Heuristics

draft-kivinen-ipsecme-esp-null-heuristics-00.txt

T. Kivinen kivinen@iki.fi
D. McDonald danmcd@sun.com

Introduction

- Detecting ESP-NULL packets without end-node modifications
- Output:
  - Encrypted ESP or ESP-NULL
  - Integrity Check Value (ICV) length
  - Initialization Vector (IV) length
- Once at the start of new IPsec flow
  - Flow identified by src-address, dst-address, protocol (ESP) and SPI-number
- All test compare between random data or clear text protocol data.

First Tests

- Find the ICV length
  - Required to get next header number
  - Start from shortest
  - Check if self-describing padding is there
    - 01, 02, ... n-1, n, n, where n is pad length
    - Examples:
      - 01 02 03 03
      - 01 01
      - 00

Protocol Tests

- Protocol specific tests
  - TCP/UDP/ICMP/tunneled IPv4/IPv6 etc
- Needed to find out IV length
  - IV exists only in GMAC macs (ICV length=128 bits)
- Provides better proof that the ICV length is correct as next header number is verified by verifying the protocol data.
- Can get complicated, but deep inspection engines already does these

Reliability

- To get reliable detection might require multiple packets
- 2% of worst case packets can pass the first tests (padding length 0)
- 0.00000002% of packets can pass 32 bits of protocol inspection
  - For example that TCP/UDP port numbers are same for two packets
    - retransmission of the TCP packet
    - UDP protocols usually consists of multiple packets between same port pairs

Conclusions

- Can be implemented on middle-boxes
- No changes to the end-nodes
- Can be implemented and deployed NOW