Network Working Group
Internet-Draft
Expires: December 28, 2003

J. Loughney
Nokia Research Center
M. Tuexen, Ed.
Univ. of Applied Sciences Muenster
J. Pastor-Balbas
Ericsson
June 29, 2003

Security Considerations for SIGTRAN Protocols
draft-ietf-sigtran-security-03.txt

Status of this Memo

Copyright Notice

Abstract

This documents discusses how TLS and IPsec can be used to secure the communication for SIGTRAN protocols. The support of IPsec is mandatory for all nodes running SIGTRAN protocols and the support of TLS is optional.

Table of Contents

1. Introduction

1.1 Overview

The SIGTRAN protocols are designed to carry signaling messages for telephony services. These protocols will be used between

- customer premise and service provider equipment in case of IUA
- service provider equipment only. This is the case for M2UA, M2PA, M3UA and SUA. The carriers may be different and may use other transport network providers.

The security requirements for these situations may be different.

SIGTRAN protocols involve the security needs of several parties: the end-users of the services; the service providers and the applications involved. Additional security requirements may come from local regulation. While having some overlapping security needs, any security solution should fulfill all of the different parties' needs.

The SIGTRAN protocols assume that messages are secured by using either IPsec or TLS.

1.2 Abbreviations

This document uses the following abbreviations:

ASP: Application Server Process.

CA: Certification Authority.

DOI: Domain Of Interpretation.

ESP: Encapsulating Security Payload.

FQDN: Full-Qualified Domain Names.

IPsec: IP Security Protocol.

IKE: Internet Key Exchange Protocol.

ISDN: Integrated Services Digital Network.

IUA: ISDN Q.921 User Adaptation Layer.

M2PA: SS7 MTP2 Peer-to-Peer User Adaptation Layer.

M2UA: SS7 MTP2 User Adaptation Layer.

M3UA: SS7 MTP3 User Adaptation Layer.

PKI: Public Key Infrastructure.

SA: Security Association.

SCTP: Stream Control Transmission Protocol.

SS7: Signaling System No. 7.

SUA: SS7 SCCP User Adaptation Layer.

TLS: Transport Layer Security.

2. Convention

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [1].

3. Security in telephony networks

The security in telephony networks is mainly based on the closed network principle. There are two main protocols used: Access protocols (ISDN and others) are used for signaling in the access network and the SS7 protocol stack in the core network.

As SS7 networks are often physically remote and/or inaccessible to the user, it is assumed that they are protected from malicious users. Often, equipment is under lock and key. At network boundaries between SS7 networks, packet filtering is sometimes used. End-users are not directly connected to SS7 networks.

The access protocols are used for end-user signaling. End-user signaling protocols are translated to SS7 based protocols by telephone switches run by network operators.

Often Regulatory Authorities require SS7 switches with connections to different SS7 to be conformant to national and/or international test specifications.

There are no standardized ways of using encryption technologies for

providing confidentiality or using technologies for authentication.

This description applies to telephony networks operated by a single operator but also to multiple telephony networks being connected and operated by different operators.

4. Threats and Goals

The Internet threats can be divided into one of two main types. The first one is called "passive attacks". It happens whenever the attacker reads packets off the network but does not write them. Examples of such attacks include confidentiality violations, password sniffing and offline cryptographic attacks amongst others.

The second kind of threads is called "active attacks". In this case the attacker also writes data to the network. Examples for this attack include replay attacks, message insertion, message deletion, message modification or man-in-the-middle attacks amongst others.

In general, Internet protocols have the following security objectives:

- Communication Security:
  - Authentication of peers.
  - Integrity of user data transport.
  - Confidentiality of user data.
  - Replay protection.
- Non-repudiation.
- System Security, avoidance of:
  - Unauthorized use.
  - Inappropiate use.
  - Denial of Service.

Communication security is mandatory in some network scenarios to prevent malicious attacks. The main goal of this document is to recommend the minimum security means that a SIGTRAN node must implement in order to achieve a secured communication. To get this goal, we will explore the different security options that regarding communication exist.

All SIGTRAN protocols use the Stream Control Transmission Protocol (SCTP) being defined in [9] and [12] as its transport protocol. SCTP provides certain transport related security features, such as resistance against:

- Blind Denial of Service Attacks such as:
  - Flooding.
  - Masquerade.
  - Improper Monopolization of Services.

There is no quick fix, one-size-fits-all solution for security.

When the network in which SIGTRAN protocols are used involves more than one party, it may not be reasonable to expect that all parties have implemented security in a sufficient manner. End-to-end security should be the goal; therefore, it is recommended that IPsec or TLS is used to ensure confidentiality of user payload. Consult [4] for more information on configuring IPsec services.

5. IPsec Usage

This section is relevant only for SIGTRAN nodes using IPsec to secure communication between SIGTRAN nodes.

All SIGTRAN nodes using IPsec MUST implement IPsec ESP [5] in transport mode with non-null encryption and authentication algorithms to provide per-packet authentication, integrity protection and confidentiality, and MUST implement the replay protection mechanisms of IPsec. In those scenarios where IP layer protection is needed, ESP in tunnel mode SHOULD be used. Non-null encryption should be used when using IPSec ESP.

All SIGTRAN nodes MUST support IKE for peer authentication, negotiation of security associations, and key management, using the IPsec DOI [6]. The IPsec implementations MUST support peer authentication using a pre-shared key, and MAY support certificate-based peer authentication using digital signatures. Peer authentication using the public key encryption methods outlined in IKE's sections 5.2 and 5.3 [7] SHOULD NOT be used.

Conformant implementations MUST support both IKE Main Mode and Aggressive Mode. For transport mode, when pre-shared keys are used for authentication, IKE Aggressive Mode SHOULD be used, and IKE Main Mode SHOULD NOT be used. When digital signatures are used for authentication, either IKE Main Mode or IKE Aggressive Mode MAY be

used. When using ESP tunnel mode, IKE Main Mode MAY be used to create ISAKMP association with identity protection during Phase 1.

When digital signatures are used to achieve authentication, an IKE negotiator SHOULD use IKE Certificate Request Payload(s) to specify the certification authority (or authorities) that are trusted in accordance with its local policy. IKE negotiators SHOULD use pertinent certificate revocation checks before accepting a PKI certificate for use in IKE's authentication procedures. See [11] for certificate revocation and [8] for online-checking.

The Phase 2 Quick Mode exchanges used to negotiate protection for SIGTRAN sessions MUST explicitly carry the Identity Payload fields (IDci and IDcr). The DOI provides for several types of identification data. However, when used in conformant implementations, each ID Payload MUST carry a single IP address and a single non-zero port number, and MUST NOT use the IP Subnet or IP Address Range formats. This allows the Phase 2 security association to correspond to specific TCP and SCTP connections.

Since IPsec acceleration hardware may only be able to handle a limited number of active IKE Phase 2 SAs, Phase 2 delete messages may be sent for idle SAs, as a means of keeping the number of active Phase 2 SAs to a minimum. The receipt of an IKE Phase 2 delete message SHOULD NOT be interpreted as a reason for tearing down a SIGTRAN session. Rather, it is preferable to leave the connection up, and if additional traffic is sent on it, to bring up another IKE Phase 2 SA to protect it. This avoids the potential for continually bringing connections up and down.

It should be noted that SCTP supports multi-homed hosts and this results in the need for having multiple security associations for one SCTP association. This disadvantage of IPsec has been addressed by [17]. So IPsec implementations used by SIGTRAN nodes SHOULD support the IPsec feature described in [17].

6. TLS Usage

This section is relevant only for SIGTRAN nodes using TLS to secure the communication between SIGTRAN nodes.

A SIGTRAN node that initiates a SCTP association to another SIGTRAN node acts as a TLS client according to [3], and a SIGTRAN node that accepts a connection acts as a TLS server. SIGTRAN peers implementing TLS for security MUST mutually authenticate as part of TLS session establishment. In order to ensure mutual authentication, the SIGTRAN node acting as TLS server must request a certificate from the SIGTRAN node acting as TLS client, and the SIGTRAN node acting as TLS client

MUST be prepared to supply a certificate on request.

[15] requires the support of the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA. SIGTRAN nodes MAY negotiate other TLS cipher suites.

TLS MUST be used on all bi-directional streams and the other uni-directional streams MUST NOT be used.

It should also be noted that a SCTP implementation used for TLS over SCTP MUST support fragmentation of user data and might also need to support the partial delivery API. This holds even if all SIGTRAN messages are small. Furthermore, the 'unordered delivery' feature of SCTP can not be used in conjunction with TLS. See [15] for more details.

Because TLS only protects the payload the SCTP header and all control chunks are not protected. This can be used for DoS attacks. This is a general problem with security provided at the transport layer.

The SIGTRAN protocols use the same SCTP port number and payload protocol identifier when run over TLS. A session upgrade procedure has to be used to initiate the TLS based communication.

The session upgrade procedure should be as follows:

- If an ASP has been configured to use TLS it sends a STARTTLS message on stream 0 and starts a timer T_TLS. This is the first message send and the ASP sends no other adaptation layer messages until the TLS based communication has been established.

- If the peer does not support TLS it sends back an ERROR message indicating an unsupported message type. In this case the SCTP association is terminated and it is reported to the management layer that the peer does not support TLS.

- If the peer does support TLS it sends back an STARTTLS_ACK message. The client then starts TLS based communication.

- If T_TLS expires without getting any of the above answers the association is terminated and the failure is reported to the management layer.

All SIGTRAN adaptation layers share a common message format. The STARTTLS message consists of a common header only using the message class 10 and message type 1. The STARTTLS_ACK message uses the same message class 10 and the message type 2. Both messages do not contain any parameters.

Using this procedure it is possible for a man-in-the-middle to do a denial of service attack by indicating that the peer does not support TLS. But this kind of attack is always possible for a man-in-the-middle.

7. Support of IPsec and TLS

If content of SIGTRAN protocol messages is to be protected, either IPsec ESP or TLS can be used. In both IPsec ESP Transport Mode and TLS cases the IP header information is neither encrypted nor protected. If IPsec ESP is chosen the SCTP control information is encrypted and protected whereas if the TLS based solution the SCTP control information is not encrypted and only protected by SCTP procedures.

In general, both IPsec and TLS have enough mechanisms to secure the SIGTRAN communications.

Therefore, in order to have a secured model working as soon as possible, the following recommendation is made: A SIGTRAN node MUST support IPsec and MAY support TLS.

8. Peer-to-Peer Considerations

M2PA, M3UA and SUA support the peer-to-peer model as a generalization to the client-server model which is supported by IUA and M2UA. A SIGTRAN node running M2PA, M3UA or SUA and operating in the peer-to-peer mode is called a SIGTRAN peer.

As with any peer-to-peer protocol, proper configuration of the trust model within a peer is essential to security. When certificates are used, it is necessary to configure the trust anchors trusted by the peer. These trust anchors are likely to be unique to SIGTRAN usage and distinct from the trust anchors that might be trusted for other purposes such as Web browsing. In general, it is expected that those trust anchors will be configured so as to reflect the business relationships between the organization hosting the peer and other organizations. As a result, a peer will typically not be configured to allow connectivity with any arbitrary peer. When certificate authentication peers may not be known beforehand, and therefore peer discovery may be required.

Note that IPsec is considerably less flexible than TLS when it comes to configuring trust anchors. Since use of Port identifiers is prohibited within IKE Phase 1, within IPsec it is not possible to uniquely configure trusted trust anchors for each application individually; the same policy must be used for all applications. This implies, for example, that a trust anchor trusted for use with a

SIGTRAN protocol must also be trusted to protect other protocols (for example SNMP). These restrictions can be awkward at best.

When pre-shared key authentication is used with IPsec to protect SIGTRAN based communication, unique pre-shared keys are configured with peers, who are identified by their IP address (Main Mode), or possibly their FQDN (AggressivenMode). As a result, it is necessary for the set of peers to be known beforehand. Therefore, peer discovery is typically not necessary.

The following is intended to provide some guidance on the issue.

It is recommended that SIGTRAN peers use the same security mechanism (IPsec or TLS) across all its sessions with other SIGTRAN peers. Inconsistent use of security mechanisms can result in redundant security mechanisms being used (e.g. TLS over IPsec) or worse, potential security vulnerabilities. When IPsec is used with a SIGTRAN protocol, a typical security policy for outbound traffic is "Initiate IPsec, from me to any, destination port P"; for inbound traffic, the policy would be "Require IPsec, from any to me, destination port P". Here P denotes one of the registered port numbers for a SIGTRAN protocol.

This policy causes IPsec to be used whenever a SIGTRAN peer initiates a session to another SIGTRAN peer, and to be required whenever an inbound SIGTRAN session occurs. This policy is attractive, since it does not require policy to be set for each peer or dynamically modified each time a new SIGTRAN session is created; an IPsec SA is automatically created based on a simple static policy. Since IPsec extensions are typically not available to the sockets API on most platforms, and IPsec policy functionality is implementation dependent, use of a simple static policy is the often the simplest route to IPsec-enabling a SIGTRAN peer.

If IPsec is used to secure SIGTRAN peer-to-peer session, IPsec policy SHOULD be set so as to require IPsec protection for inbound connections, and to initiate IPsec protection for outbound connections. This can be accomplished via use of inbound and outbound filter policy.

9. Security Considerations

This documents discusses the usage of IPsec and TLS for securing SIGTRAN traffic.

10. IANA Considerations

The message class 10 has to be reserved for STARTTLS messages for all

SIGTRAN adaptation layers. For this message class, message type 1 has to be reserved for the STARTTLS message, message type 2 for the STARTTLS_ACK message.

11. Acknowledgements

The authors would like to thank B. Aboba, K. Morneault and many others for their invaluable comments and suggestions.

12. References

12.1 Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

12.2 Informative References

[3] Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[5] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[6] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[7] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[8] Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[9] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[10] Morneault, K., Rengasami, S., Kalla, M. and G. Sidebottom, "ISDN Q.921-User Adaptation Layer", RFC 3057, February 2001.

[11] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[12] Stone, J., Stewart, R. and D. Otis, "Stream Control Transmission Protocol (SCTP) Checksum Change", RFC 3309, September 2002.

[13] Morneault, K., Dantu, R., Sidebottom, G., Bidulock, B. and J. Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer", RFC 3331, September 2002.

[14] Sidebottom, G., Morneault, K. and J. Pastor-Balbas, "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)", RFC 3332, September 2002.

[15] Jungmaier, A., Rescorla, E. and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, December 2002.

[16] George, T., "SS7 MTP2-User Peer-to-Peer Adaptation Layer", draft-ietf-sigtran-m2pa-08 (work in progress), April 2003.

[17] Bellovin, S., "On the Use of SCTP with IPsec", draft-ietf-ipsec-sctp-06 (work in progress), April 2003.

13. Authors' Addresses

John Loughney
Nokia Research Center
PO Box 407
FIN-00045 Nokia Group
Finland

EMail: john.loughney@nokia.com

Michael Tuexen
Univ. of Applied Sciences Muenster
Stegerwaldstr. 39
48565 Steinfurt
Germany

EMail: tuexen@fh-muenster.de

Javier Pastor-Balbas
Ericsson
Via de los Poblados, 13
28033 Madrid
Spain

EMail: j.javier.pastor@ericsson.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.