PEACH
FUZZER

IPSECv6 Peach Pit Data Sheet

- Peach Pit: IPSECv6
- Target: Client (AH and ESP)
- Supported Platforms: Windows, Linux, OS X

Internet Protocol Security version 6, (IPsecv6) is a protocol suite for securing Internet Protocol (IP) communications. IPsecv6 operates at Internet layer (layer 3), and provides security for almost all protocols in the TCP/IP suite.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

IPsec helps provide in-depth defense against:

- Network-based attacks from untrusted computers that can result in denial-of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Administrative control of servers, other computers, and the network.

IPsecv6 has two modes of operation:

- Transport mode is used in host-to-host communications and encrypts the payload of the IP packets in the communication.
- Tunnel mode is used in host-to-network communications (remote user access), host-to-host communications (private chats), and netowrk-to-network communications (creating Virtual Private Networks). Tunnel mode encrypts the entire IP packet, header and payload, and inserts the encrypted packet into a new packet with a new IP header.

Specifications

Specification	Title
RFC2403	The Use of HMAC-MD5-96 within ESP and AH

Specification	Title
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC2451	The ESP CBC-Mode Cipher Algorithms
RFC2857	The Use of HMAC-RIPEMD-160-96 within ESP and AH
RFC4302	IP Authentication Header
RFC4303	IP Encapsulating Security Payload

Use Cases

Messages	Specification
Authentication Header (AH)	RFC4302
Encapsulating Security Payload (ESP)	RFC4303
Transport Mode Processing	RFC4302 - Section 3.1.1, RFC4303 - Section 3.1.1
Tunnel Mode Processing	RFC4302 - Section 3.1.2, RFC4303 - Section 3.1.2
Separate Confidentiality and Integrity Algorithms	RFC4303 3.4.4.1
ICV HMAC-MD5-96	RFC2403
ICV HMAC-SHA-1-96	RFC2404
ICV HMAC-RIPEMD-160-96	RFC2857
3DES-CBC Cipher Encryption	RFC2405, RFC2451
Null Encryption	RFC2410