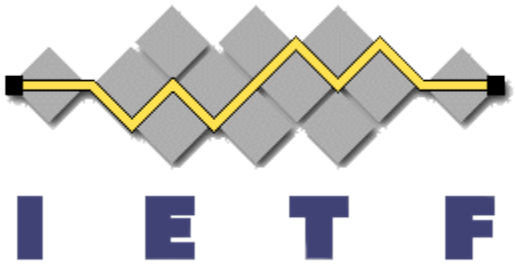

Why Call Home should not be done as part of ISMS

David Harrington

IETF64 Call Home BOF

Vancouver, BC

Call Home Goals

- Goals are not concrete:
- “Certain protocols, and in particular management protocols where devices on either end of connection take client server roles may be able to take advantage of "Call Home" functionality, when traditional roles are reversed, and a server connects to a client.”
- “During the BoF we may identify additional such issues as well as protocols other than management protocols that could benefit from this work.”
- “An additional potential question should be whether a generic standard or process should be used to implement call home, such as rules for SSH.”

ISMS WG Single Goal

- The ISMS WG goal is concrete:
- “The goal of the ISMS working group is developing a new security model for SNMP that integrates with widely deployed user and key management systems, as a supplement to the USM security model.”
- SSHSM is an SNMPv3 security model that integrates with deployed Secure Shell security.
- Call Home is NOT widely deployed, is NOT a current feature of SNMP, and is NOT a feature of widely deployed security solutions.

Does Call-Home solve an SNMP problem?

- SNMPv3 includes solutions to address firewalls and NATs and mobility
- Call-home doesn’t solve a network management problem
- Call-home doesn’t solve a security problem
- Call-home solves a transport problem

SNMPv3 Existing Solutions

- IANA-assigned ports for SNMP Firewall Rules
  - Different ports for SNMPv3/USM and SNMPv3/SSH
  - Different ports for request-response and traps
- SNMPv3 Proxy
  - Designed to pass SNMP through Firewalls and NATs
  - administratively-defined security relations
  - known managers to known agents, based on engineID
- EngineID
  - Identifies the source of the data - Identity not Address
  - For dynamic address changes (ala NAT/DHCP/mobility/multihoming)
  - Authoritative engineID associated with data to be protected
  - Authoritative engineID indicates who must know about the other
- MIDCOM MIB
  - Designed to dynamically configure firewalls and NATs
  - Designed to support SIP-initiated connectivity

Lack of Demand

- There has been no demand for call-home functionality in SNMP.
- The IAB Network Management Workshop and the O&M “World Tour” did not identify call-home as in-demand for network management.
- BOF Proposal: “protocols may be able to take advantage of call-home functionality”

Conclusion

1) Call-home is a transport solution, not an NM solution, and is not in demand for network management.
2) Call-home tries to solve a problem that is already solvable for SNMP using proxy.
3) Call-home doesn’t address all the issues proxy addresses, such as hiding devices within a NAT
4) Call-home is not backwards-compatible.
5) Call-home increases the complexity of existing network management.
6) Call-home complexity would slow the development of ISMS and Netconf solutions.

Alternate Proposal

- Allow ISMS and Netconf to be developed to meet current demand, without call-home.
- Develop call-home as an add-on to existing transports, changing only the initiator
- Develop call-home as an optional transport for SSH, that changes the initiator but NOT the client-server roles vis-à-vis the manager-agent roles, for compatibility with existing uses.
- Allow ISMS and Netconf (and other protocols) to develop additional transport mappings for the call-home transport option if demand develops.