PCC.I/RES. 46 (IV-04)[1]

SECURITY ARCHITECTURE FOR THE INTERNET PROTOCOL

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

CONSIDERING:

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

b) That IETF RFC 2401 "Security architecture for the Internet Protocol" is a framework of open standards that provides security for transmission of sensitive information over unprotected networks such as the Internet; and

c) That RFC 2401 supports different applications ranging from narrow-band to wide-band communications capability with integrated personal and terminal mobility to meet the user and service requirements,

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.; and

b) That Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated,

RESOLVES THAT:

To endorse the IETF RFC 2401 "Security architecture for the Internet Protocol" with no deletions, additions or modifications.

[1] CCP.I-TEL/doc.428/04

RECOMMENDS:

1. That the Working Group on Standards Coordination continues to monitor and determine the applicability for the Americas of the IETF RFC 2401 standard as it evolves; and

2. That the Working Group on Standards Coordination continue addressing the service needs of the Americas and provide implementation options based on IETF RFC 2401 and other evolving standards on network security.

ANNEX TO RESOLUTION PCC.I/RES.46 (IV-04)

Coordinated Standards Document
Security Architecture for the Internet Protocol

1. EXECUTIVE SUMMARY

The Internet and other communication networks are an ever-increasing part of our daily lives, so does our dependency upon their underlying infrastructure. Unfortunately, as our dependency has grown, so have hostile attacks on infrastructure by network predators. Newly discovered forms of attacks, the availability and wide distribution of attack tools, as well as the flaws in common desktop software have resulted in networks becoming increasingly vulnerable.

IP's flexibility and strength is also its weakness, the way IP routes packets makes it easy for attacks such as spoofing (in which one machine masquerades as another), sniffing (in which a transmission is monitored) or a session hijacking in which an attacker uses both techniques to impersonate one of the communicating parties.

The importance of security is recognized by both the IETF (Internet Engineering Task Force) and the ITU-T. There is a need to further understand all the issues and the implications. To address Security the IEFT created the Security Area and further subdivided the area into working groups. The ITU-T SG 17 (Data Networks and Telecommunication Software) has a security study group that targets security issues at all levels. The role of each organization is a somewhat different, the Security Area Advisory Group primary role is to provide help to IETF working groups on how to provide for security in the protocols they design. The ITU-T is focusing the need for a global approach to the dissemination of information regarding the security of critical network infrastructures and ways to stimulate international or regional cooperation with respect to critical network infrastructure.

The IETF IP Security (IPSec) suite of protocols provides security for IP traffic at the network layer. The Working Group on Standards Coordination (WGSC) started to study IPSec (PCC.I/doc. 1518/02) at the XVI meeting held in Montevideo, Uruguay in May 2002 and Section 6 of the Next Generation Networks Standards Overview document (CCP.I-TEL/doc. 112/03) provides a description of IPSec.

2. BACKGROUND

Overview of IETF RFC 2401

IPSec is described in RFC 2401 - Security Architecture for the Internet Protocol [1]. The protocol suite provides the five components described below.

Security Associations (SAs)

The function of the SAs is to provide a method for two parties to exchange secure data and both parties need to agree on the security parameters. "SAs" are defined for one-way traffic only, therefore for bi-directional traffic requires two "SAs" to be defined. The IPSec SA specifies the following parameters:

- AH authentication mode (Algorithm and Keys)
- ESP Encryption Algorithm
- How to exchange Keys
- How often the key are changed
- SA Lifetime
- SA source address

Authentication Header (AH)

AH, defined in IEFT RFC 2402 (Proposed Standard), lets parties communicating using IP to verify that the data was not modified during transmission and that it comes from the original source of the information. The AH provides connectionless data integrity, data authentication and protects against replay attacks. The AH adds a block of code to the data packet that is the result of a “hash” function applied to the entire packet. There are 2 fields in the AH header that are important:

- Security parameter Index (SPI) specifies to the receiving device what group of security protocols the sender is using.
- Sequence Number is used to prevent replay attacks by preventing the reprocessing of a packet multiple times.

The Authenticator Field on the AH is only 96-bits long, the “sender” runs the “hash” functions, truncates the resulting number to fit in to the AH Authenticator field, and sends it off. On the other side, the receiver runs the same “hash” algorithm (as specified in the SPI) on the packet and truncates the resulting number accordingly. The receiver then compares the number calculated to the number in the AH in the authenticator field. If the numbers match the number in the packet, it is accepted as not being altered. The two most widely used AH “hash” algorithms are, Message Digest 5 (MD5) defined by IETF RFC 2403 (Proposed Standard) produces a 128-bit authenticator and Secure Hashing Algorithm (SHA-1) defined by RFC 2404 (Standard) produces a 160-bit authenticator. The AH does not keep the data confidential, and is meant for occasions when “ONLY” authentication is needed.

Encapsulation Security Payload (ESP)

ESP, defined in IETF RFC 2406 (Proposed Standard), encrypts the information to prevent monitoring by a non-trusted entity. ESP can also be used for authentication. The ESP authentication field contains the cryptographic checksum that is computed over the remaining part of the ESP (minus the ESP authentication field itself). AH authentication differs from the ESP’s version in that the ESP authentication does not protect the IP header that precedes the ESP header.

The ESP authentication can be used instead of the AH to reduce the packet processing and it performs one “transform” operation instead of two steps, also prevents replay attacks by keeping track of the sequence number much like AH, however this would compromise the validity of the header. There are two types of tunnel mode in both types the original IP header information is encrypted; the down side is that it does not work across NAT (Network Address Translation). In the transport mode the original IP header is not encrypted and may work across NAT.

ESP most widely used encryption schemes are:

- Data-Encryption Standard (DES) uses a 56-bit encryption IETF RFC 2405 (Proposed Standard)
- Triple DES (3DES) uses 168-bit encryption by passing the data through the DES algorithm 3 times IETF RFC 2405

Key Management

The two most commonly used methods for key exchange, is manual keying which is suitable for a small number of sites; the other method is by a protocol defined by IETF RFC 2409 (Proposed Standard) “Internet Key Exchange (IKE)”. “IKE” is the combination of “ISAKMP” and “Oakley”, the “Internet Security Association and Key Management Protocol (ISAKMP)” defined by IETF RFC 2408 (Proposed Standard) provides the framework for authentication and key exchange, and the Oakley protocol defined by IETF RFC 2412 (Informational) describes various modes of key exchange.

Manual Key Exchange

Manual exchange is the easiest form of key management for a small number of sites. Both sides of the IPSec tunnel must be configured manually with the appropriate keys. However there are many disadvantages with manual keying:

- Manual intervention is needed to update or change the keys.
- Since manual changing of keys is normally infrequent, the attacker has more time to crack the key and to decrypt data.
- There is a chance of error in configuration since the same key needs to be configured on the two different endpoints of the IPSec tunnel.
- If the person with access to the keys leaves or becomes untrustworthy, lengthy configuration changes need to take place.
- The keys in the configuration need to be protected in some manner from outside attack.

3. CONCLUSIONS

The Fixed and Mobile Services and Network Signaling Rapporteur Group recommends the endorsement of IETF RFC 2401 “Security Architecture for the Internet Protocol” by the Members and associate members of CITEL PCC.I. Furthermore, the group recommends that RFC 2401 be accepted with no deletions, additions or modifications to its normative references.

4. FUTURE WORK

For the last three years, the Working Group of Standards Coordination has been studying multiple aspects of Next Generation Networks, including protocols definition and Network Security. Document PCC.I/doc.0202/03 [2] presents an updated version of these studies. It is therefore to be expected that future studies on various areas of that document will result on a number of future Coordinated Standards Documents.

5. RESOURCE DOCUMENTS

[1] "Security Architecture for the Internet Protocol" IETF RFC 2401.

[2] "Next Generation Networks – Standards Overview"; PCC.I/doc. 0202/03, (September 2003).