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
- Dugu 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
· no evidence of tampering

Active - · 4 basic categories
Masquerade - intruder pretending to be someone else
Replay - man in the middle, intercept message and pass on

Masquerade - [illegible]

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

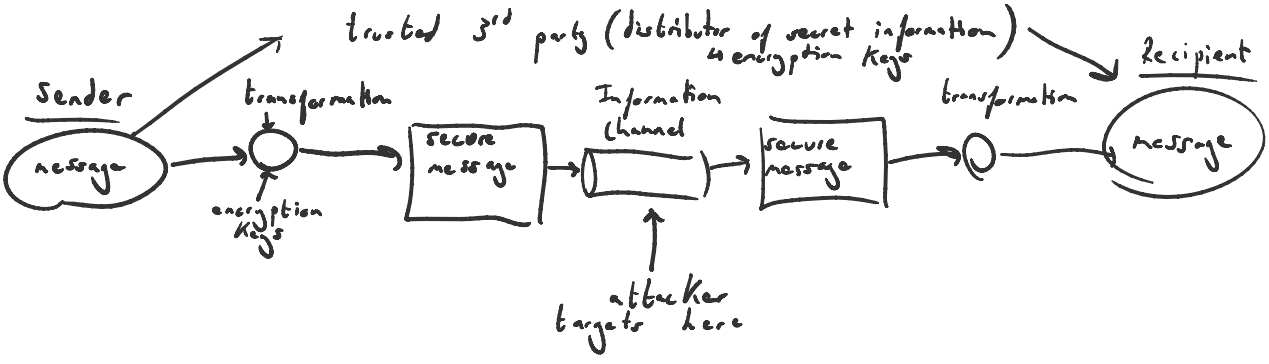
Combination of - hardware
- software
- processes

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

any exploitable weakness

anything of value

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

- 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 — 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

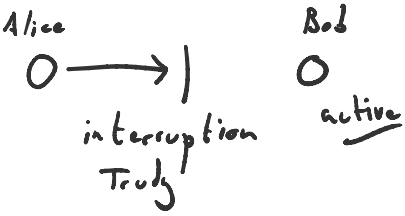
Considered an attack whether it fails or succeeds

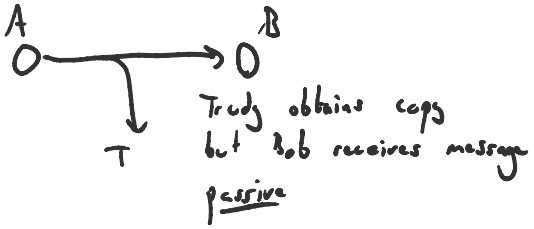
2 forms of passive attacks
- disclosure: content of message revealed to non-authorized users
- traffic analysis: simply monitoring data about a message (size, time, sender, receiver) or just the fact a message was sent can be useful

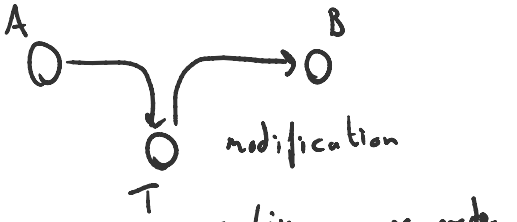
4 Forms of active attacks
- masquerade: impersonate a known person or organization (friend, Google etc)
↳ attack on authentication of origin of message
- replay: message intercepted, delayed, re-transmitted later
↳ attack on integrity of system
- financial orders, stocks, money transfers etc. all badly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

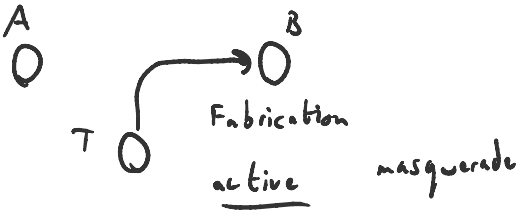
- modification

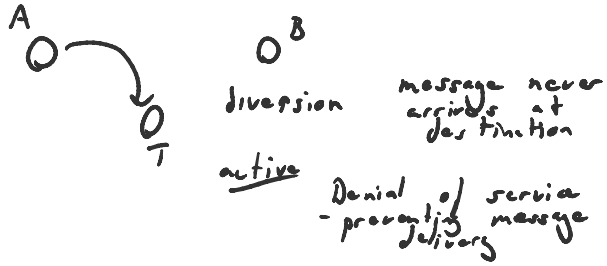
Security - Architecture Attacks





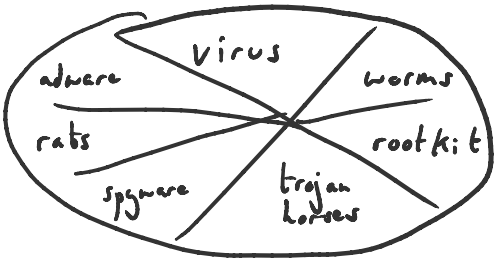






Malware and Ransomware

malicious software



polymorphic virus
- has code that can self replicate

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 :

Protection:

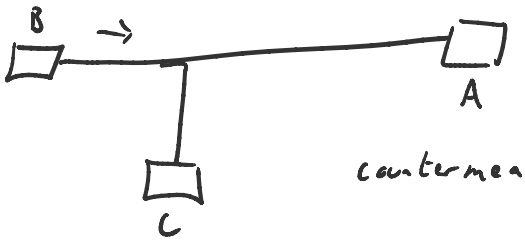
technical	administrative
anti virus	policies (password)
IPS IDS UTM	training
updates	revision and tracking ↑ up to date

Network Mapping

- checking out the network and services
- use ping to determine hosts & addresses
- port scanning, try to establish TCP with each port
- nmap (tool for exploring and auditing network)

countermeasures:
- record traffic entering network
- look for suspicious activity (IPs, ports being scanned)
- host scanner, keep inventory of hosts on network
  ↳ can see if whitelist has been tampered with

Packet Sniffing

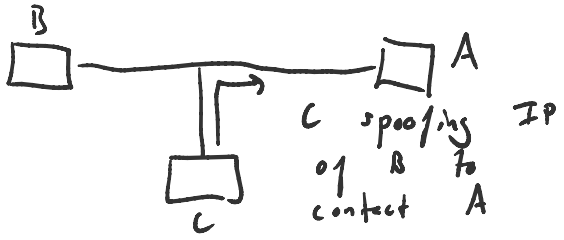


payload B → A

C sniffing packets sent from B to A

countermeasures: all hosts in organization run software that checks if other hosts are in promiscuous mode
- network card (NIC) needs to be running in promiscuous mode to packet sniff

IP Spoofing

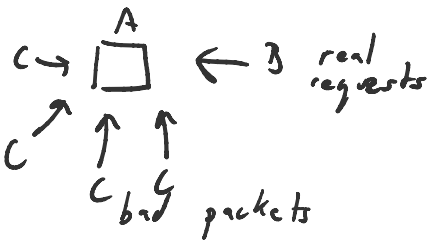


ingress filtering - partial solution
↳ routers setup to not forward invalid IP addresses
- can't mandate this on all networks

Denial of Service

Flood a service with malicious packets
- can't dedicate resources to real requests

Flood a service with malicious packets
- can't dedicate resources to real requests



countermeasures: need intelligent filtering
- filter out flooded packets before reaching host
- traceback to source of floods
  - would likely be an innocent, compromised machine

Host Insertions

- insertion of new host in the network, once attacker is internal
  - normally inserted in sleeper mode

countermeasures: Keep inventory of hosts by MAC addresses
- constantly scan for hosts that aren't present in whitelist
- missing hosts are ok

Cyber Kill Chain

1/ Recon - research & identify target
2/ Weaponization - pair malware with payload i.e. PDF
3/ Delivery - transmit to target (email, USB..)
4/ Exploitation - trigger exploit
5/ Installation - install backdoor for persistent access
6/ Command & Control - outside server communicates through backdoor
7/ Action on Objective - destroy/exfiltrate data, access another target

Social Engineering

Using someone for cyber purposes
Manipulating someone to do something they don't want to do

Tool: Setoolkit - create/clone fake websites
- setup phishing emails

Tool: Gophish - setup a phishing campaign to test your security system

CyberWarfare & Cyber Crime

Cyber Warfare & Cyber Crime

csis.org log of incidents in different countries

IBM xForce reports