UNIT 1

OSI Security Architecture

- ITU-T X.800 standard
- Internationally recognized
- Set of protocols, standards, techniques to ensure sec in env based on OSI.
- Deploy sec measures in org
- Systematic way of defining providing sec requirements at each layer
- 3 aspects: Attacks, Mechanisms, Services

Security Attacks

- Any action that compromises sec of info owned by org
- Infosec: How to prevent attacks (or detect) on info systems
- Threat = attack
- Two generic types: Passive, Active
- Passive
  - Attacker does not directly interact with data, network, parties
  - No modification of data
  - Gaining information
  - Parties unaware
  - Easier to perform, harder to detect
  - E.g. eavesdropping, replay, traffic analysis, MITM,
- Active
  - Attacker directly interacts with data, network, parties
  - Modification of data
  - Cause disruption
  - Harder to perform, easier to detect
  - E.g. modification, DoS, masquerading
- Confidentiality: Snooping, Traffic Analysis
- Integrity: Modification, Masquerading, Replaying, Repudiation
- Availability: DoS

Security Services

- Processes provided by system to protect resources
- Implement sec policies by utilizing mechanisms
- CIAAN (confi, inte, auth, access, non-repu)
- Confidentiality
  - Protection from passive attacks
  - Ensuring info is accessible only to those authorized
  - Prevent disclosure of info to unauthorized
  - Protection of traffic from analysis

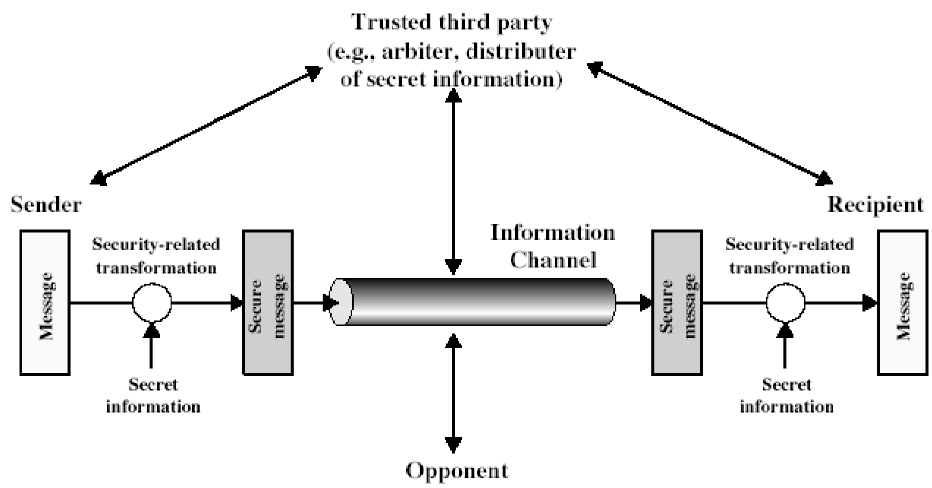
- Integrity
  - Data cannot be modified
  - Two types: connection-oriented, connectionless-oriented
  - Applied with or without recovery
- Authentication
  - Assure authentic communication
  - Peer entity auth: verify identity of peer entities (during establishment and transmission) involved, protection against masquerade
  - Data origin auth: authenticity of source of data, no protection against modification of data
- Access Control
  - Ability to control level of access entity has, how much info can they receive
  - Each entity trying to access must be auth
  - Rights tailored to individuals
- Non-Repudiation
  - Prevents entities from denying transmitted data
  - Without it, entity can deny that it did not send/receive data
  - E-commerce
- Availability
  - Property of resource being accessible (and usable) upon demand by authorized entity
  - Affected by variety of attacks

Security Mechanisms

- X.800 – those implemented by specific layer, those not specific to any service
- Specific
  - Encipherment: apply math algo for converting data (confidentiality, integrity, auth)
  - Digital Signature: append crypto data to data for proving source and integrity (integrity, auth, non-repu)
  - Access Control: enforcing access perms
  - Data Integrity
  - Auth Exchange: ensure identity of entity by info exchange (auth)
  - Traffic Padding: insert bits into gaps in stream countering traffic analysis
  - Routing Control: selection of secure routes (confidentiality)
  - Notarization: use of trusted third-party (non-repu)
- Pervasive (non-specific)
  - Trusted Functionality
  - Security Level
  - Event Detection

- Security Audit Trail
- Security Recovery

Model for Network Sec



- Data transmitted over network between parties
- Parties must cooperate for exchange
- Logical info channel established by defining route
- Use of protocols by parties
- Requirements
  - Design suitable algo for transformation
  - Generate secret info (keys) for algo
  - Develop methods to share secret info
  - Specify protocol to use transformation and secret info

Cryptography

- Terminology
  - Plaintext
  - Ciphertext
  - Cipher
  - Key
  - Encipher
  - Decipher
  - Cryptography
  - Cryptanalysis
  - Cryptology: cryptography + cryptanalysis
- Cryptography
  - Greek (concealed writing – kryptos graphia)

    - Science of transforming data to make it secure
    - Parties need unique cipher
    - Encryption needs: algo + key + plaintext
- Classified in 3 ways
    - Types of operations: substitution, transposition, product
    - Number of keys: single key, two-key
    - Way of processing plaintext: block, stream
- Cryptanalysis
    - Attempting to discover key or plaintext
    - Depends on nature of scheme used and info available
    - Cipher-text only
    - Known plaintext: CT and its PT
    - Chosen plaintext: Choose PT and generate CT
    - Chosen ciphertext: Choose CT and obtain PT

Symmetric Cipher Model

- Called conventional, single-key, private-key
- Share common key
- Classical algos
- Prior to 1970s
- Used for large data
- Same key for enc and dec (used in both directions)
- Requirements
    - Strong enc algo
    - Secret key
    - Known algo
    - Secure channel to distribute key
- Adv
    - Dec is reverse of enc
    - If enc is add + multi, then dec is div + sub
    - Efficient algos
    - Faster than asymmetric
- Disadv
    - Each pair needs unique key
    - N parties = n(n-1)/2 keys
    - Key distribution

Substitution Techniques

- Letters of plaintext are replaced by other letters/numbers/symbols

- If plaintext = bits, replace bit patterns with ciphertext bit patterns
- **Caesar Cipher**
  - Earliest known use of substi, in military
  - Julius Caesar
  - Replace each letter with letter 3 places further down
  - Shifting of letters by certain position (key = 3)
  - Wrap around if overflow
  - CT = E(PT) = (PT + k) mod 26
  - PT = D(CT) = (CT – k) mod 26
  - Only 26 possible ciphers
  - Simply broken by brute-force
- **Monoalphabetic Cipher**
  - Rather than shifting, jumble arbitrarily
  - Map each letter to different letter
  - Key length = 26
  - 26! possible keys (still not secure)
  - Human languages are redundant (letters not equally common)
  - Use frequencies of letters for cryptanalysis
- **Playfair Cipher**
  - Digram substi cipher
  - Used by British in WW-1 and Germans in WW-2
  - 5x5 matrix of letters based on key (25 letters)
  - I and J are combined
  - First fill letters of key (ignore duplicates)
  - Fill remaining letters of alphabet
  - Steps (enc and dec)
    i. Split plaintext (or ciphertext) into pairs of two letters (digraphs)
    ii. If letter left out, or same letter in a pair, use filler ‘X’
    iii. Process each pair
    iv. If both letters in same row, go to each letter’s right (left for dec) (wrap)
    v. If both letters in same column, go each letter’s bottom (top for dec) (wrap)
    vi. Else, replace each letter’s row and column intersection (in same order of PT)
  - Length of PT = Length of CT = even
  - More secure than monoalphabetic
  - 676 digrams
  - Can be broken, as follows same structure as plaintext
- **Polyalphabetic Cipher**
  - Each occurrence of character can have different substi
  - One to many mapping
  - Overcome weakness of freq analysis in monoalphabetic

- **Vigenere Cipher**
    - Blaise de Vigenere (16th century)
    - Uses successively shifted alphabets from 26x26 matrix (diff shift for each 26 letters)
    - Letters of key determine shifted alphabets used in enc and dec
    - Pad key to be same length as plaintext
    - row = key, column = plaintext, intersection = ciphertext
    - Breaking possible since reveals math principles
- **Vernam Cipher (One-Time-Pad)**
    - Gilbert Vernam (AT&T 1917)
    - Cannot be cracked, as uses one-time PSK
    - Length of PSK = Length of plaintext
    - Plaintext is paired with one-time PSK, therefore one-time-pad
    - plaintext + key = ciphertext
    - ciphertext – key = plaintext
    - Add corresponding letters of plaintext and key, subtract 26 if addition exceeds 26
    - Key discarded after use
    - Any message can be transformed into any cipher by a pad
    - Security depends on randomness of key
    - Disadv: key-stream as long as plaintext, key distribution, key management

Transposition Techniques

- Performing some sort of permutation on plaintext letters
- Characters retain plaintext form but change positions
- Characters interchanged according to key and algo
- Easily broken as letter frequencies are same as plaintext
- Can be more secure by performing multiple transpositions
- **Rail Fence Cipher**
    - Plaintext is written as sequence of diagonals, then read as rows
    - Rail depth = no. of rows/rails
    - Move downward diagonally letter-by-letter, after reaching last rail, continue upward diagonally
    -
- **Block (Single) Columnar Transposition**
    - Write plaintext letters in rows, read message column-wise
    - Key determines order of column combination

Steganography

- Science of hiding data in data
- No one other than parties know about existence of hidden data
- Replace bits of useless data
- Disadv
  - Lot of overhead for few bits
  - Useless after discovery of system

Block Ciphers

- Process messages in blocks
- Like substi on big characters
- Based on Feistel structure
  - Horst Feistel
  - Partition I/P block into two halves
  - Process through rounds
  - Perform substi on left
  - Perform round func on right and sub-key
  - Permutations swapping halves
- Confusion: make relationship b/w CT and key as complex as possible
- Diffusion: dissipate stat structure of PT over bulk CT
- P-Box
  - Permutation
  - Perform transposition at bit-level
  - Key and enc algo embedded in hardware
- S-Box
  - Substi
  - Perform substi at bit-level
  - Transpose mutated bits
  - 3 components: encoder, decoder, p-box

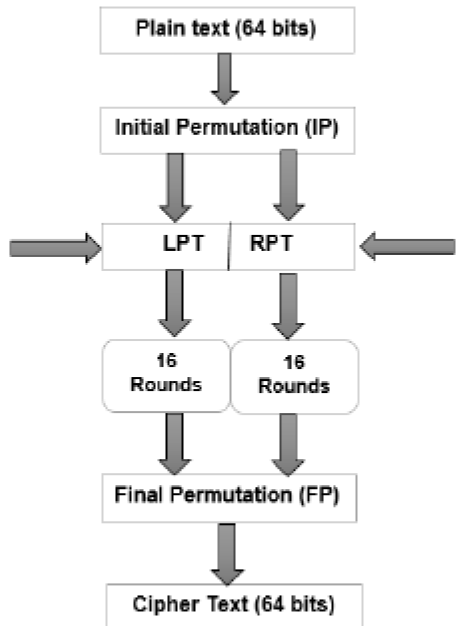
PKI

- Adv: no shared key, less number of keys 10 users = 20 keys, efficient for short messages
- Disadv: complex algo, association b/w entity and public key must be verified

DES

- Most widely used block
- NIST 1977

- Enc 64-bit data using 56-bit key
- Deprecated as short key



- Steps
    - Permute PT block and divide
    - Halves undergo rounds of ops
    - XOR b/w expanded right PT and compressed 48-bit key
    - Send output to S-box
    - XOR output and left PT and store in right PT
    - Forward both halves to next round
    - Swap left and right at last round
    - Apply IP to get CT
- Avalanche effect
    - Desirable property of algo
    - Change in one bit causes approx half output to change
    - Strong for DES

3DES

- 3 rounds of DES
- 3 keys generated using KDF
- PT subjected to IP
- PT enc 3 times, each time diff key
- FP applied to produce CT

AES

- Replacement for DES
- 128-bit data, key size = 128, 192, 256
- Key expansion: Round keys derived from cipher key using Rijndael key schedule
- Enc Steps **(ASS-M-ASS-A)**
    - Initial Round
        - Add Round Key: 128 bits of state XORed with 128 bits of round key
    - Main Round (enc)
        - Sub Bytes: Each byte of current state substi by entry in S-box, first digit -> row, second -> column
        - Shift Rows: Transposition, 4 rows shifted cyclically to left by offsets from 0 to 3
        - Mix Columns: Linear mixing op, multiply state against fixed matrix
        - Add Round Key
    - Final Round
        - Sub Bytes
        - Shift Rows
        - Add Round Key
- Dec Steps **(ASS-M-ASS-A)**
    - Initial Round
        - Add Round Key
    - Main Round (dec)
        - Inv Shift Rows
        - Inv Sub Bytes
        - Inv Mix Columns
        - Add Round Key
    - Final Round
        - Inv Shift Rows
        - Inv Sub Bytes
        - Add Round Key

RSA

- Steps
    - Two primes p and q
    - N = p * q
    - T(n) = (p-1) * (q-1)
    - Choose e, such that GCD(e, T(n)) = 1
    - Choose d, such that (d * e) mod T(n) = 1

d = (1 + k * T(n)) / e
k = 0,1,2.. and d is whole no.
  - Public key = {e, n}
  - Private key = {d, n}
- M = message
- CT = (m^e) mod n
- PT = (CT^d) mod n

DH

- Large prime q
- Choose A such that A is primitive root of q
  A^1 mod q, A^2 mod q, A^q-1 mod q = 0 to q (random order)
- Assume Xa (a private key), Xa < q
- Assume Ya (a public key), Ya < q
- Ya = A^Xa mod q
- Same for B
- Shared key (A) = Yb ^ Xa mod q
- Shared key (B) = Ya ^ Xb mod q

UNIT 2

Secure Programs

- Earlier based on penetrate and patch (done by tiger team)
- Considered proof of security if system withstood
- Pressure on specific problem led to a narrow focus on fault and not its context
- Attention on immediate cause and not underlying faults
- Fixing one caused failure somewhere else

Types of Flaws

- Landwehr divides into
  - Intentional (malicious, non-malicious)
  - Inadvertent (validation, domain, serialization, inadequate auth, boundary conditions, logic)
- Design flaws (processor design: floating point in Intel Pentium)
- Program flaws (application, system, side-channel attacks)
- Human factors (phishing, social eng)

- Hardware flaws (hardware trojans, distribution attacks)

Buffer Overflows

- Buffer: space in memory for holding data temporarily
- Finite capacity
- Dev must declare max size so compiler allocates (e.g. char sample[10] allocates 10 bytes)
- When more data tries to be allocated to buffer (exceeds), data leaks into other buffers
- Overwrite adjacent memory
- Extra overflown data may contain specific instructions, purposefully chosen by attacker, to execute arbitrary code
- E.g. pour 2L in 1L jug
- Heap-based: malloc and free
- Stack-based: ESP, EBP, EIP, ESI, EDI

Incomplete Mediation

- Refers to sec vuln occurring when app does not validate all I/P
- Allows attacker to bypass controls, gain access to data
- Injections, XSS
- Whitelist or blacklist
- Manipulate params
- Directory traversal

Brain Virus

- Basit and Amjad Farooq Alvi in 1986, computer store in Lahore, Pakistan
- Boot sector virus: area read by BIOS, when computer starts
- Spread when users infected systems by booting from infected disks
- Not to cause harm, rather to protect medical software from being copied
- One of the first self-replicating viruses
- Replaced boot sector with its own code
- Code checked presence of virus, if absent it would copy itself to boot sector and infect disks used on computer
- Stealth virus: hide from AV detection
- Prevent: AV, email filter, IDS, user training

Internet (Morris) Worm

- Designed to spread on UNIX
- Log on to remote host as user by cracking local password file (assuming multiple users used same password)
- Ran each account name and permutations, with 432 built-in passwords and all words in directory
- Exploited finger protocol
- Exploited trapdoor in debug option of remote process
- If successful, communicated with OS command interpreter

Web Bugs (Beacon)

- Simple 1x1 overlay added to HTML
- Track user activity (viewing time, IP address, browser info)
- Spread through email attachments
- Propagated as GIF

Trapdoors

- Secret (undocumented) entry point
- Gain access without usual auth/procedures
- Difficult to detect
- Only known to dev as inserted during coding

Salami Attack

- Merge bits of inconsequential data to yield powerful results
- Name: manner in which odd bits of meat combined to make salami or sausage
- Financial crimes
- Salami slicing: steal negligibly small amount from many accounts
- Penny shaving: round transactions to closes decimal

Development Controls

- Secure coding practices integrated into SDLC
- Mitigate vulnerabilities
- Collaborative effort
- Regular requirement: “do X”, security requirement: “do X and nothing more”

- Phases: Req specification, design, implementation, testing, documenting, review, deployment, maintenance
- RBAC or ABAC
- Secure config baselines
- Modularity: self-contained, isolated, problem tracing, single-purpose, independent
- High cohesion
- Low coupling (degree of independence)
- Encapsulation: hide implementation, limited sharing
- Data Hiding: only input-output should be visible, conceal internal structure

Peer Reviews

- Devs review each other's code for vuln
- Helpful for identifing vulns missed by individual devs

Hazard Analysis

- Identifying and assessing potential hazards in system
- Identify sec hazards and develop controls to mitigate
- HAZOP (hazard and operability studies): brainstorm hazard and consequence
- FMEA (failure modes and effects analysis): identify and analyze potential failures and effects
- FTA (fault tree analysis): model logical relationships between failures

UNIT 4

PGP

- Provides confi and auth service for email and file storage
- Phil Zimmermann, selected best algos and integrated
- Independent of gov orgs
- **Authentication (digital signature)**
    - Sender hashes message using SHA-1 (160-bits)
    - Hash is encrypted using RSA (sender private)
    - Encrypted hash attached to message and sent
    - Receiver receives message + encrypted hash
    - Received decrypts using RSA (sender public)
    - Receiver hashes message
    - Decrypted hash and receiver's hash compared

- **Confidentiality (encryption)**
  - Sender generates session key
  - Sender encrypts message using key (AES, IDEA, CAST-128, 3DES0
  - Sender encrypts session key using RSA (receiver public)
  - Encrypted session key attached to encrypted message and sent
  - Receiver receives encrypted session key + encrypted message
  - Receiver decrypts session key using RSA (receiver private)
  - Receiver decrypts message using decrypted session key
  - (provides no assurance to receiver the identity of sender, no auth)
- **Confidentiality + Authentication (digital sign + enc)**
  - Sender generates session key
  - Sender hashes message
  - Sender encrypts hash using RSA (sender private)
  - Encrypted hash + message = blob
  - Sender encrypts blob using session key
  - Sender encrypts session key using RSA (receiver public)
  - Sender combines encrypted session key + blob (encrypted hash + message) and sends
  - Receiver receives encrypted session key + blob
  - Receiver decrypts session key using RSA (receiver private)
  - Receiver decrypts blob (encrypted hash + message) using decrypted session key
  - Receiver decrypts hash using RSA (sender public)
  - Receiver hashes message
  - Hashes are compared
- **Compression**
  - PGP compresses message after signature before enc
  - Sign -> compress -> enc
  - Saves space for email and file storage
  - Enc after compression to strengthen cryptographic sec
- **Email Compatibility**
  - Least part of transmitted block is enc (arbitrary stream of octets)
  - Email only allow ASCII
  - Convert raw 8-bit stream to printable ASCII
  - Uses radix-64 conversion
  - Each 3-octet group is mapped to 4 ASCII
  - Appends CRC
  - Expands message by 33%
- **Segmentation/Reassembly**
  - Email often restricted length e.g. 50k octets
  - Subdivide message into segments small enough for being allowed
  - Done after all other processing (at the end)

    - Reassembly at receiver is required before verifying sign or dec (as key and sign are in first segment)
- Message Format
    - Three components: message, signature, session key
    - Message: data, filename, creation timestamp
    - Signature: creation timestamp, message digest, leading 2-octets, key ID of sender public key
    - Session key: session key, key ID of receiver public key

S/MIME (Secure Multipurpose Internet Mail Extension)

- Enhancement to MIME format standard
- MIME
    - Extension to RFC822
    - Address limitations of SMTP and RFC822 (binary exec files converted to ASCII, text limited to 7-bit ASCII, server reject large mails)
    - <u>5 Header Fields</u>: MIME-Version (1.0), Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description
    - <u>Content Types</u>: plaintext (ASCII or ISO 8859), multipart (image, video, audio, app)
    - <u>Transfer Encoding</u>: 7-bit, 8-bit, binary, printable, base64, x-token
- Enveloped data (enc content + enc content-enc key)
- Signed data (enc hash using sender private, enc hash + message encoded in base64)
- Clear-signed data (enc hash using sender private, encoded in base64)
- Signed and enveloped data (hash enc data, or enc hashed data)

Overview of IPSec

- Framework of open standards for protection comms over IP through cryptographic sec services
- Supports network-level peer auth, data origin auth, integrity, conf, replay protection
- Need: CERT in 2001 reported 52k attacks IP spoofing, packet sniffing
- Applications
    - Branch office connectivity
    - Remote access
    - Extranet and internet connectivity
    - E-commerce
- Operate in router, firewall connecting LANs to outside
- Typically, enc + compress traffic going to WAN, reverse for going to LAN

- Benefits
    - Firewall resistant to bypass
    - Transparent to end users
    - Below transport layer, transparent to apps
    - Sec for individual users

IPSec Architecture

- IPSec Documents
    - Nov 1998
    - RFC 2401, 2, 6, 8
    - Mandatory support for IPv6, optional for 4
    - Sec features implemented as extension headers following main IP header
    - Extension header for auth is AH, enc is ESP
    - Additional drafts published by IETF, IPsec protocol working group
    - Documents divided into: arch, ESP, AH, enc algo, auth algo, key management, DOI
- IPSec Services
    - Two protocols (AH and ESP) for sec at IP level
    - Connectionless integrity
    - Access control
    - Conf
    - Replay detection
    - Traffic info conf
- Security Associations (SA)
    - Specify protocol to be used
    - DB record specifying params controlling sec ops
    - Referenced by sender, established by receiver
    - One direction only, two Sas for bidirectional
    - Identified by 3 params
        - SPI (sec param index): bit string assigned to SA, enable receiver to select SA for processing
        - Dest IP: Only unicast, may be user or firewall or router
        - Sec Protocol ID: AH or ESP
    - Params
        - Seq num counter: 32-bit to generate seq num in AH or ESP
        - Seq counter overflow
        - Anti replay window: determined if replay or no
        - AH info
        - ESP info
        - Lifetime
        - IPsec protocol mode: tunnel, transport or wildcard
        - MTU

    - Transport mode: IPsec header inserted after IP header, containing sec info, used in E2E comms if IP header not protected
    - Tunnel mode: Entire IP packet encapsulated in IPsec body, with own header, no routers can check content

Authentication Header

- Support for integ and auth of IP packets
- Integ ensured undetected modification in transit is not possible
- Auth enables system to auth user and filter traffic
- Prevent spoofing and replay attack
- Auth based on MAC, parties must share key
- Fields
    - Next header
    - Payload length
    - Reserved
    - SPI
    - Seq Num
    - Auth data
- Anti-Replay
    - Use Seq Num field
    - Sender initializes to 0 when new SA established
    - Each packet sent on SA, inc by 1
    - Max is 2^32 – 1
    - Receiver should receive window of size W (default 64)
    - Right-edge highest seq num N received till now
    - Packet with seq num N-W+1 to N correctly received is marked
    - If received packet in window and new, check MAC, if correct, mark
    - If received packet to right of window and new, check MAC, if correct, shift window to its right edge and mark
    - If received packet to left of window or auth fails, discard
- Integrity Check Value
    - Value in auth data of AH or ESP
    - Determine modifications made to data
    - Also called MAC (MD5 and SHA-1 implemented with HMAC)
- Transport Mode AH
    - AH inserted after original IP header before IP payload
    - Auth covers entire packet excluding mutable fields
- Tunner Mode AH
    - Entire original IP packet is auth
    - AH inserted between original IP header and new outer IP header
    - Inner IP header contains true source and dest IP

    - Outer IP header may contain different (firewall, router, etc.)
    - Entire inner packet is protected by AH
    - Outer IP header is protected except mutable fields

Encapsulating Security Payload

- Fields
    - SPI
    - Seq Num
    - Payload Data
    - Padding
    - Pad length
    - Next header
    - Auth data
- Transport Mode ESP
- Tunnel Mode ESP

Combination of SAs

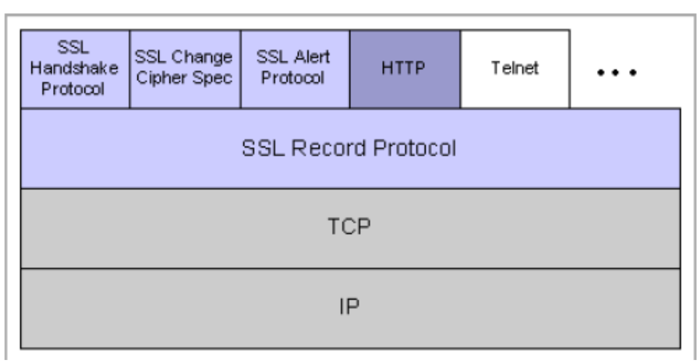
- IPsec arch doc lists 4 combinations
- Combinations must be supported by compliant IPsec hosts
    - Case 1
        - Sec provided b/w all systems implementing IPsec
        - Parties must share appropriate keys
        - Transport AH, Transport ESP, ESP followed by Transport AH
        - Any one inside Tunnel AH/ESP
    - Case 2
        - Sec provided b/w gateways and no hosts implementing IPsec
        - Simple VPN
        - Only single tunnel SA
        - Nested tunnels not req as services apply to inner packet
    - Case 3
        - Similar but provides sec even to nodes
        - Two tunnels (gateway-to-gateway, node-to-node)
        - Auth or enc or both provided using G2G
        - Additional service provided by N2N
    - Case 4
        - Suitable for remote users
        - One tunnel needed b/w remote user and org firewall

Key Management

- Determination and distribution of keys
- Two types: Manual and Automated
- Default automated is ISAKMP/Oakley
    - Oakley: key exchange protocol based on DH but added sec, no specific formats
    - Internet SA and Key Management Protocol: provides framework for IKM and provides protocol support
- Oakley Key Determination Protocol
    - Refinement of DH
    - Limitations of DH: MITM, no identity info, computationally intensive
    - Cookies to prevent attacks
    - Enables two parties to nego group (specify global DH param)
    - Nonces to prevent replay
    - Auth DH to prevent MITM
    - Cookie exchange: send pseudorandom num, cookie in initial exchange, which is ack
    - Supports use of diff groups for DH
- ISAKMP
    - Defines formats to nego SAs
    - Must follow UDP
    - Header followed by payloads

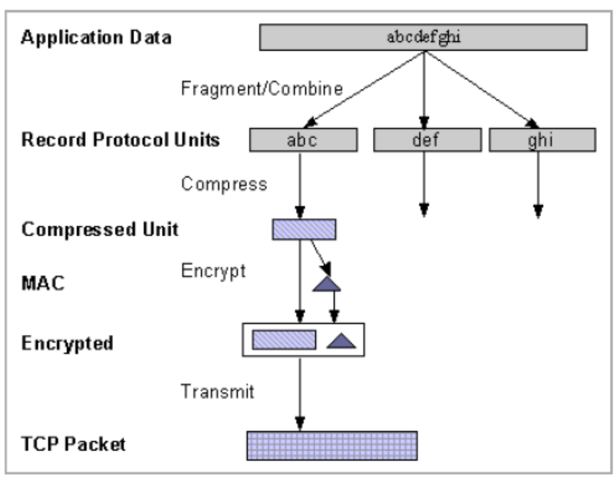
SSL/TLS

- Netscape to provide sec in transmission on Internet
- SSL is protocol layer may be placed b/w network and app layer
- Provides secure comms by allowing mutual auth, use of DS for integ, enc for privacy
- SSL 3 has support for cert chain loading, basis for TLS
- SSL is two layers of protocols



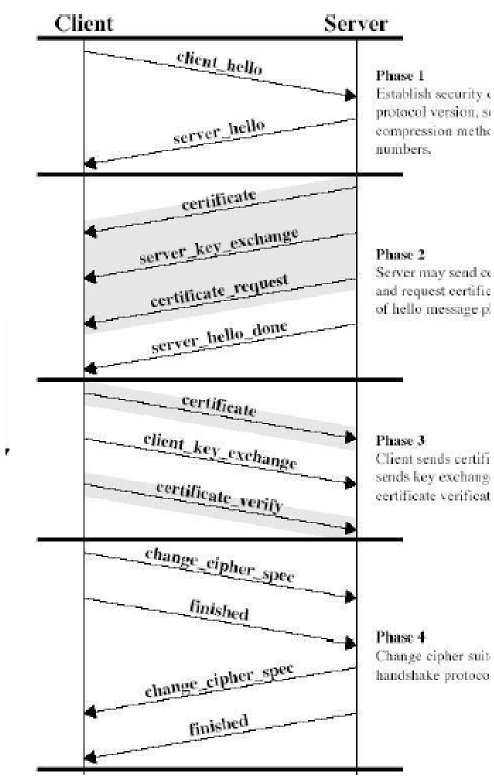
- Connection: transport providing suitable service. For TLS, P2P relationships. Each is associated to one session

- Session: Association b/w client-server. Created by handshake protocol. Define set of crypto sec params, shared among multi connections. To avoid expensive nego of new sec params for each connection.
- Sessions are stateful, defined by
  - Session ID: chosen by server
  - Peer cert: X509 cert of peer
  - Compression method
  - Cipher spec: bulk enc algo + hash algo + params (hash size)
  - Master secret
  - Resumable
  - Client-server random
  - Server-write MAC secret
  - Client-write MAC secret
  - Server-write key
  - Client-write key
  - IVs: init by handshake protocol
  - Seq nums: max 2^64 -1
- SSL Record Protocol
  - Provides two services: Confi, Integ
  - Takes message, fragments into blocks, compress, apply MAC, add header, transmit in TCP segment
  - Received, decrypted, verified, decompressed, reassembled, delivered to user



  - Header consists of: Content Type, Major Version, Minor version, Compressed Length
- SSL Change Cipher Spec Protocol
  - Uses SSL record protocol
  - Single message of single byte of value 1
  - Causes pending state to be copied to current state
  - Updated cipher suite for connection

- SSL Alert Protocol
    - Convey related alerts to peer entity
    - Message consists of 2 bytes (byte 1 – value warning or fatal, terminates if fatal, byte 2 – code for specific alert)
    - Fatal alerts: unexpected_message, bad_record_mac, decompression_failure, handshake_failure, illegal_parameter, close_notify, bad_certificate, unsupported_certificate, certificate_revoked, certificate_expired, certificate_unknown
- SSL Handshake Protocol
    - Establishment of reliable session b/w client-server
    - Allows client-server to auth each other, nego enc and MAC algos, nego keys
    - Message Fields
        - Type
        - Length
        - Content
    - Phases (CS-CSCS-CCC-CFCF)
        - Establish Sec Capabilities
        - Server Auth and Key Exchange
        - Client Auth and Key Exchange
        - Finish



TLS

- RFC2246
- Protocol for establishing sec conn b/w client-server
- Capable of auth client-server
- Used by HTTP, IMAP, POP3, SMTP
- TLS Handshake Protocol: nego key exchange using asymmetric algo
- TLS Record Protocol: opens enc channel using symmetric algo

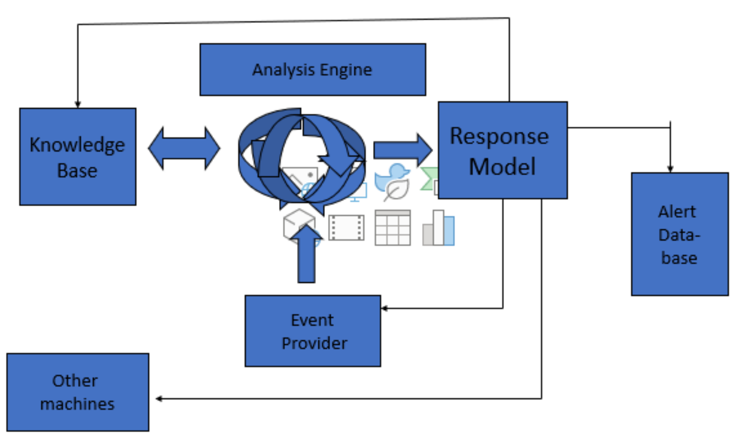
Intruders

- Entities attempting to break into system (potential misuse)
- May be from outside network or legitimate users (inside)
- Physical, system, or remote

Intrusion Techniques

- Buffer overflows
- Unexpected combinations
- Unhandled input
- Race conditions
- Phishing
- Pretexting
- Zero-day
- Injections
- DoS
- Physical Theft

Intrusion Detection

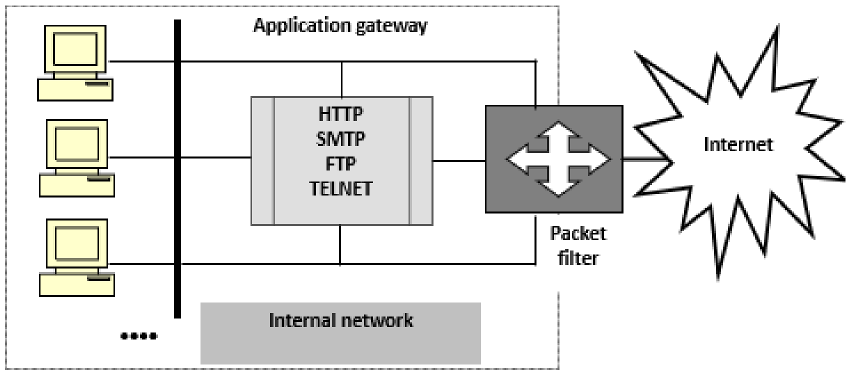


- IDS
    - Monitor system/network activities
    - Passive in nature
    - Detect malicious activities, alert admins
    - Assist in IR
    - Improve sec posture
    - Helps in compliance and auditing
- Anomaly-Based
    - Model normal usage (set baseline) as noise characterization
    - Activities deviating from baseline are flagged
    - Recognizes new attacks
    - Disadv: False positives
- Signature-Based
    - Matched description of attacked system with sensed (current) description
    - Interpret certain piece of data as attack
    - Match from DB
    - Simple pattern matching algo
    - Diadv: Cannot detect new attacks, false positives, update for every new pattern
- Host-based
    - Detect from sys/app logs
    - Analyze logs for trails of intrusion
    - Adv: verifies attack, system specific, monitor key components, real-time, no additional hardware
    - Disadv: Trained model (need experience) for detection
- Stack-based
    - Integrated with TCP/IP stack
    - Watch packets travelling through layers
    - Pull packets from stack before system can process
- Network-based
    - Look for signatures in network traffic
    - Promiscuous interface
    - Filter applied before attack recognition
    - Adv: Packet analysis, reduced cost, real-time, platform independent

Firewall Design Principles

- Firewall
    - Guard network by standing b/w inside and outside network
    - Special router
    - Controls transmission (decides allow/not allow)
    - Single choke point for protection

    - Convenient for NAT, logging (non-sec features)
    - Serve as platform for IPsec (VPNs)
- Techniques to implement policies
    - Service control (type of service that can be accessed)
    - Direction control (direction of allowed requests)
    - User control (which user is attempting access)
    - Behavior control (how services are used, email)
- Disadv: no protection against internal attack
- **Screened Host FW, Single Homed Bastion**



    - Firewalls has packet filter router and AG
    - Filter assures incoming is destined for AG
    - Examines dest IP of packets
    - Ensures outgoing is coming from AG
    - Increases sec as checking at app and packet level
    - More flexible for admins
    - Granular sec policies
    - Disadv: compromised filter exposes whole network, internal user connects to AG and filter
- **Screened Host FW, Dual Homed Bastion**
    - Improvement over single-homed
    - Connections to internal user and filter are removed
    - User only connected to AG which is only connected to filter
    - Compromised filter only exposes AG
- **Screened Subnet Firewall**
    - Highest sec
    - Two packet filters (one b/w outside network-AG, another b/w AG-internal network)
    - Three levels
- **DMZ**
    - Popular
    - Arrangement of firewalls
    - If org has servers that need to available to outside network (mail, web, ftp)

    - Three interfaces: one to internal private, one to external public, one to public servers (DMZ)

Types of Firewalls

- Packet Filters
    - Set of rules applied to each packet
    - Outcome decides discard/accept
    - Screening router/filter
    - Filter packets going in either direction
    - Rules on: headers, source IP, dest IP, port numbers
    - If no match, take default action
    - Discard all or accept all (not single)
    - Adv: simple, user unaware
    - Disadv: setup rules, lack of auth
    - Attacks: IP spoofing, source routing, fragmentation
    - Advancements: dynamic (stateful) filter, examines based on current state, adapts itself, custom dynamic rules
- Application Gateways
    - Proxy server
    - Decides flow of app traffic
    - User contacts app gateway (HTTP, SMTP, FTP telnet/rlogin)
    - Asks which remote user to setup connection for
    - Auth using ID-pass
    - AG accesses remote host instead of user (proxy)
    - Circuit Gateway
        - Additional functions on AG
        - Creates connection between remote host and AG
        - User unaware, thinks direct connection to remote host
        - CG changes source and dest IP (acts as middleman)
    - Adv: better than filters, auth instead of rule-matching
    - Disadv: Overhead in connections
    - AG = Bastion host