Privacy in EPON

Olli-Pekka Hiironen, Antti Pietiläinen,
Arne Nylund, Nokia

Supporters

- Carlos Ribeiro, CTBC Telecom
- Kent G. McCammon, SBC
- Yukihiro Fujimoto, NTT
- Charles Cook, Qwest
- Onn Haran, Passave
- Dolors Sala, Broadcom

Why privacy in EPON?

- Shared medium Ethernet enters a space ‘where no Ethernet reached before,’ i.e. public subscriber access
- Privacy is required in subscriber access by law
  - European Convention on Human Rights:
    Article 8 – Right to respect for private and family life
    "...Everyone has the right to respect for his private and family life, his home and his correspondence…"
  - Finnish Constitution:
    Section 10 - The right to privacy
    "...The secrecy of correspondence, telephony and other confidential communications is inviolable…"
  - as a consequence, in current telecom networks, including subscriber plants, all cable terminations and access points are located in locked boxes and environments. They are legally accessible by authorized operator personnel, only
- Common expectations on privacy
  - the subscribers expect that telecommunication networks, by default, can maintain basic privacy without need for any additional measures from end user

Why privacy in EPON?

- EPON uses shared medium comparable to wireless
  - eavesdropping and traffic analyzing are possible unnoticed and undisturbed 24h/day by every ONU located in end-users' premises
  - masquerading as another ONU is possible without privacy mechanism
  - severe privacy problems occurred with analog mobile systems where people easily could listen to others' mobile calls with manipulated cell phones. In some cases hackers succeeded to make mobile calls on other subscriber's expense. - GSM included privacy mechanism that eliminated the problem
- Business customers require high level of privacy
  - deployment of FDDI and SDH/SONET with ring nodes in customer premises was not accepted because the users did not trust a system where the traffic passes nodes located in neighbors' sites, though sites with access control. Acceptance was achieved when the ring nodes were located in operator's environment and user sites were connected via spurs. Similar trust problems might be faced when ONUs are located in the basements of other MDU/MTU

➔ **Privacy should be guaranteed in the EPON**

Why not use higher layer protocols?

- Privacy is expected at the link level
  - large installed base of protocols assume that privacy is already guaranteed on the underlying layers and thus *do not* implement privacy at the upper layers
  - end-users can not be expected to make extra measures to ensure privacy. Thus, all users below EPON in the access tree should be informed that their access connection is insecure and they have to make extra measures to guarantee their privacy
  - a large Ethernet network can lose guarantee of privacy if a single insecure EPON link is added into the network. EPON links themselves should be secured to avoid upgrading the privacy mechanism of the whole network
- Problems with transaction protection (e.g. SSL)
  - larger servers handling large volumes of traffic would be overwhelmed by the need to encrypt every single bit of traffic, while using different keys and privacy methods for every individual connection
  - a lot of basic protocols do not lend themselves to per-transaction protection: DNS transfers, parts of the PPP authentication message exchange, some instant messaging applications

Why not use higher layer protocols?

- Using higher layer privacy protocols in ONUs and OLT
  - to guarantee interoperability it has to be anyway agreed which standard to use and how to use it
  - ONUs and OLTs have to be IP routers in practice if layer 3 or above protocols are used, thus limiting the versatility that Ethernet would otherwise bring
- Higher layer protocols do not protect against traffic analyzing
  - giving possibility for traffic analysis may be considered as a violation of privacy law. Possibility to traffic analysis has caused bad press for cellular operators
  - privacy at the link level would allow method where traffic analysis is not possible
- Higher layer protocols for payload privacy do not protect against OAM traffic hacking or MPCP message eavesdropping
  - end users may get access to operators TMN network beyond the EPON system by hacking into OAM channels
  - downstream MPCP messages can reveal upstream traffic characteristics of each ONU
  - carrying out privacy at the link level allows protection against there threats

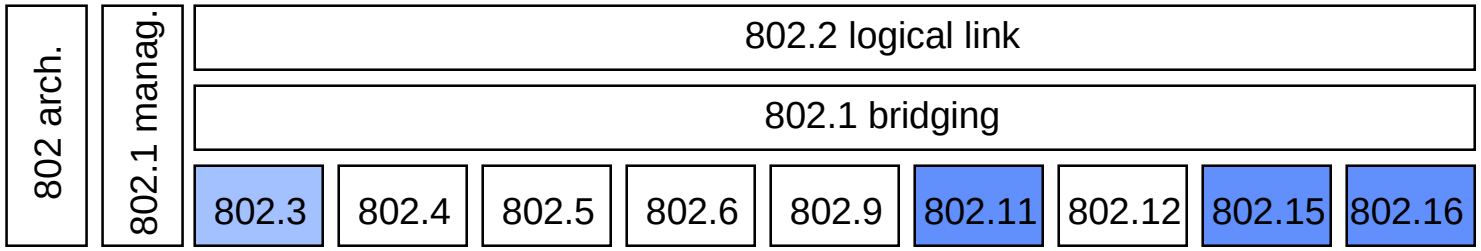
➔**Privacy in EPON should be guaranteed at the link level**

Why standardize in EFM?

- There is no link level privacy mechanism for EPON available
- Reputation and acceptance
  - without standardizing privacy in EFM there is a risk that there will come Ethernet PON systems on the market that do not fulfill privacy requirements
  - EPON and even Ethernet as a whole can lose general acceptance as an access network technology if Ethernet PON will be treated as an insecure standard
  - competing technologies might get good arguments against EPON
  - example: Wireless LAN has reputation of being an insecure standard even if there are good non-standard privacy mechanisms
- Incompatibility
  - if privacy features are agreed somewhere else, there is a risk of mutually incompatible EPON systems emerging
  - EPON will not get to mass deployment without vendor interoperability see e.g. Microsoft - Macintosh, ADSL interoperability, cell phones. Interoperability requires a common standard
  - implementation problems may appear if privacy is not designed into the system from the beginning

Why standardize in EFM?

- IEEE802 groups have standardized privacy mechanisms
  - IEEE802.11 WLAN: First version broken but new version is being developed
  - IEEE802.15 WPAN: Privacy mechanism is being developed
  - IEEE802.16 WMAN: Privacy mechanism is included



➔ **EFM should standardize privacy mechanism for EPON**

Conclusions

- Shared medium Ethernet enters public subscriber access. This brings new requirements
- Privacy should be guaranteed in EPON
  - law requires privacy in subscriber access networks
  - EPON uses shared medium which brings several privacy threats
  - business customers have high requirements which have to be met
- Privacy in EPON should be guaranteed at the link level
  - privacy is expected at the link level
  - protection against traffic analyzing
  - prevent OAM traffic hacking and MPCP message eavesdropping
- Privacy mechanism for EPON should be standardized in EFM
  - reputation and acceptance of EPON as an access technology
  - risk for incompatibility and not reaching mass deployment
  - other IEEE802 groups have standardized

➔Recommendation

- privacy mechanism is required for EPON and EFM should standardize it
- mechanism should be adequate to maintain privacy but it should meet minimal cost target

Rebuttal: Privacy mechanisms are not needed

- Ethernet does not do privacy
  - Ethernet did not include privacy because it was not needed or desirable in its earlier environments, but now, for the access network, we have a different proposition. In this regard we have the examples of 802.16 and 802.11 to follow. For example, 802.11 is standardizing privacy mechanism which uses AES for encryption and 802.1x for authentication, access control, and key exchange
- Encryption is costly
  - the average cost for the silicon to implement a proper encryption method is falling quickly, thanks to the need for it in wireless networks
- Encryption is not needed for an optical network
  - this argument is based on the idea that the optical network is somehow more immune to interference than the wireless networks. However, It is easy for an attacker to intercept signals transmitted over the PON, or even to generate fake traffic using off-the-shelf electronics

Appendix 1: Legislation

- European Convention on Human Rights

  "Article 8 – Right to respect for private and family life

  1 Everyone has the right to respect for his private and family life, his home and his correspondence.

  2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

- Finnish Constitution

  "Section 10 - The right to privacy

  Everyone's private life, honor and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.

  The secrecy of correspondence, telephony and other confidential communications is inviolable.

  Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardize the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act."

Appendix 2: Possible threats

- downstream payload of all subscribers visible in all PON ONU accesspoints
- knowledge of amount and type of traffic to neighbors may be see as privacy violation
- knowledge of MAC addresses used by neighbors may be a privacy problem
- downstream MPCP messages can reveal upstream traffic characteristics of each ONU
- upstream PON traffic may, in certain conditions, be detectable from ONU access points
- if end users succeed to hack into ONU OAM channel, they may be able to change EPON system configuration
- if end users succeed to hack into OAM channels, they may get access to operators TMN network beyond the EPON system
- if end user can decode key exchange mechanisms, he can bypass the protection system
- end user may try to disturb the PON by sending optical signals upstream, this could generate restarts which may ease hacking the protection mechanisms

Appendix 2: Possible threats

- by using information from registration and gate messages it may be possible to masquerade as another ONU
- privacy is compromised if proper authentication and data authenticity check is not carried out
- …