

CompTIA Security+

Review

Concepts

"Security is not a product, it's a process"

"(...) and it begins on the design of the process"

"Sua segurança é tão forte quanto o elo mais fraco" - o lado fraco é o atrativo

"Alarmes não funcionam para humanos. Eventos só funcionam entre sistemas"

Chapter 1

General Security Concepts

Access control models

Physical Security

Operational Security

Management & policies

Physical security

Items that can be seen, touched and stolen

Usual threads: janitors, customers, employees...

First: **Avoid**. Make the location less tempting. Doorlocks, elevator control with keys

Second: **Detect** a penetration. Cameras, motion sensors

Third: **Recover**. "What would happen if..." thinking

Operational security

Focus on how the organizations does what it does. Computers, networks and information

Access control, authentication, topologies (connections), backup and recovery plans

Everything that isn't related do design and physical security

Management and policies

Provides guidance, rules and procedures to implement security

Policies to be effective must have full support from the company management (directors)

Policies: administrative, software design, disaster recovery, information, security, usage, user management

Administrative policies

Lays out guidelines for upgrades, monitoring, backups and audits

Sysadmins use these policies to conduct business

Should identify who by title is responsible for decisions

Help administrative staff to keep focused on business

Disaster recovery plans (DRP)

Expensive to develop and test and to be kept current

Should be able to restore critical systems for production, not just IT

Information policies

Information/data security: access, classifications, storage, transmission, destruction

Typical classification levels:

Public: information posted on the web

Internal: posted on the intranet

Private: personal, customer data

Confidential: PKI information, business related ones, restricted to all but who must know

Usage policies

Cover how information and resources are used

Statements about ownership, privacy and consequences

Internet, email etc

Should also address how users should handle incidents and who they contact

User management policies

Identify various actions that must occur in normal course of employee activities

How new employees are added, trained, configured and terminated

Avoid privilege creep (forget to revoke privileges once they should change)

Goals of information security

Prevention: maintain a security plan. It's much easier to deal with before violation occurs

Detection: identify events when they occur. May only be known with post analysis

Response: deal with an attack or loss. Neutralize the threat

Access control

MAC

DAC

RBAC

Access control: MAC

Mandatory Access Control

Static, predefined set of access fo files on the system

Sysadmins establishes them for users, can be very restrictive

MAC uses labels to identify levels of sensitivity to objects

When users tries to access an object, the label is examined to see if it should occur

When MAC is applied, labels are required and must exist for every

Access control: DAC

Discretionary Access Control

Allows the owner of a resource to establish privileges for information they own

DAC != MAC since labels are not mandatory but can be applied as needed

Allows the owner to grant or revoke access

Don't be confused with information classification

Dynamic in nature

Access control: RBAC

Role Based Access Control

Allow users to act in a predetermined way to define access to the role/duties information

Common in network administrative roles

Determined by role. Privileges are predefined to roles

Authentication

Proves that a user or system is actually who they claim they are

It's prior to authorization

Part of a process called "Identification and authentication"

Identification starts when a user ID is typed

Authentication is accomplished when the user proves he is who he claims to be

Authentication: PAP

Password Authentication Protocol

No true security

Simplest form of authentication

User and pass are sent cleartext to server

Authentication: CHAP

Challenge Handshake Authentication Protocol

Challenges a system to verify identity

Makes the challenge at login and any time later

Doesn't use a ID/pass mech. The initiator send a logon request to server

Server sends a challenge back. Challenge is encrypted and sent back to server

Server compares the values from client and if they match, grants authorization

Authentication: Certificates

Another common form of authentication

A server or a CA can issue a certificate that will be accepted by the challenging system

Certificates can be physical (smart cards) or electronic

A Certificate Practice Statement (CPS) outlines the rules for managing and issuing certs. Used to enforce policies

A Certificate Revocation List (CRL) lists revocations that must be known to not accept

CIA

Confidentiality: prevent unauthorized access

Integrity: ensure the data is what it's supposed to be. Wasn't changed

Availability: the data must be available when it's need by who can need it

Accountability: mechs to not allow users to deny they did something, non-repudiation.

Security zones

Isolates networks according to their intent

Internet, Intranet, Extranet, DMZ

Technologies

VLANs:

Create groups of users and systems and segment them on the network

Reduces the size of broadcast domains

Key: Increase security by segmenting similar users/data together

NAT:

Presents a single IP to destinations

Can also act as a firewall

Business concerns to be aware of

Asset Identification: process to place a value on informations and systems

Risk assessment: identify costs of replacing stolen data or systems, downtime

Threat identification: possible problems

Vulnerabilities: software, design etc

Summary

Be able to explain the relative capabilities of the technologies available to you for network

security. In most situations, you can create virtual LANs, create connections that are

encrypted, and isolate high-risk assets from low-risk assets. You can do so using tunneling,

DMZs, and network segmenting.

Summary

Three primary access control methods are used in computer systems today: MAC, DAC, and

RBAC. The MAC method establishes all connections and relationships between users stati-

cally. The DAC method allows the user to have some control over what information and

resources are accessible. The RBAC method sets access levels and permissions based on the

role the user plays in a particular situation or job.

Summary

Asset Iden-

tification, Risk Assessment, Threat identification, and Vulnerabilities are the four primary

business requirements that must be considered in a security design.

Tips:

IM are insecure by nature (social engineering, hostile code)

Multi-factor using cards, biometry etc are NOT authorization, are authentication

Tokens: provide single session credentials

Chapter 2

Identifying potential risks

Access attacks

Motivation is to gain access to information (Confidentiality)

Gain unauthorized access

Dumpster diving: papers on recycle bin for example

Eavesdropping: process listening a conversation. Passive

Snooping: someone looking through your files hoping to find something

Interception: active or passive. Passive: routinely monitor the network. Active: putting a computer system between the sender and receiver.

Modification and repudiation attacks

Motivation is to plant information, fraud (integrity)

Repudiation attacks usually begin as access attacks

DoS and DDoS attacks

Motivation is to prevent access to resources (availability)

Common: ping-of-death, buffer-overflow, Syn flood,

Common attacks: back doors

Original term referred to troubleshooting and developer hooks

Examples: NetBus and Back Orifice

Now, typically installed using a trojan horse program Examples:
NetBus and Back Orifice

Common attacks: spoofing attacks

Attempt by someone or something to masquerade as someone else

Usually an access attack

Common: IP spoofing and DNS spoofing

Think of spoofing as fooling

Common attacks: man in the middle

Is an access attack. Starting point for a modification attack

Is an active attack

Common attacks: replay attacks

Access or modification attacks

Replaying captured network traffic, certificates, kerberos tickets
etc

Common attacks: password guessing

Brute-force: guess passwords until a successful guess

Dictionary attack: common words

Rainbow tables: worst nightmare. Lists of already computed hashes for many passwords. Since computation of hashes takes the most time, these lists presents a fast way to match a hash

TCP/IP model

Application: HTTP, SMTP

Host-to-host or Transport layer: TCP/UDP

Internet layer: IP routing, ARP, ICMP

Network Interface layer: physical

TCP/IP attacks: SYN or ACK flood

Motivation is to deny access

DoS or DDoS

TCP/IP attacks: sequence number attack

Goal is to kick the attacked end off the network

Can be used to disrupt or to hijack a session

TCP/IP attacks: TCP/IP hijacking

Also called as active sniffing

Actually disconnects the attacked end

Inserts another host in place

ICMP attacks

Smurf

Uses IP spoofing and broadcast

Sending a broadcast ping with spoofed address

ICMP tunneling

ICMP data inside packets used to control a backdoor for example

Types of viruses

Polymorphic: changes form to avoid detection, mutation

Stealth: avoid detection masking itself. Can attach to boot sector

Retrovirus: attacks or bypasses the AV software

Multipartite: infects files, boot sector etc. Hope that you can't correct all of them

Armored: covers itself with protected code

Companion: attaches itself to legitimate programs

Malware: Trojan

Enters under the guise of another program

Could create a backdoor

Primary distinction from a companion virus is that you always intentionally obtained the trojan and didn't know that something more was in it

Example: spyware, which is often installed as part of another program

Malware: Logic bombs

Triggered by a specific event

The infected system can do a DDoS attack to another victim

Malware: Worms

Can reproduce itself, it's self contained

Made to propagate itself

Social engineering

May occurs over the phone, mail, visit

Best defense is user awareness

Phishing is an example

Chapter 3

Infrastructure and connectivity

Firewalls

First line of defense

Can be a dedicated device or included in others such as routers or servers

Works like one or more of: packet filter, proxy firewall and stateful inspection

Firewalls - packet filter

Doesn't analyze the contents of a packet

Is based on packets information like IPs and ports

This type of filter is also included in many routers

Firewalls - proxy firewall

Proxy firewalls is an intermediary between networks (or the Internet)

Can analyze the data, but must understand that application

Proxies do hide IP addresses, so, it's doing NAT

Provides better security as it analyzes the data

Typically uses two NICs (dual-homed. More than 1 NIC is always multihomed)

In a proxy-only mode, the IP forwarding should be disabled

Firewalls - stateful inspection

Keeps track of every communication channel

Occurs at all levels of the network

Provides additional security especially in connectionless protocols like ICMP and UDP

DoS attacks can overload the connection table

Hubs

Broadcast traffic echoes in all ports

Single broadcast and collision domain

Unsecure, should be replaced with switches

Single broadcast and collision domain

Switches

Improves network efficiency

Typically has small amount of information about systems in the network

It combines the best capabilities of routers and hubs

Separates collision domains, but 1 broadcast domain

Routers

To connect two or more networks

They store information about networks they're in

Most routers can act as a packet filter firewall too

Also used to translate LAN framing to WAN framing (ex.: 100BaseT to T1)

Such routers are called border routers

Broadcasts don't traverse routers. Network segmentation decreases traffic

Separates broadcast domains

Wireless access points, WAPs

Are insecure

At bare minimum, WEP should be used

War driving is to drive around the town looking for WAPs that can communicate

Never assume that a wireless connection is secure

Hide the SSID increases security

Modems

Connects digital signals with an analog network (such as telephone line)

Auto-answer is a security problem

RAS: remote access services

Is any server service that offers the ability to connect remote systems

Access can be via dial-in, VPNs, DSL etc

Popular examples are VNC and PC Anywhere

Telecom/PBS systems

Remember Asterisk

Allows to have a single connection for all communications (voice, data...)

Because moderns PBX has many of the features as other network components, it's subject to same issues such as open TCP ports

VPNs

Can be used to connect LANs together

Typically uses L2TP, IPsec or PPTP

IDS

IDSs can respond like a burglar alarm

Wireless Application Protocol: WAP

Mobile devices, pagers, PDAs

Wireless Session Protocol(WSP) manages session and connection between devices

Wireless transaction Protocol (WTP) provides services similar to TCP and UDP

Wireless Datagram Protocol (WDP) provides common interfaces between devices

Wireless Transport Layer Security (WTLS) is the security layer

Point-toPoint protocol: PPP

Doesn't provide data security

Provides CHAP authentication

Encapsulates network traffic in Network Control Protocol (NCP)

Authentication is handled by Link Control Protocol (LCP)

Unsuitable for WAN connections. Good for dial-up connections

Tunneling protocols: PPTP

Created by Microsoft

Encapsulates and decrypts PPP packets

The negotiation between the two ends is done in clear text, and therefore the data is encrypted

Weakness: a capture device that captures the negotiation information

Tunneling protocols: Layer 2 forwarding (L2F)

Created by Cisco

To create tunnels primarily for dial-up connections

Provides authentication but no encryption

Uses 1701 TCP port

Shoudn't be used for WANs

Tunneling protocols: L2TP

Created by Microsoft and Cisco

Combination between PPTP and L2F

Still a point-to-point protocol

Major problem is that doesn't provide data security, information is not encrypted

Data security should be provided by protocols like IPsec

Uses port 1701 UDP

Tunneling protocols: IPsec

Isn't a tunneling protocol

Used in conjunction with tunneling protocols

Oriented to LAN-to-LAN, but also used by dial-up too

Provides authentication and encryption to data and headers

Can be used in transport or tunneling mode

Tunneling: data and payload are encrypted

Transport: only the payload is encrypted

802.1? wireless protocols

IEEE 802.1? refers to broad range of wireless protocols

Two major families: 802.11 and 802.16

802.11: short-range systems. Campus, buildings etc

802.16 (2002): broadband wireless metropolitan networks

Radius

Remote Authentication Dial-In User Service, IETF standard

Can be managed centrally

Servers that allows access to network can verify with a radius server if the caller is authorized

Should use radius when you want to improve security by implementing a single service to authenticate users who connect remotely

Many radius systems allows multiple servers to increase reliability

Tacacs+

Terminal Access Controller Access Control System

Client/server environment similar to radius

Allows credentials such as kerberos

Cisco uses it widely

Tacacs is expected to be accepted as an alternative to radius

Radius and Tacacs can be used to authenticate connections

Email

IMAP is becoming popular for email access

Many IMAP implementations also allows access via browsers

S/MIME and PGP are two popular methods for email security

SSL/TLS

SSL: uses an encryption scheme between the two systems

TLS: newer protocols that merges SSL with other protocols to provide encryption

TLS supports SSL for compatibility, but supports other encryption protocols like 3DES

HTTP/S: uses SSL or TLS

S-HTTP is a different protocol that lets systems negotiate an encrypted connection

S-HTTP can provide some of the HTTP/S capabilities, but it is as secure

ActiveX

Created by Microsoft to add features to increase the usability of web systems

Authenticode is the certificate technology used to validate ActiveX components

Buffer overflows

When a program receives more data than it's programmed to accept

Can cause an application to terminate or to write data beyond the allocated space

Coax: Coaxial Cable

Supports baseband and broadband (single channel and multiple channel)

Example: TV channels, more than 2 computers with coax segment

More expensive than UTP cable per foot

Vulnerabilities: if one puts a vampire tap and a T connector with a sniffer

UTP

7 categories:

1: voice-grade (telephones and modems)

2: 4Mbps (used in older mainframes and some token ring)

3: 10Mbps ethernet

4: 16-20Mbps (used in token ring networks)

5: 100Mbps (used in 10, 100 and 1000Base-T networks, most common)

6: 100Mbps (used in high speed networks. Not so common)

7: 100Mbps (very-high speed. Not available yet, just proposed)

Fiber Optic

Less likely to be affected by interference problems because it uses light

Security issue is that most likely they connect with wire connection

Infrared

Uses infrared radiation

Tend to be slow

IR is line of sight, isn't secure and can be intercepted

Think of remote controlled TVs

Microwave

Uses RF spectrum

Used by cellulars, police, broadband telecom etc

Operates in 2.5 to 5.0Ghz range

Many newer devices includes encryption similar to IPsec

Removable medium

Tape: old standard for backup

CDs, DVD

Hard Drivers

Flash cards or memory sticks

Smart cards: generally used for access control. Stores permissions and access information. Hard to counterfeit but easy to steal. Can be used for storage too

All vulnerable to viruses

Chapter 4

Monitoring activity and intrusion detection

IDS

Monitor events in a network to determine if an intrusion is occurring

Intrusion is any attempt to undermine or compromise integrity, confidentiality or availability

Activity: suspect network traffic

Administrator: responsible for the IDS configuration and responses to attack

Alert: a message from the analyzer that something has occurred

Analyzer: the component that analyzes the sensor's data, events

Event: occurrence in a data source that a suspicious activity has occurred. Events are logged for future reference. They can trigger

IDS

Sensor: component that collects data from the data source and passes it to the analyzer

Can be a program on a system or a black box on a segment

Is the primary data collection point for the IDS

Many sensors on different segments send data to a central analyzer

IDS are intended as traffic-auditing, although it can be used to block traffic

IDS Types

Misuse detection: based on attack signatures and audit trails

Anomaly detection: based on deviations of the learned ordinary traffic

IDS: NIDS

Place sensors in segments

Best is to place sensors in front and behind the firewall

Passive response: logging, notifications

Active response: take an action to reduce event's potential impact (terminate the connection, firewall blocking etc. least common)

Honey pots

Designed to be a target for attacks

For research and to distract attackers

Types:

Enticement: inviting attacker to the system. Research

Entrapment: encouraging an attacker to perform an act even if they don't want to do it. Can be used in a legal defense

Incident response

Steps to Identify, investigate, repair, document and adjust procedures to prevent another incident

The IRP outlines the steps and who is responsible for deciding how to handle the situation

Two types: internal responses and law enforcement

Law enforcement are governed by rules of evidence, and their response will be out of your control

You should consult management before decide to use law enforcement

Incident response

Chain of custody: keep track of the evidency and show at all times who has it, who seen it and where it has been

Incident response

Step one: Identifying the incident

If it's not a false positive, decide how to handle it

Escalation involves consulting policies and determining how best to conduct an investigation

Incident response

Step two: investigating the incident

Searching log files and other data sources

Is the incident is happening now ? Should deal with it same way that if it has occurred before you knew it.

Incident response

Step three: response. Repairing the damage

How to restore acces that have been compromised

Incident response

Step four: documenting the response taken

Write down the steps used to identify, detect and repair the system affected by the incident

Incident response

Step five: adjusting procedures

Prevent another occurrence

Wireless protocols

802.11: 1Mbps or 2Mbps, 2.4Ghz

802.11b: (called Wi-Fi or high-rate) 11Mbps, 2.4Ghz

802.11g: 54Mbps, 2.4Ghz

802.11a: 54Mbps, 5Ghz (orthogonal frequency division multiplexing)

Wireless networks are vulnerable to site survey

IM vulnerabilities

Common attacks:

Jamming: interject or flood a channel with garbage data. Goal is to disrupt

Malicious code, trojans and DoS attacks can also be used against IM

Social engineering is very common

Malformed MIME message can cause a buffer overflow

Footprint

Process of systematically identifying the network and its security posture

Example of footprinting: examine the source code of the web site

Footprinting is to get information of the systems

An attacker can query DNS servers and see the records to help footprint your network

Scanning

Process of getting information on how your network is configured

Network scans, tracerouting etc can provide your network topology to an attacker

Chapter 6

Securing the network and environment

Physical barriers

Many concepts are shared with network security like perimeter and security zones

Must have a minimum of 3 barriers

First: perimeter security

Second: entrance to computer center

Third: entrance to computer room itself

Perimeter security

First line of defense

Prevent external access to the building

Locks, doors, alarms and surveillance systems

Security zones

Area inside the building where access is individually monitored and controlled

In a building, floors, sections etc can be broken into smaller areas - security zones

Partitioning

Typically more detailed than security zones

Ex: a security zone would encompass one entire floor, while the rooms are examples of partitions

Mantraps

Require visual identification as well as authentication

Makes it difficult to access in number, allows only one or two people per time

Can use a security guard

GSM Global system for mobile communications

Works in conjunction with a SIM (subscriber identification module)

Offers encryption

Wireless encryption

WTLS: wireless transport layer security

ECC: Elliptic curve cryptography (low cpu)

Environmental control systems

Temperature and humidity control

Usually, systems are located in the middle of the building, and ducted separately from the rest

Tip: humidity can't drop below 50%. eletrostatic damage may occur

Also concern water, flood and fire supression

Moisture sensors would kill power in a computer room if moisture is detected (flood)

Fire suppression

In most buildings, consists of water under pressure. Problem in computer rooms

To have fire: heat, fuel and oxygen. Most suppression systems work with this concept

Fire suppression

Two types: fire extinguishers (portable) and fixed systems

Fire extinguishers types:

A	wood and paper	largely water or chemical
B	flammable liquids	fire-retardant chemicals
C	electrical	nonconductive chemicals
D	flammable metals	varies, type specific

Fire suppression

Fixed systems are usually part of the building

Most common is to combine fire detection with fire suppression systems

Common fire suppression systems use water or gas

Drawback for gas based is that requires sealed environments and are expensive

Power systems

Computer are susceptible to power and interference problems

Flutuations in AC power can cause chip creep: unsoldered chips slowly loose contact with the socket

Surge protectors:protect against momentary increases (spikes)

Power conditioners: active devices isolate and regulate voltage. Includes filters, surge suppressors and voltage regulation. Can also have backup power supplies

Shielding

Preventing electronic emissions from computers from being used to gather intelligence

Is like eavesdropping

Prevents against external to internal too

Example: surrounding the computer room with a faraday cage

Shielding

EMI: electromagnetic interference and RFI: radio frequency interference

Motors, lights, electromechanical objects causa EMI

May causa circuit overload, spikes, component failure

RFI is the byproduct of electrical processes, similar to EMI

RFI is usually projected across a radio spectrum

Can cause receivers in wireless units to become deaf, called desensitizing, and occurs because of the volume of RF energy

Shielding

Project TEMPEST

Certificate that the system doesn't emit any significant amounts of EMI or RFI

TEMPEST certified equipments usually costs twice as non certified

BCP: business continuity planning

Implements policies, controls and procedures to counteract effects of losses, outages or failures of critical business **processes**

Must ensure critical business functions can be done when business operations are disrupted

Key components: Business Impact Analysis (BIA) and risk assessment

BIA: Business impact analysis

Process of evaluating all critical systems to determine impact and recovery plans

Isn't concerned with external threats or vulnerabilities. Focus on the impact of a loss

Key components:

Identify critical functions to continue operations: will point which systems must operate to business to operate

Prioritizing critical business functions in order of essential to nonessential

Calculating how long can survive without a critical function

Estimate tangible and intangible impact

Assessing risk

Deals with threats, vulnerabilities and impacts on information-processing

Prioritize, because some events have a greater likelihood to happen

ARO: Annualized rate of occurrence

SLE: single loss expectancy

$ARO \times SLE = ALE$

ALE: annual loss expectancy

Policies

Provide people with guidance about their expected behavior

Are clear and concise

Outline consequences when they aren't followed

Standards

Deals with specific issues or aspects

Derived from policies

Should provide detail that an audit can be performed to see if standard is being met

Example: important aspect of performance criteria is benchmarking

Guidelines

Different from policies and standards

Help to implement and maintain standards by providing information on how to accomplish policies and standards

Less formal than policies and standards

Example: how to install a service pack and steps before/after it

Roles in the information security process

Owner: responsible for establish the protection and use of the data

Custodian: maintain and protect the data

User: who use the data

Auditor: ensures that policies, practices and guilines are followed

Information access controls models

Bell La-Padula: interacts with every access, allowing it or not

No read for levels up, no write for lower levels

Creates upper and lower bounds for information storage

Biba: designed after the Bell La-Padula

no write up or read down

Clark-Wilson: data can't be accessed directly. Must use applications that have predefined access capabilities. Focus on

Tips

Humidity control won't reduce EMI

Break a large area into smaller: security zones, focused video camera etc

Building walls in an office: partitioning

Perimeter security is preferable physical one, like chain link fence. Video can just help

All wireless are line-of-site

Process of reducing interference is shielding. Tempest is a certification

CC Common Criteria is a security certification to OSes

Chapter 7

Cryptography basics, methods and standards

Cryptography

Cryptography is the art of concealing information

Individuals who develop and make code are cryptographers

Individuals specialized in breaking codes are crypanalysts

Major goal: Confidentiality

Another goal: integrity. Ensure that a message wasn't modified.
Can be accomplished using hashes

Common method to verify integrity is adding a MAC (message auth code), derived from the message and a key

Cryptography categories

Physical cryptography

Substitution, transposition and steganography

Any method that doesn't alter the value using mathematical process

Mathematical cryptography

Physical criptography

A cipher is a method to encode characters to hide their value

Ciphering is a process os using a cipher to encode a message

Substitution or stream ciphers: substitute each character. Ex.:
rot13

Transposition or block ciphers: the message is divided in blocks
and ciphered

Stenanography: priority is to HIDE a message

Example: "meet the mini me that ate later" meaning "meet me later"

Symmetric algorithms

DES: old 64bit-block with a 56bits key. Replaced by AES

3DES

AES: based on Rijndael block cipher. Keys of 128, 192 and 256 bits

IDEA: used by PGP. 64bits blocks and 128bits key

RC5: variable key up to 128bits and blocks up to 2048. Made by RSA

Symmetric algorithms

All ends should have the same key (think of 50 people to keep a key secret)

Keys should be sent using an out-of-band method

Faster and easier to implement. Lower overhead

Asymmetric algorithms

Two keys: public encrypts, private decrypts

Private key is known only by the owner (receiver)

Asymmetric algorithms

RSA: Both encryption and signatures. SSL can use it. De facto standard

Diffie-Hellman key exchange: algorithm to send keys across public networks. Isn't used to crypt/decrypt messages, only to transmit keys in secure manner

ECC: similar use to RSA. Lower overhead.

El Gamal: used for key exchange like diffie-hellman. Based on logarithmic numbers

Digital signatures

Similar to a standard signature

Validates the integrity of the message and the sender

The message is encrypted and the digital signature is added

A hash can be generated with the private key, and the public key is sent to decrypt the hash. The receiver decrypts using your public key and see the hash. The hash proves the integrity of the message.

Digital signatures, ex:

Need more study in how this all works