INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

COM 17 – D 101 – E

(WP 2/17)

English only

Question(s): 10/17

STUDY GROUP 17 – DELAYED CONTRIBUTION 101

Source: Canada

Title: Proposal for Signalling Security Requirements at PSTN Interconnection with VoIP networks

Abstract

The Public Switched Telephone Network (PSTN) today is a well-trusted and secured network where reliable telephony service is provided to the general public. With the standardization of IP Telephony in ITU and IETF, carriers and service providers will be implementing Voice over Internet Protocol (VoIP) services where interconnection to the PSTN will be required. The Internet today is an open network where security and vulnerability is a major issue, in comparison to the PSTN. As such, the interconnection of service provider and carrier VoIP to the PSTN must be carefully considered and examined.

Background

As VoIP service becomes more widespread and interconnected, the need for Internet users to communicate with PSTN users becomes more realistic. The PSTN has been providing reliable service to its users for many generations and is considered a trusted network. In emergency situations, the PSTN is also the life line for the public to reach local authorities. Telephone Operating Companies rely on the PSTN for continuous revenue generation, which in turn fuels the economy. Since 9/11, for many governments, the PSTN has been listed as a national critical infrastructure.

On the other hand, the Internet is subject to many security and vulnerability issues causing network outages and downtime. The Internet's openness and transparency are exploited by hackers and terrorists alike. As such any node or network, once attached to the Internet, may inherit many of the known and future unknown security threats that trouble all nodes or networks on any IP-based network.

Contacts:

Peter Chau
Industry Canada
Canada
Tel: +1 613 998 4861
Fax: +1 613 957 8845
Email: Chau.Peter@ic.gc.ca

Bill McCrum
Industry Canada
Canada
Tel: +1 613 990 4493
Fax: +1 613 957 8845
Email: McCrum.William@ic.gc.ca

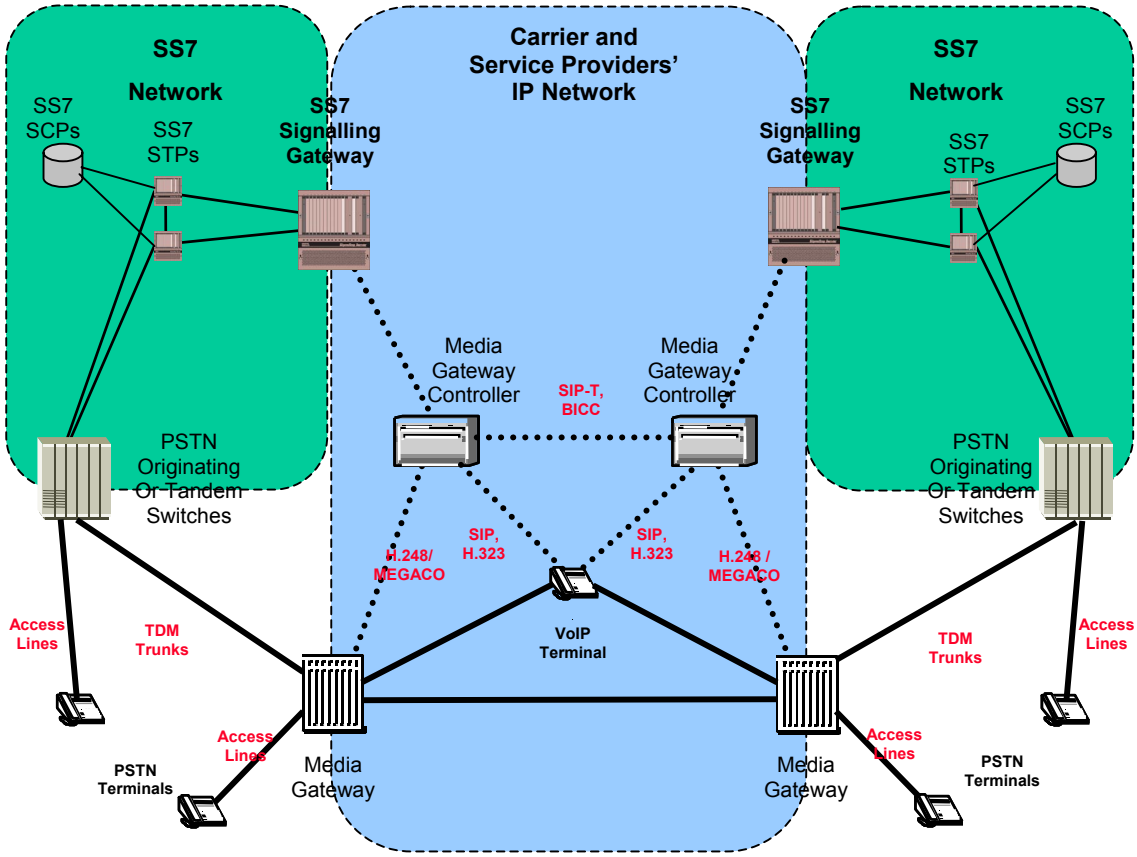
VoIP is defined as providing voice communication over an IP based network. Significant implementation of VoIP has occurred within the enterprise space – i.e. Enterprise VoIP. Enterprise VoIP allows a corporate data network to be used for transporting voice, thus saving on toll charges and trunk resources for the corporation. The H-Series (i.e. H.323) protocol developed by ITU Study Group 16 has been used for a majority of multimedia services implementations, including enterprise VoIP.

Some carriers and service providers have deployed VoIP in their networks. When deployed in the carriers and service providers' environment, these VoIP networks interconnect with the PSTN through the Signalling System No. 7 (SS7) networks. SS7 is the standard signalling protocol for the PSTN. A generally accepted carrier and service provider VoIP reference model developed by IETF, ITU and ETSI standards bodies is depicted in Figure 1. This architecture applies to both wireline and wireless IP networks.

For call signalling and control data, the interconnection between the PSTN and the IP Network is at the Signalling Gateway. For bearer information, the Media Gateway is the interface. The protocol at the signalling gateway has been specified by IETF and it is called SigTran (Signalling Transport). Equipment at this interface supports various SS7 signalling variants, high scalability, and carrier-grade reliability

All gateways connecting to the PSTN need to be scrutinized for security concerns. For the purpose of this contribution, the signalling interconnection will be the focus of discussion.

Figure 1 – ITU, IETF & ETSI VoIP Architecture for Carriers and Service providers



Proposal

As a national critical infrastructure, the PSTN is critical to the health, safety, security and economic well-being of citizens and to the effective functioning of governments. Therefore, it is imperative that this infrastructure be protected and secured. At the same time, as Internet's popularity grows, more users will be using the Internet for voice communication. The growth of carrier and service provider VoIP is inevitable.

Member states that are new to this type of technology and service may need assistance and advice to help ensure that their PSTN is not compromised when introducing carrier and service provider VoIP.

It is proposed that the signalling interconnection interface – the Signalling Gateway, between the PSTN and the VoIP network be examined for protocol vulnerability, secured communication and industry best practices. A set of security requirements and specification pertaining to the above for the Signalling Gateway shall be available as a result.

Study Group 17, as the lead group for Communication Systems Security (CSS), is responsible for defining the scope of requirement for a secured interconnection between the PSTN and the VoIP network. This study group in defining security requirements for communication systems has produced a Draft Recommendation X.css – Security Architecture for Systems Providing End-to-End Communications. The author would like to refer to this draft recommendation.

A secured interconnection interface for carrier and service provider VoIP falls in the domain of securing the Infrastructure Layer of the Management Plane, the End-User Plane and Control Plane, as per Draft Recommendation X.css. For example, security at the Control Plane consists of securing the control or signalling information that resides in the network elements and server platforms that comprise the network as well as securing the receipt and transmission of control or signalling information by the network elements and server platforms.

It is proposed that an evaluation of the communication protocol and system in question, against the following Security Dimensions, as defined in Draft Recommendation X.css:

- Access Control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication Security
- Data Integrity
- Availability
- Privacy

Please refer to Draft Recommendation X.css for the security objectives of each of the dimensions.

As a result, it is proposed that liaison be sent to the respective Study Groups – SG4 for Management Plane; SG9/SG11/SG13/SG16/SSG for Control Plane and End-User Plane, requesting an evaluation of the protocols and interfaces under their jurisdiction. It is expected that liaison with the IETF on the SigTran protocol will be required in the process of the evaluation.

Further, the liaison should indicate that the respective work plans of the Study Groups and any Recommendations to ensure compliance with the Security Requirements Recommendation X.css are to be communicated to SG17, so that proper control and coordination over the project by SG17 can be continued. The liaison and the individual Study Groups should strongly encourage equipment vendors, telephone operators and Internet service providers to participate in this exercise.

It is expected that at the end of the evaluation, a report, in the form of a Recommendation, that consolidates the Security Requirement and Specification of the Signalling Gateway be available.

_____