Integrated Security Model For SNMP (ISMS)

Wes Hardaker
<hardaker@tislabs.com>

2004.Aug.09
Overview

- 05m  Agenda Bashing
- 20m  Problem History
- 15m  Requirements Bashing
- 30m  Charter Bashing
- 40m  Proposal Bashing
  - EUSM
  - KSM
  - SBSM
- 40m  Proposals Comparison
Meeting requirements

Need someone to:
- Take minutes
- Jabber scribe
- Blue sheets
David’s slides
Problem History

○ This is the second BOF
  ○ Last time: unanimous audience support.
  ○ But... no operators were present.
    □ ADs needed operator opinion

○ Since then:
  ○ Operators polled at NANOG
  ○ Electronic survey
    □ 149 responses
    □ Overwhelmingly a problem

○ And beyond:
  ○ Primary goal of this BOF: A charter
  ○ Secondary goal: technical
Survey Results -- Respondents

Who are you?:

- Network Operator
- Research
- Software Vendor
- Device Vendor
- SNMP Toolkit Vendor
- Did not state
Survey Results -- Current SNMP Usage

How are you using SNMP in your network?

- Monitoring your networks (collecting data / graphs)
- Alarms and Events (notifications)
- Configuring your networks
- Performing actions (fixing things, but not configuration)
Survey Results -- Current SNMP Usage

Which versions of SNMP do you use today:

- SNMPv1
- SNMPv2c
- SNMPv3
Survey Results -- Current SNMP Usage

Do you find SNMPv3/USM easy to setup, deploy and use?

- Yes
- No
- Abstain
Survey Results -- Current SNMP Usage

Is the current SNMPv3 with USM sufficiently secure for your needs?

- Yes
- No
- Abstain
Survey Results -- Authentication Requirements

Which user authentication mechanisms do you use?

- local-accounts
- ssh-keys
- radius
- TACACS+
- x.509-certificates
- kerberos
- ldap
- SecureID
- PAM
- Windows AD
Survey Results -- Authentication Requirements

Which other user authentication mechanisms would you like to use or may use but aren't now:

- radius
- ssh-keys
- kerberos
- x.509-certificates
- TACACS+
- LDAP
- local-accounts
- SQL
- OTP
Survey Results -- Is ISMS needed

Would you find it useful if SNMPv3 supported the above authentication methods you checked?

- Yes
- No
- Abstain
Survey Results -- Is ISMS needed

Would adding these new security services to SNMP be good?

- Yes
- No
- Abstain
If all your devices supported all of the above checked authentication mechanisms, would you still use SNMPv3 with its existing USM support?

- Yes: [Bar]
- No: [Bar]
- Abstain: [Bar]
Requirements Discussion

- must be possible to integrate with existing infrastructure
- can’t be less secure than SNMPv3/USM
- must not modify SNMPv3 full standards documents
- must work with all SNMPv3v message types
- must be able to manage the box during times of network instability
- minimal impact on applications and agents
- minimal impact/setup/operation in the eyes of the users
- minimal impact on performance of network management tasks
- resulting system must be manageable by SNMP
Integrated Security Module for SNMP [ISMS]

○ Chair(s):
  ○ TBD

○ Security Area Director(s)
  ○ Steven Bellovin <smb@research.att.com>
  ○ Russell Housley <housley@vigilsec.com>

○ Mailing Lists:
  ○ Address: sbsm@machshav.com
  ○ Subscribe: sbsm-request@machshav.com
  ○ Archive: https://www.machshav.com/mailman/listinfo/sbsm
Version 3 of the Simple Network Management Protocol (SNMPv3) was completed recently and added security to the previous versions of the protocol. Although the enhanced protocol was secure, operators and administrators found that deploying it could be problematic in large distributions. This was due primarily to the addition of a SNMPv3-specific authentication database which must be supported in addition to existing deployed security infrastructures. Most of these devices already contained local accounts and/or the ability to negotiate with authentication servers (e.g. RADIUS servers). However, SNMPv3 did not make use of these authentication mechanisms, and this caused additional synchronization burdens.
The ISMS working group will focus primarily on creating a security model for SNMPv3 that will meet the security and operational needs of network administrators. The work will include the ability to make use of existing and commonly deployed security infrastructure. Security infrastructures that must be usable by the end solution include:

- Local accounts
- Radius
- TACACS+

Additionally, the following account infrastructures should be considered:

- X.509 Certificates
- Kerberos
- SSH identities
- LDAP
Charter Bashing -- Requirements

The work should not modify the other aspects of SNMP protocol (EG, by adding new PDUs or behavior) in order to achieve these goal of integrated security. It should also be compliant with the security model architectural block of SNMPv3, as outlined in RFC 3411.

The working group may consider adding additional security features not present in SNMPv3’s user based security model as long as the new features does not significantly impact the speed at which the newly designed security model is designed, implemented and deployed.
Charter Bashing -- Work items & Timeline

○ Work Items:
  ○ A document defining an integrated authentication security model for SNMPv3.

○ Goals and Milestones:
  ○ Aug 04  BOF
  ○ Nov 04  Decision about which solution approach the WG will concentrate on and first publication of a WG solution draft
  ○ Nov 05  Work submitted to the IESG for publication as proposed
Technical Proposals

- Presentations about existing work:
  - EUSM: Extended User Based Security
  - KSM: Kerberos-based Security Model
  - SBSM: Session Based Security Model

- Ideas floated, no IDs yet:
  - TLS: Transport Layer Security
## Comparison

<table>
<thead>
<tr>
<th>KRB5</th>
<th>USM</th>
<th>EUSM</th>
<th>SBSM</th>
<th>TLS</th>
<th>KRB5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can use account infrastructure</td>
<td>No</td>
<td>AAA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexible identification methods</td>
<td>No</td>
<td>AAA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>session-keys; central ident != integrity (pair-wise dynamic keys)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Negotiated auth/priv algorithms</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>central</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated SNMP Params</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>True replay protection</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

KRB5: The KDC picks what to use based on config, what the server/service supports and what the user/client supports. IE, the kdc controls the client/server negotiations. It is probably possible to generate krb5 tickets from alternative mechanisms rather than negotiating typically kerberos through the KDC, though the work has not been standardized to date.

The important SNMP parameter that needs negotiation is the SNMP EngineID to be used for the contextEngineID. Negotiating this would require administrators to hand-populate management stations with context engine IDs in addition to ip addresses, etc. Currently, applications get around this when using USM by assuming that the negotiated security engine ID should be the default context engine ID to use unless the user has directly specified a different one to use.

Ken Hornstein's KSM proposal negotiates this (in a yet-unpublished version of the draft). It's not a part of kerberos, but part of how kerberos is used in the model.

TLS doesn't provide generic negotiation so any negotiation would have to happen in the draft defining how TLS was to be used. It would likely have to happen *after* tls got started.

There is work that has been done to make TLS work over UDP: "Datagram Transport Layer Security", Eric Rescorla, 13-Jan-04, <draft-rescorla-dtls-00.txt> It's not standardized yet though. See below as well.

The session keys are randomly generated, but enclosed in the tickets which are encrypted with the host and client secret keys which are long lived. If those are compromised then all previous traffic is also compromised if it was kept because the session keys can be extracted at any time after the host/client keys are broken.

SBSM provides true reordering protection if you set a sequence window size of 1, otherwise it's a configurable level of reordering support.
Survey Results --

Would it useful to protect the identity of the user name within the packet?

- Yes
- No
- Abstain
Path Forward

- WG creation -- AD approval?
- Decide on solution path: November