IPsec ESP Extensions for Traffic Visibility

Ken Grewal

Gabriel Montenegro

Problem Description

- Scope: Traffic visibility for ESP traffic only
  - Very important in enterprise deployments
  - AH can be used, but not NAT friendly (And yes, there are NATs inside enterprise environments)
- IPsec is predominantly used for remote access / VPNs
  - Transport mode IPsec still needs good standard support
- Enterprise environments require not only security, but also traffic visibility
  - Firewalls and Traffic-shaping tools
  - Network monitoring tools
  - Deep packet inspection and scanning (for worms/viruses)
  - Intrusion Detection & Prevention Systems (IDS/IPS)
- Current IPsec specs do not allow deterministic differentiation between ESP-NULL and ESP-encrypted traffic

Proposed Solution

- New protocol ‘wrapper’ for existing ESP packet format
- Wrapper defines the packet encapsulation
- Stateless, efficient parsing of ESP-NULL packets using data within the packet
- Enables E2E security with traffic visibility

Alternative Proposals

2 proposals submitted:

- draft-hoffman-esp-null-protocol-00.txt
  - Paul Hoffman & David McGrew
  - Expired?
- draft-grewal-ipsec-traffic-visibility-01.txt
  - Ken Grewal & Gabriel Montenegro

draft-hoffman-esp-null-protocol

- 2 new protocols for identifying ESP-NULL
  - ESP-AUTH-ONLY-NO-IV
  - ESP-AUTH-ONLY-8-OCTET-IV
- IKE Dependencies
  - New transforms with new protocol numbers
  - If recognized, use it (based on policy), else fall back to protocol 50 (ESP)

draft-grewal-ipsec-traffic-visibility

- 1 new protocol for identifying “Extended ESP”
- UDP encapsulation compatibility for NAT-T
- IKE Dependencies
  - New transform with new protocol number
  - If recognized, use it (based on policy), else fall back to protocol 50 (ESP)

ESP Extensions

```
 0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header    |  HdrLen       | TrailerLen    | Flags          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Security Parameters Index (SPI)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      IV (variable)                             |
~                                                                ~
|                                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Payload Data                              |
~                                                                ~
|                                                                |
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |            TFC Padding * (optional, variable) |
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               | Padding (variable)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Padding (0-255 bytes)          |PAD Length     | Next Header    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Integrity Check Value-ICV (variable)              |
~                                                                ~
|                                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- Next Header: Next protocol
- HdrLen: offset in octets to start of payload
- TrailerLen: Offset from end of packet to end of payload
- Flags:
    - 2 bits Version
    - 1 bit Integrity Only
    - 5 bits reserved

UDP-Encapsulation

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Src Port (4500)        | Dest Port (4500)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Checksum                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Protocol Identifier (value = 0x00000001)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   |  HdrLen       | TrailerLen    | Flags         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Security Parameters Index (SPI)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      IV (variable)                            |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Payload Data                             |
~                                                               ~
|                                                               |
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |            TFC Padding * (optional, variable) |
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               | Padding (0-255 bytes)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Padding (0-255 bytes)          |PAD Length     | Next Header   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Integrity Check Value-ICV (variable)             |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- Protocol Identifier: Fixed value
  - e.g. 0x01
  - Differentiate between IKE/ESP/XESP packets
- Preserves UDP 4500 for NATs
- All other fields as in previous slide

Compatible with and preserves NAT-T encapsulation

Summary

- XESP critical to Enterprise based IPsec deployments
- Applicable to XESP only (does not impact AH or ESP)
- XESP ‘wrapper’ concept is similar to NAT-T
  - Extends ESP, instead of breaking it
- Aids Transport-mode IPsec deployment in Enterprises

Questions?