Network Security

Created by Omar Alkhateeb

For more MindMaps
Check our Blitz Website
https://blitz.develpix.com/

IP Security

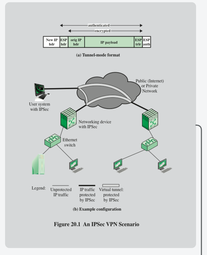


Figure 20.1 An IPSec VPN Scenario

- **Transport** Mode
  - Provides protection primarily for upper-layer protocols
    - include a TCP or UDP segment or an ICMP packet
  - used for end-to-end communication between two hosts
  - **ESP** (**E**ncapsulating **S**ecurity **P**ayload) in transport mode encrypts and optionally authenticates the IP payload but not the IP header
  - **AH** (**A**uthentication **H**eader) in transport mode authenticates the IP payload and selected portions of the IP header
- **Tunnel** Mode
  - Provides protection to the entire IP packet
  - Used when one or both ends of a **S**ecurity **A**ssociation (**SA**) are a security gateway
    - may engage in secure communications without implementing IPsec
  - number of hosts on networks behind firewalls
  - ESP in tunnel mode encrypts and optionally authenticates the **entire** inner IP packet, including the inner IP header
  - AH in tunnel mode authenticates the **entire** inner IP packet and selected portions of the outer IP header

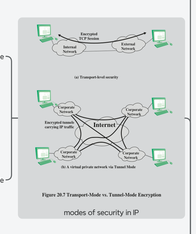


Figure 20.7 Transport-Mode vs. Tunnel-Mode Encryption

modes of security in IP

- **Security Association** (**SA**)
  - **definition**
    - one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it
  - In any IP packet
    - the SA is uniquely identified by the Destination Address in the IPv4 or IPv6 header
      - and the SPI in the enclosed extension header (AH or ESP)
  - identified by **three** parameters
    - **S**ecurity **P**arameters **I**ndex (**SPI**)
      - 32-bit unsigned integer assigned to this SA and having local significance only
    - **Security protocol identifier**
      - Indicates whether the association is an AH or ESP security association
    - **IP Destination Address**
      - Address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router
- **S**ecurity **A**ssociation **D**atabase (**SAD**)
  - Defines the parameters associated with each SA
    - Security parameter index
    - Sequence number counter
    - Sequence counter overflow
    - Anti-replay window
    - AH information
    - ESP information
    - Lifetime of this security association
    - IPsec protocol mode
    - Path MTU
- **E**ncapsulating **S**ecurity **P**ayload (**ESP**)
  - what is it?
    - Used to **encrypt**
      - Payload Data
      - **Padding**
        - Padding field serves several purposes
          - the Padding field is used to expand the plaintext to the required length
          - plaintext to be a multiple of some number of bytes
          - Note: If the algorithm requires cryptographic synchronization data then these data may be carried explicitly at the beginning of the Payload Data field
      - Pad Length
      - Next Header fields
    - **ICV** (**I**ntegrity **C**heck **V**alue)
      - computed after the encryption is performed
      - an optional ICV field is present only if the integrity service is selected
      - and is provided by either
        - a separate integrity algorithm
        - or a combined mode algorithm that uses an ICV

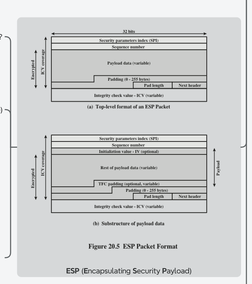


Figure 20.5 ESP Packet Format

ESP (Encapsulating Security Payload)

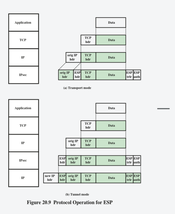


Figure 20.9 Protocol Operation for ESP

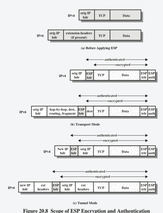


Figure 20.8 Scope of ESP Encryption and Authentication

- **Internet Key Exchange**
  - The key management portion of IPsec involves the determination and distribution of secret keys
  - A typical requirement is **four keys** for communication between two applications
    - Transmit and receive pairs for both integrity and confidentiality
  - can be
    - **Manual**
      - system administrator manually configures each system with its own keys and with the keys of other communicating systems
      - This is practical for small, relatively static environments
    - **Automated**
      - Enables the on-demand creation of keys for SAs
      - and facilitates the use of keys in a large distributed system with an evolving configuration

TLS (Transport-Layer Security)

- Properties of TLS
  - One of the most widely used security services
  - Defined in RFC 5246
  - Is an Internet standard that evolved from a commercial protocol known as **S**ecure **S**ockets **L**ayer (**SSL**)
    - Is a general purpose service implemented as a set of protocols that rely on TCP
  - Could be provided as part of the underlying protocol suite
    - and therefore be transparent to applications
  - Can be embedded in specific packages
  - Most browsers come equipped with TLS
    - and most Web servers have implemented the protocol

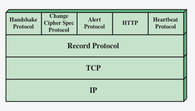
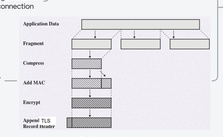


Figure 17.2 SSL/TLS Protocol Stack

Figure 17.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

- **TLS Architecture**
  - Two important TLS concepts
    - TLS **connection**
      - A transport that provides a suitable type of **service**
      - For TLS such connections are **peer-to-peer** relationships
      - Connections are **transient**
      - Every connection is associated with **one session**
    - TLS **session**
      - An association between a **client** and a **server**
      - Created by the **Handshake** Protocol
      - Define a set of cryptographic **security parameters**
        - which can be shared among **multiple connections**
      - Are used to **avoid** the expensive negotiation of new security parameters for each connection



TLS **Record** Protocol

- Protocol provides two services for TLS connections
  - **Confidentiality**
    - Handshake Protocol defines a shared secret key that is used for conventional encryption of TLS payloads
  - **Message integrity**
    - The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC)

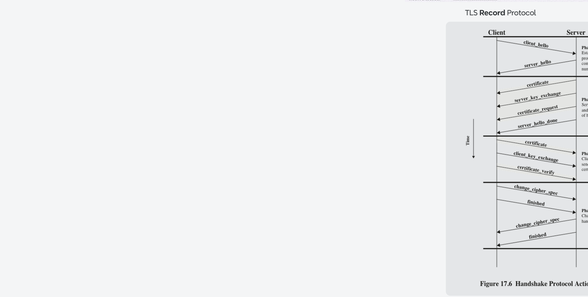


Figure 17.6 Handshake Protocol Action

- **Remote User-Authentication Principles**
  - **definition**
    - The process of verifying an identity claimed by or for a system entity
  - consists of **two steps**
    - Identification step
      - Presenting an identifier to the security system
    - Verification step
      - Presenting or generating authentication information
        - that corroborates the binding between the entity and the identifier

Authentication Architecture Model

- **Means of User Authentication**
  - Something the individual **knows**
    - Password
    - Pin
    - answers to questions
  - Something the individual **possesses**
    - cryptographic keys
    - electronic keycards
    - smart cards
    - physical keys
  - Something the individual **is** (static biometrics)
    - fingerprint
    - retina
    - face
  - Something the individual **does** (dynamic biometrics)
    - voice pattern
    - handwriting characteristics
  - can be used alone or in combination
    - but network-based user authentication
      - methods involve cryptographic keys and something the individual knows
      - like a password

User Authentication

- **Kerberos**
  - **definition**
    - term for managing access to a network
    - Authenticates users logging into the network
      - and determines what data they can access and actions they can perform
    - Also examines the health of the user's computer or mobile device
  - **Elements** of a **NAC** System
    - Subtopic 1 — **Access requester (AR)**
    - **Policy server**
      - Determines what access should be granted
      - Often relies on backend systems
    - **Network access server (NAS)**
      - Functions as an access control point for users in remote locations
        - connecting to an enterprise's internal network
      - aka
        - Media Gateway
        - Remote Access Server (**RAS**)
        - **policy server**
      - May include its own authentication services or rely on a separate authentication service from the policy server
  - Network Access **Enforcement Methods**
    - IEEE 802.1X
    - Virtual local area networks (VLANs)
      - applied to regulate access to the enterprise network
    - Firewall
    - DHCP management

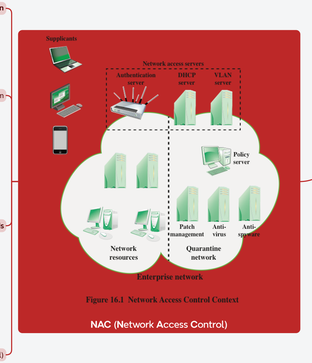


Figure 16.1 Network Access Control Context

NAC (Network Access Control)

- **EAP** (**E**xtensible **A**uthentication **P**rotocol)
  - provides a **generic** transport service
    - for the exchange of authentication information between a client system and an authentication server
  - supported EAP Methods
    - Transport Layer Security
    - Tunneled TLS
    - Generalized Pre-Shared Key
    - IKEv2

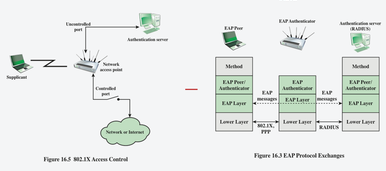


Figure 16.5 802.1X Access Control

Figure 16.3 EAP Protocol Exchanges

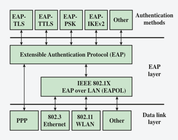


Figure 16.2 EAP Layered Context

- **Kerberos**
  - **V4**
    - make use of **DES**
    - it consists of
      - **Authentication Server**
        - Knows the passwords of all users and stores these in a centralized database
        - Shares a unique secret key with each server
      - **Ticket**
        - Created once the AS accepts the user as authentic
        - contains the user's ID and network address and the server's ID
      - **Ticket-granting server**
        - Issues tickets to users who have been authenticated to AS
        - Each time the user requires access to a new service the client applies to the TGS using the ticket to authenticate itself
        - The TGS then grants a ticket for the particular service
        - and uses it to authenticate its user to a server each time a particular service is requested
          - The client saves each service-granting ticket

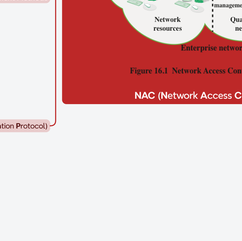


Figure 15.2 Overview of Kerberos

Kerberos

- **Realms**
  - usually
    - full-service Kerberos environment consisting of
      - Kerberos server
      - number of clients
      - number of application servers
    - require that
      - Kerberos server must have the user ID and hashed passwords of all participating users in its database
        - all users are registered with the Kerberos server
      - server must share a secret key with each server
        - all servers are registered with the Kerberos server
      - server in each interoperating realm shares a secret key with the server in the other realm
        - the two Kerberos servers are registered with each other
  - The database resides on the **Kerberos Master Computer System**
    - which should be kept in a **physically** secure room
    - set of managed nodes that share the same **Kerberos database**
    - but the **realm** has the following properties
      - **read-only copy** of the Kerberos database might also reside on other Kerberos computer systems
      - All changes to the database must be made on the master computer system
      - Changing or accessing the contents of a Kerberos database requires the Kerberos **master password**

Figure 15.4 Request for Service in Another Realm

- **Federated Identity Management**
  - use of a common identity management scheme
    - across multiple enterprise and numerous applications and supporting many users
  - services provided including
    - Point of contact
    - SSO protocol services
    - Trust services
    - Key services
    - Identity services
    - Authorization
    - Provisioning
    - Management

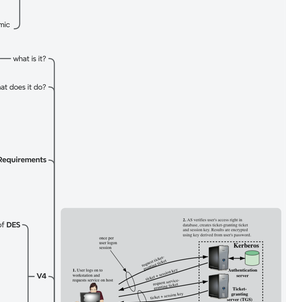


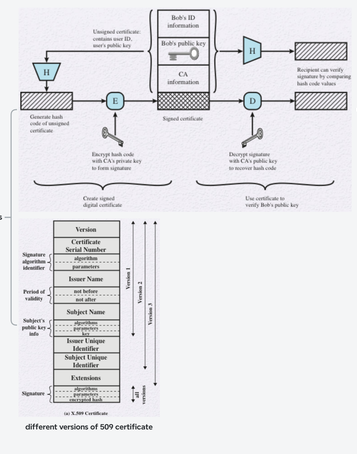
Figure 15.6 Federated Identity Operation

Federated Identity Management

- Key Standards and components used in auth.
  - **XML** (**E**xtensible **M**arkup **L**anguage)
    - uses sets of embedded tags or labels to characterize text elements within a document
  - **SOAP** (**S**imple **O**bject **A**ccess **P**rotocol)
    - Enables applications to request services from one another
      - using XML format
  - **WS Security**
    - set of SOAP extensions for implementing message integrity and confidentiality in **W**eb **S**ervices
  - **SAML** (**S**ecurity **A**ssertion **M**arkup **L**anguage)
    - An XML-based language for the exchange of security information

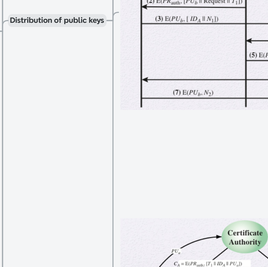
Key Management and Distribution

- Distribution of public keys
  - Public-key authority
  - Public-key certificates
    - use of it



different versions of 509 certificate

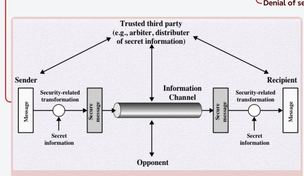
- Obtaining a certificate
  - User certificates generated by a CA have the following characteristics
    - Any user with access to the public key of the CA can verify the user public key that was certified
    - No party other than the certification authority can modify the certificate without this being detected
  - Because certificates are unforgeable
    - they can be placed in a directory without the need for the directory to make special efforts to protect them
    - a user can transmit his or her certificate directly to other users
- Certificate Revocation
  - Each certificate includes a period of validity
  - Typically
    - a new certificate is issued just before the expiration of the old one
  - It may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons
    - The user's private key is assumed to be compromised
    - The user is no longer certified by this CA
    - The CA's certificate is assumed to be compromised
  - Each CA must maintain a list consisting of all revoked but not expired certificates issued by that CA
    - These lists should be posted on the directory



PKIX Architecture model

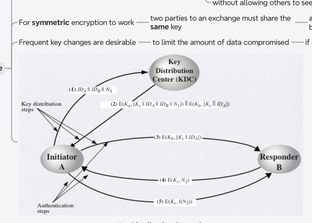
Concepts

- **Cryptographic Algorithms**
  - **Symmetric Encryption** — Used to conceal the contents of blocks or streams of data of any size
  - **Asymmetric Encryption** — Used to conceal small blocks of data
    - such as encryption keys
    - and hash function values
      - which are used in digital signatures
  - **Data Integrity Algorithms** — Used to protect blocks of data — such as messages — from alteration
  - **Authentication Protocols** — use of cryptographic algorithms — designed to authenticate the identity of entities
- **Network Security** — measures to
  - deter
  - prevent
  - detect
  - correct
    - security violations — that involves the transmissions of information
- **Computer Security Objectives**
  - **Confidentiality**
    - Data confidentiality — Assures that private or confidential information is not made available or disclosed to unauthorized individuals
    - Privacy — Assures that individuals control or influence what information related to them
      - may be collected and stored and by whom
      - and to whom that information may be disclosed
  - **Integrity**
    - Data integrity — Assures that information and programs are changed only in a specified and authorized manner
    - System integrity — Assures that a system performs its intended function in an unimpaired manner
  - **Availability** — Assures that systems work promptly and service is not denied to authorized users
  - these and
- **Security Requirements**
  - **Authenticity**
  - **Accountability**
- **OSI Security Architecture**
  - Security **Attack** — Any action that compromises the security of information owned by an organization
  - Security **Mechanism** — A process (or a device incorporating such a process)
    - that is designed to
      - detect
      - prevent
      - recover
        - from a security attack
  - Security **Service** — processing or communication service
    - that enhances the security of the data processing systems
    - and the information transfers of an organization
      - Intended to counter security attacks — and they make use of one or more security mechanisms to provide the service
- **Threats & Attacks**
  - **Threat** — potential for violation of security
  - **Attack**
    - assault on system security
    - 2 types
      - **passive** attacks
        - attempts to learn or make use of information — does not affect system resources
        - like
          - The release of message contents
          - Traffic analysis
      - **active** attack
        - attempts to alter system resources or affect their operation
        - like
          - **Masquerade** — one entity pretends to be a different entity
          - **Replay** — passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
          - **Modification of messages** — message is altered, or messages are delayed or reordered to produce an unauthorized effect
          - **Denial of service** — Prevents or inhibits the normal use or management of communications facilities



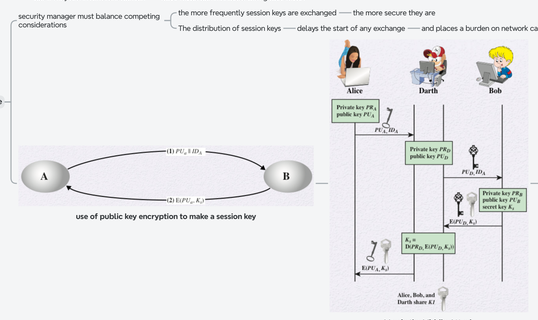
Network Security Model

- Key Distribution Technique
  - **definition** — refers to the means of delivering a key
    - to two parties who wish to exchange data
    - without allowing others to see the key
  - For **symmetric** encryption to work — two parties to an exchange must share the **same** key
    - and that key must be **protected** from access by others
  - Frequent key changes are desirable — to limit the amount of data compromised — if an attacker learns the key



Key Distribution Scenario

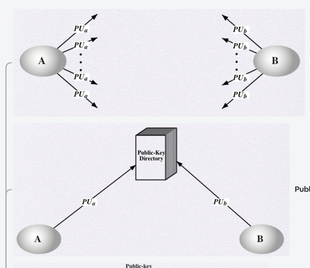
- Hierarchical Key Control
  - means that Local KDC (Key Distribution Center) — is responsible for local key distribution
  - but if they are in different domain — local KDCs communicate with global KDCs
- Session Key Lifetime
  - security manager must balance competing considerations
    - the more frequently session keys are exchanged — the more secure they are
    - The distribution of session keys — delays the start of any exchange — and places a burden on network capacity



use of public key encryption to make a session key

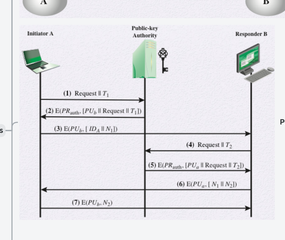
Man in the Middle Attack

public key distribution of secret keys



Public announcement

Publicly available directory



Public-key authority

Created with Blitz