Security Aspects of the OAM Protocol for EFM

Dan Romascanu – Avaya Inc.

Carlos Ribeiro - CTBC Telecom

Outline

- Concerns
- Security Threats and Counter-measures
- A Possible Security Framework
- What Next?

Concerns

- 802.3ah enters a space ‘where no Ethernet reached before’
  - Subscriber access - managed CPE does not belong to the organization that provides the management services
  - Partially exposed infrastructure – how different from existing carriers infrastructure?
  - Partially shared infrastructure
  - SLAs with economic impact are in place between providers and subscribers
- 802.3ah provides a well documented OAM interface which:
  - May allow for security attacks to be performed by means of the protocol
  - May contain sensible information with economic content (at least for the SLA between providers and subscribers)
- Security is a **Risk Management** problem: goal risk reduction at a reasonable cost; risk exposure is known and accepted
  - Assess threats/risk
  - Select cost effective counter-measures (technology, procedures, or documentation)

Precedents and Goals

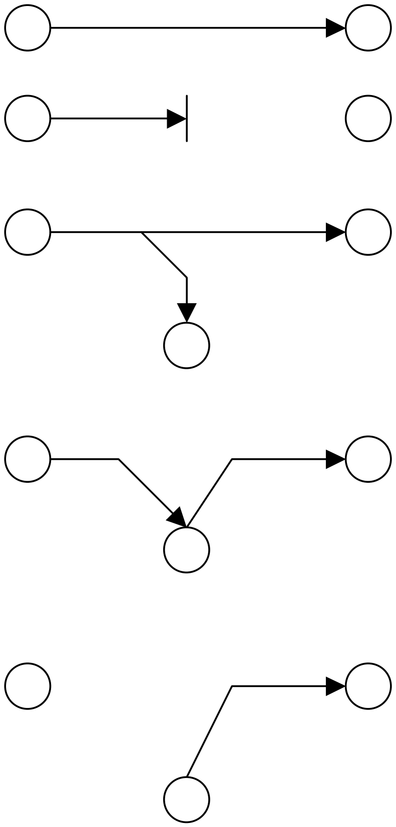
- What other Standards Groups Do?
  - IETF
    - mandatory security analysis for all protocols
    - Management protocols (SNMP, COPS) have administrative framework including optional counter-measures against security threats
    - Management protocols are ‘IP in-band’ and protection is layer 3 and higher
- Goals
  - Analyze security threats
  - define possible counter-measures
  - estimate if the cost is worth
  - All wrt. the EFM OAM protocol
- Non-goals
  - Discuss security of data carried by EFM

Scope

- Cover all EFM flavors
  - p2p fiber
  - p2mp fiber
    - “partially shared infrastructure”
    - May need a control protocol for special PON purposes – registration, upstream BW allocation
    - Can a single framework be used?
  - p2p copper
- Need to have a multi-layered view of the management and security framework
  - What is in the scope of EFM OAM
  - What is being left for the in-band upper layer management protocols (like SNMP)
- Protect EFM OAM basic functions
  - Link management
  - communications channel for the OLT to gather low-level information about the ONUs
  - service activation/provisioning between the ONU and OLT

The Threats

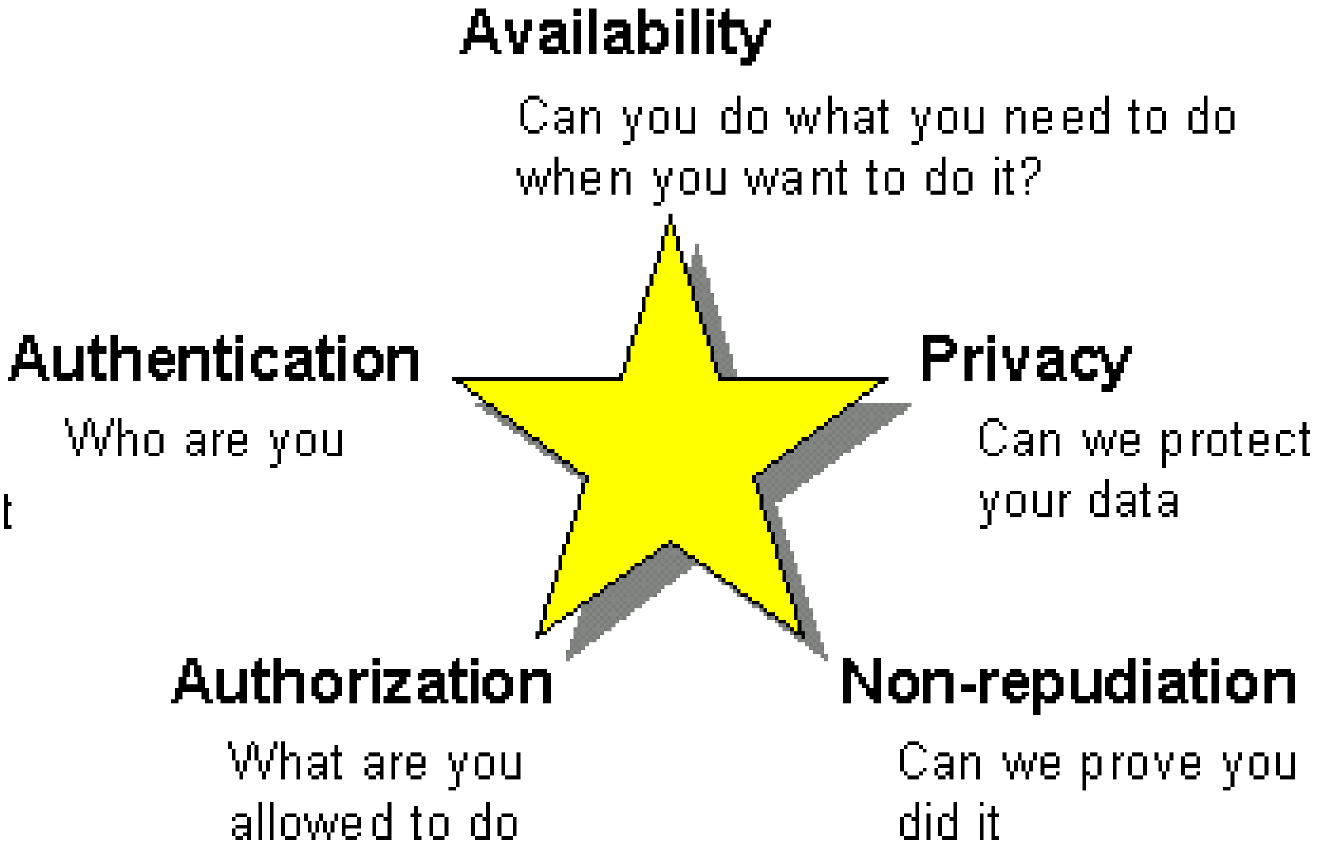
- Normal flow
- Interruption
- Interception
- Modification
- Fabrication



How Threats Affect Services

- Interruption
  - Link is destroyed, or becomes unavailable for usage – threat to availability of data and OAM
- Interception
  - An unauthorized party gains access to OAM information – threat to privacy
- Modification
  - An un-authorized party modifies or replays OAM messages (masquerade)
  - threat of availability and theft of service, opportunity for denial of service
  - Threat in both directions of the OAM flow
- Fabrication
  - Counterfeit OAM traffic
  - Same threats as in modification

Threats and Security Services



Availability

Can you do what you need to do when you want to do it?

Authentication

Who are you

t

Privacy

Can we protect your data

Authorization

What are you allowed to do

Non-repudiation

Can we prove you did it

Chart derived from Gartner Symposium ITXPO 2001

Security Services – Basics

- Access Control –
  - Only those authorized may access the resource
  - Various levels of granularity: system, data, service, etc.
- Protection from unauthorized disclosure –
  - e.g., a conversation, a message, data
- Integrity –
  - e.g., can not be spoofed, altered, removed in an unintended manner by an unauthorized person
- Non-repudiation –
  - a message/transaction/action can not be denied by a party e.g., recant voicemail: “that wasn’t me”
- Protection from Denial-of-Service attack –
  - preventing an intentional system disruption (slow down, crash, hang)
- Protection from Theft of Service –
  - e.g., Toll Fraud

Authentication for an OAM Protocol in EFM

- Authenticate the subscribers that connect in order to receive service
  - Authentication can be performed at higher layers
    - 802.1x for CO port
    - DHCP with Digital Signature (MD5) for station authentication
    - RADIUS for users authentication
  - For authentication to work, link needs to be established
  - Minimal OAM for before link establishment and authentication is confirmed
  - OAM entity needs confirmation about authentication from MAC client

Authorization for OAM in EFM

- Not relevant if we do not allow for SET operations
- Any SET operation raises the issue of authorization
  - Keep Sets operations at minimal
  - This includes the capability of resetting the remotely located MAC entity
- Levels of complexity
  - Non-repudiation
  - Protect against replay
  - Protect against modification
  - Protect against fabrication
- Protection includes
  - Physical protection of the links and equipment
  - OAM messages to detect false commands – e.g. trap sent on the link after reception of a RESET command with confirm info
  - Per message authentication – digital signature (e.g. MD5) with shared or public key

Privacy for OAM in EFM

- What information needs to be protected?
  - Registration of users identified by MAC addresses
  - Utilization figures in traffic counters
- Methods of protection
  - Physical protection
  - Encryption (e.g. – DES based algorithms)
  - Layer 3 protection mechanisms (like IPSec) will not work because they require the OAM messages to be visible to MAC clients
- Is preamble-based OAM more robust vs. eavesdropping attacks?
  - Marginal advantage – if an OAM protocol is adopted, tools for protocol decoding will emerge for good and bad reasons

Denial-of-Service in OAM for EFM

- Possible types of attacks
  - Saturate the line with OAM messages
  - Perform intrusive SET actions to the remote station (if SETs allowed)
- Counter-measures
  - Throttle OAM messages on the receiving side
    - Will download the MAC, but not the line
  - Localize and disconnect attacker
  - Separate services (one client MAC mis-behavior should not affect other client MAC services)

Theft of Service in OAM for EFM

- Un-authorized clients try to connect in order to receive services
  - Use authentication mechanisms for port, station, and user
- Billing
  - Raises the issue whether OAM information should be used for billing purposes
    - Maybe not
    - If yes, authentication, non-repudiation, and maybe privacy are required

A Possible (and maximal) Security Framework for OAM in EFM

- Set of administrative recommendations for physical protection of links and CPEs
- An optional authentication mechanism
- An optional authorization mechanism
- An optional privacy mechanism for p2mp EFM
- A mandatory DoS avoidance mechanism

- What does ‘optional’ mean in this standards context?
  - The optional mechanisms are fully defined and documented in the standard
  - Implementations SHOULD include support for the security features
  - Operational mode flags allow for the activation and deactivation of the security features
  - Plug-and-play default mode is non-secure

Open Issues

- Layers relationship
  - Some of the counter-measures may be implemented at the higher layer. This is out of the scope of EFM but we might want a mechanism to allow for OAM to be aware about the results
  - E.g. – full OAM enters in effect after port, station, and user are authenticated
  - Breaks the layering model?
- Where is the demarcation of the EFM link?
  - In the equipment to which the subscriber has the ultimate control
  - Terminates in equipment outside of the subscriber’s ultimate control
- P2mp issues
  - Is p2mp a ‘shared’ system? Are extra measures for privacy needed?
  - To what extend separation of services is possible?

What next?

- We need to understand if
  - Customers are concerned by the security issues
  - The solutions that we are proposing are worth the value of the information and resources that are being protected
- If the answer is yes to the above
  - Document threats
  - Define the mix of technical and administrative measures that map into the layers and scope of the project and make them part of the 802.3ah standard
  - Document best practices