VoIP Security and Privacy Threat Taxonomy

Public Release 1.0
24 October 2005

Table of Contents

Introduction

This Taxonomy defines the many potential security threats to VoIP deployments, services, and end users.

The overall goal is to help drive VoIP security awareness with the press, industry and public. In particular this Taxonomy provides a detailed structure for technical vulnerabilities that informs the following constitutencies:

- Press and public
- *All vendors* across the value chain including:
    - carriers,
    - service providers,
    - equipment vendors
    - software developers, and
    - system integrators
- The technical community of designers and experts
- Media and entertainment content developers and publishers
- The policy and regulatory community
- The law enforcement community

This Taxonomy also provides a clear definition of security to make security measurable, actionable and subject to economic and social trade-off analysis.

An example of the benefit of this Threat Taxonomy is the qualification of risks. While some early press accounts focused on potential VoIP spam and VoIP call hijacking, the consensus of learning from this project is that there are many other threats that may more prevalent or significant as risks today including economic threats from deceptive practices, malware (such as viruses and worms) and denial of service.

A further benefit is the discovery that there are fundamental gaps in infrastructure between different parts of the Internet which require cooperation. Vendors can not act in isolation and expect to secure traffic across the value chain. Security and privacy is more than zero defects in current product.

Other key benefits of this project include:

- Connecting security and privacy
- Informing a dialog between law enforcement, policy regulators and industry
- Advancing the art of security and privacy as an engineering discipline

Next steps in the framework include vetting and incorporation of comment, expansion and adjustment to add risk metrics. This will continue in parallel with other work in VOIPSA now ongoing.

Active Contributors

Project Director: Jonathan Zar

The Taxonomy is the collaboration of a worldwide team of project leaders, authors and editors. VOIPSA gives thanks to the following people and teams without whom this project would not be possible:

Principal Authors & Editors:

David Endler

Dipak Ghosal

Reza Jafari

Akbal Karlcut

Marc Kolenko

Nhut Nguyen

Wil Walkoe

Jonathan Zar

Interactive Writing Workshop:

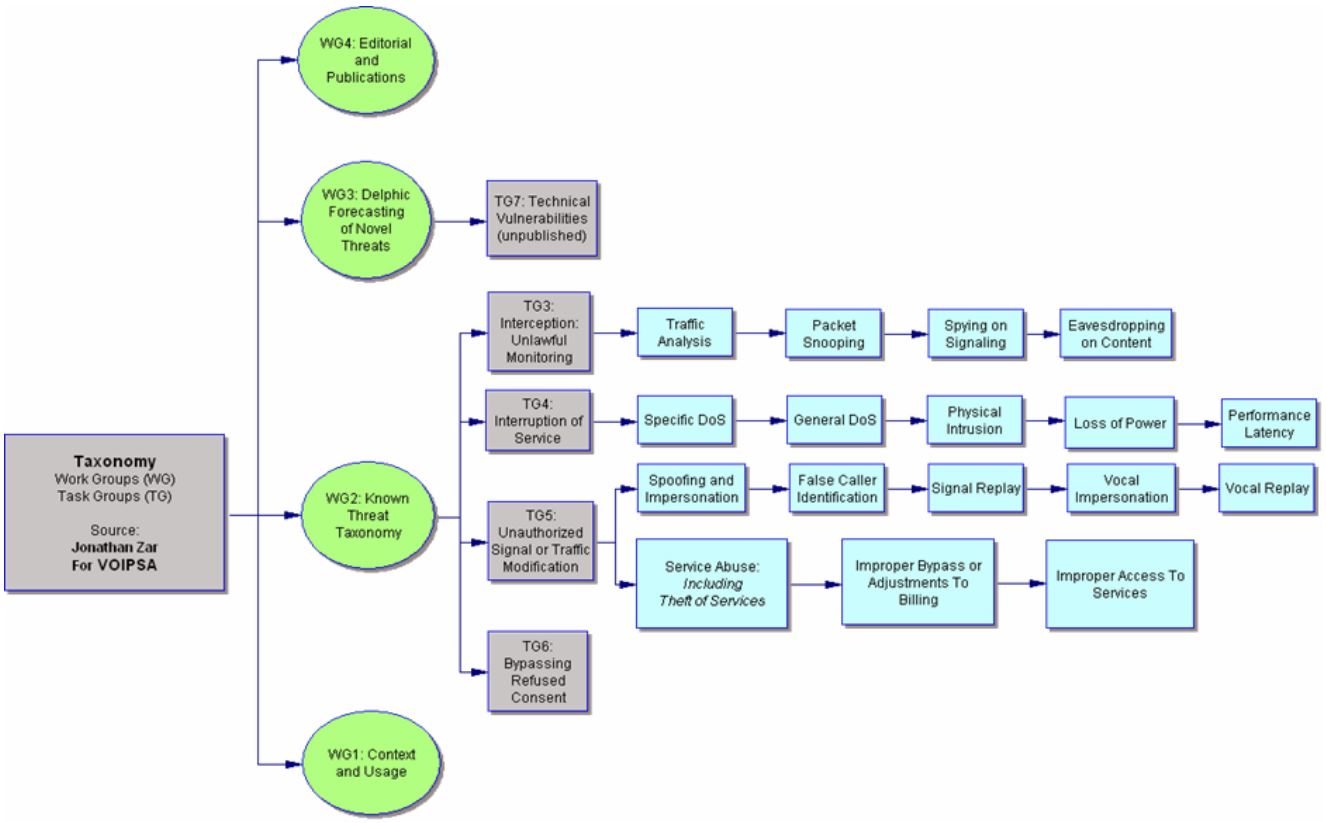
Shin Adachi	Will Chorley,	Dipak Ghosal
Reza Jafari	Akbal Karlcut	Sourabh Satish
Brian Tolly	Wil Walkoe	Jonathan Zar

Special thanks to Sourabh Satish and Brian Tolly
for sponsoring on-site and on the web

Wiki Sponsors/Coaches:

David Endler
Kartik Trivedi
Dan York
The Jotspot Team http://www.jotspot.com

Project Teams:



Participating Team Members:

Bruce Abernethy
Sherly Abraham
Mihai Amarandei-Stavila
Scott Beverly
Antoine Borg
Stefano Brusotti
Thomas B. Cross
Ram Dantu
Guy Denton
Laurent Dinard
Ido Dubrawsky
Dan Frank
Joe Franklin
Dipak Ghosal
Paul E. Gibson
Ben Halpert
Bill Hasell
Candace Holman
Vinay Igure
Gustavo de Los Reyes
Hadriel Kaplan
Robert Kelly
Allan Konar
Tim Kramer
Santhosh Kumar
Vinod Kumar
Paolo De Lutiis
John Morano
Richard Polishak
Sourabh Satish
Carl Silva
Michael L. Smith
Ari Takanen
Mark Teicher

1.0 Basic VoIP Terminology

The following terms are defined to provide a basic dictionary for interpreting the work within VOIPSA and for general understanding in the field of VoIP:

Term	Definition
Denial of Service (DoS)	An attack on a system that causes loss of service to the users of that system.
Call Signaling Protocol	Any protocol, *e.g.* SIP and H.323, that is used between Endpoints and a Call Controller to establish and teardown VoIP calls.
Call Controller	Any Entity that interacts with Endpoints to manage VoIP call establishment, reporting, and teardown. Multiple Call Controllers may exist within a Network.
Call Processor	Any Entity that that interacts with the Endpoints to manage content exchanged between Endpoints. The functions of a Call Processor may co-exist with those of a Call Controller in some protocols and may be absent in others.
Communication	Any collection of traffic among participating nodes. A communication may have any number of parties and include any forms of media, including mixed media. Examples include without limitation: a telephone call, a voice conference call, a video conference call, a text message, a facsimile and mixed media instant messaging
Endpoint, End-Point	Any Device that is capable of originating or terminating a voice or video call, including a desk-set or a soft-phone.
Endpoint Element	Any embedded or downloaded subcomponent of an Endpoint including hardware, firmware or software.

Basic VoIP Terminology - Continued

Term	Definition
Gateway	A network device that provides the interworking functions to bridge two or more different networks. For example, a Trunking Gateway provides functions to connect VoIP media (RTP streams) with voice circuits or trunks that carry Time Division Multiplexing (TDM) data in the Public Switched Telephone Network (PSTN.)
Hub	A device that provides interconnecting function to multiple networking devices via a shared channel. An example is an Ethernet hub that interconnects a number of Ethernet network interface cards in a LAN. A hub works at layer 2 of the OSI reference model.
ID	An identifier that designates a User or Entity.
Interruption of Service	Any loss of any Service.
Network	Any interconnect however realized which when represented in the art of communications as a graph of nodes and arcs carries any form of voice or video between two or more designated Nodes.
Network Component	The union of Network Elements and their Protocols.
Network Element	Any Network Node or its Physical Media Dependent.
Network Infrastructure	The collection of all of the parts and places of a Network and more specifically all of the devices on a Network including their embedded or downloaded subcomponents.
Network Node, Entity	Each device on a Network this is capable of identification, address or logical function.

Basic VoIP Terminology – Continued

Term	Definition
Number "as an ID"	A number, when used in the sense as a 'telephone number' or number within a 'dialing plan' is simply a form of an identifier that designates or identifies a user or entity.
Physical Layer, Physical Network	The Physical Media Dependent and all of the analog and mixed signal circuits to which it connects.
Physical Media Dependent	Media specific interconnects, whether wire-line or wireless required for any communications medium.
Protocol	Rules governing the communication of Nodes on any medium.
Provisioning Application	Any service which handles and propagates administrative changes to the Network, such as Endpoint adds, drops, and moves.
Router	A networking device that provide functions to route packets to their destination in a network. A router works at layer 3 in the OSI reference model.
Server	A device that is involved in providing a function/component of VoIP Service to multiple Endpoints. Examples are devices such as the Call Controller, Call Processor, and Call Gateway.
Service, VoIP Service	Any function, capability or feature of a Network at any layer, including, but not limited to, the ability to initiate, accept or refuse, identify, authenticate, connect, maintain, route, process, store, retrieve, and disconnect any voice or video content with any number of parties desired by the User(s).

Basic VoIP Terminology – Continued

Term	Definition
Switch (Networking Device)	A switch, similarly to a hub, provides interconnection function to multiple network devices at layer 2 of the OSI reference model. But unlike a hub, which provides interconnection via a shared channel, a switch provides interconnection by switching frames of data to their destination.
Switch (Telephone)	A switch in a telephone network sets up, tears down and manages connections between telephone circuits.
Traffic	The flow between any collection of network nodes.
User	Any natural person or automated process initiated for the benefit of a natural person.

2.0 Relevant Protocols

The following protocols are referenced in the various projects within VOIPSA. The list is not exhaustive as development of new protocols for VoIP is ongoing.

Protocol	Description
COPS	Common Open Policy Service. A simple query and response protocol for exchanging policy information between a policy server and its clients. [IETF-COPS]
DHCP	Dynamic Host Configuration Protocol. A protocol used to automate the setting of various TCP/IP configuration settings (such as the IP address, subnet mask, default router, DNS server, etc.) on hosts. [IETF-DHCP]
DIAMETER	The Diameter protocol provides an authentication, authorization and accounting framework for applications such as network access or IP mobility. [IETF-DIAMETER]
DNS	Domain Name Service, a network service used to translate between domain name and IP addresses. [IETF-DNS]

Relevant Protocols – Continued

Protocol	Description
FTP	File Transfer Protocol. A protocol for transfer files that uses TCP as the underlying transport. [IETF-FTP]
H.323	"Umbrella" specification that describes the usage of other protocols (such as H.225, H.245, and T.120) for delivery of packet-based multimedia communications systems. [ITU-T-H323]
HTTP	Hypertext Transfer Protocol. An application-level protocol for distributed, collaborative, hypermedia information systems and is the de facto standard for transferring World Wide Web documents. [IETF-HTTP]
IEEE 802.3	This is the standard for link-level data delivery on a wired Ethernet LAN. [IEEE-802-3]
IEEE 802.11	A family of wireless layer 2 LAN protocols that provide functionality similar to Ethernet via radio transmission. [IEEE-802-11]
IEEE 802.16	A family of protocols for wireless data access over a wide area, with cellular frequency re-use based on a larger cell size and higher bit rate than 3G cellular access networks. Still at the work in progress stage, IEEE 802.16 will eventually include both a fixed wireless access protocol and a mobile wireless access protocol. The commercial term WiMax is currently used for both types of IEEE 802.16 access. [IEEE-802-11]
IP	Internet Protocol. IP is the network layer (layer 3) protocol used in the Internet. [IETF-IP]
Megaco MGCP	Used between elements of a decomposed multimedia gateway which consists of a Call Agent (containing the call control "intelligence"), and a Media Gateway (containing the media functions). (Megaco is also known as H.248.) [IETF-MEGACO] and [IETF-MGCP].
MidCOM	A protocol for applications to communicate their needs to the devices in the network (referred to as 'middleboxes') that provide transport policy enforcement. The purpose of this protocol is to provide a standardized language for exchanging control information. Various existing protocols, e.g. SNMP, COPS and MEGACO, have been evaluated as a MIDCOM protocol. [IETF-MIDCOM]
Party / Parties	One or more users within a communication, whether simultaneous or successive.

Relevant Protocols – Continued

Protocol	Description
RADIUS	Remote Authentication Dial-In User Service, is used to provide centralized authentication, authorization, and accounting for dial-up, virtual private network, wireless network access, etc. [IETF-RADIUS]
RTP	Real Time Protocol. RTP is used to exchange media information such as voice or video. [IETF-RTP].
RTCP	Real Time Control Protocol. RTCP is used to control aspects of RTP sessions. [IETF-RTP]
SIP	Session Initiation Protocol. Application layer signaling protocol for the establishing, modifying and terminating of multimedia sessions or calls. [IETF-SIP]
SNMP	Simple Network Management Protocol. A management protocol used to retrieve or modify select information from a 'managed' device. [IETF-SNMP]
SS7	Signaling System Number 7. SS7 is the signaling protocol suite used in Public Switched Telephone Network (PSTN) to exchange signaling information between network nodes, e.g. telephone switches. Also known as CCS7, Common Channel Signaling number 7.
TCAP	Transaction Capabilities Application Part. TCAP is a protocol used to support transaction based services associated with wire-line and wireless telephony networks.
TCP	Transmission Control Protocol, which is a widely used transport layer (layer 4) protocol for reliable, connection-oriented data delivery. It is part of the TCP/IP protocol suite which is widely used in the Internet. TCP is a connection-oriented protocol, i.e. a connection must be set up before communicating entities can send protocol data units. [IETF-TCP]
Telnet	Protocol used to provide remote text-based command line sessions between hosts. [IETF-TELNET]
TFTP	Trivial File Transfer Protocol, is a simple protocol that uses UDP to transfer files. [IETF-TFTP]
UDP	User Datagram Protocol, is also a transport layer protocol. Unlike TCP, UDP is a connection-less protocol and does not validate the accuracy of the data transmission or recover lost or corrupted packets. [IETF-UDP]

3.0 Relevant Services

The various functions that comprise a VoIP architecture may be implemented in one or more collections of services, often implemented as distinct groups of services which communicate with each other as peers or as clients and servers.

Service	Definition
Call Control Service	Call Control Service includes call establishment, reporting, mid-call service features, and teardown. The Call Control Service is provided by a Call Controller. Multiple Call Controllers may exist within the VoIP Network.
Directory Service	VoIP protocols typically use a service that can translate an alias, user name, extension, E.164 number into an Endpoint transport address.
Gateway Service	There is often the requirement to inter-work between two different types of networks. The Gateway Service, on a Gateway, provides this functionality.
Network Service	VoIP Service may make use of a number of generic Network Services such as DNS, TFTP, FTP, DHCP, HTTP, Telnet, RADIUS, and DIAMETER.
Session Border Control Functions	A set of call processing and filtering functions that are applied to signaling and/or bearer traffic as it crosses a trust boundary (e.g. between an access network and a core network, or between two autonomous systems in the core).

4.0 Social Threats

4.1 Introduction

Security and privacy are important social needs that planners balance against other vital needs such as return on investment and convenience.

To put security and privacy into a social context VOIPSA has adopted three models:

- A basic model for multi-party freedom applicable to any public communications system;
- A basic model defining privacy and relating it to security; and
- A social responsibility model based on widely accepted principles in the civil and common law.

Together these models provide a simple framework for balancing security and privacy with other needs.

4.2 Basic Multi-party Freedom Model

Modern interactive communication systems can include more than two people in a session and people can move fluidly from role-to-role, including:

- Initiating contact
- Joining communication in progress
- Accepting contact
- Terminating communication in progress
- Refusing contact.

Multi-party freedom is the continuity of freedom created when roles shift between an indeterminate number of people having potentially differing needs and wants.

Multi-party freedom is a practical requirement for any scalable communication system. In particular it is an implicit operating requirement for VoIP.

The basic multi-party freedom model is a communication system which meets the following criteria for all users:

1. user is able to invite anyone
2. user is able to join multiple parties
3. user is able to refuse an invite
4. user is able to drop out of a session
5. user is able to indicate consent for any and all contact and reporting
6. user is able to refuse consent for any and all contact and reporting
7. user is assured confidentiality and immunity for lawful communication
8. user is able to set policies for the user and all legally subordinate domains

4.3 Privacy Model; Security as Dual of Privacy

The Privacy Concept is the privilege of all people to have their communication systems and content free from unauthorized access, interruption, delay or modification.

Unauthorized access is determined by the consent of the person claiming privacy within the limits of the law. In some cases the law may give some claim of privacy to the property owner of a network rather than its user.

VOIPSA defines Security as the dual of privacy and in particular as:

Security is defined as: 1) the right to protect privacy, 2) a method of achieving privacy and 3) ways to keep communication systems and content free from unauthorized access, interruption, delay or modification.

For a discussion of the concept of the terms “privilege” and “right” see literature tracing from: 23 Yale Law Journal 16-59 “Some Fundamental Legal Conceptions as Applied in Judicial Reasoning” (Hohfeld, W. N. 1913)

4.4 Basic Social Responsibility Model

The basic social responsibility model determines responsibility by looking to both the intention and impact of a persons conduct before making judgment about what a system should deny, tolerate or permit.

Intention is measured by states of mind recognized under the law including for example actions which are purposeful, knowing, reckless, negligent or reasonable.

With very limited exception, conduct is measured by physical action which causes measurable harm.

Sometime intentional and harmful conduct is excused because it serves other more important social requirements, such as interrupting a communication system to aid in a rescue or prevent a disaster.

For background on the concepts in this section see U.S. and international literature citing the Model Penal Code (ALI 1962) and prior history [Coke] on the concepts of *mens rea* and *actus reus*.

4.5 Misrepresentation

The term misrepresentation is generically used to mean false or misleading communication.

Misrepresentation includes the delivery of information which is false as to the identity, authority or rights of another party or false as to the content of information communicated.

As defined here it does not include the concealment of information for which there is an independent legal duty to make disclosure but it does include false information made false by expressly editing data to alter a communication from one meaning to another.

For historical background on misrepresentation and examples of national and international regulation *see*: [Prosser & Keeton], [FTC Act], and [OLAF Act]

4.5.1 Misrepresenting Identity

Identity misrepresentation is the intentional presentation of a false identity as if it were a true identity with the intent to mislead.

Note that misrepresentation of identity excludes communications in channels where identity is often masked, where there is communications between parties consenting to a false marking of identity or where communication would reasonably be understood to be under a pseudonym for privacy e.g. “Jane Doe”.

Subject to the above, identity misrepresentation includes:

- presentation of a false caller ID name or number with the intent to mislead
- presentation of a false voice, name, or organization in a voice/video mail with the intent to mislead
- presentation of a false email with the intent to mislead
- presentation of false presence information with the intent to mislead

Identity misrepresentation is a common element of a multi-stage attack such as phishing.

4.5.2 Misrepresenting Authority

Authority misrepresentation is the intentional presentation of a false authority as if it were a true authority with the intent to mislead.

Authority misrepresentation consists in either bypassing an authentication mechanism to create the appearance of authentication when there was none or by presenting false information to an authentication mechanism to permit access where it would otherwise be denied.

Subject to the above, authority misrepresentation includes:

- presentation of a password, key or certificate of another with the intent to mislead
- circumvention of conditional access with the intent to mislead
- false claim of government authority bypassing ordinary authentication

Benefits sought may include improper access to toll calling features, conferencing features and access to the logs or presence information of others.

Authority misrepresentation is a common element of a multi-stage attack such as phishing.

4.5.3 Misrepresenting Rights

Rights misrepresentation is the intentional presentation of a false right as if it were a true right with the intent to mislead.

Right misrepresentation consists in either bypassing an authentication mechanism to create the appearance of rights otherwise lacking or the presentation of false information to an authentication mechanism to permit access to rights which would otherwise be denied.

Subject to the above, rights misrepresentation includes:

- presentation of a password, key or certificate with the intent to gain rights not granted
- circumvention of conditional access with the intent to gain rights not granted
- modification of access control lists with the intent to gain rights not granted

Rights misrepresentation is a common element of a multi-stage attack such as phishing.

4.5.4 Misrepresenting Content

Content misrepresentation is the intentional presentation of false content as if it were true content with the intent to mislead.

Content misrepresentation includes confidence scams and phishing where the content of a communication falsely implies a trusted source of origin.

Content misrepresentation includes:

- false impersonation of the voice of a caller with the intent to mislead
- false impersonation of the words of a caller with the intent to mislead
- misleading printed words, still images or moving images in video
- modifications of spoken, written or visual content with the intent to mislead

4.6 Theft of Services

Theft of services is any unlawful taking of an economic benefit of a service provider by means intended to deprive the provider of lawful revenue or property. Such theft includes:

- unauthorized deletion or altering of billing records
- unauthorized bypass of lawful billing systems
- unauthorized billing
- taking of service provider property

4.7 Unwanted Contact

Unwanted contact is any contact that either requires prior affirmative consent (opt-in) or bypasses a refusal of consent (opt-out).

4.7.1 Harrassment

Harassment is any form of unwanted communication which embarrasses, intimidates, vexes, annoys or threatens the receiver of the communication with actions which are improper under the law.

While a communication system may not be able to detect harassing content it can honor the stated refusal of consent of a receiver to any future communication from the originating party or parties.

Once a party to a communication refuses consent to ongoing or future harassment then attempts at such harassment become attempts at bypassing refused consent and are independently actionable within the mechanism of a communication system.

This recourse to the communication system is independent of any legal recourse.

Additionally, a person claiming receipt of unwanted communications may desire a logging feature as forensic proof.

4.7.2 Extortion

Extortion is any act to induce another to do or refrain from any conduct or give up any freedom, right, benefit or property, under a threat of loss or harm to the person, their reputation, property or the health, safety, reputation or welfare of anyone they know.

While a communication system may not be able to detect extorting content it can honor the stated refusal of consent of a receiver to any future communication from the originating party or parties.

Once a party to a communication refuses consent to ongoing or future extortion then attempts at such extortion become attempts at bypassing refused consent and are independently actionable within the mechanism of a communication system.

This recourse to the communication system is independent of any legal recourse.

Additionally, a person claiming receipt of unwanted communications may desire a logging feature as forensic proof.

4.7.3 Unwanted Lawful Content

Including VoIP SPAM and Other Subjectively Offensive Content

Unwanted lawful content, such as lawful pornography or solicitations of lawful products and services, share the characteristic of being items which users may wish to filter by the true identity of the sending party or by the description of content. Content of this type includes VoIP Spam.

VOIPSA recognizes that unwanted lawful contact is subjective, that is that other parties including the intended sender may have rights to attempt such communication and the content is presumed by itself to be legal.

Once a party to a communication refuses consent to ongoing or future contacts of this type, without their express request, then attempts at such solicitation become attempts at bypassing refused consent and are independently actionable within the mechanism of a communication system.

5.0 Eavesdropping

Eavesdropping attacks describe a method by which an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP endpoints, but cannot or does not alter the data itself.

5.1 Call Pattern Tracking

Call Pattern Tracking is the unauthorized analysis by any means of any traffic from or to any node or collection of nodes on the network. It includes monitoring and aggregation of traffic for any form of unauthorized pattern or signal analysis. Call Pattern Tracking is a technique for discovery of identity, affiliation, presence and usage. It is a general technique that enables unauthorized conduct such as theft, extortion and deceptive practices including phishing.

5.2 Traffic Capture

Traffic Capture is the unauthorized recording of traffic by any means and includes packet recording, packet logging and packet snooping for unauthorized purposes. Traffic capture is a basic method for recording a communication without the consent of all the parties.

5.3 Number Harvesting

Number Harvesting is the authorized collection of IDs, which may be numbers, strings, URLs, email addresses, or other identifiers in any form which represent nodes, parties or entities on the network. Number Harvesting is an unauthorized means of capturing identity and enabling subsequent unauthorized communication, theft of information and other deceptive practices.

5.4 Conversation Reconstruction

Conversation Reconstruction is any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation and/or feature extraction of any audio or voice portion of any communication including identity, presence or status. Conversation Reconstruction is a means for collecting, duplicating or extracting information on the audio content of a conversation, encapsulated in any one or more protocols and however encoded, which is done without the consent of all parties to the communication.

5.5 Voicemail Reconstruction

Voicemail Reconstruction is any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of any voice mail message.

5.6 Fax Reconstruction

Fax Reconstruction is any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of any document image in any communication including identity, presence or status. The communication may contain image data only or may be converged with other media such as voice, text and video. Fax reconstruction is a means for collecting, duplicating or extracting information from the visual image of a communication, encapsulated in any one or more protocols and however encoded, which is done without the consent of all parties to the communication.

5.7 Video Reconstruction

Video Reconstruction is any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of any moving images in any communication including identity, presence or status. The communication may contain video data only or may be converged with other media such as voice, text and document images. Video reconstruction is a means for collecting, duplicating or extracting information from the visual moving images of a communication, encapsulated in any one or more protocols and however encoded, which is done without the consent of all parties to the communication.

5.8 Text Reconstruction

Text Reconstruction is any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of any text in any communication including identity, presence or status. The communication may contain text data only or may be converged with other media such as voice, video and document images.

6.0 Interception and Modification

These class of attacks describe a method by which an attacker can see the entire signaling and data stream between two endpoints, and can also modify the traffic as a intermediary in the conversation.

6.1 Call Black Holing

Call Black Holing (also known as "call blackholing") is any unauthorized method of dropping, absorbing or refusing to pass IP or another essential element in any VoIP protocol which has the effect of preventing or terminating a communication. Call Black Holing is defined to include any VoIP protocol for any form of communication, whether voice only or converged with other media including video, text and images.

6.2 Call Rerouting

Call Rerouting (also known as "call sinkholing") is any method of unauthorized redirecting of an IP or other essential element of any VoIP protocol with the effect of diverting communication. A consequence of Call Rerouting is to include unauthorized nodes, corresponding to unauthorized parties or other entities, into a communication. Additionally, Call Rerouting may have the effect of excluding authorized nodes, corresponding to parties or other entities from a communication. Call Rerouting is defined to include any VoIP protocol for any form of communication, whether voice only or converged with other media including video, text and images.

Note: When authorized, Call Rerouting may be a defensive technique against attack or an enabler for other services.

6.3 Fax Alteration

Fax Alteration is any unauthorized modification of any of information in a facsimile or other document image, including header, cover sheet, status and/or confirmation data.

6.4 Conversation Alteration

Conversation Alteration is any unauthorized modification of any of information in the audio, video and/or text portion of any communication, including identity, status or presence information.

6.5 Conversation Degrading

Conversation Degrading is the unauthorized and intentional reduction in quality of service (QoS) of any communication. Conversation Degrading is a method of attack on QoS that limits or frustrates communication. Unauthorized Degrading does not include lawful reductions in quality of service by the owners or operators of a communication system essential for network management.

6.6 Conversation Impersonation and Hijacking

Conversation Impersonation and Hijacking is the injection, deletion, addition, removal, substitution, replacement or other modification of any portion of any communication with information which alters any of its content and/or the identity, presence or status of any of its parties. Conversation Impersonation and Hijacking is a method of attack that applies to any communication including any voice, video, text and/or imaging data however encapsulated or encoded.

6.7 False Caller Identification

False Caller Identification is the signaling of an untrue identity or presence.

7.0 Service Abuse

Service abuse is a large category of improper use of services and includes:

7.1 Call Conference Abuse

Call Conference Abuse is an abuse of a VoIP call service as a means to hide identity for the purpose of committing fraud.

7.2 Premium Rate Service (PRS) Fraud

Premium Rate Service Fraud is a method of artificially increasing traffic without consent or purpose other than to maximize billing.

7.3 Improper Bypass or Adjustment to Billing

Improper Bypass or Adjustments to Billing are method of avoiding authorized service charges or for concealing other fraud by altering billing records (CDRs).

7.4 Other Improper Access To Services

Other methods of service abuse include:

- Various forms of call bypass connection via conferencing, signaling and transferring means to add unauthorized parties, possibly dropping connections to conceal the fraud.
- Various forms of identity theft where legitimate credentials obtained without consent are used for access without permission of their rightful owner.
- Various forms of internal fraud exploiting internal access access into authentication systems (e.g. RADIUS, LDAP, Active Directory, VOIP gateway and signaling switches).
- Registration attacks in which an attacker exploits vulnerabilities in registration injecting themselves into a signal path.
- Misconfiguration of end-points.
- Various methods of concealing fraud by spreading access across multiple accounts to avoid detection by fraud analytical analysis and reporting software.

8.0 Intentional Interruption of Service

VoIP Networks are presumed to consist of one or more logically distinct Networks. VoIP Networks are presumed to include a mix of heterogeneous Physical Networks. The concept of an interruption in service presumes a continuity of service as the norm.

Interruptions of service are classified into the following categories:

Specific Denial of Service (DoS)	Denial of service threats that are specific to the various known VoIP protocols or to particular attributes of the VoIP application.
General DoS	General denial of service threats that can impact a VoIP Service but are not specific to a VoIP protocol.
Physical Intrusion	Key physical vulnerabilities of relevance for the rest of VOIPSA to consider.
Resource Exhaustion	Interruptions of service that can arise because of any resource other than independently supplied power.
Loss of External Power	Classification of loss of external power by point of failure and scope of power outage.
Performance Latency	Known types of performance latency that impact local, national, and international VoIP and distinguish these from malicious attacks.

8.1 Denial of Service

8.1.1 VoIP Specific DoS

8.1.1.1 Request Flooding

The following sub-sections cover DoS attacks that involve overwhelming the target with a number of valid and/or invalid requests.

8.1.1.1.1 User Call Flooding

A DoS attack on a user, carried out by sending a large number of valid requests. While the associated Endpoint is able to process the requests, the user is continually interrupted.

8.1.1.1.2 User Call Flooding Overflowing to Other Devices

A DoS attack on a user, carried out by sending a large number of valid requests. While the associated Endpoint is able to process the requests, the user is continually interrupted. The difference from the previous case is that some of these calls may overflow to other resources including voice mail servers or call gateways whose resources may be exhausted.

8.1.1.1.3 Endpoint Request Flooding

A DoS attack on an Endpoint could consist of sending large number of valid/invalid call set up messages (e.g., SIP INVITEs) which could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources including that of the User Agent. This may be observable by the end user, as some of the requests will be result in valid call setups. This type of attack can also impact the Call Processor if the attack is launched in such manner that it arrives from the PSTN.

8.1.1.1.4 Endpoint Request Flooding after Call Setup

A DoS attack on an Endpoint could consists of sending a large number of valid/invalid call control messages (e.g., SIP RE-INVITEs) after a call has been successfully established which could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources. This may also result in dropping the existing connection.

8.1.1.1.5 Call Controller Flooding

A DoS attack to a Call Controller could consists of sending a large number of valid/invalid call set up messages (e.g., SIP INVITEs) which could cause the Call Controller to crash, reboot, or exhaust all call controller resources. This can affect a large number of Endpoints at one stroke, leaving them unable to initiate or receive calls.

8.1.1.1.6 Request Looping

A DoS attack may exploit loop and spiral implementation on a Call Controller to have two Endpoints across domains or within the domain continually forwarding a single request message, back and forth, to each other so as to exhaust resources on the Call Controller. This can affect a large number of Endpoints at one stroke, leaving them unable to initiate or receive calls.

8.1.1.1.7 Directory Service Flooding

A DoS attack could consist of sending large number of valid queries to the on a support server providing a VoIP services such as a Directory Server, DHCP Server, DNS server, etc. This could cause the associated server to crash, reboot, or exhaust all processing resources. The Endpoints that rely on this service would then be taken out of service, unless there exists some sort of redundancy in place.

8.1.1.2 Malformed Requests and Messages

The specifications for control messages in many VoIP implementations are deliberately open-ended, to allow for the addition of additional capabilities over time. The downside of this type of specification is that it is not possible to test an implementation either for correct processing of all valid messages or for accurate recognition of invalid messages. As a consequence, valid but complex messages are at risk of being discarded, and the processing systems themselves are at risk if they are sent sufficiently devious invalid messages. The ability of complex invalid messages both to be accepted by a call processing element and to trigger self-destructive behavior in that element creates the threat of DoS via “killer messages.”

8.1.2.2.1 Disabling Endpoints with Invalid Requests

A DoS attack on an Endpoint could consist of sending a number of invalid call set up messages (e.g., ACKs when none is expected) that could cause the Endpoint to crash, reboot, or exhaust all Endpoint resources including that of the User Agent. This may not be observable by the User Agent since a lower layer protocol processing engine would process and drop the messages. It is not always necessary to overload the Endpoint with the sheer volume of invalid messages. Unless the message is recognized as invalid and quickly discarded some invalid messages can consume a considerable amount of processing capacity, and they can corrupt the protocol processing engine by overflowing the message buffers.

8.1.2.2.2 Injecting Invalid Media into Call Processor

This form of DoS can be triggered by the injection of invalid media into the call processor by the caller or by a third party (by guessing the appropriate control headers of the media stream). This will cause the Endpoints to crash, reboot, or exhaust all call processing capacity.

8.1.2.2.3 Malformed Protocol Messages

This form of attack consists of sending malformed signaling messages (messages with overflow or underflow). These messages are sent to the processing node degrading its performance resulting in its inability to process normal messages and setup and tear down calls.

Fuzzing involves creating unanticipated types of packets for a protocol, which contain data that pushes the protocol's specifications to the point of breaking them. These packets are sent to a processing node that acts on the target protocol, to disable the processing node or degrade its performance (crash, resource consumption, etc.).

A well known SIP public fuzzer is the PROTOS suite developed by the University of OULU in Finland.

8.1.1.3 QoS Abuse

Quaility of Service (QoS) abuse involves an attacker violating the QoS negotiated at setup. For example, it could use a different media coder than what was declared during call setup.

It is also possible for data applications to encroach on or misuse the QoS defined for voice. This would have the effect of introduced latency which adversely affects voice quality during a call.

8.1.1.4 Spoofed Messages

If an attacker can inject fake messages into the signaling path and have these spoofed messages accepted as the real thing, the call processing system can be disrupted in a number of ways.

8.1.1.4.1 Faked Call Teardown Message

This type of DoS attacks disrupts services by causing a session to end prematurely, thus denying service to the users.

For example, if during a SIP session, the communicating User Agent receives a BYE message that belongs to that session, it infers that the other end wants to finish the session and tears the session down. If an attacker manages to send a BYE message to a User Agent who is engaging in a session, the User Agent will

tear down the session prematurely, thus denying the service to the user.

An attacker may gather information about an on-going session then inject a BYE message to the User Agent to end the session prematurely.

For example, when a SIP BYE message is received by the Call Controller it also interprets that the User Agent wants to end the session. If an attacker sends a BYE message for a session to the Call Controller, the Call Controller tears the session down prematurely, thus denying the service to the user.

8.1.1.4.2 Faked Response

For example, a perpetrator may send a 'Busy Here' or an error response message when replying to an incoming call, thus denying the delivery of the call to the victim. The victim is not able to receive any incoming call.

8.1.1.5 Call Hijacking

When security is compromised, the system is susceptible to attacks that aim at hijacking information exchanged during sessions between a VoIP Endpoint and the network. Hijacking occurs when some transactions of a VoIP Service are taken over by an attacker. The hijacked transactions may be signaling, media or both. These attacks lead to interruption of service, as the victim will not be able to obtain the service from the network.

8.1.1.5.1 Registration Hijacking

A perpetrator may alter the registration messages of the victim to redirect signaling messages to another Endpoint. As a result the victim can not make or receive VoIP calls.

For example, when Endpoint A registers with a Location Server, an attacker could modify it as a registration request for Endpoint B, which is under the attacker's control. All calls would therefore be rerouted to Endpoint B.

8.1.1.5.2 Media Session Hijacking

In this type of attack, the attacker hijacks the media session by spoofing a "redirect' message to the calling Endpoint or a server to trick it to send the call to another Endpoint, or for example, another voice mail box.

When attacks of this type occur, the victim will only be able to 'talk' with the Endpoint to which the attacker has redirected media.

8.1.1.5.3 Server Masquerading

When a perpetrator is able to impersonate a VoIP Server and trick the victim to send requests to the masqueraded server, the victim will not be able to receive any services from the server that has been masqueraded.

8.1.2 Network Services DoS

A variety of network based attacks exist that can disrupt or degrade VoIP services. An infrastructure DoS attack against a VoIP network device or essential VoIP network service can occur through exploitation of buffer overflows of a specific network component (router, switch, proxy, etc.) resulting in a crash or reboot, traffic flooding all available bandwidth (SYN attack, Smurf Attack, etc.), or through unauthorized reconfiguring of the behavior of the device or dependent service (DHCP, AAA, TFTP, etc.).

8.1.3 Underlying Operating System/Firmware DoS

VoIP devices such as IP phones, Call Processor, Gateways, and Proxy servers inherit the same vulnerabilities of the operating system or firmware they run on top of. For instance, some versions of the Cisco Call Manager were typically installed on Windows 2000 and thus vulnerable to the Nimda worm. There are hundreds of remotely exploitable vulnerabilities in flavors of Windows for which there are numerous “point-and-shoot” exploits freely available for download on the Internet. No matter how secure an actual VoIP application happens to be, this becomes moot if the underlying operating system is compromised. It is typically incumbent upon the vendor to upgrade the underlying operating system or firmware.

8.1.4 Distributed Denial of Service

In a distributed DoS attack, a large number – perhaps millions – of computers simultaneously generate traffic designed to exhaust network or application resources. The attack may be carried out in two stages, first infiltrating a hidden control program, or “stealth worm” into network-attached computers, and then using these controls to cause the infected computer to launch the actual DoS attack. The second stage of the attack might or might not involve any direct action by the attacker; the attack could easily be launched automatically at some pre-specified time.

The simplest way to use an army of infected computers to block Internet services would be to have all of the stealth worm instances simply “blow their cover” at the scheduled time and start replicating themselves across the Net, in the manner of a traditional Internet worm. Unlike a typical Internet worm attack, however, the stealth worm would get a big head-start – instantly hitting the Internet from, say, a million sources, with no warning and no ramp-up interval.

As critical Internet resources – routers, DNS servers, etc. – get overloaded and fail, traffic and queries would be rerouted to alternate facilities, directing an increasing load on these resources until they fail. If the attack disrupts all Internet connectivity between any two edge locations, all VoIP traffic that rides the Internet will be cut off between those edge nodes, regardless of any higher-level safeguards the voice path might have.

Yet another alternative is to overload the call control servers, gateways, etc. that manage the voice application itself.

Suppose that a stealth worm causes all infected PCs to call 911 during the expected busy hour on Mother's Day. According to the latest regulations, all VoIP services will have direct gateway connections to the high-priority switching systems that connect the PSTN to emergency service centers. So one or all of the following would happen:

Since it is unlikely that the VoIP gateways would be engineered to handle the artificial flood of calls caused by the computer worm, a lot of emergency call attempts on the VoIP networks – including some real emergency calls – may not go through.
If the VoIP network gives priority to emergency calls, the 911 call flood will also prevent any other calls from going through.
If the interconnections of VoIP gateways to the PSTN's priority call routing system are engineered on the assumption that they will not all deliver 100% of their capacity at the same time, the PSTN's emergency calling system will start dropping 911 calls, both from the VoIP gateways and from the PSTN itself.
If the emergency service centers had been upgraded to support VoIP directly, no gateways would be needed – and the 911 flood would hit the emergency centers at full force.

The PSTN operators would then have to make an impossible choice between letting their emergency services degrade or else shutting the VoIP services off.

8.2 Physical Intrusion

Physical intrusion of a premise via the compromise of lock and key entry systems, alarm systems, surveillance systems, and security guards can seriously impact VoIP Service.

Physical intrusion is not limited to a building or facility. The Physical Layer of the OSI Reference Model must also be considered.

A number of possible interruptions of service arise when physical access is gain to components within the VoIP Network.

- ARP spoofing/poisoning
- IP spoofing
- Unauthorized configuration changes
- Intentional loss of power

Sources/threats of Physical Intrusion ISC2-CISSP-CBK, COMMWEB-1 include:

Physical access to facilities containing networking equipment

- Location where the facility which may be at a sensitive site
- Entry Points including windows, doors, wiring closets, maintenance and roof entrances, floors, emergency exits, and shipping and receiving areas.

Physical access to the cable and wire system in such facilities

- Access to electrical signals conducted over copper wires through an antenna or inductive coil.
- Fiber optics systems that are physically wiretapped
- Wireless systems - antennas in proximity to the target system and RF signals that are interfered with or intercepted.

Physical access to systems and equipment

Vulnerability to social engineering attacks

- Classic social engineering of enterprise personnel via phone, direct contact or email
- Impersonation
- False ID
- Surreptitious Entry
- Unmonitored/uncontrolled access, entry

To determine the degree of risk associated with each threat source or target, a detailed vulnerability assessment may be required to accurately determine the quantitative risk and estimate single loss expectancy, annualized rate of occurrence, and annualized loss expectancy.

9.0 Other Interruptions of Service

9.1 Loss of Power

When data network infrastructure (network ingress/egress points, wiring closets, servers, switches, routers, security devices, and in general, all DCE/DTE) lose power, and unless a back-up battery system or UPS system is widely deployed, and capable of providing emergency power for more than reasonable period of time, the communication capability of the VoIP Service will be lost.

Intentional sources/threats of loss of power due to human interference include: terrorism, vandalism, theft, overt/covert disruption of service, and power distribution systems destruction.

Companies should have backup power sources in place such as UPS or fuel-powered generators. Measures should also be taken to minimize the effects of electromagnetic interference and radio frequency interference. You local Power Company can assist you with assuring the appropriate regulators and line conditioners are in place to protect against these discrepancies.

As previously mentioned, the degree of risk associated with these power loss threats should also be include in any detailed vulnerability assessment to determine the quantitative risk; this includes calculations for single loss expectancy, annualized rate of occurrence, and annualized loss expectancy.

Loss of power may occur at an Endpoint making VoIP Service unavailable for the user.

Endpoints that rely on Power-over-Ethernet IEEE-802-3af, are susceptible to loss of power on events such as disconnect of the network cable and loss of power at the supplying Ethernet switch.

Endpoints such as wireless handheld phones, which use an internal power source, are prone to loss of power. This weakness can be leverage as a DoS by flooding the Endpoint with messages causing the battery to drain unnecessarily.

9.2 Resource Exhaustion

- Deficiencies in software or hardware that causes depletion of memory resource (e.g. buffers) in a network element.
- Deficiencies in software or hardware that consumes most of CPU resource in a network element.
- Hardware or software errors that limit available bandwidth of a communication link.
- Software or hardware deficiencies that generate unnecessary messages reducing bandwidth resources.
- Errors in operations by network management system or by craft personnel resulting in limited or unavailable memory, CPU or bandwidth resources.
- Attacks in this security threat category may target Endpoints, Servers, or both:

9.3 Performance Latency

Performance latency affects the two aspects of VoIP: signaling and media, in different ways.

VoIP signaling is affected by performance latency in areas such as dial tone delay and call setup time after dialing.

Excessive latency or packet loss results in unintelligible or choppy media exchange. When this impacts consecutive media packets, the quality is degraded to a greater extent than if the impact was spread over a number of media packets.

Media packets received out-of-order also affect quality by introducing jitter. Excessive jitter may lead to packet loss (as packets are received outside their permitted arrival window).

Performance Metrics

To be considered as providing same or better than toll quality telephony service provided by the PSTN, the following media performance metrics are defined in ITU-T-G113 and ITU-T-G114:

· Latency < 150 ms

A latency of 150ms – 200ms, though usable, results in 'choppy' media exchange. Latency greater than 200ms, is typically considered unusable as delays prevent normal 'conversation'.

· Jitter < 25ms

Buffering at the receiver can reduce the effect of jitter.
Excessive jitter introduces delays and affects media exchange in similar ways as latency.

· BER < 0.25%, Packet Loss < 5%

As media typically uses UDP, an unreliable IP transport protocol, there is only limited recovery from packet errors and loss. Packet loss below the specified threshold is usually imperceptible. Excessive packet loss introduces delays and affects media exchange in similar ways as latency.

Call setup time is another important performance metric that needs attention in a VoIP network. After full deployment of SS7 signaling, PSTN call setup times settled down to 0.8 seconds for calls that only involved a local switch, and 1.0 second for calls routed through an access tandem switch. This became a competitive requirement, and some of the FCC's orders regulating access to toll-free number databases came close to making it a regulatory requirement as well.

References

- [Hohfeld] W. N. Hohfeld, 3 Yale Law Journal 16-59 “Some Fundamental Legal Conceptions as Applied in Judicial Reasoning” (1913)
- [Coke] Coke's *Institutes*, Part III (1797 edition) chapter 1, folio 10
- [MPC] Model Penal Code, American Law Institute (1962) http://www.ali.org/
- [Prosser & Keeton] Prosser & Keeton, The Law of Torts, Chapter 18 “Misrepresentation and Nondisclosure” (5th ed. 1984 West Publishing)
- [FTC Act] U.S. Federal Trade Commission Enabling Act of Sept. 26, 1914, ch. 311, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § § 41-58 (1994))
- [OLAF Act] European Anti-Fraud Office (OLAF) by EC, ECSC Decision 1999/352 of 28 April 1999 http://europa.eu.int/comm/dgs/olaf/mission/index_en.html
- [CERT-H323] CERT® Advisory CA-2004-01 Multiple H.323 Message. Vulnerabilities, CERT (http://www.cert.org/advisories/CA-2004-01.html)
- [CERT-SIP] CERT® Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP), CERT. (http://www.cert.org/advisories/CA-2003-06.html)
- [COMMWEB-1] VoIP Security: Loose IPs Sink Ships, CommWeb. (http://www.commweb.com/23905157)
- [DISA-VOIP] Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide, Defense Information Systems Agency. (http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V1R1R-4PDF.pdf)
- [IEEE-802-3] IEEE 802.3 CSMA/CD (Ethernet) Working Group. (http://grouper.ieee.org/groups/802/3/)
- [IEEE-802-3af] IEEE 802.3 Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI). (http://standards.ieee.org/getieee802/download/802.3af-2003.pdf)
- [IEEE-802-11] IEEE 802.11 Wireless LAN Working Group. (http://grouper.ieee.org/groups/802/11/)

- [IEEE-802-16] IEEE 802.16 Broadband Wireless Working Group. (http://grouper.ieee.org/groups/802/16/)
- [IETF-COPS] The COPS (Common Open Policy Service) Protocol, IETF RFC 2748. (http://www.ietf.org/rfc/rfc2748.txt)
- [IETF-DHCP] Dynamic Host Configuration Protocol, IETF RFC 1541. (http://www.ietf.org/rfc/rfc1541.txt)
- [IETF-DIAMETER] Diameter Base Protocol, IETF RFC 3588. (http://www.ietf.org/rfc/rfc 3588.txt)
- [IETF-DNS] Domain Names – Concepts and Facilities, IETF RFC 1034. (http://www.ietf.org/rfc/rfc1034.txt)
- [IETF-FTP] File Transfer Protocol, IETF RFC 959. (http://www.ietf.org/rfc/rfc959.txt)
- [IETF-HTTP] Hypertext Transfer Protocol -- HTTP/1.1, RFC 2616. (http://www.ietf.org/rfc/rfc2616.txt)
- [IETF-IP] Internet Protocol, IETF RFC 791. (http://www.ietf.org/rfc/rfc791.txt)
- [IETF-MEGACO] Megaco Protocol (1.0), IETF RFC 3015. (http://www.ietf.org/rfc/rfc3015.txt)
- [IETF-MGCP] Media Gateway Control Protocol (1.0), IETF RFC 3435. (http://www.ietf.org/rfc/rfc3435.txt)
- [IETF-MIDCOM] Middlebox Communication Working Group. (http://www.ietf.org/html.charters/midcom-charter.html)
- [IETF-RTP] A Transport Protocol for Real-Time Applications, IETF RFC 3550. (http://www.ietf.org/rfc/rfc3550.txt)
- [IETF-SIP] Session Initiation Protocol, IETF RFC 3261. (http://www.ietf.org/rfc/rfc3261.txt)
- [IETF-SNMP] A Simple Network Management Protocol, IETF RFC 1157. (http://www.ietf.org/rfc/rfc1157.txt)
- [IETF-RADIUS] Remote Authentication Dial In User Service, IETF RFC 2865 (http://www.ietf.org/rfc/rfc2865.txt)
- [IETF-TCP] Transmission Control Protocol, IETF RFC 793. (http://www.ietf.org/rfc/rfc793.txt)

- [IETF-TELNET] Telnet Protocol Specification, IETF RFC 854. (http://www.ietf.org/rfc/rfc854.txt)
- [IETF-TFTP] The TFTP Protocol (Revision 2), IETF RFC 1350. (http://www.ietf.org/rfc/rfc1350.txt)
- [IETF-UDP] User Datagram Protocol, IETF RFC 768. (http://www.ietf.org/rfc/rfc768.txt)
- [ISC2-CISSP-CBK] ISC2 CISSP CBK Student Manual, v2.1
- [ITU-T-G113] Transmission impairments due to speech processing, ITU-T Recommendation G.113. (http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-G.113).
- [ITU-T-G114] One-way Transmission Time, ITU-T Recommendation G.114. (http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-G.114)
- [ITU-T-H323] Packet-based multimedia communications systems, ITU-T Recommendation H.323. (http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.323)
- [NIST-VOIP] NIST Security Considerations for Voice Over IP Systems, National Institute of Standards and Technology NIST SP 800-58. (http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf)
- [USENIX-VERN] How to Own the Internet in your Spare Time, Staniford, Paxson, Weaver, 11th USENIX Security Symposium, 2002. (http://www.icir.org/vern/papers/cdc-usenix-sec02/)

