ATIS-0100036.2013 (R2018)

MEDIA PLANE PERFORMANCE SECURITY IMPAIRMENTS FOR EVOLVING VoIP/MULTIMEDIA NETWORKS

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0100036.2013(R2018), *Media Plane Performance Security Impairments for Evolving VoIP/Multimedia Networks*

Is an American National Standard developed by the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0100036.2013(R2018)

American National Standard for Telecommunications

Media Plane Performance Security Impairments for Evolving VoIP/Multimedia Networks

Alliance for Telecommunications Industry Solutions

Approved: January 23, 2013

American National Standards Institute, Inc.

Abstract:

This ATIS Standard is intended to provide awareness and information regarding the use of security mechanisms in support of Next Generation Network (NGN) National Security and Emergency Preparedness (NS/EP) Services. When introducing network security mechanisms (e.g., IPSec) into Evolving Voice over Internet Protocol (VoIP)/Multimedia Networks, one may encounter impairments introduced or exacerbated by those network security mechanisms. One may need to explore tradeoffs between security and QoS to achieve the necessary communication channel during NS/EP conditions.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantage.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PRQC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PRQC, which was responsible for its development, had the following leadership:

P. Tarapore, PRQC Chair (AT&T)
J. Colombo, PRQC Vice-Chair (Verizon)
A. Webster, Technical Editor (US Department of Commerce)
A. Nguyen, Technical Editor (National Communications Systems)
C. Underkoffler, ATIS Chief Editor

Active Participants:

K. Biholar
J. Colombo
C. Dvorak
G. Linnell
A. Nguyen
P. Tarapore
A. Webster
O. Lima
S. Makris

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Voice over Internet Protocol (VoIP) Quality of Service (QoS) may worsen during times of congestion. There are many factors affecting QoS, including: packet loss, packet retransmission, packet delays, jitter, out-of-sequence packets, codec selection, and noise levels. Network congestion at routers leads to increased delays and potentially lost packets that may become compounded when the need for cryptographic services is present. Network security mechanisms such as IP Security (IPSec) and Secure Real-Time Transport Protocol (SRTP) introduce overhead to packets and may cause new points of potential congestion, such as the ingress/egress of an IPSec tunnel.

In order to understand the impact of adding network security services to VoIP calls, network modeling was conducted using a variety of voice codecs across three scenarios: 1) no congestion (baseline), 2) congestion at three times the baseline traffic; and 3) congestion at three times the baseline traffic while security services are used for calls. Mean Opinion Score (MOS) as estimated by the E-Model is used extensively to measure QoS throughout the modeling efforts for a select number of the modeled calls in the system. MOS is a subjective measure of call quality while the E-Model is a numerical approximation of MOS. It was demonstrated that low-bandwidth codecs are more easily able to withstand the effects of congestion, as well as the security measures, at the cost of lower initial call quality. In fact, the highest quality modeled codec, G.711, had the lowest final MOS when using security under congestion. Additional modeling showed that with increased priority weight at routers and priority queuing for IPSec cryptography engines, even G.711 could meet the Class 1 QoS requirements listed in ITU-T Y.1541. Class 1 QoS is defined as having an upper delay bound of no greater than 400 ms and packet loss no greater than 0.1%.

While network security mechanisms are not always pertinent for VoIP users, they may be important for users such as those in the United States National Security and Emergency Preparedness (NS/EP) community. Providing mechanisms which may improve voice QoS for certain high-priority calls during national security events and other periods of high congestion is essential for ensuring that those calls complete successfully. Three solutions are identified that could provide acceptable QoS to specific calls:

1. Increasing queuing priority at routers over the value held for public VoIP traffic.
2. Establishing priority queuing at both the IPSec ingress and egress.

   NOTE: This may require the copying of the Differentiated Services Code Point (DSCP) from the inner header to the IPSec header when entering an IPSec tunnel, so that the priority markings may be accessed by the egress cryptographic engine.
3. Adapting codec selection and the use of security services depending on the immediate conditions of the network. For instance, it may be worthwhile to switch to a low-bandwidth codec when facing severe congestion.

Implementing just the last two solutions in the modeling showed that packet loss could be reduiced from over 58% to 0.10%.

.

American National Standard for Telecommunications on –

Media Plane Performance Security Impairments for Evolving VoIP/Multimedia Networks

1 Introduction

Service quality in packet-based networks can be negatively affected by numerous conditions such as congestion, link bit error rates, or use of various security mechanisms. This document discusses the impacts of implementing security standards, including an evaluation by estimated mean opinion score (MOS) in a network model.

An overview of the purpose of this document is given in section 2, while section 3 lists all references from standards and provides a table of acronyms. Section 4 provides light background on the role that Quality of Service (QoS) plays in media services. Section 5 highlights modeling results from a simulation involving MOS and cryptography services for a standard voice call both with and without congestion. Finally, section 6 discusses Next Generation Network (NGN) National Security and Emergency Preparedness (NS/EP) services and highlights several proposed changes to support them. In addition, there are four annexes designed to provide a good set of background information on QoS and security services.

2 Scope, Purpose, & Application

This document focuses primarily on media flow performance, specifically the transfer of voice, all forms of video, high fidelity audio, and other information that is time sensitive. Voice over Internet Protocol (VoIP) and multimedia applications are evolving to use NGNs that are packet-based. These services use multiple broadband QoS-enabled transport technologies where service related functions are part of the service stratum and are independent of technologies in the transport spectrum.

Section 6 discusses NGN NS/EP service and how new proposed security features could improve their performance and survivability during heavy network congestion.

The NGN architecture is defined in ITU-T Y.2011 and ATIS-1000018, *NGN Architecture*. The performance objectives for Internet Protocol (IP)-based services are described in ITU-T Y.1541. With the use of resource and admission control functions defined in ITU-T Y.2111, QoS-related decisions are made based upon service level agreements, service priority and multiple domains.

ATIS-0100014, *Information and Communications Security for NGN Converged Services IP Networks and Infrastructure*, discusses the security requirements and mechanisms to be considered in offering NGN services. The use of the security mechanisms discussed in the ATIS-0100014, such as various forms of encryption, impact the QoS objectives and requirements for offered services. This document addresses the selection of appropriate security support while meeting the performance (QoS) objectives, especially with consideration for NGN NS/EP services, which aim to provide priority telecommunications capabilities over NGN networks to personnel involved with national security or public safety. It is based off of the legacy Government Emergency Telecommunications Service (GETS), which was created in the mid-90s to provide the same capability over the Public Switched Telephone Network (PSTN).