Security Threats and Defense Models in EPON

Olli-Pekka Hiironen and Antti Pietiläinen, Nokia

Ali Abaye, Centillium

Onn Haran, Passave

Two cases

- Fiber to the home (FTTH)
  - It is assumed that regulations that govern access network cabling equipment spaces are followed. Fiber and splices are not easily accessible and cross connects are locked up both in operator space and in the space of the property owner.
- Fiber to the business (FTTBusin.)
  - In this paper FTTBusin. is based on a “worst case” scenario where many companies are located in the same property. Fibers are drawn through the building passing many companies where fibers connecting one company may be accessible by people working in the other companies. Cross-connect room may be accessible by many people and full security can not be assumed. In this case a physical man-in-the-middle risk is faced.

Security threats in P2MP (FTTH)

(SEVERITY)

- **PON medium is broadcast in downstream (VERY HIGH)**
  - Every ONU located in end-users' premises can eavesdrop downstream traffic unnoticed and undisturbed 24h/day using a standard Gb Ethernet interface.
  - The attacker can know the MAC addresses and LLIDs used by neighbors.
  - The attacker could infer the amount and type of traffic to neighbors by monitoring LLIDs and Ethernet MAC addresses.
  - Downstream MPCP messages can reveal upstream traffic characteristics of each ONU.

Security threats in P2MP (FTTH)
(SEVERITY)

- **PON medium is multi-point-to-point in upstream (HIGH)**
  - The attacker can masquerade as another ONU (using MAC address and/or LLID) and gain access to privileged data and resources in the network.
  - The attacker can steal the service by overwriting the signal with higher power. 6dB-10dB higher power is enough.
  - The intruder can flood the network with either valid or invalid messages affecting the availability of the network resources or OAM information, e.g. counters in OLT.
  - End user may try to disturb the PON by sending any optical signals upstream (e.g. signal from standard Ethernet long wavelength interface). This could generate restarts which may ease hacking the protection mechanisms.

Security threats in P2MP (FTTH) (SEVERITY)

- **PON medium may have discrete reflections (LOW)**
  - Upstream traffic of one ONU may be detectable in some cases at another ONU location by using advanced equipment.
  - In this case the attacker could intercept upstream frames by using reflections from PON, modify frames, and send them to OLT.

Threat model in P2MP (FTTH)

- **PON medium is broadcast in downstream**
  - Confidentiality
  - Identity protection
- **PON medium is multi-point-to-point in upstream**
  - Authentication
  - Access control
  - Data origin authentication
  - Denial of service prevention
- **PON medium may have discrete reflections**
  - Confidentiality
  - Data integrity

Security Threats (FTTBusin.)

- Here a possibility of man-in-the-middle is assumed. In this case all security threats mentioned earlier and more apply to both upstream and downstream.
- PON medium does not compromise security any more than the man-in-the-middle does.

Security objectives in P2MP

(IMPORTANCE)

- **Confidentiality (MUST):** Keeping information secret from all but those who are authorized to see it
- **Authentication (MUST):** The network wants to be sure about ONU’s identity
- **Access control (MUST):** Network wants to control the access of ONU's to network resources.
- **Message authentication (data origin authentication) (MUST):** A type of authentication whereby a party which receives a message have assurance of the identity of the party which originated the message
- **Data integrity (MUST):** The receiver wants to be sure that the received message has not been modified
- **Identity protection (IMPORTANT):** It is not possible to infer confidential data by passive attacks, e.g. analysis of traffic volume or destination

Security objectives in P2MP
(IMPORTANCE)

- **Denial of service prevention (IMPORTANT):** Enemies can neither prevent the use of any resources to legitimate users nor decrease system performances
- **Non-repudiation of origin (WISH):** The sender can not deny that he sent a message
- **Non-repudiation of delivery (WISH):** The receiver can not deny that he received the message

Defense model

- Confidentiality
  - Encrypt data messages.
- Identity protection
  - Encrypt MAC addresses
- Authentication
  - Authentication
- Access control
  - Access control
- Data origin authentication
  - Message authentication
- Denial of service prevention
  - Message authentication, fix auto-discovery problems,...
- Data integrity
  - Integrity protection

Requirements (Downstream)

		Security mechanisms					Req. in EPON	
Security objectives	Severity * probability	Authentication	Encryption	Mess. Auth.	Data integrity	Digital signature	**FTTH**	**FTTBusin.**
Confidentiality	very high		x				yes	yes
Authentication	low	x					no	yes
Message authentication	low	x		x			no	yes
Data integrity	low	x			x		no	yes
Access control	low	x		x			no	**maybe**
Identity protection	high		x				yes	yes
Non-repudiation of delivery	moderate	x			x	x	?	**?**
Denial of service prevention	low						no	**?**

Requirements (Upstream)

Security objectives in EPON	Severity x probability	Security mechanisms in EPON					Req. in EPON	
		Authentication	Encryption	Mess. Auth.	Data Integrity	Digital Signature	FTTH	FTTBusin.
Confidentiality*	low – mod.		x				maybe	yes
Authentication	very high	x					yes	yes
Message authentication	high	x		x			yes, encrypted FCS ok	yes, man-in-the middle resistant
Data integrity*	low – mod.	x			x		maybe	yes
Access control	high	x		x			yes	yes
Identity protection*	low – mod.		x				maybe	yes
Non-repudiation of delivery	moderate	x			x	x	?	?
Denial of service prevention	high						?	?

*Because directionality of splitters protects ONUs from each other in upstream quite well, confidentiality, data integrity and identity protection may be considered to be in control.

MPCP control messages may reveal identity of ONUs and their traffic profiles upstream. For achieving identity protection, MPCP messages should not include identifiers which remain the same from day to day and week to week that correspond to a real user.

Mechanisms Summary

	FTTB		FTTH	
	Upstream	Downstream	Upstream	Downstream
Encryption	Yes	Yes	No	Yes
Authentication	Yes	Yes	Yes	No
Message authentication	Yes	Yes	Yes	No
Data integrity	Yes	Yes	No	No
Digital signature	No	No	No	No

Open Issues

- Threat model
  - Which model should be used (FFTH / FTTB / combination)?
- Security objective
  - Confine to scope
- Mechanisms
  - Decide on the ones to be addressed
  - Select / specify each mechanism