Security Attacks, Actors, Motives

05 August 2020 18:29

Actors

Hackers
Someone who is paid by a organisation
Or someone who has time and knowledge

Hacktivists
Similar to governments but no much financial power
Normally reveal information to public

Internal Users
Most likely to cause security problems
Intentional or not - sale of information most common

Governments
Have most power and can impact economy or geopolitics

Motivations

- Gain Money
- Hire me!
- Just play
- Political movements

Types of Attacks (Major ones)

Supply Chain - ASUS's auto-update process hacked to deliver malware

SWIFT - Financial data i.e. VISA transfers

Tools

- SeaDaddy & SeaDuke
- BlackEnergy
- Shamoon
- Duqu and Flame
- DarkSeoul
- WannaCry

→ infrastructure and data access

Attack Classification

Passive - .eavesdropping, traffic analysis, messages
.undetected for a long time
.hard to detect
.messages are still received and pass security checks
.[illegible] evidence of tampering

- messages are still received and pass
- Low evidence of tampering

Active - . 4 basic categories
Masquerade - intruder pretending to be someone else
Replay - man in the middle, intercept message and pass on
Modification - intercepted data can be modified
Denial of service - stop data being received at other end
Goal - detect these ASAP

Security Services

Specific kind of protection
Intended to counter security attacks
Enhance security of data processing and transfers

X.800 - high level definitions of security services
RFC 2828 -

Authentication
Access control
Data Confidentiality
Data Integrity
Non-repudiation - protects against denial by one of the parties in a communication
Availability

Security Mechanisms

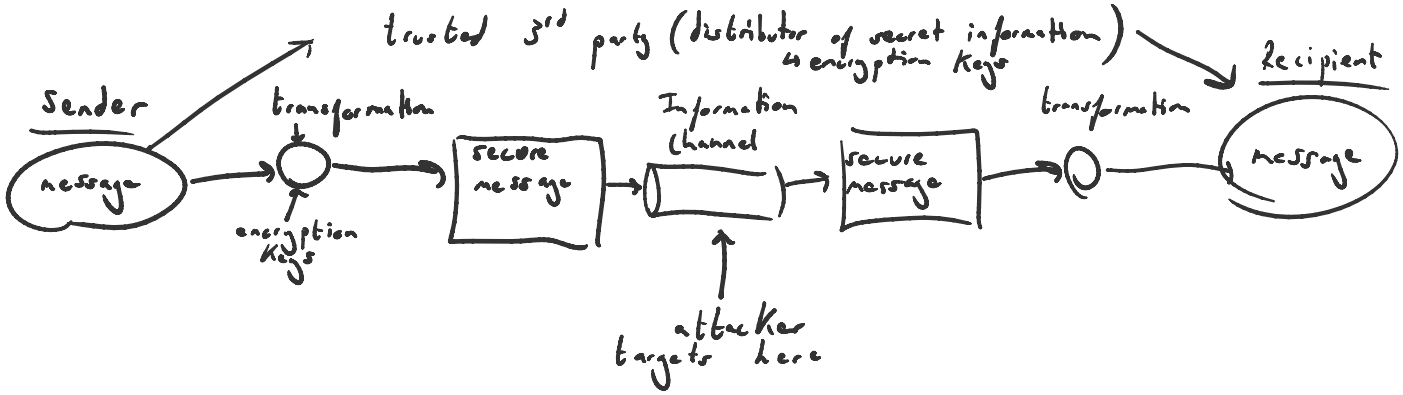
Combination of - hardware
- software
- processes

Use security services to enforce security policy

Examples : cryptography
digital signatures
access controls
traffic padding
routing control
} X.800

Network Security Model

General model



Security : minimizing vulnerabilities of assets and resources

vulnerabilities: any exploitable weakness

assets: anything of value

Motivation / security in open systems
- increasing dependance on computers
- more desire for data protection - v. valuable

To protect : - data / information
- communication
- equipment + Facilities

Threats

Destruction
Corruption / modification
Theft, removal, loss
Disclosure
Interruption of services

} of data/information

Corruption / modification: harder to detect

Accidental - not malicious
Intentional - human with intent
↘ if results in action => becomes attack

Passive - no immediate change to system
Active - significant change to system

Attacks

Considered an attack whether it fails or succeeds

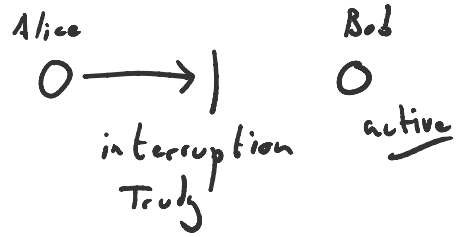
2 forms of passive attacks
- disclosure : content of message revealed to non-authorized users
- traffic analysis : simply monitoring data about a message (size, time, sender, receiver) or just the fact a message was sent can be useful

4 Forms of active attacks
- masquerade : impersonate a known person or

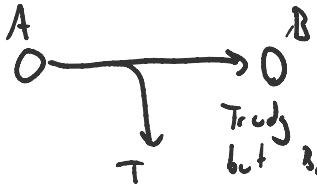
4 Forms of active attacks

- masquerade : impersonate a known person or organization (friend _ Google etc)
  ↳ attack on authentication of origin of message
- replay : message intercepted _ delayed _ re-transmitted later
  ↳ attack on integrity of system
  - financial orders stocks money transfers etc. all badly affected by delays
- denial of service : prevent authorized users from accessing system
  ↳ attack on availability
- modification

Security - Architecture Attacks

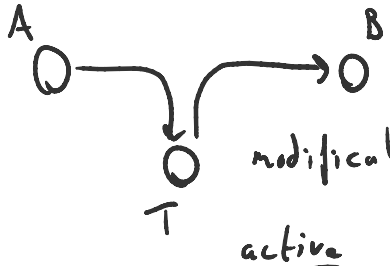


active



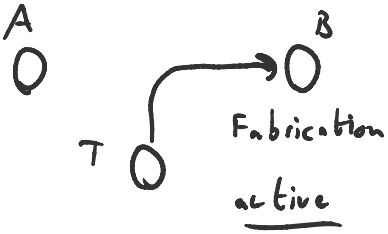
Trudy obtains copy but Bob receives message

passive



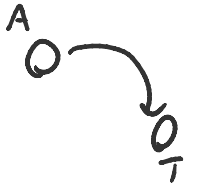
modification

active masquerade + maybe replay



Fabrication

active masquerade



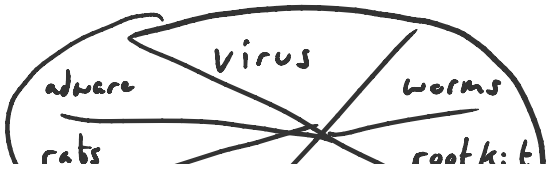
diversion message never arrives at destination

active

Denial of service - preventing message delivery

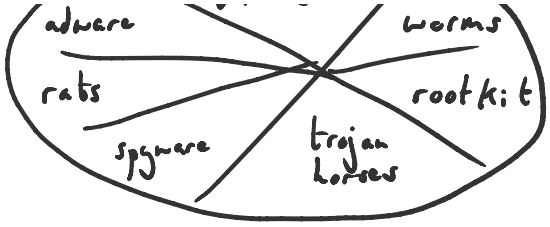
Malware and Ransomware

malicious software



polymorphic virus
- has code that can self replicate

worms - turns computer into zombie



worms - turns computer into zombie

ransomware - data and access taken hostage

others ...

botnets - take over computers (zombies, drones) to maliciously attack others (large scale DoS)

logic bombs - dormant code which is triggered by event

keyloggers - records keystrokes

APTs - get access and monitor network

Protection:

technical	administrative
anti virus	policies (password)
IPS IDS UTM	training
updates	revision and tracking ↑ up to date