Security Models and Transport Layer Security for the Simple Network Management Protocol

SNMP Research International, Inc.
Knoxville, Tennessee

Date: 25Apr2011

1 Overview

This document describes the two prominent security models available with the SNMPv3 architecture: The User-based Security Model (USM) and the Transport Security Model (TSM). Network administrators need to decide how each is suited for use in their secure network management solution. TSM provides a framework for secure communication with transport-based security protocols such as Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS). TLS is the successor to Secure Sockets Layer (SSL). The Transport Security Model addition to the SNMPv3 framework along with (D)TLS specifications allow organizations to bring SNMP users, applications, and devices under the umbrella of an X.509 public key infrastructure.

2 What is Available?

The SNMPv3 architecture defines that a single protocol entity may provide simultaneous support for multiple security models. In 2003, when SNMPv3 became Full Standard and the IETF-recommended version of SNMP, only the User-based Security Model (USM) was available for SNMP usernames and key management. Protocols used by the User-based Security Model are based on symmetric cryptography (i.e., private key mechanisms) and provide security of individual messages sent using the User Datagram Protocol (UDP).

The Transport Security Model (TSM) is an additional component of the SNMPv3 architecture that enables security to be applied at the transport layer. Protocols used by the Transport Security Model, such TLS, and DTLS, are based on asymmetric cryptography (i.e., public-key mechanisms) and provide security of the

Copyright © SNMP Research International, Inc. (SECMODELLIT172)

transport layer on which messages are sent. Each of the protocols have a different specification to define how it works with the TSM. For example, the Transport Layer Security Transport Model (TLSTM) defines how TLS and DTLS are used with TSM. Figure 1 shows that SNMP Entities, agents and managers, can exchange messages securely with both message-based and transport-based security models.

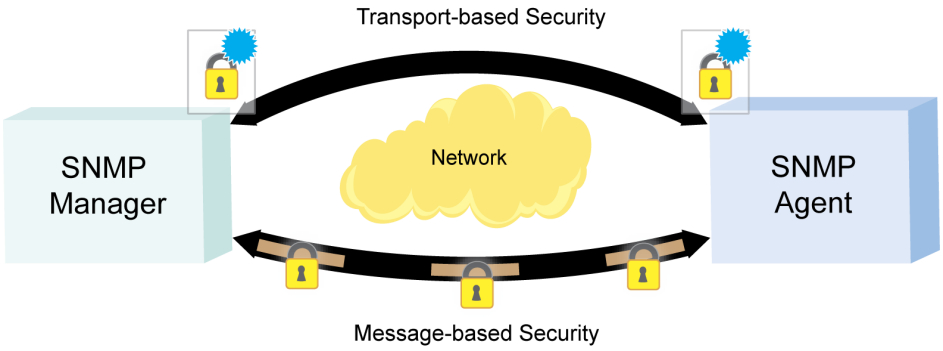

Figure 1: SNMP Entities can use Transport-based Security and Message-based Security

2.1 User-based Security Model

RFC 3414, the “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3),” describes the User-based Security Model for SNMPv3. It defines the elements of procedure for providing SNMP message-level security. RFC 3414 includes a MIB document for remotely monitoring and managing the configuration parameters for the USM, including key distribution and key management. The User-based Security Model provides mechanisms for the following security features:

- Symmetric or private-key cryptography (username/passwords).
- Digest computation with keyed hashing algorithms (message integrity)
- Time indicators and automatic clock synchronization
- Data encryption

2.2 Transport Security Model for SNMP

RFC 5591, the “Transport Security Model (TSM) for the Simple Network Management Protocol (SNMP),” updates the SNMP architecture by adding the Transport Security Model for SNMP. TSM is a framework that allows TLS, DTLS, and other protocols to provide a secure communication channel for securing SNMP messages. The Transport Security Model provides a foundation for the following security features:

- Asymmetric (public-key) cryptography
- Server authentication
- Confidentiality
- Message integrity
- Optionally provides client authentication

Copyright © SNMP Research International, Inc. (SECMODELLIT172)

2.3 (D)TLS

Transport Layer Security (TLS), successor to Secure Sockets Layer (SSL), is a public-key technology that protects information passed over connection-oriented protocols such as TCP. For example, a Web server may use TLS to protect data sent between itself and a Web browser. X.509 certificates are used for authenticating the server, and, optionally, the clients. Organizations may assign certificates to users and applications and use public-key infrastructure (PKI) for key management and access control.

Datagram Transport Layer Security (DTLS) is TLS implemented on top of datagram protocols such as UDP. DTLS provides the same security for datagram protocols that TLS provides for stream protocols. (D)TLS is a term that collectively refers to TLS and/or DTLS.

With TLS and DTLS, SNMP messages can be exchanged over secure communication channels. While the security provided is the same, messages are exchanged and handled differently. Table 1 compares the factors an application developer and a network administrator may want to consider when developing and deploying applications that send SNMP messages using TLS over TCP connections and DTLS over UDP connections. Note that the properties of DTLS over UDP apply also to non-(D)TLS SNMPv3 messages.

Table 1: TLS and DTLS Comparison Table

	TLS/TCP	DTLS or SNMPv3/UDP
Connection Type	Connection-oriented	Connectionless
Max. Message Size	Very large maximum	Supported datagram size
Packet Loss	Handled by TCP	Handled by application
Timeouts/Retries	Controlled by TCP	Controlled by application

3 Choosing a Primary Security Model

With two security models available, application developers designing network management applications and the operators who use them must select which options should be made available and configured. Should the User-based Security Model be implemented alone, or should the Transport Security Model be enabled and configured in SNMP-based network management solutions?

SNMP over (D)TLS is an additional or alternate security mechanism to SNMP's User-Based Security Model (USM). The main advantage of using SNMP over (D)TLS is the ability to integrate SNMP management into an organization's existing X.509 public-key security infrastructure. Also, using SNMP over TLS can be helpful to network management when very large SNMP messages need to be sent during normal network operation when problems with throughput may not be an issue. With SNMP over DTLS, messages are exchanged over a datagram protocol which helps provide message exchange during times of network stress. With SNMPv3 over UDP, messages also have a greater chance of success when the network is under severe stress because there is less information exchange is required to send messages.

Copyright © SNMP Research International, Inc. (SECMODELLIT172)

When to consider SNMP over (D)TLS

Organizations may consider implementing SNMP over (D)TLS if they:

- already have an X.509 public key infrastructure,
- need to deploy an X.509 public key infrastructure, or
- do not have a system for managing SNMP's USM private keys.

When to use USM Only

Organizations may consider using only SNMP's USM if they:

- do not need to deploy an X.509 public key infrastructure, or
- already have a system for managing SNMP's USM private keys.

Organizations that have a system for managing SNMP's USM private keys and do not otherwise need an X.509 public-key infrastructure may find that implementing SNMP over (D)TLS would require the effort and expense of deploying an X.509 infrastructure with no technical or economic benefit.

4 Using a Complete Approach

SNMP over (D)TLS is designed to integrate network management with an organization's existing X.509 key management system. However, traditional USM is still very necessary to maintain the integrity and reliability of network operations in times of network stress (such as Denial of Service attacks) when the services depended upon by the transport security model can fail. RFC 5590 "SNMP Transport Subsystem" emphasizes in Section 7 "Security Considerations" that operators employing the Transport Security Model should continue to provision "authPriv" USM to supplement any Security Model or Transport Model that has external dependencies:

> In times of network stress, a Secure Transport Model might not work properly if its underlying security mechanisms (e.g., Network Time Protocol (NTP) or Authentication, Authorization, and Accounting (AAA) protocols or certificate authorities) are not reachable. The User-based Security Model was explicitly designed to not depend upon external network services, and provides its own security services. It is RECOMMENDED that operators provision authPriv USM as a fallback mechanism to supplement any Security Model or Transport Model that has external dependencies, so that secure SNMP communications can continue when the external network service is not available.

Creating both USM and TSM configurations is not required. However, based on the warning from RFC 5590, SNMP Research suggests creating equivalent USM provisions for (D)TLS configurations. Essentially, when planning TSM configurations, it is a good idea to create USM equivalents as a backup measure.

Copyright © SNMP Research International, Inc. (SECMODELLIT172)

5 Threats and Goals

SNMP management framework and architecture (RFC 3411) defines security threats that should be addressed by a security model. This section summarizes the approach taken by both security models to protect against the threats. Each threat is defined and followed first by the the User-based Security Model (USM) approach. Second, the measures taken by the Transport Layer Security Transport Model (TLSTM) working through the Transport Security Model for SNMP (with TLS or DTLS) are described.

Modification of Information is the threat that an unauthorized entity may alter in-transit SNMP messages generated on behalf of an authorized principal in such a way as to effect unauthorized management operations, including falsifying the value of an object.

The USM utilizes MD5 and the Secure Hash Algorithm (SHA-1) as keyed hashing algorithms for digest computation to provide data integrity to directly protect against data modification attacks.

With the TLSTM, (D)TLS provides verification that the content of each received message has not been modified during its transmission through the network, data has not been altered or destroyed in an unauthorized manner, and data sequences have not been altered to an extent greater than can occur non-maliciously.

Masquerade is the threat that management operations unauthorized for a given principal may be attempted by assuming the identity of another principal that has the appropriate authorizations.

The USM utilizes MD5 and the Secure Hash Algorithm (SHA-1) as keyed hashing algorithms for digest computation to indirectly provide data origin authentication and to defend against masquerade attacks.

The TLSTM allows the identity of the (D)TLS server and client to be verified through the use of the (D)TLS protocol and X.509 certificates. A TLSTM implementation MUST support the authentication of both the server and the client.

Message stream modification is the threat that messages may be maliciously re-ordered, delayed or replayed to an extent that is greater than can occur through the natural operation of connectionless transport services, in order to effect unauthorized management operations.

The USM uses loosely synchronized monotonically increasing time indicators to defend against certain message stream modification attacks. Automatic clock synchronization mechanisms based on the protocol are specified without dependence on third-party time sources and without relying on other technologies with possibly insufficient security.

With the TLSTM, (D)TLS provides replay protection with a Message Authentication Code (MAC) that includes a sequence number. Since UDP provides no sequencing ability, DTLS uses a sliding window protocol with the sequence number used for replay protection (see RFC 4347).

Disclosure is the threat of eavesdropping on the exchanges between SNMP engines.

The USM can use the Data Encryption Standard (DES) in the Cipher Block Chaining mode (CBC-DES) to protect against disclosure. Extended security options can be used, including the Advanced Encryption Standard (AES) in 128-, 192-, and 256-bit CFB mode and Triple-DES in 168-bit EDE Cipher Block Chaining mode.

With the TLSTM, (D)TLS provides protection against the disclosure of information to unauthorized recipients or eavesdroppers. All TLSTM implementations must allow traffic between SNMP engines to be encrypted to protect sensitive data from eavesdropping attacks.

Copyright © SNMP Research International, Inc. (SECMODELLIT172)

Denial of Service is a broad range of attacks by which service on behalf of authorized users is denied.

RFC 3411 determines that denial-of-service (DoS) attacks are indistinguishable from the types of failures typically handled by viable network management software. DoS attacks need not be addressed by an SNMP security protocol. Refer to Section 4 for more information.

With the TLSTM, (D)TLS can be used and describes a cookie mechanism to protect against spoofed IP addresses. Note that this mechanism does not provide any defense against DoS attacks mounted from valid IP addresses.

6 Conclusion

Because both the Transport Security Model, with TLS or DTLS, and the User-based Security Model offer comparable protection against security threats, the network manager can choose which should be used based on the type of key management system that works best for the organization. An organization with an existing system for managing SNMP's USM user keys need not migrate to a X.509-based security infrastructure solely for the purpose of security for SNMP. However, organizations that have already invested in an X.509 public key infrastructure can reap further benefit by managing SNMP users, applications, and devices under the same system. Remember, though, when implementing new configurations for transport-based security including SSL, TLS, and DTLS, it is a good idea to also configure USM users as a backup measure.

7 SNMP Research DTLS-Enabled Agents and Managers

SNMP Research offers solutions that unlock the full potential of the SNMPv3 architecture, including public-key security with SSL, TLS, and DTLS. SNMP Research makes software development and configuration easier by providing working examples, valid configuration files, and sample certificates for testing. Network managers can bring SNMP users, applications, and devices under the umbrella an X.509 public key infrastructure using SNMP Research's (D)TLS-enabled products:

- The (D)TLS Option for SNMP agents and Subagent Development Toolkits
- The (D)TLS Option for SNMP managers and Management Application Development Toolkits

Contact SNMP Research sales by phone at +1 865 579 3311 or email **sales@snmp.com** to learn how you can use SNMP over (D)TLS with SNMP Research's solutions.

8 For More Information

- Internet Engineering Task Force (IETF)
  Refer to **http://www.ietf.org** for information on receiving the freely available IETF standards.
- SNMP Research Web Site
  Refer to SNMP Research's Web Site **http://www.snmp.com/** for information about SNMP over (D)TLS and SNMP Research products.

Contact Information

Worldwide Headquarters

SNMP Research International
3001 Kimberlin Heights Road
Knoxville, TN, USA 37920-9716
Phone: +1 865 579 3311
Fax: +1 865 579 6565

Sales Query: http://snmp.com/salesquery.shtml
Information E-mail: info@snmp.com
Sales E-mail: sales@snmp.com