PCC.I/RES. 45 (IV-04)[1]

COORDINATED STANDARD DOCUMENT FOR ITU-T RECOMMENDATION X.805, "SECURITY ARCHITECTURE FOR SYSTEMS PROVIDING END-TO-END COMMUNICATIONS"

The IV Meeting of the Permanent Consultative Committee I: Telecommunication Standardization,

CONSIDERING:

a) That secure information networks play an important role for the critical infrastructure of all OAS Member States, their economies and their societies;

b) That, with the development of information and communication technologies and networks have given rise to ever-growing security challenges; and

c) That the Permanent Executive Committee of the Inter-American Telecommunication Commission (COM/CITEL) has identified building a culture of cyber security as an important objective for CITEL (COM/CITEL/RES. 151 (XII-02)),

RECOGNIZING:

a) That telecommunications carriers and service providers of the region are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, etc.;

b) That ITU.T Recommendation X.805, "Security architecture for systems providing end-to-end communications" defines an architecture that can be applied to various kinds of networks where the end-to-end security is a concern and defines the general security-related architectural elements that are necessary for providing end-to-end security; and

c) That the ITU-T Study Group 17 approved Recommendation X.805 in October 2003 under the "Alternative Approval Process" (AAP) and it is now in force,

RESOLVES:

To endorse ITU.T Recommendation X.805 Security architecture for systems providing end-to-end communications" with no deletions, additions or modifications.

RECOMMENDS:

1. That the Working Group on Standards Coordination continues to monitor the security work of ITU-T Study Group 17 and determine its applicability for the Americas as this work evolves; and

2. That the Working Group on Standards Coordination continues addressing the security needs of the Americas and provides additional recommendations for endorsing standards that serve to enhance network security.

---

[1] CCP.I-TEL/doc.393/04

ANNEX TO RESOLUTION PCC.I/RES.45 (IV-04)

Coordinated Standards Document
Security Architecture for Systems Providing End-to-End Communications

1. EXECUTIVE SUMMARY

The Working Group on Standards Coordination (WGSC) has addressed network and protocol security as part of its studies of standards for Next Generation Networks (NGN), Services, Signaling, and Operations as they relate to the security needs of the Americas. Part of this activity has included monitoring the work of the ITU-T. ITU-T Study Group 17 (Data Networks and Telecommunication Software) has been designated as the Lead ITU-T Study Group for Communication System Security. In this capacity, Study Group 17 created a security architecture document (draft Recommendation X.css, "Security architecture for systems providing end-to-end communications") to define the general security-related architectural elements necessary for providing end-to-end security. Draft versions of Recommendation X.css were reviewed at the PCC.I Meetings in Guatemala City (April 2003) and Mexico City (September 2003). At the Third Meeting of PCC.I (Mexico City; September 2003), it was reported that draft Recommendation X.css had been put forward by Study Group 17 for approval as ITU-T Recommendation X.805. The WGSC has recommended that CITEL PCC.I endorse Recommendation X.805. Since the standard was still in the approval process, PCC.I chose to defer its endorsement until the Fourth Meeting of PCC.I (Quito; March 2004). Therefore, this Coordinated Standards Document (CSD) now presents ITU-T Recommendation X.805 to PCC.I for its endorsement for the region of the Americas.

2. BACKGROUND

ITU-T Recommendation X.805, "Security architecture for systems providing end-to-end communications", defines a network security architecture for providing end-to-end network security. This architecture can be applied to various kinds of networks where the end-to-end security is a concern and is independent of the network's underlying technology. This Recommendation defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of this Recommendation is to serve as a foundation for developing detailed recommendations for the end-to-end network security.

This security architecture was created to address the global security challenges of service providers, enterprises, and consumers and is applicable to wireless, optical and wire-line voice, data and converged networks. The architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. It provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to detect, predict, and correct security vulnerabilities.

The security architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks. Three architectural components are addressed: security dimensions, security layers and security planes.

2.1. Security Dimensions

A security dimension is a set of security measures designed to address a particular aspect of the network security. This Recommendation X.805 identifies eight such sets that protect against all major security threats. The security dimensions are:

1. Access control
2. Authentication
3. Non-repudiation
4. Data confidentiality
5. Communication security
6. Data integrity
7. Availability
8. Privacy

2.2. Security Layers

In order to provide an end-to-end security solution, the security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as security layers. Recommendation X.805 defines three security layers:

1. Infrastructure Security Layer
2. Services Security Layer
3. Applications Security Layer

The security layers are a series of enablers for secure network solutions: the infrastructure layer enables the services layer and the services layer enables the applications layer. The security layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security.

2.3. Security Planes

A security plane is a certain type of network activity protected by security dimensions. Recommendation X.805 defines three security planes to represent the three types of protected activities that take place on a network. The security planes are:

1. Management Plane
2. Control Plane
3. End-User Plane

These security planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly.

Recommendation X.805 summarizes the dimensions of the security architecture with the following figure:

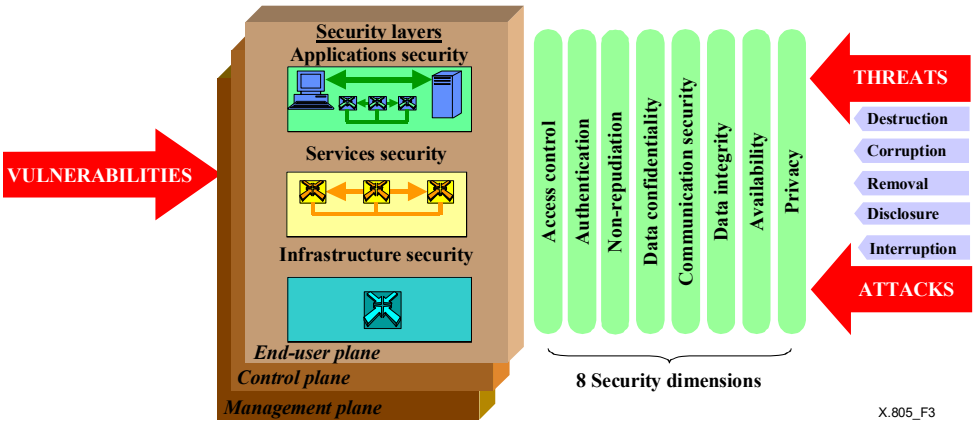

Figure 3/X.805 – Security architecture for end-to-end network security

The security architecture described in Recommendation X.805 can be used to guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each security dimension at each security layer and plane during the definition and planning phase. The security architecture can also be used as the basis of a security assessment that would examine how the implementation of the security program addresses the security dimensions, layers and planes as policies and procedures are rolled out and technology is deployed.

3. CONCLUSIONS

The Working Group on Standards Coordination recommends that CITEL PCC.I endorse ITU-T Recommendation X.805, "Security architecture for systems providing end-to-end communications" with no deletions, additions or modifications.

4. FUTURE WORK

The Working Group on Standards Coordination will continue to monitor the evolving security work of the ITU-T (especially Study Group 17), ISO, IETF, and other relevant standards groups that address the security needs of the Americas. The objective of Recommendation X.805 is to serve as a foundation for developing additional, detailed recommendations for end-to-end network security and ITU-T Study Group 17 has already drafted additional security-related Study Questions. As appropriate, the WGSC will recommend endorsement of additional standards that serve to enhance network security in the Americas.

5. RESOURCE DOCUMENTS

[1] "Security Architecture for Systems Providing End-to-End Communications", Draft Recommendation X.css; CCP.I-TEL/doc.118/03, Guatemala City, Guatemala, 7-11 April, 2003; ITU-T COM 17, Delayed Contribution 79, (Nov 2002).

[2] "Security Architecture for Systems Providing End-to-End Communications", powerpoint overview of draft Recommendation X.css; CCP.I-TEL/doc.118/03 add.1, Guatemala City, Guatemala, 7-11 April, 2003.

[3] "Security Architecture for Systems Providing End-to-End Communications", Draft Recommendation X.css; CCP.I-TEL/doc.208,/03 Mexico City, Mexico, 22-26 September, 2003; ITU-T COM 17, Contribution 52, (July 2003).

[4] "Security Architecture for Systems Providing End-to-End Communications", powerpoint overview of draft Recommendation X.css; .CCP.I-TEL/doc.208/03, Mexico City, Mexico, 22-26 September, 2003.

[5] "Security Architecture for Systems Providing End-to-End Communications", ITU-T Recommendation X.805 (October 2003).