Advanced Cryptography Concepts

Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+ ITIL

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Goals of Cryptography
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Layer 1 HW, Cables, Fiber
- Layer 2 Data Link Encryption
- Layer 3 IP SEC
- Layer 4 TLS TCP/UPD
- Layer 5 Handshake, DNSEC, EMAIL, PGP
- Layer 6 compression encryption and decryption)
- Layer 7 SHTTP, HTTPS, IMAP, SNMP,

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Transport Layer Security (TLS)
- Improved upon weakness of SSL with more secure Hashing
- Secures port 80, HTTP, for *HTTPS*
- Uses TCP port 443 (works at higher ports)
- Encrypts the channel
- S-HTTP-
  - Encrypts the individual message and does not require the client-side public key, certificate
  - Supports symmetric cryptography only

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

1. HTTPS request made
2. Server send a digital certificate with public key
3. Client authenticates server's certificate
    1. The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period
    2. The client verifies that the issuing Certificate Authority (CA) is on it's list of trusted CA's
    3. The client uses the CA's *public* key to validate the CA's digital signature. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA
    4. To protect against Man in the Middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate. If all checks are successful, the client continues with the SSL handshake process
4. Browser generates session key one time for this session using an IV sent from server
5. Server decrypts session key with private key
6. Secure connection is made using session key, to include clients PII and other information is decrypted and processed

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Virtual Private Networks

- Creates a virtual connection across untrusted networks for remote users
- Packets are encrypted
- Links are encrypted
- Tunnels are encrypted
- Can be site to site
- Client to client
- Client to site
- Router to router

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Point to Point Tunneling Protocol (PPTP)

- Oldest tunneling protocol
- Extension of PPP by encryption packets and authenticating users
- Works at data link layer (L2) uses two different methods for authentication
  - Uses EAP for authentication,
  - Also uses CHAP for authentication
- Microsoft Point to Point Encryption MPPE for packet encryption
- Uses DES

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Layer 2 Tunnels Protocol (L2TP)

Replaces PPTP, or sought to improve

Works at L2

Uses IPsec for encryption

Offers more methods for authentication

- CHAP
- EAP
- PAP
- SPAP
- MS-CHAP

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Internet Protocol Security (IPSEC)

- A set of protocols to provide data security in transit
- Allows for devices, users, applications, sites, routers, clients, to communicate securely without prior communication
- Used Diffie-Hellman among other protocols for key generation
- IS not native with with IPv4,must be built in
- Uses two different modes AH and ESP
  - Can work in tunnel or transport
- Protects against unauthorized retransmission of packets *(spoofing and MITM)*

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Security associations (SA)
- Security parameter index (SPI)
  - Value for correct SA
- Internet key exchange (IKE)
- ISAKAMP
- OAKLEY
- AH
- ESP

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Security associations (SA)
  - Each device as two
  - Send and receiving
  - Mitigates IP spoofing and MITA
  - Stored in SA data base with servers that have many SAs
- Security parameter index (SPI)
  - Value for correct SA

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Internet key exchange (IKE)
  - Used for secure key exchange to set up the SA
  - Based on , DH, Oakley and ISAKMP
  - Uses Certificates

ISAKAMP

  - Protocol used within a framework for establishing an SA

- OAKLEY
  - Protocol for authentication when using DH

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

AH

- Provides authentication
- Provides integrity
- ICV value changes for integrity, could create problems with NAT environments

ESP

- Encryption (entire payload and IP Header)
- Authentication
- Integrity

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

IPSEC can operate in two different modes

Tunnel mode or Transport mode –
Can work with ESP or AH
Tunnel is encrypted

- Gateway to gateway
- Client and gateway
- IPSEC header (AH or ESP) is inserted between the IP header and the upper layer protocol

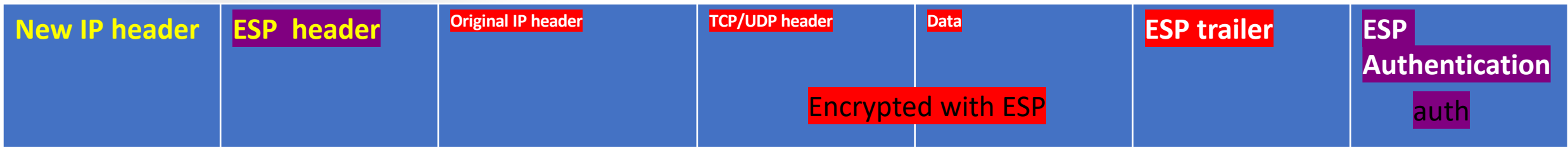
Transport Mode

- End to end communications
- Client and server
- Remote desktop
- Desktop to server

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Tunnel mode with ESP

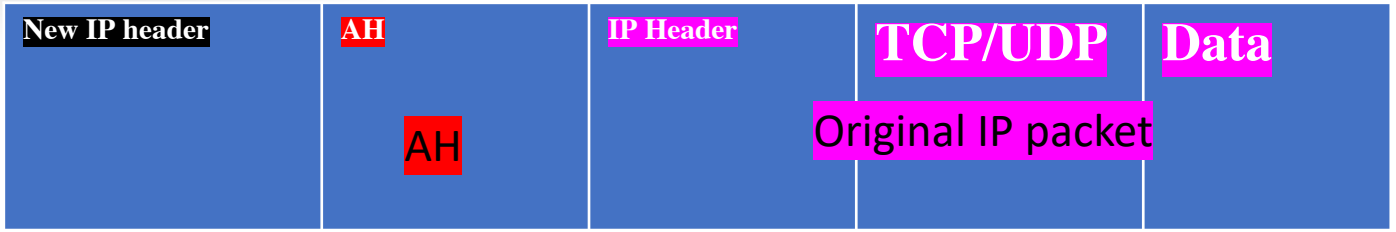
- Tunnel is encrypted
- Gateway to gateway
- Client and gateway
- IPSEC header (AH or ESP) is inserted between the IP header and the upper layer protocol



Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Tunnel mode with AH

- Does not protect entire packet
- AH protects everything that does not change in transit



Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Transport mode with ESP

Original header	ESP header	Original IP header	TCP/UDP header	Data	ESP trailer	ESP Authentication
			Encrypted with ESP			auth

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Transport mode with AH

Original header	AH header auth	IP header	TCP/UDP header	Data
		Original IP packet		

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Cryptanalysis: the study and practice of finding weaknesses, not just to fix, but where it is most effective (stream, block, etc.) *from the eyes of the bad guy)*

Cryptanalysis Resources

Time- the number of primitive operations that must be performed

Memory- amount of storage required to perform the attack

Data- amount of data of both plaintext and cipher text

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Social Engineering
- Frequency attacks
- Algebra Attacks
- Hash Attacks
- Collision Attacks
- Dictionary Attacks
- Brute force attacks
- Rainbow tables
- Plaintext only attacks
- Chosen Plane Text Attacks
- Cipher Text Only Attacks
  - Adaptive attacks
- Linear Attacks
- Differential Attacks
- Standards

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- **Social Engineering-** a form a trickery, attacking the human
- **Frequency analysis attacks-** frequency of letters, common letters, patterns repea**ting characters, "EE" , "OO"**
- **Algebra Attacks-** attacking the math, attacker goes atter the bits or arithmetic logic or algorithm
- **Hash Attacks –** Attacks that exploit weakness of hash algorithms to create collisions

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Dictionary Attacks
  - List of know passwords
  - Passwords stowed in the SAM-windows, hashed value windows\system32\config\sam

- Brute force attacks with dictionary and or pre commuted rainbow table
  - Use SALT

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

- Plaintext only attacks
  - An encrypted text and its plaintext is known. The goal is to determine the key
- Chosen Plane Text Attacks
  - attacker can freely choose a text that is to be encrypted and subsequently has access to the resulting encrypted text.

- Cipher Text Only Attacks
  - Only the encrypted text is known
- Adaptive attacks
  - Attacker has access to device and can modify results
- Linear Attacks
  - Looks for similarity in text
- Differential Attacks
  - Looks is differences in text

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

NIST - is responsible for developing cryptographic standards and guidelines for the protection of information for non-national security systems that are used the Federal Government

(Federal Information Processing Standards (FIPS) are a set of standards that document many encryption algorithms for use within non-military government agencies

Public Key Cryptography Standards (PKCS) are a group of public key cryptography standards developed and published by RSA

NSA participates in a lot of work, and with lost of classified work, with two suits and 4 types

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

FIPS 180-2: Secure Hash Algorithm (SHA-1)
FIPS 186: Digital Signatures
FIPS 197: AES
FIPS 141-3 used to approved cryptographic modules for HW and SW testing
FIPS 198: Hash-based Message Authentication Code (HMAC)
PKCS #1- RSA Cryptography Standard
PKCS #3- DH- Key Agreement Protocol
PKCS #14- PRNG

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

NSA

Suite A

- Not Published
- Classified
- Contains algorithms that will not be release
- Used to encrypt especially sensitive information , ECDSA, ECDH, SHA-256, SHA-384)

Suite B

- Published
- Includes various AES key sizes

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Type 1

- Used for classified or sensitive government information, to include crypto equipment

NSA certified Type 1 products

Type 2

Used for unclassified cryptographic equipment, *endorsed* by NSA

Type 3

- SBU, Examples include AES, 3DES, SHA
- Does not include National Security Systems

Type 4

Algorithms that are registered by NIST, but are NOT published by FIPS

Cryptographic Secure Channels, Defense Counter Measures, Cryptanalysis Attacks, and Standards

Conclusion Thanks for Joining us Dr. Hodges