrect routing and addressing of messages.
- Various forms of interruption preventing access or communication.
- Unauthorized modification of information.
- Denial of service.
- Incorrect billing.
- Loss of trust.
- Loss of customers.

8.6.3 Possible Countermeasures

- Authentication (see clause C.1).
- Access Control (see clause C.3).
- Secure Configuration of Operating Systems (see clause C.5).
- Secure Configuration of Network Elements (see clause C.6).

8.7 Repudiation

One or more users involved in a communication deny participation. More information can be found in annex B.

8.7.1 Possible Attack Methods

- Denial of transmission.

- Denial of data receipt.
- Denial of data access.
- Denial of modification of data.

8.7.2 Impact

- Loss of revenue.
- Loss of trust.
- Loss of customers.

8.7.3 Possible Countermeasures

- Access Control (see clause C.3).
- Secure Configuration of Network Elements (see clause C.5).
- Non-repudiation measures (see clause C.12).

9 Risk Assessment

A potential threat is doing no harm unless there is a corresponding weakness in the system and until the point in time when the intruder exploits a weakness. Thus, the threats must be evaluated, i.e. it should be attempted to characterize them according to cost/effort involved (occurrence likelihood) and according to potential benefit/damage that can be done (impact value).

9.1 Methodology

In a first step all threats are evaluated according to the following scheme:

- evaluate impact (= "I") on each threatened subject, e.g. using three different levels (1 through 3);
- identify likelihood of occurrence (= "0") for each threat, using three different levels (1 through 3);
- calculate a risk factor (= "Ix0") for each threat;
- put all this information into the threat evaluation table;
- identify "minor", "major" and "critical" risks.

NOTE: In the list above "risk factor" is equivalent to the term "exposure factor" in ETR 332 [1].

For the risk assessment, the occurrence likelihood of threats is estimated with values from "1" to "3". The meaning of a certain value associated to the occurrence likelihood of a particular threat is explained as follows:

Table 1: Occurrence likelihood

1	For "unlikely"	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.
2	For "possible"	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	For "likely"	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

The impact of a threat is also estimated with values from "1" to "3". However, the impact may differ with respect to the affected party. Threats that are devastating for a subscriber may be of minor immediate impact on a service provider, and vice versa. In such cases the lower and the upper bound of the impact are given. The meaning of a certain value associated to the impact is explained as follows:

Table 2: Impact

	Threat level	General description	
		Impact affects subscribers	Impact affects the system
1	For "low impact"	The affected party is not harmed very strongly; possible corruption is reversible.	
		Subscribers are annoyed.	System remains operable in general, while increased efforts in administration are necessary. While outages of individual services may occur, these are tightly limited in time. And/or A small number of subscribers suffer medium impact.
2	For "medium impact"	The threat addresses the interests of the affected party and cannot be neglected.	
		Subscriber suffers tightly limited financial loss and/or equivalent inconveniences (loss of privacy etc). And/or Services are not available for a considerable time.	The system in general is not operable for a tightly limited time. and/or Outages of individual services and/or corruption of system assets occur, leading to limited financial loss (immediate and/or legal claims of business partners and/or bad reputation). And/or A small number of subscribers suffer high impact.
3	For "high impact"	A basis of business is threatened and severe damage might occur in this context.	
		Subscriber suffers substantial financial loss and/or equivalent inconveniences And/or Services are not available for such a long time that essential customer needs are violated.	The system in general is not operable for a considerable time. And/or Outages of services and/or corruption of system assets occur, leading to severe financial loss (immediate and/or legal claims of business partners and/or bad reputation). And/or Laws are violated.

The product of occurrence likelihood and impact value gives the risk, which serves as a measurement for the risk, that the concerned management function is compromised.

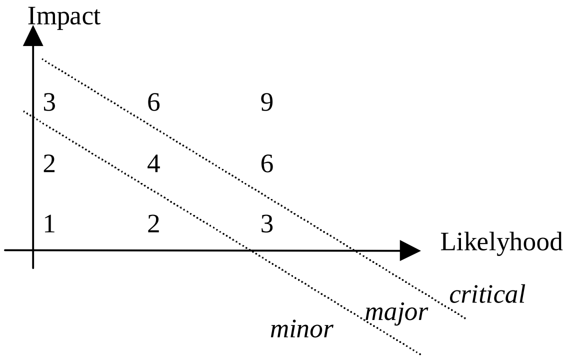


Figure 8: Risk classification

The result is classified into the following three categories:

Table 3: Risk factors

1, 2	for "minor risk"	Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats causing minor risks have no primary need for countermeasures.
3, 4	for "major risk"	Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimized as soon as possible.
6, 9	for "critical risk"	Critical risks arise, when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks shall be minimized with highest priority.
NOTE: The values 5, 7, and 8 cannot occur.		

9.2 Evaluation of Risks

This clause gives figures for likelihood and impact of identified attack scenarios and calculates the risk factors for TIPHON compliant systems.

It shall be noted that this threat analysis identifies and analyses threats on network elements and reference points from a generic point of view. Thus it does not reflect possible physical implementations and configurations. In addition a threat analysis can be performed from various viewpoints, e.g. from of a user's or a systems operator's perspective. The present document falls in the latter category.

As a result the values given in the table 4 may not be given as precise value but cover a range (e.g. non-redundant centralized systems are much more vulnerable as redundant distributed systems).

Table 4: Risk factors for TIPHON network architecture

	Attack scenario	Threat Reference	Possible occurrence of threats (entities/reference points)	Motivation	Likelihood	Impact	Risk factor
Denial of Service							
1	Flooding the target for Denial of Service	8.1	T, GK, MGC R1, C1, R2, C2, S2, SC2, M1, M3, N1, C3	Sabotage, attacker satisfaction	3	3	9
2	Modifying stored information	8.1	GK, UP, BRF S2, SC2, R1, R2, C1, C2	Sabotage, disabling and harming of individual subscribers, attacker satisfaction	2	3	6
Eavesdropping							
3	Attaching a protocol analyser to any accessible link	8.2	--- R1, C1, R2, C2, C3, SC2, N3, M1, M3,	Espionage, getting information (e.g. prerequisite for masquerade and sabotage), attacker satisfaction	2-3	2-3	4-9
4	Illegal use of lawful interception facilities	8.2	(note 1) (note 1)	Espionage, getting information, attacker satisfaction	1	1-3	1-3
5	Illegal activation of optional features/tools	8.2	T, GK, MGC C1, C2, C3, R2	Espionage, getting information, attacker satisfaction	1	1-3	1-3
Masquerade							
6	Hijacking a link after authentication has been performed.	8.3	GK, SGW (note 2) C1, C2, C3, M1, M3	Fraud, harming subscribers, sabotage, getting information, attacker satisfaction	2	3	6
7	Using authentication information, which has been obtained by eavesdropping.	8.3	T, GK, UP R1, C1, S2, R2, C2, SC2	Fraud, harming subscribers, sabotage, getting information, attacker satisfaction	3	3	9

	Attack scenario	Threat Reference	Possible occurrence of threats (entities/reference points)	Motivation	Likelihood	Impact	Risk factor
Unauthorized access							
8	Exploiting system weaknesses	8.4	T, GK, UP, BER, MGC, MGW, SGW R1, R2, C1, C2, SC2, S2, M1, M3, C3, N3	Fraud, harming providers, sabotage, getting information, attacker satisfaction	2-3	2-3	4-9
9	Masquerading as an entity with higher access permission	8.4	T ,GK, MG, MGW, SGW R1, C1, R2, C2, C3, M3, M1, N3	Fraud, harming providers, sabotage, getting information, attacker satisfaction	1-2	2-3	2-6
Loss of information							
10	Deletion of data	8.5	T, GK, UP, BER, MGC, SGW, MGW R1, C1, R2, C2, C3, M3, M1, N3	Sabotage, harming providers and individual subscribers, fraud	1-2	2-3	2-6
11	Modification of access rights of other parties	8.5	GK; UP; BER, R1, S2, R2, SC2	Harming providers and individual subscribers	2-3	3	6-9
Corruption of information							
12	Modifying transmitted information	8.6	--- R1, C1, R2, C2, C3, M3, M1, N3	Sabotage, harming providers and individual subscribers	1	3	3
13	Modifying stored information	8.6	T, GK, UP, BER, MGC, SGW, MGW R1, C1, R2, C2, C3, M3, M1, N3	Sabotage, harming providers and individual subscribers	2	3	6
Repudiation							
14	Denial of data transmission	8.7	GK, UP R1, C1, R2, C2	Fraud, harming providers and subscribers	1	3	3
15	Denial of data receipt	8.7	GK, UP R1, C1, R2, C2	Fraud, harming providers and subscribers	1	3	3
16	Denial of having accessed data in a database	8.7	GK, UP, BER R1, C1, R2, C2	Fraud, sabotage	1-2	3	3-6
NOTE 1: Technical implementations are subjects to national law. NOTE 2: Signalling Gateway is included because of SCN subscriber dialer scenario.							

9.3 Effectiveness of Countermeasures

This clause applies the countermeasures as listed in clause 10.1 and generally described in annex C to all threats classified as critical risks (i.e. risk factors 6 and 9), associates new values for likelihood and impact (named L* and I*) and calculates the residual risk factor (as RF*). It is assumed that the impact may not alter after implementation of security countermeasures. In cases where RF* is not less than 6, more than one countermeasures have to be combined to further reduce RF*.

Table 5: Effectiveness of countermeasures for TIPHON network elements

Threat	Threat Reference	Original			Countermeasure	CM Reference	Residual		
		L	I	RF			L*	I*	RF*
Denial of Service									
Flooding the target for Denial of Service	8.1	3	3	9	Authentication	C.1	2	3	6
					Access Control	C.3	1	3	3
Modifying stored information	8.1	2	3	6	Authentication	C.1	1-2	3	3-6
					Access Control	C.3	1-2	3	3-6
					Securing Configuration of Networks	C.6	1-2	3	3-6
Physical removing of resources	8.1	2	3	6	Physical Protection	C.8	1-2	3	3-6
Eavesdropping									
Attaching a protocol analyser to any accessible link	8.2	2-3	1-3	2-9	Access Control	C.3	1-2	1-3	1-6
					Securing the operating system	C.5	1-2	2-3	2-6
					Secure configuration of networks	C.6	1-2	2-3	2-6
					Physical Protection	C.8	1-2	1-3	1-6
					Encryption	C.9	1	1-3	1-3
Masquerade									
Hijacking a link after authentication has been performed.	8.3	2	3	6	Authentication	C.1	1	3	3
					Physical Protection	C.8	1-2	3	3-6
					Encryption	C.9	1	3	3
Using authentication information, which has been obtained by eavesdropping.	8.3	3	3	9	Authentication	C.1	1	3	3
					Encryption	C.9	1	3	3
Unauthorized access									
Exploiting system weaknesses	8.4	2-3	2-3	4-9	Authentication	C.1	1-2	2-3	2-6
					Access Control	C.3	1-2	2-3	2-6
					Securing the Operating System	C.5	1-2	2-3	2-6
					Secure configuration of networks	C.6	1-2	2-3	2-6
Masquerading as an entity with higher access permission	8.4	1-2	2-3	2-6	Authentication	C.1	1-2	2-3	2-6
					Access Control	C.3	1-2	2-3	2-6
					Securing the Operating System	C.5	1-2	2-3	2-6
					Secure Configuration of networks	C.6	1-2	2-3	2-6
Loss of information									
Deletion of data	8.5	1-2	3	3-6	Secure configuration of networks	C.6	1	3	3
Modification of access rights of other parties	8.5	2-3	3	6-9	Secure configuration of networks	C.6	1-2	3	2-6
Corruption of information									
Modifying transmitted information	8.6	1	3	3	Secure Configuration of Networks	C.6	1	3	3
					Encryption	C.9	1	3	3
Modifying stored information	8.6	2	3	6	Authentication	C.1	1-2	3	3-6
					Access Control	C.3	1	3	3
					Securing the Operation System	C.5	1	3	3
					Secure Configuration of Networks	C.6	1-2	3	3-6
Repudiation									
Denial of having accessed data	8.7	1-2	3	3-6	Secure configuration of networks	C.6	1	3	3
					Access Control	C.3	1	3	3
					Intrusion Detection Systems	C.10	1	3	3
Denial of having modified data	8.7	1-2	3	3-6	Secure configuration of networks	C.6	1	3	3
					Access Control	C.3	1	3	3
					Intrusion Detection Systems	C.10	1	3	3

<table>
<tr><th rowspan="2">Threat</th><th rowspan="2">Threat Reference</th><th colspan="3">Original</th><th rowspan="2">Countermeasure</th><th rowspan="2">CM Reference</th><th colspan="3">Residual</th></tr>
<tr><th>L</th><th>I</th><th>RF</th><th>L*</th><th>I*</th><th>RF*</th></tr>
<tr><td colspan="10">NOTE 1: The use of more than one of the indicated countermeasure may reduce the possible likelihood, thus reducing the risk factor.
NOTE 2: The residual likelihood values used in conjunction with encryption measures are dependent on the algorithm strength and the chosen key length. This is also valid for the authentication mechanisms, i.e. the use of strong authentication reduces the likelihood of an attack much better than simple passwords.
NOTE 3: Impact values remain unchanged given if one or more countermeasure(s) are implemented.</td></tr>
</table>

10 Recommendations

10.1 Security Policy

Operators and service providers of TIPHON compliant systems shall establish and apply a security policy. It is a set of rules and practices that specify or regulate how a system or organization provides security to protect sensitive and critical system resources.

The threat analysis as performed in the clauses prior to this, has shown technical weaknesses to the TIPHON network and its environment. To secure a TIPHON compliant system, consisting of a large number of individual subsystems it is inevitable for each subsystem to set up an individual security policy and to perform an individual threat analysis, where the present document can be used as **a baseline document** giving guidance and examples.

It should clearly be pointed out, that an individual threat analysis does not contain only technical issues as described in the present document. It should also focus on:

- Force Majeure
  This category includes threats based upon the environmental events and conditions, like: magnetic fields, dust, burning cables, humidity, etc.

- Human Failure
  Human failures very often are seen as part of deliberate acts, but a distinction should be made between intentional (deliberate) acts and unintentional actions (e.g. caused by personal not-well trained, faulty systems administration and operation) because of different applicable countermeasures.

- Organizational shortcomings and threats
  This category should play a major role in the security policy of a company as shortcomings may cause large impact. Possible shortcomings are: Inadequate maintenance, inadequate access rights and access controls, inadequate capacities and resources, etc.

- Environmental threats
  This category covers threats existing in the natural environment, like lightning, fire, water, etc.

- Deliberate Acts
  Deliberate acts cover intentional actions taken by people to destroy or damage buildings, systems or parts of it, such as vandalism, theft, etc.

More detailed information can be found in [7].

Basic countermeasures against these threats should be implemented within the lawful or regulatory framework of the individual country, where TIPHON compliant services are publicly offered. Additional countermeasures depend on service providers preferences.

Generally, the security policy should be visible for the users.

10.2 Recommendation to the TIPHON Security Profiles

As to be seen in clause 9.3. some countermeasures are identified as means to secure a wide range of threats. Especially Authentication and Encryption are mentioned in numerous circumstances. These countermeasures, however, can be implemented in various ways and thus offer high or only medium security.

For all implementations of TIPHON compliant systems security profiles have to be developed in order to assure a certain level of security and to allow a secure interoperation between networks and services. Such profiles can be found in [11]. However as [11] is limited to the H.323 [12] compliant systems further security profiles might be necessary.

It is therefore recommended to generally take the countermeasures given in annex C into account.

10.3 Recommendation to the TIPHON network architecture

Based on the security objectives and identified threats it is highly recommended to consider security measures while developing the network architecture. An example may be redundant systems to meet the availability requirements.

The security objectives should also be adapted at the real implementation by network operators and services providers as well as manufacturers.

10.4 Recommendation to TIPHON Services

For each TIPHON Service it may be necessary to additionally establish a service specific security policy. It should contain e.g. administrative rights, access rights for users and operators, ...

For further study

Annex A: Legislation Issues

The following areas of legislation may have influence on the realization of security.

A.1 Privacy

Privacy legislation is of increasing importance; there are strong restrictions in many countries with regard to storage and visibility of data. Therefore, when offering a TIPHON service, or when designing data processing functions and defining the kind of data being generated or stored within TIPHON systems, TIPHON service providers shall consider the relevant national data protection laws.

The definition of privacy for TIPHON includes:

- **privacy of information:** keeping information exchanged between TIPHON service functions away from third parties;
- **limitations on collection, storage and processing of personal data:** personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of TIPHON services;
- **disclosure:** the obligation of a network and service providers to keep information concerning customers away from third parties; and
- **inspection and correction:** the right of the customer to inspect and correct information about himself stored by the service and/or network provider.

Privacy legislation will mostly concern the security objectives regarding "data confidentiality" and "data integrity". For TIPHON special concern in this respect shall be paid to the contents of personal data in the TIPHON service profile. These data and the access conditions to it for the service provider's personnel, the subscriber and the user himself shall be limited, in accordance with the relevant European guidelines and national laws.

A.2 Security Order

National laws concerning the security order:

- demand proper protection of information and infrastructure to ensure the availability and the integrity of the telecommunication network (including the TMN); and
- may restrict the usage of cryptographic methods.

This legislation will mostly concern the security objectives regarding "data confidentiality", "data integrity" and "availability".

A.3 Lawful Interception

Lawful interception means the obligation of the network operator/service provider/ access provider to co-operate and provide information based on existing regional and national laws and regulations (see TR 101 750 [3]).

This legislation will mostly influence the security objectives regarding "data confidentiality".

A.4 Contract

It shall be possible to use information concerning the contract for communication services between two entities in case of a dispute in a court of law.

This legislation will mostly influence the security objectives regarding "accountability" and "data integrity".

Annex B: Description of Threats

The descriptions of threats in this annex are ordered alphabetically as listed in clause 8.1 Threat Categories.

B.1 Denial of services

In February 2000 denial of service attacks on commercial sites such as AOL, eBay and Amazon.com sounded an alarm throughout the e-business community. What was noteworthy about these attacks was that the intruders used distributed tools to launch them. These tools allow the hacker to orchestrate a large number of coordinated hosts to simultaneously launch attacks against a victim. Both the target site as well as the sites used by the hackers to launch the attack can experience serious denial of service problems. The hackers use UDP, ICMP echo, SYN packets and other methods to flood the target with the goal of consuming all of the target's network capacity and other resources including processes, CPU time, disk space, nodes, ports and directories.

B.1.1 Denial of Service on Network Elements

This attack is made by continuously sending data to the TIPHON network elements so that no more resources are available for other TIPHON users.

B.1.2 Denial of Services

This threat might be a result of the previous one. If the relevant network elements are no longer able to perform a user request the TIPHON services could not be offered to the users any longer.

B.2 Eavesdropping

Eavesdropping is a threat against the confidentiality. Intercepting the line between the sender and the receiver performs it. The decision to intercept a line will essentially depend on whether the information to be obtained will be worth the technical (financial) expenditure and the risk of being detected. The attacker's means and interests will largely determine the answer to this question. Therefore, definitive identification of the targeted information, and thus of the lines which might be intercepted, is not possible.

In most cases, eavesdropping is used to obtain data (e.g. such as user identification and authentication data) to be able to perform more serious threats at another point in time, like masquerade, unauthorized access.

B.2.1 Eavesdropping of content of communication

This threat is an attack against the privacy and confidentiality of data. Since this are fundamental security requirements procedures must be deployed to counter this attack.

B.2.2 Eavesdropping of network element IDs

Network element IDs are used by entities to authenticate each other prior to the exchange of data. If attackers know these IDs, they can use them to run masquerade attacks to a later point of time to some NE. This can be the predecessor of other attacks like unauthorized access to NEs and confidential data as well as Denial of Service attacks. This attack may be part of clause B.2.4 (Eaves-dropping of network element authentication data).

B.2.3 Eavesdropping of service authorization data

If several different kinds of services are provided to the user, the user has to be authorized for each service and then select the specific service he wants to use. Eavesdropping of the service authorization data may lead to subsequent attacks, like e.g. masquerade, unauthorized access.

B.2.4 Eavesdropping of network element authentication data

Prior to the exchange of information either inter- or intra-domain, the network elements involved have to be authenticated to each other. Eavesdropping of these data may lead to subsequent attacks, like e.g. masquerade, unauthorized access.

B.3 Masquerade

A perpetrator to feign a false identity uses masquerading. For instance, he will obtain a false identity by spying out the user ID and password, by manipulating the originator field of a message or by manipulating the I/O address within the network.

A user who has been deceived as regards the identity of his communication partner can in that case easily be induced to disclose sensitive information.

A perpetrator can also use masquerading to try and tap an existing connection without having to authenticate himself, as this step has already been taken by the original participants in the communication (see also *Eavesdropping*).

The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

B.3.1 Masquerade as legitimate user during the registration process

If an attacker knows the authentication data of a legitimate user, he can e.g. illegally register and place calls for which the attacked user has to pay. Additionally he may feign action not intended by the attacked user without his knowledge to either harm him or to get personal advantages. Another attack may be to change the correct destination terminal of a user to his own one having the following consequences:

- the attacker may get unauthorized access to the content of the attacked user's communication;
- the attacked user may have to pay for forwarded calls to other terminals.

B.3.2 Masquerade as network entity during the registration process

If an attacker masquerades during the registration process as another network entity, he may get access to the personal authentication data of legitimate users. He can later on use them to get access to the TIPHON environment e.g. to place calls the attacked user has to pay for.

B.3.3 Masquerade as legitimate user during the authentication process

Before a subscriber may use a service (either registering or setting up calls) he must be identified and authenticated by the TIPHON environment. If an attacker knows the authentication data of a legitimate user, he can e.g. illegally register and place calls for which the attacked user has to pay. Additionally he may feign action not intended by the attacked user without his knowledge to either harm him or to get personal advantages.

B.3.4 Masquerade as network entity during the authentication process

If an attacker masquerades during the authentication process as another network entity, he may get access to the personal authentication data of legitimate users. He can later on use them to get access to the TIPHON environment e.g. to place calls the attacked user has to pay for.

B.3.5 Masquerade as calling party during call setup

After a legitimate user has been successfully authenticated and registered he may now place calls. This threat allows the attacker to place calls charged to the attacked user.

B.3.6 Masquerade as called party during call setup

If an attacker masquerades as called party, the call will be routed to a different terminal as the calling user has intended. This may lead to denial of service attacks to the attacked user.

B.3.7 Masquerade as non-terminating network entity during call setup

If an attacker masquerades as a non-terminating network entity during the call setup process, this may cause rerouting of calls to another domain e.g. to perform subscription fraud. An example for this attack might be the exchange of free phone numbers with Premium Rate Services (PRS) numbers to run billing frauds. In this case the attack is run against the user. The following scenario is possible here:

- After the user has entered the called party number a request is sent to his home domain to check whether the calling user is allowed to call the called party. In the case where the home domain sends back a positive notification to the GK where the calling user is registered, the call is routed to called party. If on the way to the called party an attacker tries to change the called party number to a PRS number the call will be routed to this number causing that the calling user has to pay the high rates.

B.3.8 Masquerade as conference call party during an active connection

If a call has already been set up between at least two parties, another user might masquerade as a legitimate user being allowed to participate in the conference call. By doing this, he might be able to eavesdrop the call. See clause B.2.1 Eavesdropping of content of communication.

B.3.9 Masquerade as non-terminating network entity during an active connection

After successful call setup an attacker may masquerade as another network entity in order to obtain parts of the content of communication (e.g. one time password). Information being obtained by such an attack may later be used for fraudulent activities (e.g. modification of content of communication). An example of this could be a banking application where specific actions, e.g. transactions are secured by one-time passwords. An attacker may masquerade as "man-in-the-middle" and through eavesdropping means may wait until one-time passwords are exchanged. At that specific point in time the attacker may play the role as bank (in the direction to the user) and "accept" the one-time password. The bank, however, doesn't know about the transaction and the use of that one-time password, so in subsequent connections would accept that one-time password as valid. The attacker could later use that one-time password for a fraudulent transaction.

B.4 Modification of information

In this case, data is corrupted or rendered useless through deliberate manipulation. The consequences of this are the rejection of authorized accesses to network resources.

In principle, it is not possible to prevent users from deliberately manipulating data or destroying a database within the scope of the access rights allocated to them. However, if access rights can be circumvented (e.g. due to incorrect administration of the DBMS), then even unauthorized parties can gain access to the database and manipulate the data contained therein.

Attackers may be interested in modifying either the information required during the registration or the call set up phase. Reasons for this might be to use a service for which the attacked user has to pay.

Generally modification of information may be a starting point for denial of service or masquerade and fraud attacks.

B.4.1 Modification of Terminal IDs

The terminal ID is allocated by the GK and included in the H.225.0 Registration, Admission and Status (RAS) Registration Confirm (RCF) message sent back to a terminal as response to a prior sent Registration Request (RRQ) RAS message. In all subsequent RAS messages this terminal ID should be present and will be used for identifying the associated terminal.

If this ID would be changed this could lead to other attacks such as denial of service, which may be used, with a masquerade attack.

B.4.2 Modification of call setup information

The following are only some examples for attacks that are possible when modifying the call setup information:

- modification of the calling ID could result in masquerade attacks and further on in billing frauds against the calling party;
- modification of the called ID could result in denial of service attacks to the called party;
- modification of the service number might result in billing frauds against the ITSP (e.g. replacing a PRS number with a low rate number).

B.4.3 Modification of routing information

Routing information has to be stored in each domain (e.g. either in the GK or the AD-BES). Modification of this information may lead to denial of service attacks or to billing fraud against ITSPs as well as against users.

B.4.4 Modification of user access authentication data (e.g. for subsequent use)

The service profile of each user stored in the AD-BES contains the identification and authentication data. Before a user may place a call he must identify and authenticate himself to the environment of his ITSP.

If this data would be modified it will result in denial of service attacks to the user wanting to get access to the environment of the ITSP.

If this data would be modified and made available to other users so that they could place calls on behalf of the user whose authentication data have been changed, this could cause problems not only for the user who has to pay for the calls but also for the ITSP.

NOTE: Therefore the possibility for this threat is higher at the GK and the AD-BES where these data are stored.

B.4.5 Modification of data exchanged in the registration process

Before a user is able to place a call he must register to the TIPHON environment. If the call is originated from an IP Terminal, sending an H.225.0 Registration Request (RRQ) message to an adjacent GK does this. If the call is initiated from an SCN terminal the user has to call a special number provided by his ITSP and then enter his identification and authentication data. If the user is correctly registered, the AD-BES has to be informed that this special user is now registered for incoming, outgoing or both types of calls.

Generally modifying these data could lead to other threats like denial of service, masquerade or fraud attacks.

B.4.6 Modification of content of communication

This threat is considered to be not very relevant for voice communication since this is a mostly real-time communication. One possible case is the case where there is a speech recognition device present changing the content of communication. Other possible scenarios are communication with the digital voice box of a user or adding some kind of noise leading to a denial of service attack.

B.4.7 Modification of network element IDs

Each network element must have a unique ID so that it can be identified in the whole environment. If the IDs of special network entities would be modified so that the calls are routed to wrong entities possessed by attackers, the attackers would have access to private data (e.g. authentication data).

This threat can be seen as predecessor of other threats like masquerade, denial of service, unauthorized access.

B.4.8 Modification of service authentication data (i.e. part of content of communication)

An ITSP may provide different kinds of services. For each subscriber of these services his service profile specifies which services the subscriber is allowed to use and how much he has to pay for using it.

If these data would be modified, a user might change the entries in his service profile to enable himself to use special services he is currently not allowed to use or to change the rates he has to pay for using the services.

B.4.9 Modification of network element authentication data

In some cases like for the communication between the AD-BES and the global services like RS and CH access to these global services should be restricted to special network elements. If these data would be changed unauthorized network elements would get access to private data. These could enable attackers to perform other threats like masquerade, unauthorized access and denial of service.

B.4.10 Modification of billing data

Settlement data are exchanged either by the use of a centralized CH by sending OSP messages between the GK of the ITSP and the CH or by bilateral agreed protocols.

One possible example for an attack is to exchange PRS numbers with freephone numbers. This attack is run against the ITSP and leading to loss of revenue.

A description of the three terms can be found in RFC 2194 [16].

B.5 Unauthorized access

Access to network entities must be restricted and inline with the security policy in place. If attackers get unauthorized access to any of the network entities this could generally lead to various other attacks like denial of service, eavesdropping or masquerade. Likewise it is possible that unauthorized access is also a consequence of the other threats mentioned above.

An entity accesses data in violation to the security policy in force.

B.5.1 Unauthorized access to a network element

If this attack is done as a consequence to a masquerade attack, the unauthorized user will have the same access as the authorized user. This may e.g. lead to unauthorized access to network data so that the network capability could be modified. Additionally this may lead to unauthorized access to service elements as well, e.g. modification of user specific data.

B.5.2 Unauthorized access on service elements

If an attacker gets unauthorized access to service elements this might lead to unauthorized usage of the service as well as to the possibility to change user specific data in a user's service profile.

Annex C:
Description and possible examples of Countermeasures

Countermeasures can generally be categorized as preventive or as detective Countermeasures.

The Countermeasures listed below can either be described as security services or as security mechanisms.

Generally security services can deploy one or more security mechanisms e.g. an Authentication service. A service offering Authentication may be built by various combinations of mechanisms e.g. cryptographic certificates, passwords.

To some Countermeasures, additional controls have to be taken by the user. These additional controls are not pointed out within this edition.

C.1 Authentication

Authentication provides assurance of the claimed identity of an entity. It is applicable in communication relationships between a principal (claimant) and a verifier (entity authentication). Examples of principals that can be identified and hence authenticated are:

- human users;
- non-human users.

A verifier is or represents the entity requiring an authenticated identity and includes functions necessary for authentication information exchanges [4].

Authentication can be unilateral or mutual. Mutual authentication provides assurance of the identities of both entities, which should normally be the procedure in TIPHON.

Authentication can be based on different methods. Inherent weaknesses of the individual methods lead to combination of methods. Descriptions of authentication mechanisms can be found in [5] and [6]. Mechanisms with different strength shall be identified in the following:

C.1.1 Authentication with password

Authentication with password either used by human users or e.g. processes is considered weak due to threats such as guessing and replay. Observation of the following rules, which can partly be enforced by the application process, can increase the strength of this mechanism:

- it must not be possible to guess the password as easily as names, motor vehicle license numbers, birth dates, or the like;
- the password should comprise at least one non-letter character (special character or number);
- the password should consist of at least 6 characters. The number of password digits checked by the computer must be tested;
- preset passwords (e.g. by the manufacturer at the time of delivery) must be replaced by individually selected passwords;
- passwords must not be stored on programmable function keys;
- the password must be kept secret and should only be known personally to the user;
- the password should be laid down in writing only for the purpose of its depositing when it will be kept safely in a sealed envelope. If an additional written record is made, the password should be kept at least as safely as a check identification card or a bank note;
- the password must be altered regularly, e.g. every 90 days;

- the selection of trivial passwords (BBBBBB, 123456) must be prevented;
- every user must be able to alter his own password at any time;
- for initial log-on of new users, one-time passwords should be assigned, i.e. passwords which must be discarded after their first use. In networks in which passwords are transferred in non-encrypted form;
- the constant use of non-recurrent passwords is recommended;
- after three unsuccessful attempts to enter the correct password, a lockout should be imposed which can only be cancelled by the system administrator;
- during authentication of networked systems, passwords should not be transmitted in a non-encrypted form;
- the password must be entered covertly, i.e. the entry shall not be displayed on the monitor;
- passwords should be stored in the system in a way preventing unauthorized access, e.g. by means of encryption;
- password alteration must be initiated by the system on a regular basis;
- re-use of previous passwords in the case of password alteration should be prevented by the IT system (password history).

C.1.2 Authentication based on one-time passwords

This method is considered to provide higher security than static passwords as described in C.1.1. However, it does require that lists of one-time passwords are distributed securely. This is a major drawback for remote users:

- because one-time passwords are usually distributed as lists, it is not required that the chosen passwords are easy to remember;
- passwords should be stored in the system in a way preventing unauthorized access, e.g. by means of encryption;
- password lists should be laid down in writing only for the purpose of its depositing when it will be kept safely in a sealed envelope. If an additional written record is made, the password lists should be kept at least as safely as a check identification card or a bank note;
- the generation of one-time passwords should provide passwords resembling random character sequences;
- the password should comprise at least one non-letter character (special character or number);
- the password should consist of at least 8 characters. The number of password digits checked by the computer must be tested;
- after three unsuccessful attempts to enter the correct password, a lockout should be imposed which can only be cancelled by the system administrator.

C.1.3 Authentication based on secret key

This method is considered strong. It does not authenticate a human user directly but an intelligent device he is using (which may be a smart card which itself must be activated by entering a PIN). The method may appropriately be implemented in network elements to mutual authenticate processes.

The basic principle is to use the secret key as input for a transformation (e.g. one way function, encryption) of time variant parameters such as a time stamp, sequence number or random number. In a specific implementation (challenge-response), the random number may be generated by the verifier and sent to the claimant as challenge. The output from the claimant's transformation process is sent as response to the verifier, which compares it with a value locally generated with the identical secret key, transformation and random number.

More details can be found e.g. in [5] and [6].

C.1.4 Authentication based on digital signature

This method is a specific variant of Authentication based on secret key as described in clause C.1.3. It is also considered to be strong. For further details see clause C.2.

C.2 Digital Signature

If only the integrity of data intended for transfer is to be protected, it should be clarified whether the protection should suffice only for incidental alterations, i.e. due to transmission errors, or also for manipulation. If only incidental alterations are to be detected, checksum procedures (e.g. Cyclic Redundancy Checks) or error correction codes can be used. Protection against manipulation is also offered by processes which create a so-called Message Authentication Code (MAC) using a symmetrical encryption algorithm (e.g. DES) from the information to be transmitted. Other processes use an asymmetrical encryption algorithm (e.g. RSA) in combination with a hash function and create a "digital signature". The resulting "fingerprints" (checksum, error correct codes, MAC, digital signature) are transferred together to the recipient and can then be checked by the latter.

The principle of the digital signature

The digital signature is based on an asymmetrical cryptographic method. This means that at the signature formation another key is used than upon the signature examination. To this is a key couple of corresponding keys produces or uses user obtained. A key, the so-called public key, is announced publicly. The other key, the so-called private key, has to be kept secret absolutely. A digital signature that was produced with the private key can be verified with the accompanying public key and only with this. If one wants to guarantee authenticity of the public keys in addition, it requires a safeguarding infrastructure with a so-called "trustworthy third party" who confirms the assignment of a person to a public key by a certificate.

The private keys have to be kept secret in every case. It is the surest to generate the key couple on an individual chip card and to export the private key never from this. To prevent the danger now that somebody publishes a public key under wrong name, it is necessary that all participants of a communication domain identify himself opposite a third party appreciated by all of them when trustworthy. This issues a so-called key certificate, which the identity of the participant immediately connects with the corresponding public key and this in list generally accessible to one publishes.

If Bob (communication partner B) and Alice (communication partner A) want to use digital signatures for example, each of them needs an individual key couple. The key production is carried out in safe surroundings with the user or by the trustworthy third party. The respective public keys are then replaced under each other or published for everyone.

With help of this certificate the originator of a signed document can to state therefore in the context of the signature examination beyond all doubt, whether this one is, for this one he claims to be.

At the signature formation the data that have to be signed are compressed to a characteristic value, the so-called fingerprint, by means of a Hash method. This fingerprint is then signed under use of the private key of the signatory. As result one gets the signature which can be transferred together with the signed data to a possible receiver.

The receiver or the verifier must more generally calculate the fingerprint from the data in question using the same hash method like the signatory. Then he has to "encrypt" the received signature using the public key of the signatory and the same encryption method. The result of this examination produces the same hash value if the integrity is fulfilled. If the values are different there might be integrity loss or one uses a wrong or, incorrect public key (authenticity loss).

C.3 Access Control

Access control is defined in [2] as the prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner.

Access control activities include:

- establishing access control policy;
- establishing access control information (ACI) (i.e. access rights);

- allocating and binding ACI to elements (entities (e.g. users, administrators, network elements), targets (user profiles, software objects);
- authorization.

Fore more details see [10].

Access control should be supported by logging and auditing (see clause C.11).

C.4 Virtual Private Network

VPNs are being established by the following security features:

- Access Control;
- Encryption.

Other features for VPNs may include NAT (Network Address Translation) to establish closed user groups (CUG).

C.5 Secure Configuration of Operating Systems

Each Operating System supports some security mechanisms. The use of fully documented OS should be preferred. It is recommended to enable the built-in security features of the OS. To ensure an adequate level of security, especially for those parts of a TIPHON system which are connected to the Internet, the following actions are recommended:

- All non-needed features (e.g. TCP/ UDP ports) should be disabled.
- Remote access
  The remote access feature for internal and external access should be disabled. If this feature is necessary for the maintenance logging, and auditing of all activities should be established.
- Server Console
  The server console, that controls all possible features of the Operating System should be protected. (Each OS has some special feature to secure this console).
- Logging and Auditing
  Logging and auditing of the complete System should be applied. The frequent check of the log file is recommended in this case. (Note: Logging and the auditing features may lead to a decreasing systems performance).

A critical issue in this context is to ensure that the OS is administered properly and in particular available security features like patches and updates must be used.

C.6 Secure Configuration of Networks

Secure Configuration of Networks includes e.g:

- change default passwords;
- disable unused ports;
- password history;
- entity authentication;
- configuration control, provides an assurance against introduction of malicious code and malicious change of hardware.

Other security measures as described in annex C.

C.7 Protection from Denial of Service Attacks on Hosts and Media Streams

There are several tools and procedures currently recommended for thwarting denial of service attacks. The list of these tools and their effectiveness will continue to grow as the security community works to address these problems that they consider to be high priority.

C.7.1 Filtering at network ingress

RFC 2267 [20] describes filtering at ingress routers (this is the network edge or border point where traffic enters the network). The simple idea is to examine all packet headers of packets leaving border to enter the network and to discard any packets that have invalid source IP addresses. Packets to discard are identified by checking for source addresses that could not have been generated by any devices on your side of the network and thereby prevent network entry of packets with spoofed IP addresses.

C.7.2 Filtering at network egress

Network egress is the network edge or border where traffic leaves the network. This type of filtering is more difficult than ingress filtering. The goal is to filter out the packets that are the "attack" packets. Due to the high traffic load during these attacks, it might not be possible to analyse all packets, differentiate attack from legitimate traffic and throw away attack packets. In order to handle the network load, sometimes the best solution is to have the victim "black holed" or to discard all of its packets without analysis. Although this is not a good solution for the victim, it will allow other hosts on the network to continue to receive their network traffic.

C.7.3 Disable directed broadcast

In current practice directed broadcast mechanisms are principally used by malicious hackers. For example, directed broadcast messages (e.g. ICMP echo request) using spoofed source IP addresses can cause a flood of messages (ICMP echo response) to be transmitted to the victim. Therefore, the Computer Emergency Response Team [CERT] recommends two mitigations to this threat:

- that sites disable IP directed broadcasts at all routers;
- all operating systems be configured to prevent responses to ICMP packets that were sent to broadcast addresses.

RFC 2644 [19] describes the change in default requirements for directed broadcasts in routers. Prior to the issue of RFC 2644 [19] the default requirement was for routers to receive and forward all broadcast messages. RFC 2644 [19] changes the default to disable the ability to receive and forward broadcast messages. New routers will be built with this improved default status.

C.7.4 H.235v2 Media Anti-spamming method for RTP channels

Current H.323 [12] and H.235 [13] based multimedia systems do not provide explicit means against denial-of-service attacks. The attacks can be launched using distributed toolkits and flooding open RTP[RTP]/UDP media ports. This is of concern in mission-critical VoIP systems that require high availability and must resist basic attacks. A goal of H.235v2 is to provide a simple, lightweight security means that is sufficiently effective without the necessity to integrity-protect the complete media packet. Integrity protecting the entire packet is a problem for performance reasons. Some simple, lightweight security means are necessary to counter the flooding attack on a UDP port. As a result of a successful attack, the end system (e.g. terminal, gateway, MCU) may no longer provide its service or function appropriately.

Such an attack using IP spoofing techniques is basically possible on any H.323 system, regardless of whether H.235 media (voice/video) encryption is implemented or not. While firewalls usually cannot counter this kind of attack once the UDP ports have been connected through, the countermeasure could be implemented in the end-system. For an attacker listening to the media port negotiation (H.245 [14] or H.225.0 [**Error! Reference source not found.**]), the DoS attack is quite easy to perform. The attacker either sends arbitrary media packets with meaningful RTP header information or even replays intercepted RTP media packets on the discovered port. The attacker may even probe the destination ports without listening to a signalling connection.

H.235v2 describes a simple mechanism using lightweight authentication to thwart DoS attacks. The basic idea is to utilize the end-to-end secret that can be negotiated by means of H.235 and apply it cryptographically to a short, non-constant portion of the RTP packet and compute a digest; actually this is a cryptographic message authentication code. Rapid checking of the digest allows the receiver to filter out unauthorized packets from unknown sources before spending any further resources processing the malicious packet. We call this security mechanism the **"media anti-spamming method".**

The media anti-spamming for RTP protects both H.235 encrypted media streams as well as unencrypted RTP payload data. H.235 [13] defines the necessary key-management with automatic, integrated session key distribution; key update/synchronization and security capability negotiation using H.245 open logical channel signalling. H.235 also allows manual key management with statically configured keys. RTP does not define any key management and defines key management tasks as by non-RTP means. Thus this mechanism fits the current RTP approach and concept.

C.7.5 Tools to scan for distributed drones

Vendors offer a scanning tool which checks to determine if the system has a hacker installed drone that can be remotely directed by a hacker to run denial of service attacks against a victim. Removal of these drones will prevent a site from experiencing DoS problems along with the helping the intended victim.

C.7.6 Procedures and plans for crisis management:

Refer to [DISTTOOLS] for a lengthy discussion of management and system administration planning and implementation. The description includes management education, security policies, use of security tools and a discussion of establishing alternate communication mechanisms for use during a crisis.

C.8 Physical Protection

Physical protection deals with safeguarding of technical equipment and cabling, of buildings and rooms where technical and operational equipment is located and of user premises. It includes:

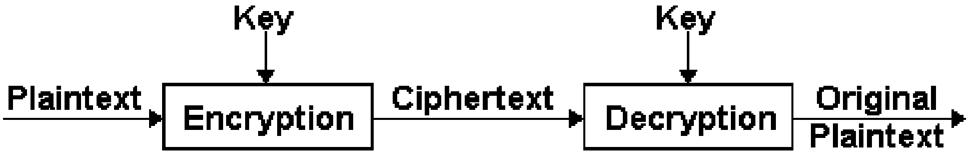
- physical protection of keying material in user and operator equipment;
- definition of cabinets and rooms in the building requiring protection;
- entry regulations and controls of entry rights to buildings, rooms, cabinets, distributors;
- identification systems up to one-by-one checks of persons;
- fire detection and protection devices;
- safeguard water pipes, temperature, air-conditioning, humidity;
- uninterruptible power supply and lightning protection;
- protection against electromagnetic radiation;
- intruder detection against thefts, vandalism, attacks;
- remote indication of malfunctions.

Organizational countermeasures are out of scope of the present document for various reasons. However, it is strongly recommended to identify appropriate organizational countermeasures when performing a threat analysis on an individual level. Examples are:

- division of responsibilities and separation of functions assigned to persons;
- granting of site access rights to persons and documentation of it;
- look-up plan. Handling and issue of keys. Key control for floors, hallways, protective cabinets and rooms necessary;
- supervising or escorting outside staff and visitors;
- maintenance and repair regulations.

C.9 Encryption

Encryption should be used to transform confidential information into unintelligible data i.e. if somebody is able to get hold of this data, they shouldn't be able to decrypt the included information. The decisive feature of any encryption procedure is the quality of the algorithm in addition to the selected key.



C.9.1 Algorithms and Keys

A **cryptographic algorithm**, also called a **cipher**, is a mathematical function and is used for encryption and decryption. (Generally, there are two related functions: one for encryption and the other for decryption.)

Since a mathematical function is deterministic, some secret information has to be brought into the picture. Otherwise, everybody who knows the mathematical function is able to decrypt the encrypted data.

Enter the secret key. With a secret key it is possible to encode data, to transfer these across an insecure transportation channel and to decode afterwards again. While earlier on both, the used key and the algorithm, were kept secret, nowadays the algorithm is published for analysis by experts.

C.9.2 Symmetric and Public-Key Algorithms

There are two general types of key-based algorithms: symmetric and public-key. **Symmetric algorithms**, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and the receiver agree on a key before they can communicate securely or the key must reach the receiver by a secure way. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret. Therefore, symmetric algorithms require a suitable key management.

Symmetric algorithms can be divided into two categories. Some operate on a single bit (or sometimes byte) of the plaintext at a time; these are called **stream algorithms** or **stream ciphers**. Others operate on the plaintext in groups of bits. The group of bits are called **blocks** and the algorithms are called **block ciphers**. For modern computer algorithms, a typical block size is 64 bits **-** large enough to preclude analysis and small enough to be workable.

Public-Key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key and vice versa. The algorithms are called "public-key-algorithms" because the encryption key can be made public. This eases the requirements in key management: No key has to be transmitted securely. A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the **public key** and the decryption key is often called the **private key**.

Using the process in the opposite direction, high-quality authentication is possible: Information encrypted with the secret key may be decrypted by everybody who is in possession of the public key. But nobody else than the holder of the secret key is able to produce the encrypted message. Therefore, the reader may be reasonably sure about the identity of the sender.

While public-key algorithms offer advantages in key management, their performance with respect to the amount of data encrypted per CPU-time is dramatically inferior to symmetric algorithms, in particular when the individual messages grow large.

This is the reason why often one wants to deploy a combination of an asymmetric cipher and a symmetric one: use the asymmetric cipher to exchange a secret "session" key for the symmetric cipher, and encrypt the actual data with the symmetric cipher and this "session" key. This grants ease of key management and reasonable performance at the same time.

C.9.3 Hardware and Software

For the purpose of encryption there are different possibilities to transform the information. One can on the one hand encode the information by software, on the other hand special hardware offers also this functionality. These possibilities bring in advantages but also disadvantages. An algorithm should always be specified and implemented depending on purpose and requirements of the usage.

Provided that the data to be looked at for the signalling and the data stream ("media stream") are separate, one can encrypt them also separated since different requirements hold for this.

C.9.4 Security on call management

Call management security has impacts to all information handled over the TCP/IP connection. This includes encryption of transferred messages, e.g. call configuration, call release, and charging/billing information transfer. There might be a need for a high quality authentication process, particular when mobile equipment is involved.

Reliability, as well as security must be granted for that part. Cryptographic methods as used in the Internet might be used to grant security.

It shall be considered to provide or use existing trust centres to apply cryptographic techniques that must operate between multiple network nodes.

C.9.5 Security on the voice data stream

Here, some legal restrictions apply on cryptographic methods. In fact, lawful interception must be granted in some countries. Basically the following rules are applied:

- in case encryption is done on the transmission network, the network provider must be able to decrypt such streams for the authorities;

- on the other hand, if encryption is done in the terminal (user), there is no requirement for the network operator to decrypt streams for the authorities.

C.10 Intrusion Detection Systems

Intrusion Detection Systems (IDS) are a useful preventive countermeasure against internal and external intruders. The aim of such a system is discovering possible targets and to find out attacking attempts which taken place. Properly configured they detect unusual and suspicious behaviour in a system or a specific part of it.

IDS are based upon the idea that intruders leave traces of their doing which differs from the behaviour of regular authorized users.

IDS analyse, amongst others, possible anomalies like:

- long connections;
- unusual number of failed logins;
- attempted access on systems programs or parts and configuration files;
- unusually high data transfer;
- finding out modifications on important files of central security components, e.g. by using cryptographic hash-values.

IDS usually work on-line, e.g. in case of anomalies detected alarm scenarios are started, either resulting in on-line surveillance of the specific connection or cutting connections.

Other IDS scenarios could be compared to virus detection systems. Such systems are not based on the detection of anomalies, but they actively detect known intrusion sequences by correlation and analysis or possibly identify the address of the machine by which an attack was tried.

C.11 Auditing and logging

Appropriate logging, auditing and review constitute essential factors related to network security. These mechanisms help to control the efficiency of countermeasures that prevents attacks.

Logging in a network management system or on certain active network components allows the storage of particular states (generally requiring definition) for the purpose of subsequent evaluation. Typical items which can be logged include faulty packets which have been transmitted to a network component, unauthorized access to a network component, or the performance of the network at certain points in time. An evaluation of such protocols with suitable aids makes it possible, for example, to determine whether the bandwidth of the network fulfils present requirements, or to identify systematic intrusions into the network.

Auditing implies the use of a service which deals, in particular, with events critical to security. This can take place online or offline. During online auditing, events are scrutinized and evaluated in real time with the help of a tool (e.g. a network management system). During offline auditing, the data are logged or extracted from an existing log file. Items monitored via offline auditing frequently include data on utilization times and incurred costs.

During *review*, data gathered as part of offline auditing are examined by one or more independent employees (two-person rule) in order to detect any irregularities during the operation of IT systems and to monitor the administrators' activities.

The logging and auditing functions offered by a network management system should be activated to a sensible extent. In addition to performance measurements for monitoring the network load, it is particularly advisable to evaluate the events generated by the network management system.

A large number of entries are usually generated during logging, so that a tool is required to analyse them efficiently. Auditing focuses on the monitoring of events critical to security. Auditing often also involves the collection of data on utilization periods and incurred costs.

The following events are of particular interest during auditing:

- data on the operating times of IT systems (which IT system was activated/deactivated when?);
- access to active network components (who logged on when?);
- security-critical access to network components and network management components, with or without success;
- distribution of network loads over an operating period of one day/one month, and the general performance of the network.

The following events should also be logged, as they may cause e.g. Denial of Service:

- hardware errors which might lead to the failure of an IT system;
- impermissible changes to the IP address of an IT system (in a TCP/IP environment).

Auditing can be performed online or offline. During online auditing, categorized events are reported directly to the auditor, who can initiate measures immediately, if required. These events must be assigned to suitable categories, so that the responsible administrator or auditor can retain a clear perspective and respond to important events immediately without being overwhelmed by a flood of information. During offline auditing, data from log files or special auditing files are prepared with the help of a tool and then examined by the auditor. In this case, measures for maintaining or restoring security can only be initiated after a time delay. Generally it is advisable to employ a mixture of online and offline auditing. During online auditing, security-critical events are filtered and reported to the auditor immediately. Events of a less critical nature are analysed offline.

On no account should user passwords be collected as part of auditing or logging! A high security risk would arise if unauthorized access were gained to this data. Incorrect password entries should not be logged either, as they usually differ from the corresponding, correct passwords only by one character or two interchanged characters.

A code of practise as part of the security policy is also required as to who will analyse the logs and audit data. A suitable distinction must be made here between the originator of events and the evaluator of events (e.g. administrator and auditor). Regulations concerning data privacy must also be adhered to.

Log files and audit files must be analysed at regular intervals. Such files can quickly grow to large proportions. To keep the size of log files and audit files within a useful range, the evaluation intervals should not be impractically short, but short enough to allow a clear examination.

C.12 Non-Repudiation measures

Non-Repudiation is a property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

This feature can be realized by a variety of mechanisms as described in [8], e.g. by security tokens, time stamps, and digital signature. In case of digital signature non-repudiation evidence consists of a digitally signed data structure. Further details to digital signature see clause C.2.

Annex D: Threat and Countermeasure Template for Providers

Each Provider as a checklist to see which countermeasures he has in place against the major threats could use this annex.

	Attack scenario	Threat Reference	Countermeasure used to prevent the threat	Countermeasure used to detect the threat	Countermeasure used to react when the threat occurred
Denial of Service					
1	Flooding the target for Denial of Service	8.1			
2	Modifying stored information	8.1			
3	Physical removing of resources	8.1			
4	Cutting off network connections	8.1			
Eavesdropping					
5	Attaching a protocol analyser to any accessible link	8.2			
6	Illegal use of lawful interception facilities	8.2			
7	Illegal activation of optional tools	8.2			
Masquerade					
8	Hijacking a link after authentication has been performed.	8.3			
9	Using authentication information, which has been obtained by eavesdropping.	8.3			
Unauthorized Access					
10	Exploiting system weaknesses	8.4			
11	Masquerading as an entity with higher access permission	8.4			
Loss of information					
12	Deletion of data	8.5			
13	Modification of access rights of other parties	8.5			
Corruption of information					
14	Modifying transmitted information	8.6			
15	Modifying stored information	8.6			

	Attack scenario	Threat Reference	Countermeasure used to prevent the threat	Countermeasure used to detect the threat	Countermeasure used to react when the threat occurred
Repudiation					
17	Denial of data transmission	8.7			
18	Denial of data receipt	8.7			
19	Denial of having accessed data in a database	8.7			

Annex E: Bibliography

- ITU-T Recommendation E.164: "The international public telecommunication numbering plan".
- ITU-T Recommendation E.168: "Application of E.164 numbering plan for UPT".
- ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues".
- ITU-T Recommendation H.225: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".
- ISO/IEC JTC 1/SC 27 N 2582: "Working draft 15947, Information technology - Security techniques - IT intrusion detection framework".

History

Document history		
V1.1.1	April 2001	Publication