Implementation and Performance Analysis of SNMP on a TLS/TCP Base

X. Du, M. Shayman *M. Rozenblit*

University of Maryland *TeraBurst Networks Inc.*

Research supported by Laboratory for Telecommunications Science

Implementation and Performance Analysis of SNMP on a TLS/TCP Base

- Motivation
- Implementation
- Measurements and Results
- Conclusions

Motivation

- SNMP/TCP has performance benefits for bulk transfer and simplifies management applications.
- TLS is a natural choice for security when using SNMP/TCP. However, it must be demonstrated that the additional overhead associated with TLS is not excessive.
- SNMPv3 has some security features. It is interesting to compare SNMP/TLS/TCP with SNMPv3 which use User-based Security Model (USM).

Implementation

- We implemented SNMP/TLS/TCP based on UC Davis UCD-SNMP source codes which can run over TCP, we only need to implement TLS into the SNMP/TCP structure.
- OPENSSL is used as the TLS 1.0 (SSLv3.0) source codes .
- TLS Handshake Protocol and TLS Record Protocol are implemented over TCP socket. First, a TCP connection is set up. Second, a TLS connection is set up over the TCP connection.Then the client and server begin communication using TLS/TCP.

Performance Tests and Results

- Major performance issues are:
  1. Overhead of TCP vs UDP
  2. Overhead of TLS
  3. Comparison of SNMP/TLS/TCP and SNMPv3 (USM)

- Ran several experiments to measure these overheads.
  - SNMP Management Station is run in a SUN Sparc 10
  - SNMP Agent is in a SUN Sparc 5

- Results are clearly platform dependent
  - For example, the TLS Setup Time is about 300 ms in Sparc 5 while in a Sparc 10 it is about 160 ms.

Test 1: Overhead of TLS Security

- We compared SNMPv1/TLS/TCP with no security, with integrity protection only, and with both integrity and privacy protections.
- There are three main security related operations that introduce overhead into TLS: MAC computation, compression, and encryption.
- There are four corresponding situations to investigate:
  - (a). No security: no compression, no MAC, no encryption.
  - (b). Integrity protection only: no compression, has MAC, no encryption.
  - (c). Privacy protection only: has compression, no MAC, has encryption.
  - (d). Integrity and privacy protection: has compression, has MAC, has encryption.

Test 1 -- Results

- MD5 is used as the MAC algorithm and the encryption algorithm is DES.
- The tests are performed in both short sessions (snmpget) and long sessions (snmpwalk) .

Time (ms)	a	b	b - a	c	c-a	d	d - b	d - a	(b-a)/d	(d-b)/d	(d-a)/d
Snmpget	774	805	31	823	49	840	35	66	4. 01%	4. 52%	8. 53%
Snmpwalk	1,044	1,120	76	1,186	142	1,273	153	229	7. 28%	14. 7%	21. 9%
Snmpwalk/msg	31	33	2.2	33	2.1	37	4.4	6.7	0. 21%	0. 43%	0. 64%

Table 1: session times for short and long sessions.

- The larger percentage of the security overhead in long session can be explained as follows: The setup times for SNMP, TCP and TLS are incurred only once per session. But the MAC and encryption overheads are incurred for each message in the session and hence are substantially larger for the long session. The actual latency per message decreases for longer sessions.

Test 2: Overhead of TLS/TCP Session Setup

- A major issue with SNMP/TLS/TCP is the substantial overhead for setting up a session. In contrast, SNMP/UDP does not incur this penalty.
- However, for a long session the costs of setting up the session are amortized over a large number of messages and therefore the overhead per message is small.
- Since SNMPv1/UDP does not provide any security, a fair comparison of overheads is obtained by using SNMPv1/TLS/TCP with peer entity authentication at session setup time, but without integrity or privacy protection for the SNMP messages.

Test 2 -- Results

- When the message number (1 - 2,000) in one session is small (<500), the TLS session time is about 1.4 ~1.6 times the UDP session time.
- As the message number increases, the ratio declines to approximately 1.2 for sessions containing at least 500 messages.
- Comparing the TLS time with UDP time shows that the **TLS overheads are not large (20%)**, especially when the message number is large; the overheads are acceptable.

Test 3: SNMP/TLS/TCP vs SNMPv3 with USM

- SNMPv3 has some security features. It has authentication and encryption.

- It is interesting to compare SNMP/TLS/TCP and SNMPv3 with USM when the similar security features are enabled.

- SNMPv3 with USM recognizes three levels of security:

- • without authentication and without privacy (**noAuthNoPriv**).
- • with authentication but without privacy (**authNoPriv**).
- • with authentication and with privacy (**authPriv**).

Test 3: SNMP/TLS/TCP vs SNMPv3 with USM

- We compared SNMPv3/TLS/TCP with SNMPv3/TCP (USM) and SNMPv3/UDP (USM) in the above three security levels.
- We also compared SNMPv1/TLS/TCP with SNMPv3/TCP (USM) and SNMPv3/UDP (USM) in the similar way.
- The same security algorithms are used in two cases. MD5 is used as the authentication protocol and DES is used as the encryption algorithm.
- We performed tests with both short sessions (snmpget) and long sessions (snmpwalk).

Test 3 – Results

- Snmpget

SNMP-v1 security feature	a	b	b - a	d	d - b	d - a
Or corresponding SNMP-v3 security level	NoAuth NoPriv	Auth NoPriv		Auth Priv		
Snmpget-v1/UDP	472					
Snmpget-v1/TCP	523					
Snmpget-v1/TLS/TCP	774	805	31	840	35	66
Snmpget-v3/TLS/TCP	976	989	13	1,124	135	148
Snmpget-v3/UDP (USM)	665	1,632	967	2,735	1,103	2,070
Snmpget-v3/TCP (USM)	881	1,990	1,109	3,634	1,644	2,753
Ratio :v3-UDP (USM)/ v1-TLS-TCP	85.9%	203%		326%		
Ratio :v3-UDP (USM)/ v3-TLS-TCP	68.1%	165%		243%		
Ratio :v3-TCP (USM)/ v1-TLS-TCP	114%	247%		433%		
Ratio :v3-TCP (USM)/ v3-TLS-TCP	90.3%	201%		323%		

Table 2 (a). snmpget

Test 3 – Results

- Snmpwalk

SNMP-v1 security feature	a	b	b - a	d	d - b	d - a
Or corresponding SNMP-v3 security level	NoAuth NoPriv	Auth NoPriv		Auth Priv		
Snmpwalk-v1/UDP	678					
Snmpwalk-v1/TCP	762					
Snmpwalk-v1 TLS/TCP	1,044	1,120	76	1,273	153	229
Snmpwalk-v3/TLS/TCP	1,063	1,135	72	1,323	188	260
Snmpwalk-v3/UDP (USM)	648	1,848	1,200	2,976	1,128	2,328
Snmpwalk-v3/TCP (USM)	947	2,025	1,078	3,305	1,280	2,358
Ratio :v3-UDP (USM)/ v1-TLS-TCP	62.1%	165%		234%		
Ratio :v3-UDP (USM)/ v3-TLS-TCP	60.9%	163%		225%		
Ratio :v3-TCP (USM)/ v1-TLS-TCP	90.7%	181%		260%		
Ratio :v3-TCP (USM)/ v3-TLS-TCP	89.1%	178%		249%		

Table 2 (b). snmpwalk

Test 3 – Results

- When security level is NoAuthNoPriv , the SNMPv3-UDP session times are always smaller than SNMPv3 (or v1)-TLS-TCP session times. This can be explained that there are TLS and TCP setup times in the later cases. And there is no large difference between the session times of SNMPv3/TCP and SNMPv3 (or v1)/TLS/TCP (ranging from 89.1% to 114%).

- But when security is added, the SNMPv3 with USM session time is much larger than (from 163% up to 433% of) SNMP/TLS/TCP session time.

- Our experiments show that **SNMP/TLS/TCP is more efficient than SNMPv3 with USM**, when using similar security features.

Conclusions

- We have constructed an implementation of SNMP on a TLS/TCP base and conducted experiments to determine whether the additional overhead introduced is acceptable.
- Our results indicate that both the session set up overhead and per message security overhead are not excessive (Totally about 36%).
- Consequently, SNMP/TLS/TCP appears to be a valid choice for secure network management that takes advantage of the efficiency of TCP.
- Both SNMPv3/TLS/TCP and SNMPv1/TLS/TCP are more efficient than SNMPv3/UDP (USM) and SNMPv3 /TCP (USM) , for similar security levels.