TECHNICAL REPORT

ISO/IEC TR 16166

First edition
2010-08-01

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Security of session-based communications

Technologies de l'information — Téléinformatique — Réseaux d'entreprise de prochaine génération (NGCN) — Sécurité des communications sur la base de sessions

Reference number
ISO/IEC TR 16166:2010(E)

ISO copyright office
Case postale 56 CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 16166 was prepared by Ecma International (as ECMA TR/100) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

This Technical Report is one of a series of Ecma publications that explore IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on inter-domain communication, including communication between parts of the same enterprise, between enterprises and between enterprises and carriers. This particular Technical Report discusses issues related to the security of session-based communications and builds upon concepts introduced in ISO/IEC TR 12860.

This Technical Report is based upon the practical experience of Ecma member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus. In particular, Ecma acknowledges valuable input from experts in ETSI TISPAN.

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Security of session-based communications

1 Scope

This Technical Report is one of a series of publications that provides an overview of IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on session level communication based on the Session Initiation Protocol (SIP) [4], with an emphasis on inter-domain communication. This includes communication between parts of the same enterprise (on dedicated infrastructures and/or hosted), between enterprises and between enterprises and public networks. Particular consideration is given to Next Generation Networks (NGN) as public networks and as providers of hosted enterprise capabilities. Key technical issues are investigated, current standardisation work and gaps in this area are identified, and a number of requirements and recommendations are stated. Among other uses, this series of publications can act as a reference for other standardisation bodies working in this field, including ETSI TISPAN, 3GPP, IETF and ITU-T.

This particular Technical Report discusses security of session-based communications. It uses terminology and concepts developed in ISO/IEC TR 12860 [1]. It identifies a number of requirements impacting NGN standardisation and makes a number of recommendations concerning deployment of enterprise networks. Also a number of standardisation gaps are identified. Both signalling security and media security are considered.

The scope of this Technical Report is limited to communications with a real-time element, including but not limited to voice, video, real-time text, instant messaging and combinations of these (multi-media). The non-real-time streaming of media is not considered. For media, only security of transport (e.g., securing the Real-time Transport Protocol, RTP [6]) is considered, and higher level security measures (e.g., digital rights management) are not considered. Peer-to-peer signalling between SIP user agents (without involving SIP intermediaries) is not considered.

Detailed considerations for lawful interception are outside the scope of this Technical Report, although general considerations for call recording and audit are discussed.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] ISO/IEC TR 12860, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — General

[2] ISO/IEC TR 12861, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Identification and routing

[3] ISO/IEC TR 16167, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Emergency calls

[4] IETF RFC 3261, SIP: Session Initiation Protocol

[5] IETF RFC 3325, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[6] IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications

[7] IETF RFC 3711, The Secure Real-time Transport Protocol (SRTP)

[8] IETF RFC 3830, MIKEY: Multimedia Internet KEYing

[9] IETF RFC 3893, Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format

[10] IETF RFC 4119, A Presence-based GEOPRIV Location Object Format

[11] IETF RFC 4301, Security Architecture for the Internet Protocol

[12] IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1

[13] IETF RFC 4347, Datagram Transport Layer Security

[14] IETF RFC 4474, Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)

[15] IETF RFC 4567, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)

[16] IETF RFC 4568, Session Description Protocol (SDP) Security Descriptions for Media Streams

[17] IETF RFC 4650, HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)

[18] IETF RFC 4738, MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)

[19] IETF RFC 4916, Connected Identity in the Session Initiation Protocol (SIP)

[20] IETF RFC 4961, Symmetric RTP / RTP Control Protocol (RTCP)

[21] IETF RFC 5626, Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)

[22] IETF RFC 5630, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)

[23] IETF RFC 5761, Multiplexing RTP Data and Control Packets on a Single Port

[24] IETF RFC 5763, Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)

[25] IETF RFC 5764, Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)

[26] IETF draft-ietf-sip-connect-reuse-14, Connection Reuse in the Session Initiation Protocol (SIP)

NOTE At the time of publication of this Technical Report, the IETF had approved this draft as a standards track RFC but had not published the RFC and had not allocated an RFC number. If the draft is no longer available, readers should look for the RFC with the same title.

[27] IETF draft-ietf-sipcore-location-conveyance-02, Location Conveyance for the Session Initiation Protocol

NOTE At the time of publication of this Technical Report, the IETF had not completed the approval process for this draft and had not allocated an RFC number. If the draft (or a later version) is no longer available, readers should look for the RFC with the same title.

[28] IETF draft-zimmermann-avt-zrtp-16, ZRTP: Media Path Key Agreement for Secure RTP

NOTE At the time of publication of this Technical Report, the IETF had not published this as an informational RFC. If the draft (or a later version) is no longer available, readers should look for the RFC with the same title.

[29] ITU-T Recommendation E.164, The international public telecommunication numbering plan

[30] ISO/IEC 9594-8 | ITU-T Rec. X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

[31] 3GPP TS 33.203, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)

[32] 3GPP TS 33.210, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Network domain security; IP network layer security (Release 8)

[33] 3GPP TS 33.310, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network domain security; Authentication Framework (AF) (Release 8)

[34] ETSI TS 187 003, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture

[35] IEEE 802.1x, IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control (2004)

[36] IEEE 802.11, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements - Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications (2007)

[37] OASIS, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (March 2005)

[38] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 External definitions

This Technical Report uses the following terms defined in ISO/IEC TR 12860 [1]:

- Domain
- Enterprise network
- Next Generation Corporate Network (NGCN)
- Next Generation Network (NGN)
- Private network traffic
- Public network traffic
- Session Service Provider (SSP)

- SIP intermediary

3.2 Other definitions

None.

4 Abbreviations

AIB	Authenticated Identity Body
AKA	Authentication and Key Agreement
CA	Certification Authority
B2BUA	Back-to-Back UA
DECT	Digital Enhanced Cordless Telecommunications
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
DNS	Domain Name System
GAN	Generic Access Network
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
MIKEY	Multimedia Internet KEYing
NAT	Network Address Translation
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
PAI	P-Asserted-Identity
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S/MIME	Secure Multi-media Internet Mail Extensions
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure RTP
SSP	Session Service Provider
TCP	Transaction Control Protocol
TLS	Transport Layer Security
UA	User Agent

UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Universal Resource Identifier
VPN	Virtual Private Network
WLAN	Wireless LAN

5 Background

General concepts of NGCNs are discussed in ISO/IEC TR 12860 [1]. In particular, that document describes use of the Session Initiation Protocol (SIP) [4] for session level communications within enterprise networks and with other domains. It focuses on enterprise networks based on enterprise infrastructure (NGCN), but also covers hosting on other networks, in particular NGNs, using the same infrastructure that supports public networks.

ISO/IEC TR 12860 describes the basic communications architecture of an NGCN as comprising three levels (transport, session and application), together with security and management capabilities spanning all three levels. This reflects the fact that security vulnerabilities can arise at all three levels, and therefore appropriate security measures need to be put in place at and across all three levels. Security measures aim to ensure data integrity and confidentiality, authentication of parties, authorisation, and prevention of denial of service (DoS) attacks. For example, at the transport level, measures may be taken to authenticate equipment when connecting to a Local Area Network (LAN), e.g., using IEEE 802.1x [35] or to protect communications on a Wireless LAN (WLAN), e.g., using Robust Security Network Association (RSNA) [36] (known commercially by the WiFi Alliance as Wireless Protected Access 2, WPA2). Alternatively Virtual Private Network (VPN) technologies can be used (e.g., based on TLS [12] or IPsec [11]), particularly when accessing an NGCN from an untrusted LAN or WLAN. Session level and application level communications can to some extent rely on underlying security at the transport level, but in general this is insufficient for achieving end-to-end security.

At the session level, the signalling protocol (SIP) is used to negotiate the parameters needed to allow session-related media streams to flow between endpoints. In the case of real-time media (audio, video), transport is achieved using the Real-time Transport Protocol (RTP) [6]. For non-real-time media conventional transports such as the Transport Control Protocol (TCP) can be used directly. Both the security of SIP signalling and the security of media need to be considered.

This Technical Report analyses the needs and available mechanisms for securing SIP signalling and for securing real-time media transported over RTP. Signalling security is discussed in clause 7. Media security, including the security of any signalling in support of media security, is discussed in clause 8. The securing of non-real-time media is not considered.

6 General principles

6.1 Threats and counter-measures

Information technology security involves the careful balancing of threats and counter-measures. Threats can be assessed in terms of:

- how easily can a vulnerability be exploited; and
- the amount of damage that can be inflicted by a successful attack.

Counter-measures generally incur some costs, such as:

- the cost of purchasing or licensing additional hardware or software (e.g., card readers, biometric devices);

- ongoing operational costs (in terms of dealing with forgotten passwords, handing out and replacing certificates, etc.);
- inconvenience to the user (e.g., the need to enter passwords and Personal Identification Numbers (PINs));
- reduced performance arising from increased computation times.

Thus costly measures are not normally put in place to counter an attack that is difficult to stage and can inflict relatively little damage. On the other hand, an attack that is easily staged and can inflict substantial damage will almost certainly need to be countered.

In enterprises, damage is often assessed in terms of the amount of financial damage that can be inflicted on the enterprise, either directly (e.g., by stealing money or goods) or indirectly (e.g., by stealing trade secrets or marketing plans, or by causing disruption to an enterprise's normal operations). Also enterprises have certain legal and moral obligations (e.g., data protection, retention of data), and damage can be done to a company's reputation if these obligations fail to be met because of inadequate security. The term enterprise network is often applied to similar communication networks operated by non-commercial organisations (e.g., military, educational, medical), and similar security principles apply to these networks, although weightings might be different. For example, in a military network the consequences of certain attacks might be considered greater, and therefore more costly counter-measures might be justified.

For a given enterprise, security policy [38] will determine the particular measures taken. Security policy can change as an enterprise becomes aware of or the victim of new threats. Tools exist to assist in analysing risks and recommending counter-measures.

6.2 Threats to session level security

A secure network aims to support communications with the following properties (among others):

- authenticity, whereby the claimed identity of an entity (e.g., a user) is correct;
- integrity, whereby information has not been altered or destroyed in an unauthorised manner;
- confidentiality, whereby information has not been disclosed to an unauthorised individual;
- privacy, which is closely related to confidentiality and concerns the right of an individual to control how information related to the individual is held or disclosed to others;
- availability, whereby network services to legitimate users are not denied through unauthorised intervention;
- non-repudiation, whereby proof of involvement of a party in certain actions (e.g., sending or receiving a message, stating something during a call) is secured and stored for later use.

For session level communications, successful attacks can compromise these properties in various ways, e.g.:

- eavesdropping on media (e.g., voice, video, messaging);
- discovery of call details (who called whom and when);
- discovery of private information relating to a user (e.g., his current geographic location);
- discovering a user's password, PIN or other credentials;
- masquerading, such as calling somebody and presenting a false caller identifier;
- injecting unwanted media into a call between two legitimate users;