11.7.28

IPsec Security for Packet based Synchronization

on behalf of
Yixian Xu, Huawei Technologies
IETF 81, Quebec City

Introduction

- **Security issues on time synchronization**
  - e.g., Femtocell, a home base station in cellular network
  - a public network is used to establish connectivity between Femtocell and core network elements (e.g., Security Gateway, Femto Gateway, Clock server, etc.)
- **Security Requirement on time synchronization**
  - Client SHOULD be prevented from connecting to rogue clock servers
  - Clock servers SHOULD be prevented from providing service to unauthorized synchronization client
  - Minimize any degradation in performance
- **Protection**
  - Authentication based: IEEE 1588, no key sharing method defined
  - Encryption based: IPsec, not able to recognize time message

Issues in the Implement

- **Tictoc has discussed the advantages to identify the content of an IPsec tunnel as “special” packets from a timing perspective, the conclusion is:**
  - This may allow a specific handling of the packet both for intermediate nodes and slave
  - The problem is how to identify the timing packet when the content of the timing packet is encrypted

What we need to do

- **Identify 1588v2 packets**
  - ESP is usually used
  - Considerations on cost
- **Extend WESP defined in RFC 5840 to add the identifier**
  - Simple
  - Extend the use for WESP
- **Provide integrity protection to the extension**
  - Protect against from tamper attack

Difference from v00

- **WESP Extension**

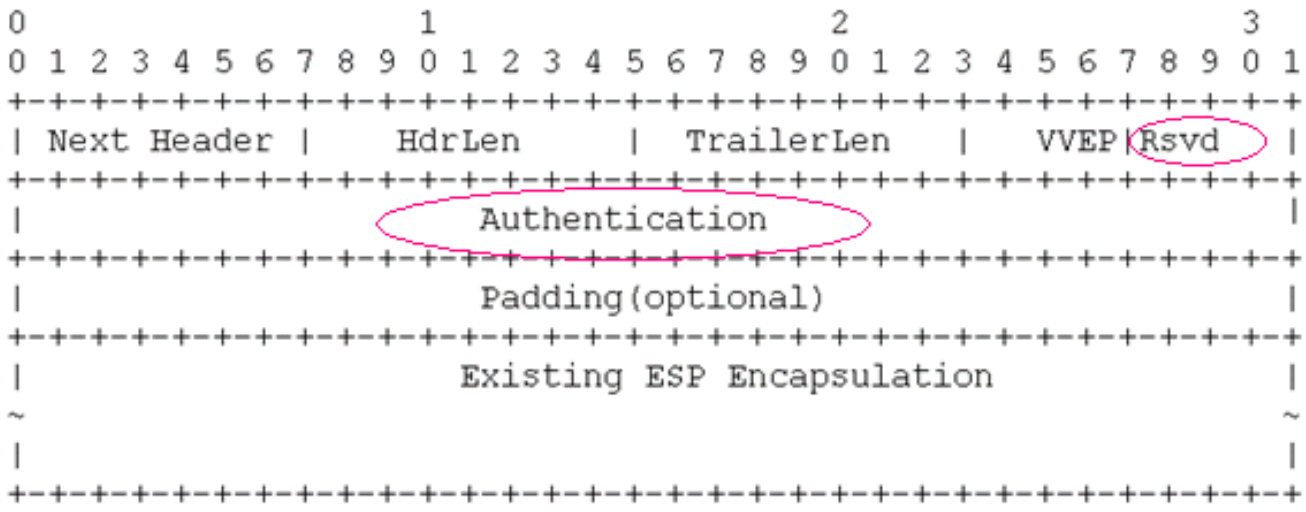

Fig 1. the format of WESP Extension

Extension used for 1588v2

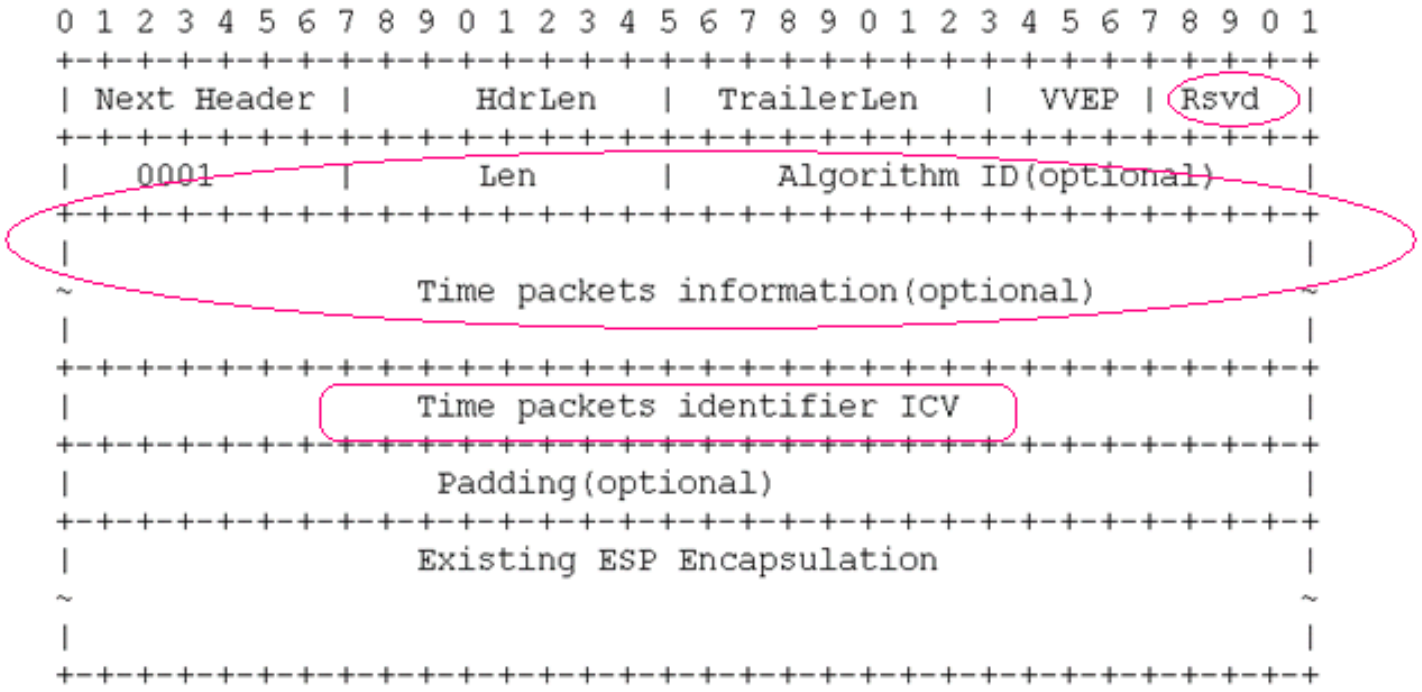

Fig 2. the format of WESP Extension with time packet

Thank you