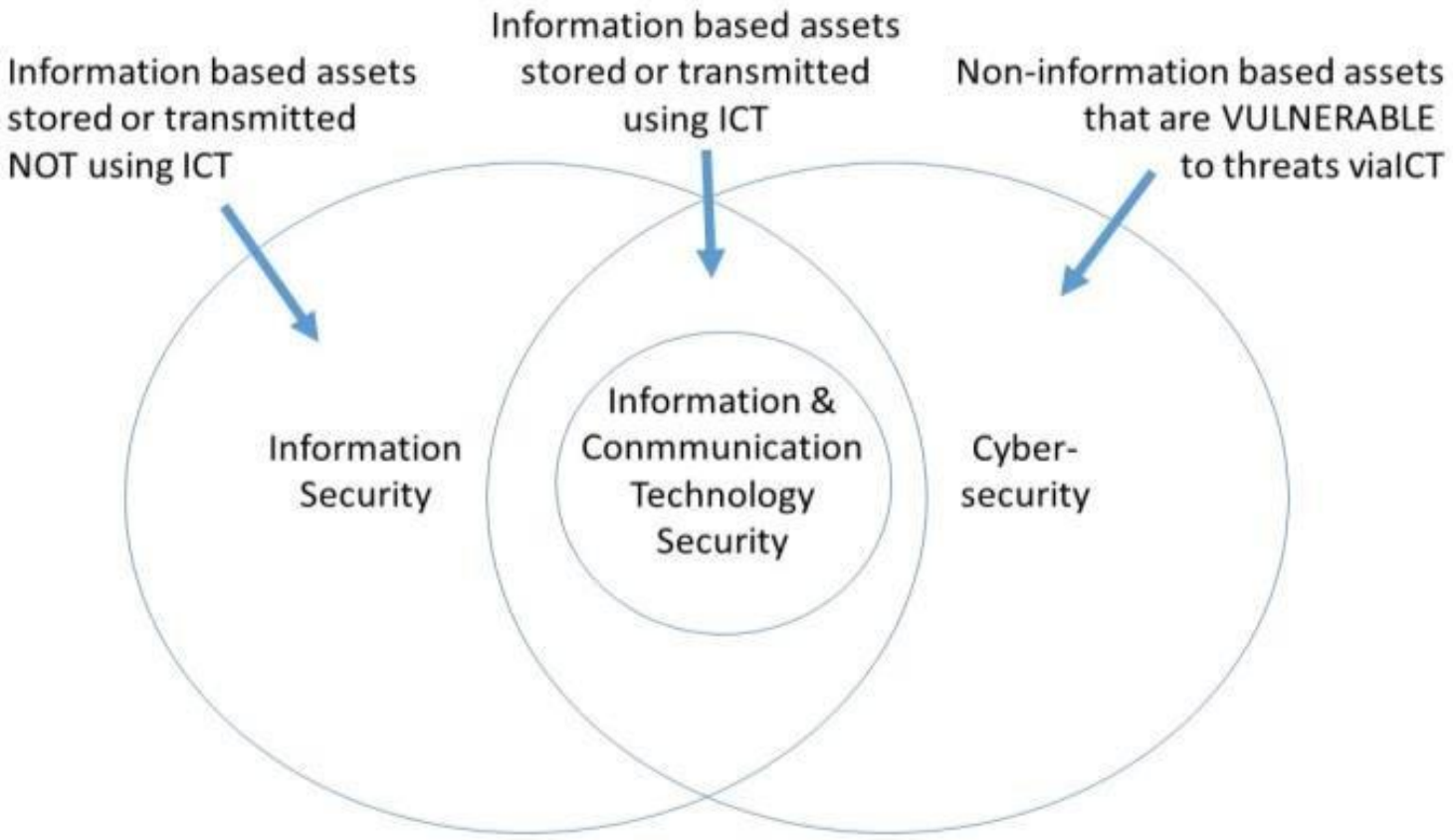
Security



* Information Security is protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide confidentiality, integrity, and availability; both digital and analog information

Information security includes personnel, physical, ICT (information and communication technology), and document security.

* IT security is protection of information technologies. Practically, there is no difference between ICT security and IT security.

* Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks. It includes information and non-information, such as cars, traffic lights, electronic appliances, etc.

* Going by these definition, cyber security is all about security of anything in cyber realm (space), while information security is all about security of information regardless of the realm.


IDENTIFY
• Asset Management
• Vulnerability Assessment
• Governance, Risk & Compliance
RECOVER
• Continuity of Operations
• Disaster Recovery
• Threat Mitigation
PROTECT
• Threat Prevention
• Access Control
• Data Security
CYBER SECURITY
RESPOND
• Incident Response
• Malware Analysis
• Forensic Remediation
DETECT
• Continuous Monitoring
• Anomaly Detection
• User & Application Awareness

Security

info sec.: C.I.A.

confidentiality: only sender, intended receiver should “understand” message contents

- sender encrypts message
- receiver decrypts message

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection (hash functions and digital signatures)

access and availability: services must be accessible and available to users (disaster recovery plan, redundancy)

non-repudiation: knowing who sent or received information (digital signatures)

authentication: sender, receiver want to confirm identity of each other (something you know, have, are)

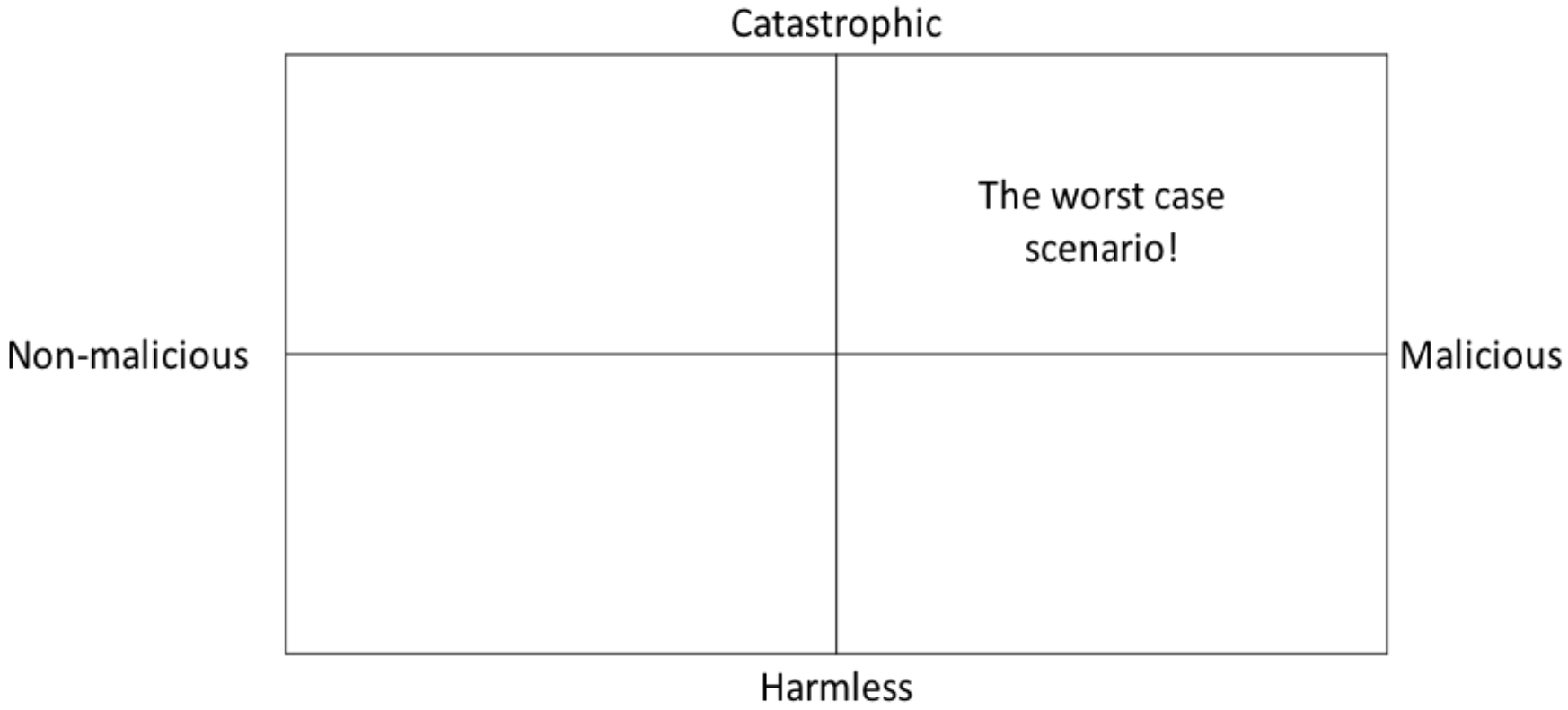
information assurance: C.I.A. + authentication + non-repudiation

authorization: determining if the client has permission to use or access a resource

Cyber security

- Aim: Protecting cyber realm towards to cyber attacks and reducing the risks
- General idea of unrelated people: There are lots of hackers, cyber terrorists and spies
- Reality:
  - Risks stem from errors of hardware & software
  - We can’t protect every asset

Hardware & Software errors



Cyber security

Three basic components

- Vulnerability

  - Weakness of a system; when exploited, loss and damage may ocur (e.g. transferring data clear text)

  - Exploiting a vulnerability intentionally is called an attack

- Threat

  - Situation resolved when weakness is prevented, may be an attack or innocent fault of a person

- Countermeasure

  - Resolving a vulnerability (e.g. updating the OS)

Cyber security

Risk is the potential for loss, damage, or destruction of an asset, as a result of a threat exploiting a vulnerability.

May be defined as the multiplication of threats and vulnerabilities.

Example: in a system that allows weak passwords;
A password is vulnerable for dictionary or exhaustive key attacks: vulnerability.
An intruder can exploit the password weakness to break into the system: threat.
Resources within the system are prone for illegal access/modify/damage by the intruder: risk.

*** BCP: Business Continuity Planning**

Cyber security

Cyber resilience

- continuously deliver the intended outcome despite adverse cyber events
- involves collaboration of people, processes, technology and facilities
- cyber security + keeping things running

Cyber security

Attackers

- Amateur: mostly script kiddies

- Hacker (Cracker): hackers are innocent, testers; crackers are malicious

- State-funded spy

- Terrorist

Hackers

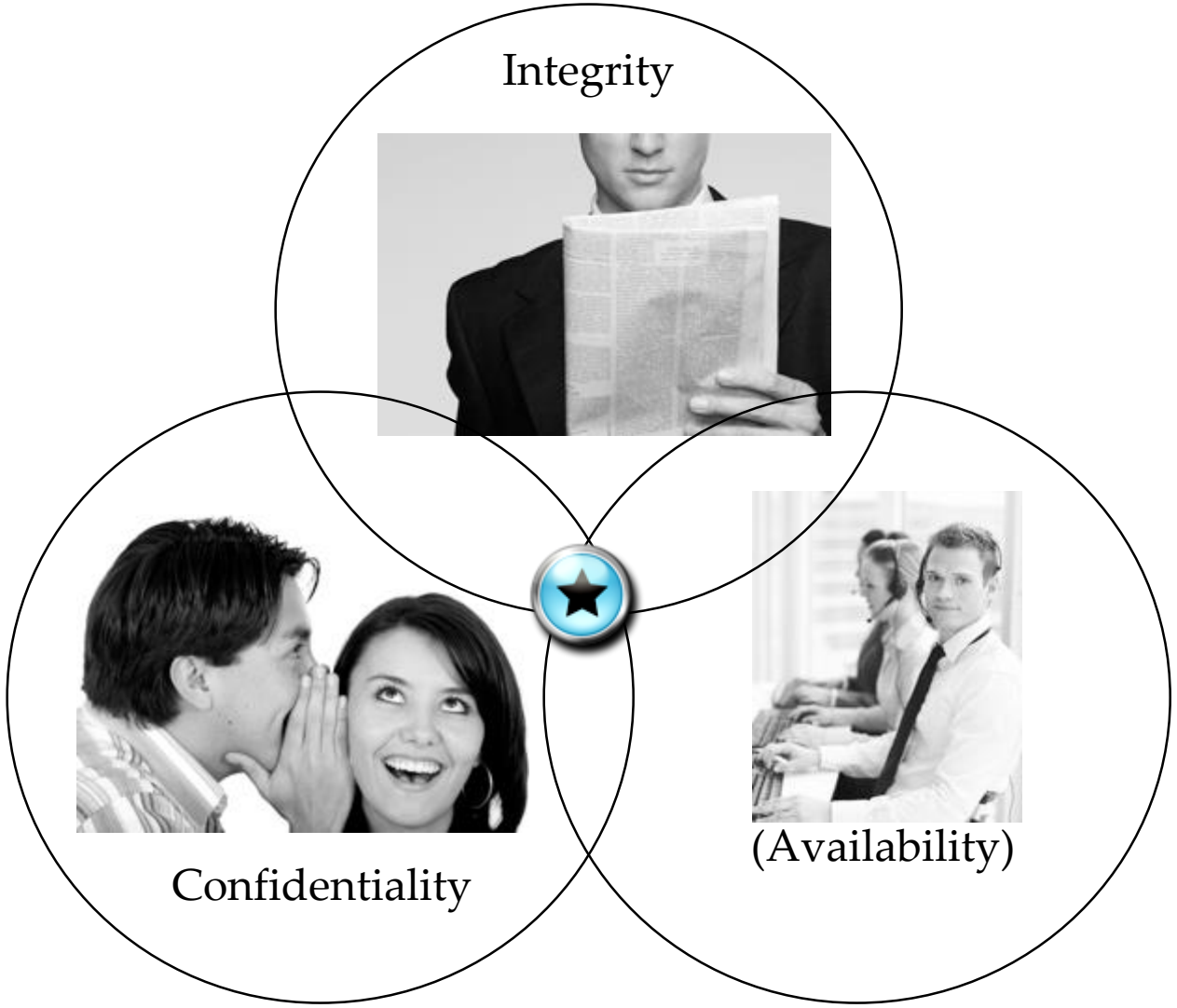
Ethical hackers

- Work with professional and ethical values
- Obtain ‘Get Out of Jail Free’ doc
- Must report of the findings
- Must respect privacy
- Shouldn’t crash tested systems

Hackers vs malicious users

- Have a common goal, compromising sensitive information
- Hackers: External, unauthorized
- Malicious users: Internal, authorized

Threats



Main types of threats

- Disclosure: unauthorized access to information, e.g. eavesdropping
- Deception: modification, spoofing, repudiation of origin, denial of receipt
- Disruption: corruption, e.g. Denial of Service (DoS)
- Usurpation: hijacking

Attacks (Insider & Outsider)

- Buffer overflow
- Brute force
- Replay
- Sniffing, man in the middle
- Session hijacking
- Denial of Service
- Phishing
- Malware

Buffer overflow

```
#include <stdio.h>
#define MAX_IP_LENGTH 15
int main(void) {
  char file_name[] = "ip.txt";
  FILE *fp;
  fp = fopen(file_name, "r");
  char ch;
  int counter = 0;
  char buf[MAX_IP_LENGTH];
  while((ch = fgetc(fp)) != EOF) {
    buf[counter++] = ch;
  }
  buf[counter] = '\0';
  printf("%s\n", buf);
  fclose(fp);
  return 0;
}
```

occurs when a program or process attempts to write more data to a fixed length block of memory (a buffer), than the buffer is allocated to hold

by sending crafted input to an application, an attacker can cause the application to execute arbitrary code, possibly taking over the machine

reading an IP address from a text file, assumption: IP address, will never exceed 15 bytes

fake string will cause our program to overflow the destination buffer

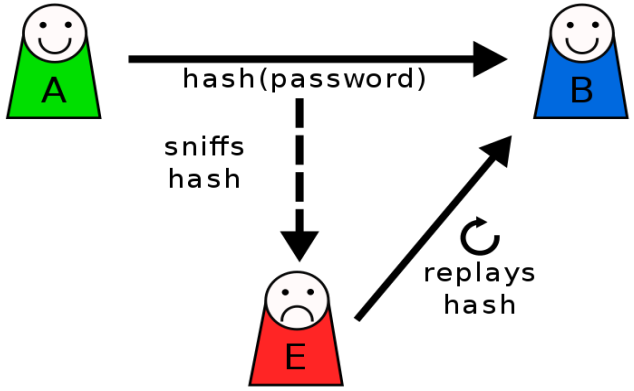
Proper: 255.255.255.255

Fake: 19222222222.16888888.0.1

Brute force

- An attempt to crack a password or username, find an enc. key
- Trial and error approach, aim: making a correct guess

Replay attack



1. Eavesdrop on a secure network communication
2. Intercept it
3. Delay or resend it to misdirect the receiver

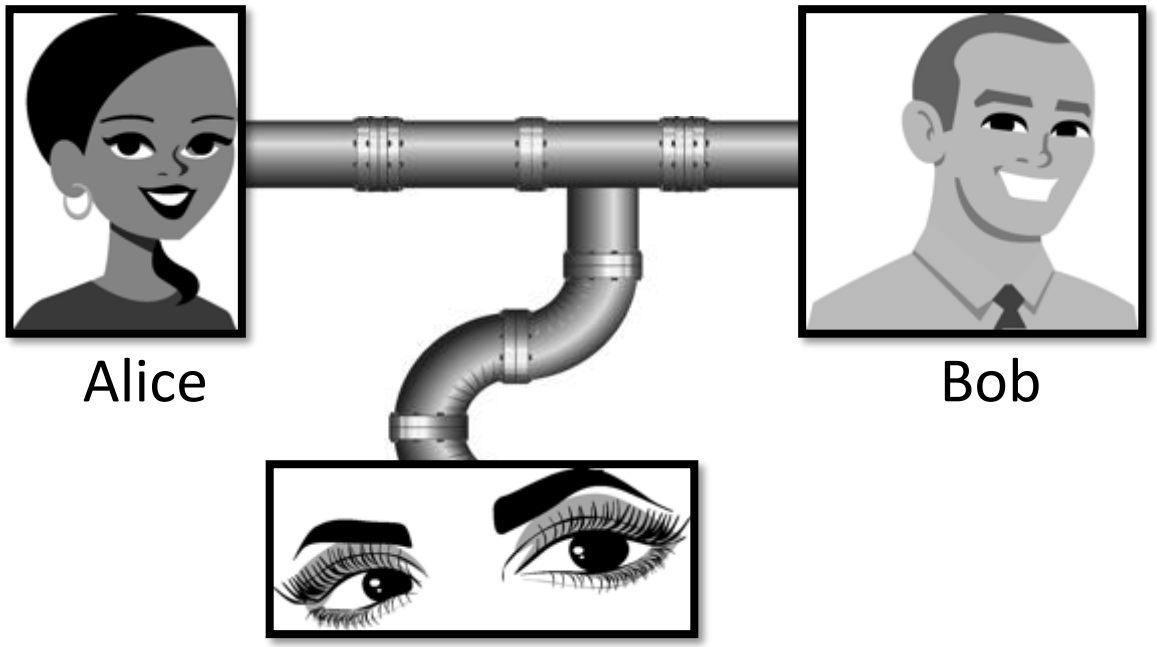
no need advanced skills to decrypt a message, could be successful simply by resending the whole thing

-Suppose Alice wants to prove her identity to Bob
-Bob requests her password as proof of identity (possibly after some transformation like a hash function)
-Meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash)
-After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session which Bob accepts, thus granting Eve access

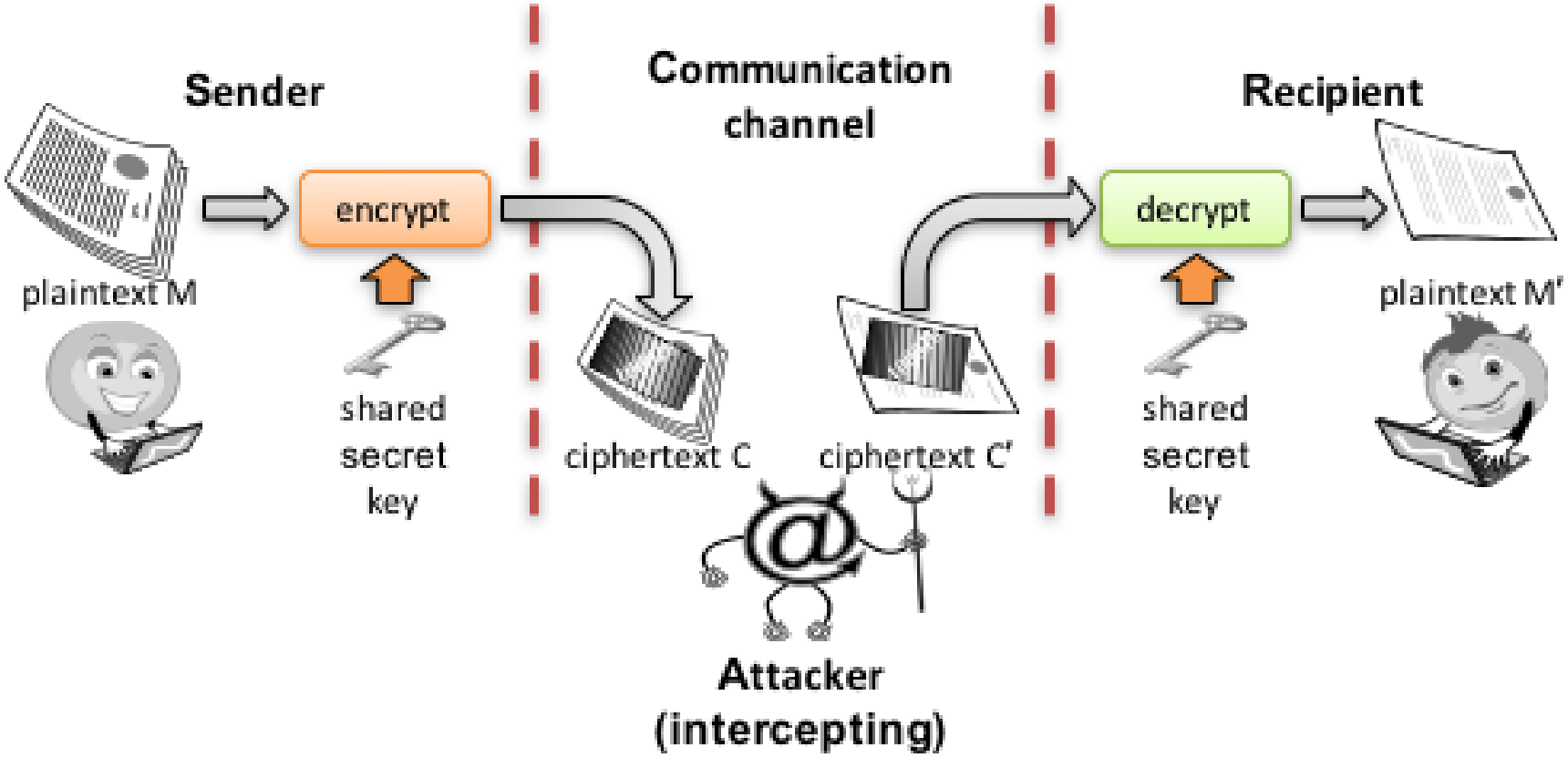
Prevention: completely random session keys, timestamps, pw for each transaction

Sniffing

- Eavesdropping
- Usually passive
- Acquisition of knowledge



Sniffing



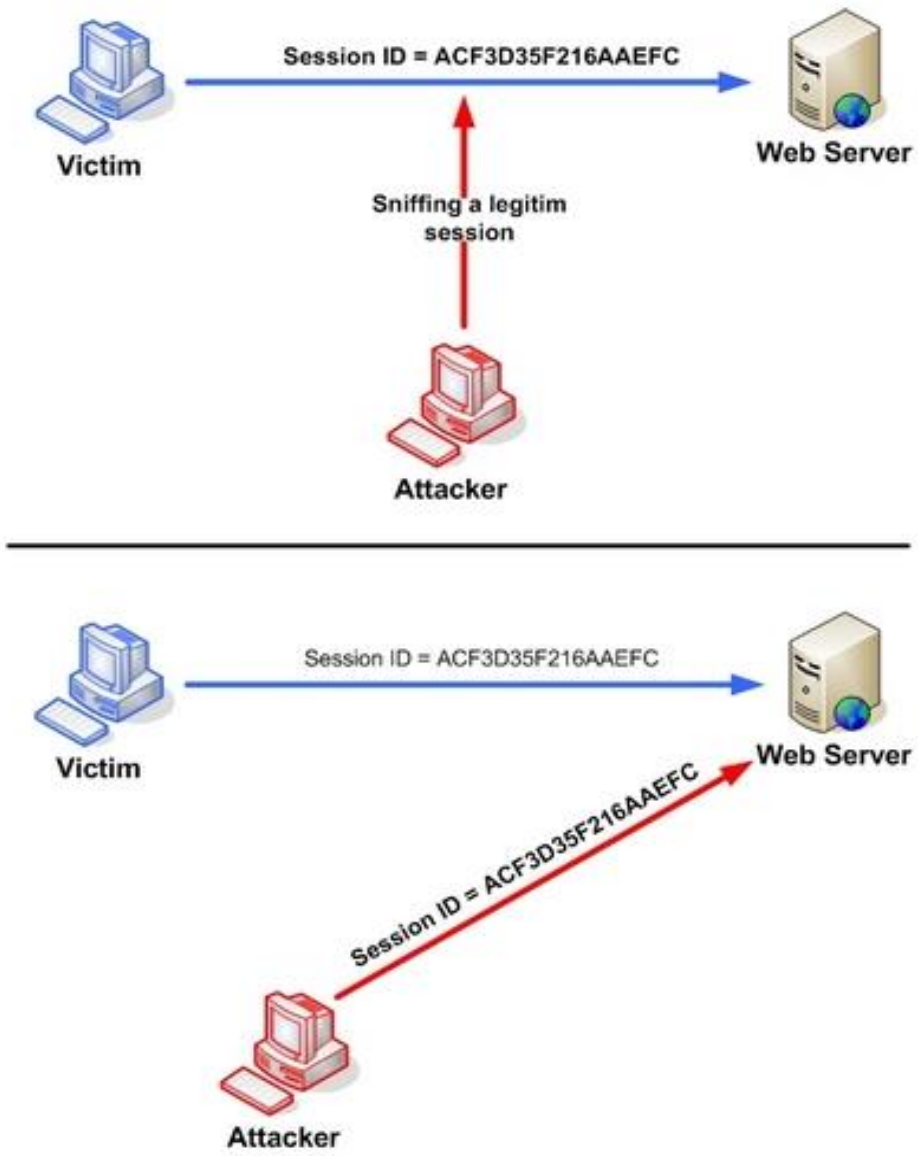
- Sniffing maybe active: man-in-the-middle attack
- Interception and decryption, aims at changing the flow

Types of MITM Attacks

- **Rogue Access Point:** setting up a fake wireless AP and trick nearby devices to join that domain
- **ARP Spoofing:** an attacker wishing to pose as another host could respond to requests it should not be responding to with its own MAC address
- **DNS Spoofing:** act of entering false information into a DNS cache, DNS poisoning

Session hijacking

- Session ID (token) is captured using sniffers
- Captured token is used to access the web server
- Prevention:
  - Changing IDs for each session
  - Using timestamps



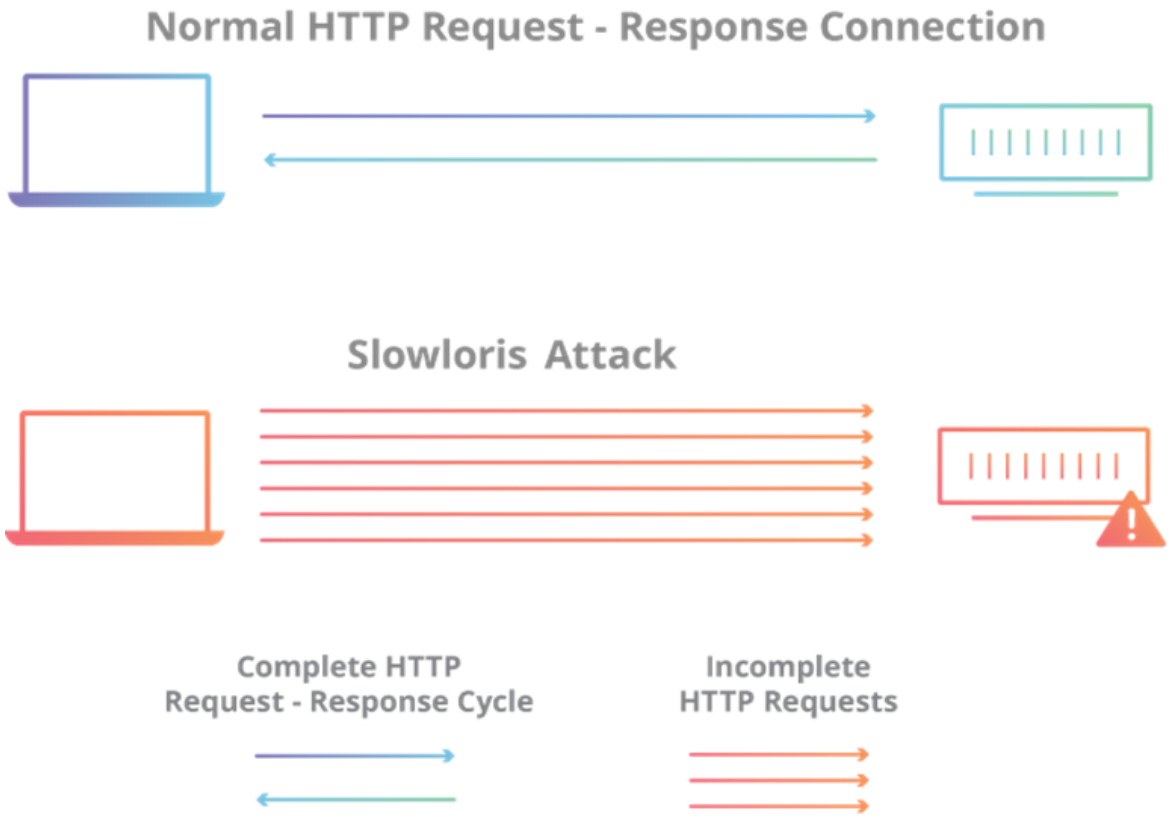
Denial of service

- Shut down a machine or network
- Can cost the victim a great deal of time and money to handle

Denial of service

- Flooding services: too much traffic, slow down and stop
- Crashing services: exploiting vulnerabilities
- DDoS

Denial of service



- multiple connections to the targeted server by sending multiple partial HTTP request headers
- target opens a thread for each incoming request (If a connection takes too long, the server will timeout the long connection, freeing the thread up for the next request)
- to prevent the target from timing out the connections, attacker periodically sends partial request headers and so keep the request alive (“I’m still here! I’m just slow, please wait for me.”)
- targeted server is never able to release any of the open partial connections. Once all available threads are in use, the server will be unable to respond to additional requests, this results in denial-of-service.

Denial of service

How to mitigate?

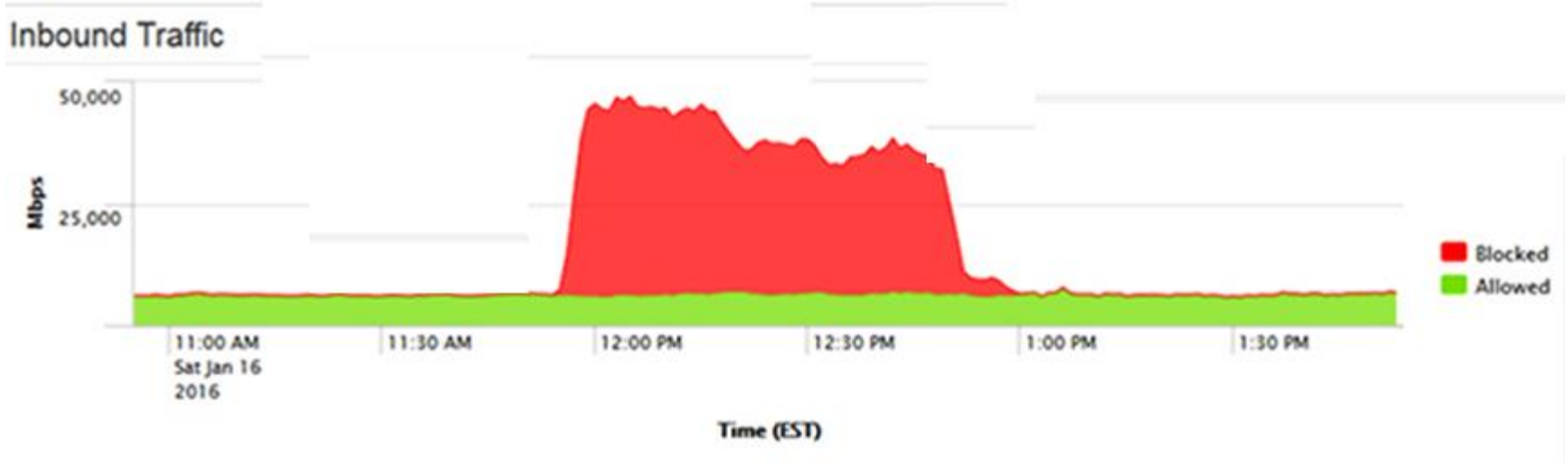
- **Increase server availability**
- **Rate limit incoming requests:** limiting the max number of conn. a single IP address is allowed to make, and limiting the max time a client is allowed to stay connected
- **Cloud-based protection:** reverse proxy, protect the origin server

Denial of service

DDoS Types

- volumetric (bps---bits per second)

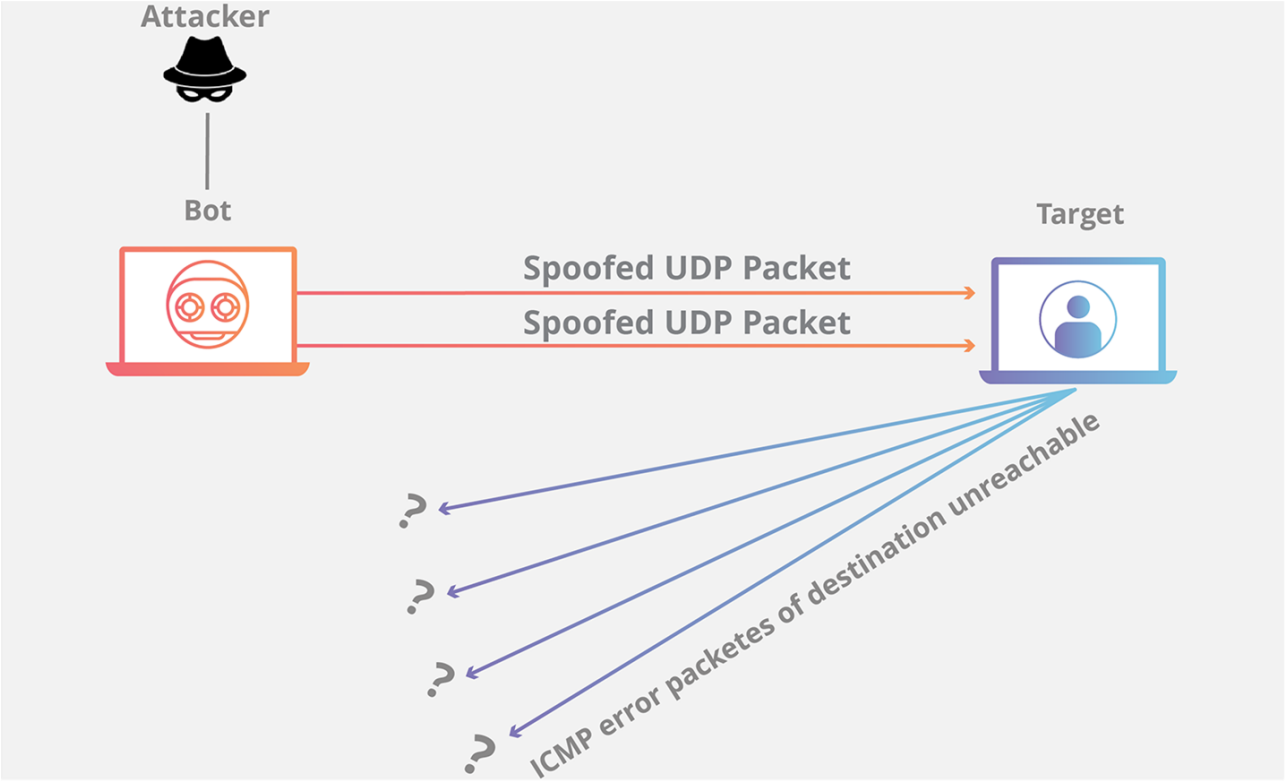
  - DSL routers, surveillance cameras, and IoT devices can be used



- protocol (pps---packets per second) : OSI Layer 3 or Layer 4
- application layer(rps---requests per second): OSI Layer 7

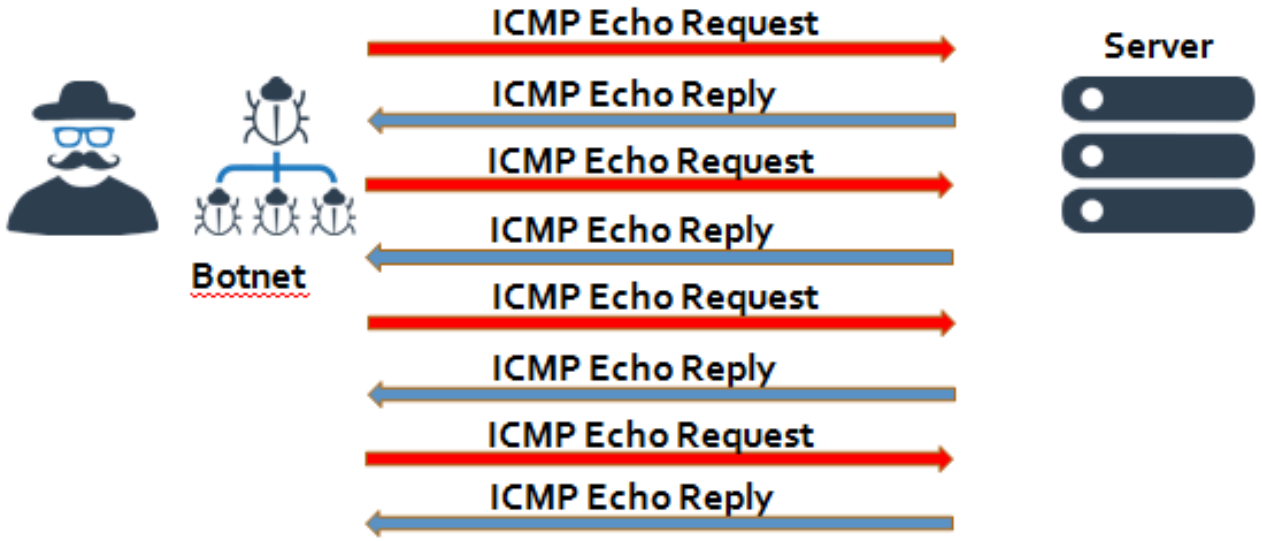
Denial of service

UDP Flood (Vol.)



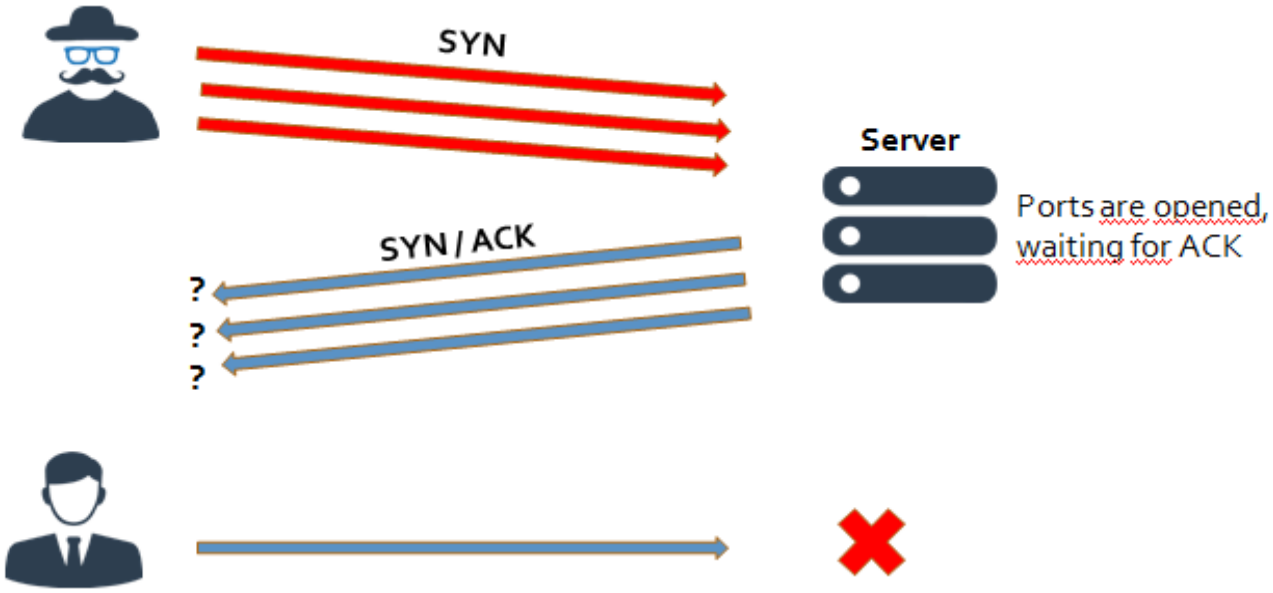
Denial of service

ICMP (Ping) Flood (Vol.)



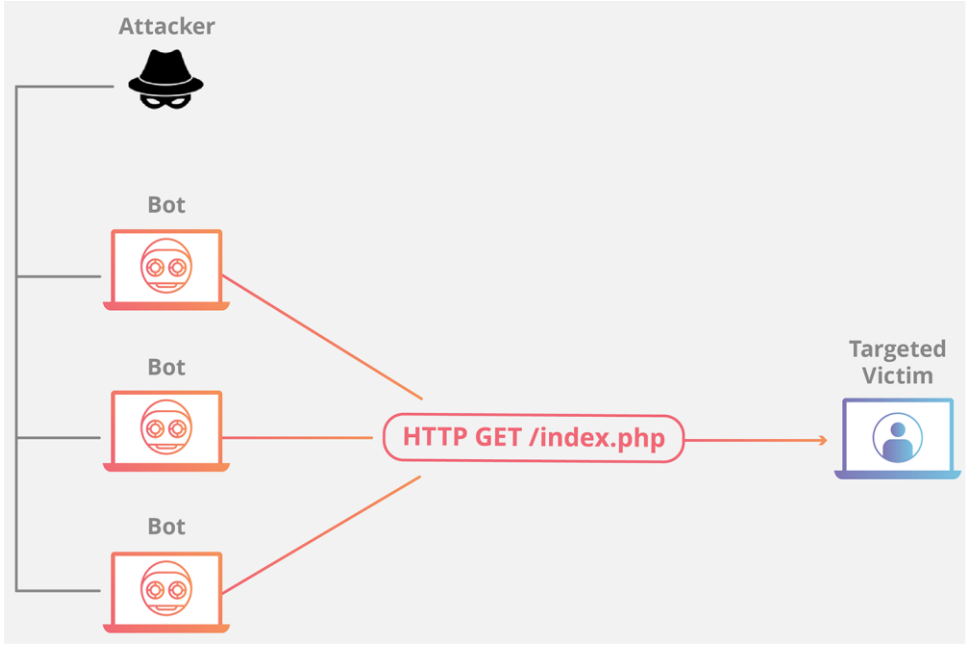
Denial of service

Syn Flood (Protocol)



Denial of service

HTTP Flood (App. Layer)



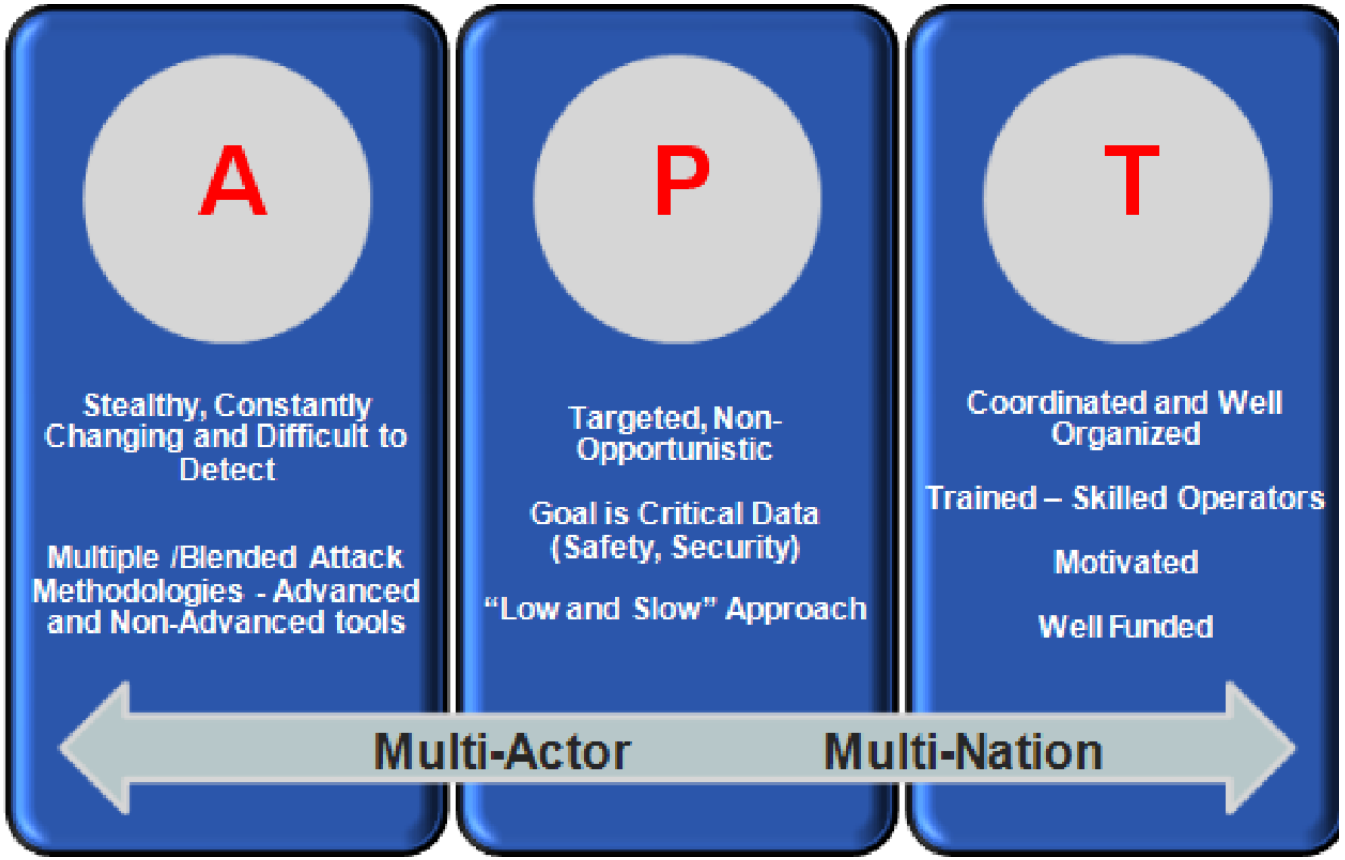
Phishing

- Social engineering
- Used to steal data
- Tricky email, instant message, or text message
- Recipient is then tricked into clicking a malicious link

Malware

- Virus: infect other files, need end users to kick them of
- Worm: self-replicating and spreads without end-user action
- Trojan: masquerades as legitimate programs, works when the victim executes
- Ransomware: encrypts all files

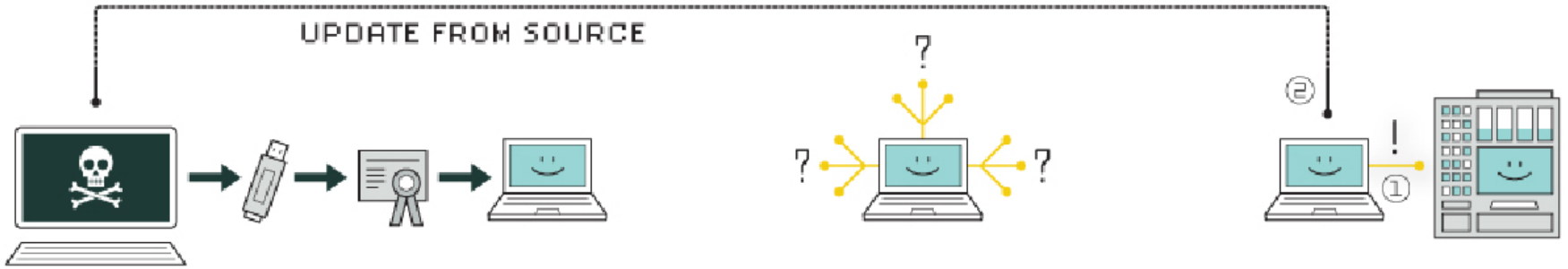
APT



- broad term: an intruder, or team of intruders, establishes an illegal, long-term presence on a network, in order to mine highly sensitive data

- Stage 1 – Infiltration: through the compromising of one of three attack surfaces: web assets, network resources or authorized human users.
- Stage 2 – Expansion: attackers move to broaden their presence within the network
- Stage 3 – Extraction: stolen information is stored in a secure location inside the network and then extracted without being detected

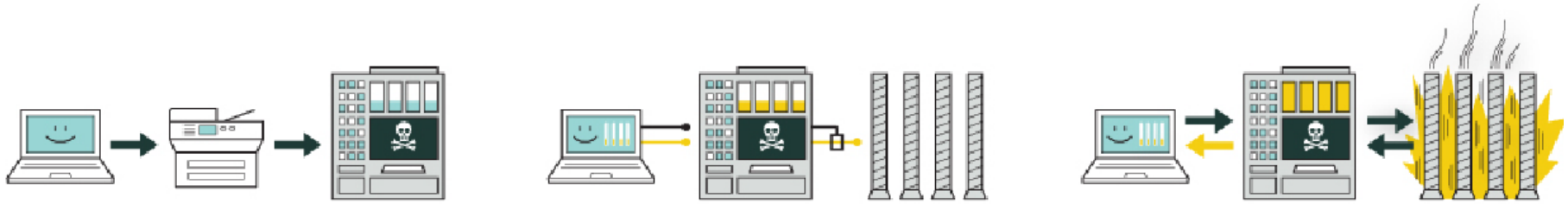
APT



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

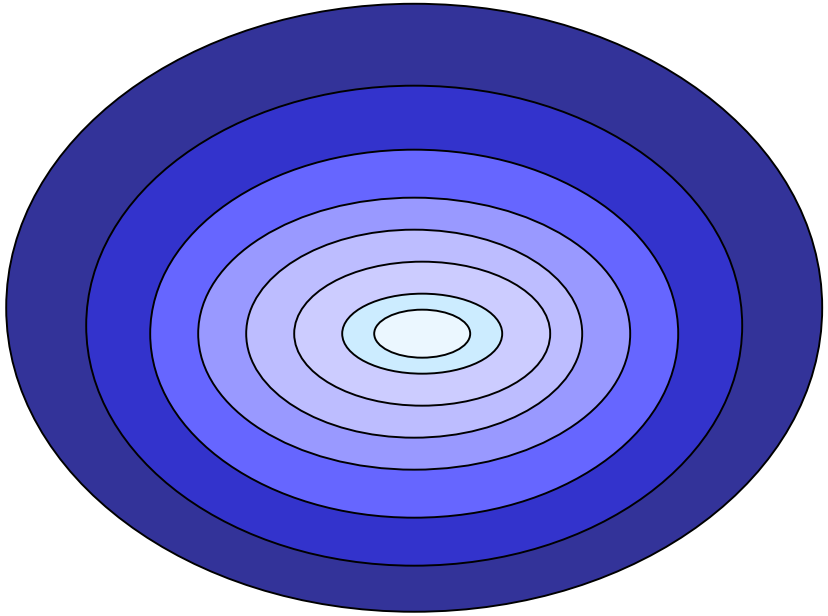


4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Security: Defense in Depth



like layers of an onion or a castle with multiple layers of defense:

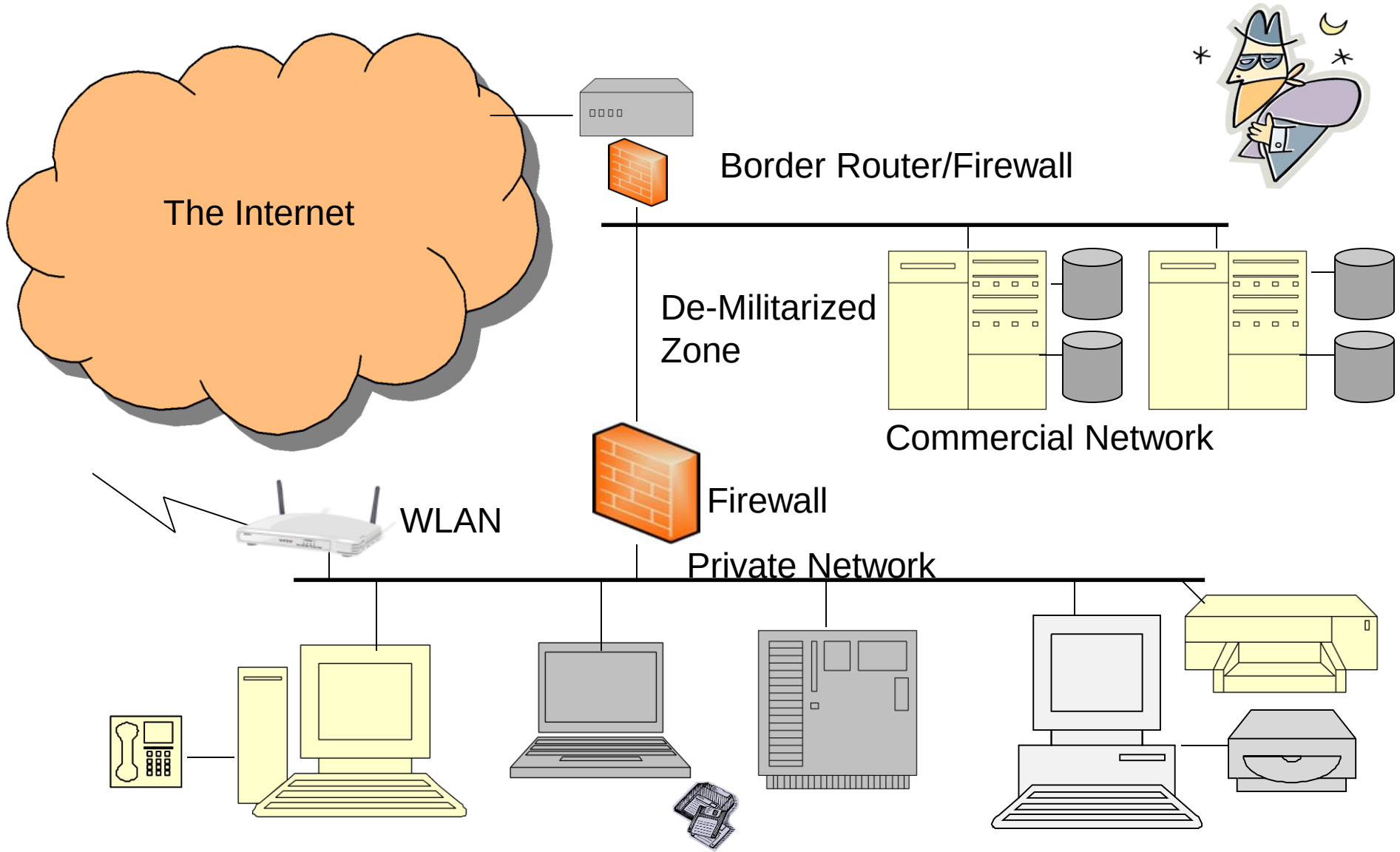
Border Router
Perimeter firewall
Internal firewall
Intrusion Detection System
Policies & Procedures & Audits
Authentication
Access Controls

Bastion Host

* Computer fortified against attackers
* Applications turned off
* Operating system patched
* Security configuration tightened

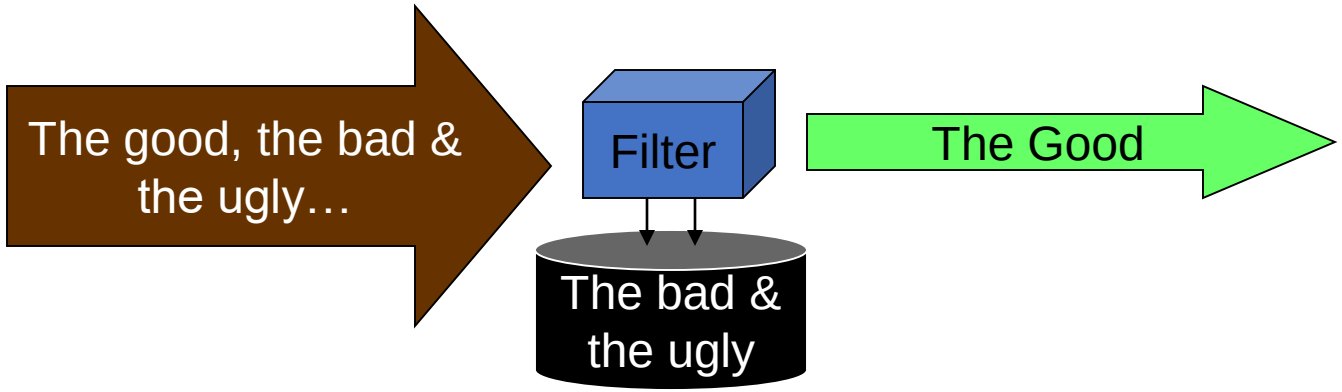
Attacking the Network

What ways do you see of getting in? Which one is the easiest?



- A good network: divided into sections
- De-Militarized Zone here is for public access.
- A DMZ contains external-facing services to an untrusted network, such as the Internet.
- Purpose of a DMZ is to add an additional layer of security to an organization's LAN.
- Private Network is for internal access, and requires going through 2 firewalls, each with filtering.

Filters: Firewalls & Routers



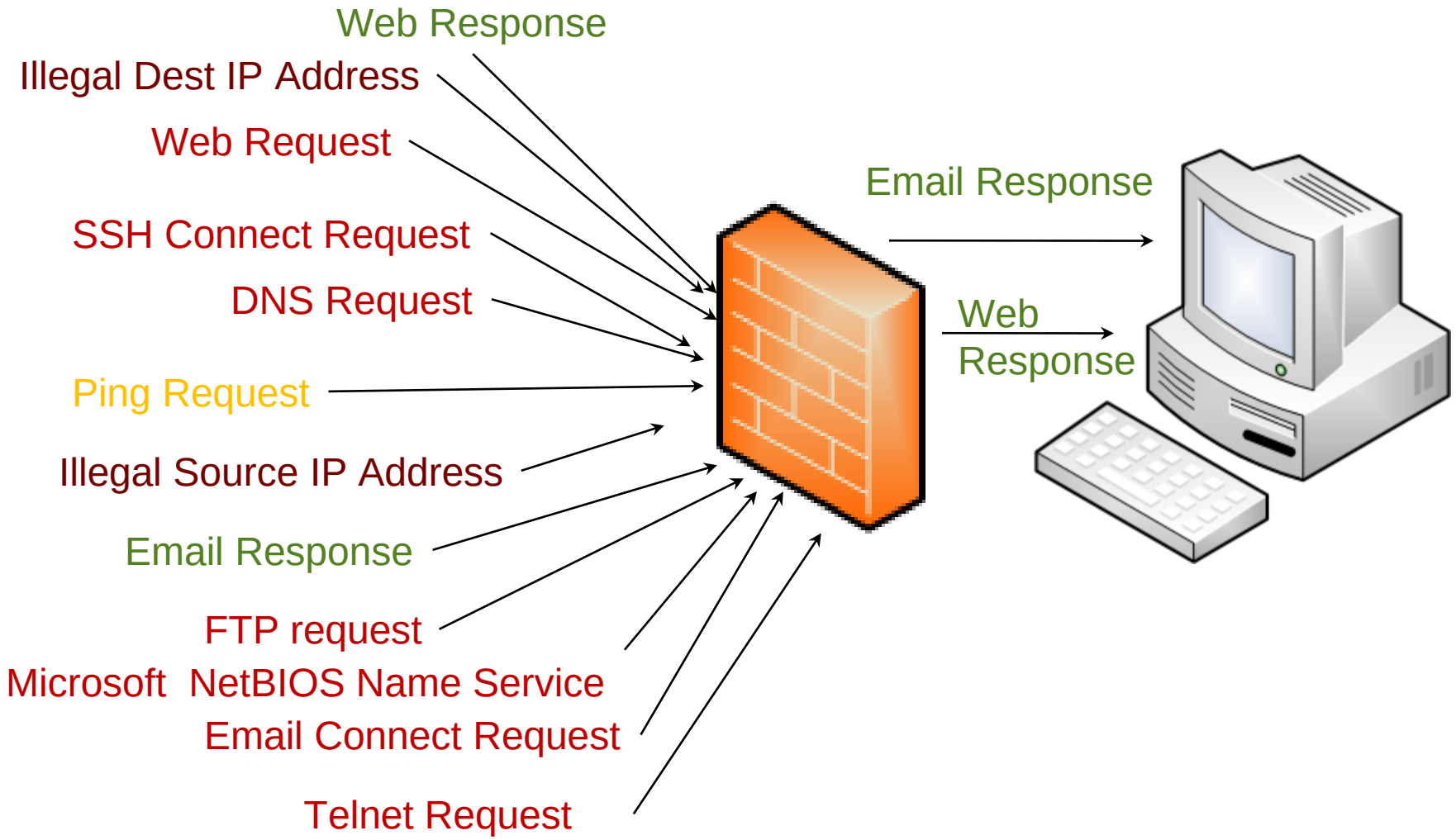
- Route Filter: Verifies source/destination IP addresses
- Packet Filter: Scans headers of packets: computer IDs and service IDs
- Content Filter: Scans contents of packet (e.g., IPS)

Fail Safe, Fail Close, Fail Secure: Default Deny - Any packet not explicitly permitted is rejected

Fail Open: granting all access

In which design availability is important more than security?

Packet Filter Firewall



Firewalls

Commercial

- Palo Alto Networks
- Check Point
- Fortinet
- Cisco

Open Source

- iptables
- pfSense

Leaders: execute well against their current vision and are well positioned for tomorrow

Visionaries: understand where the market is going or have a vision for changing market rules, but do not yet execute well

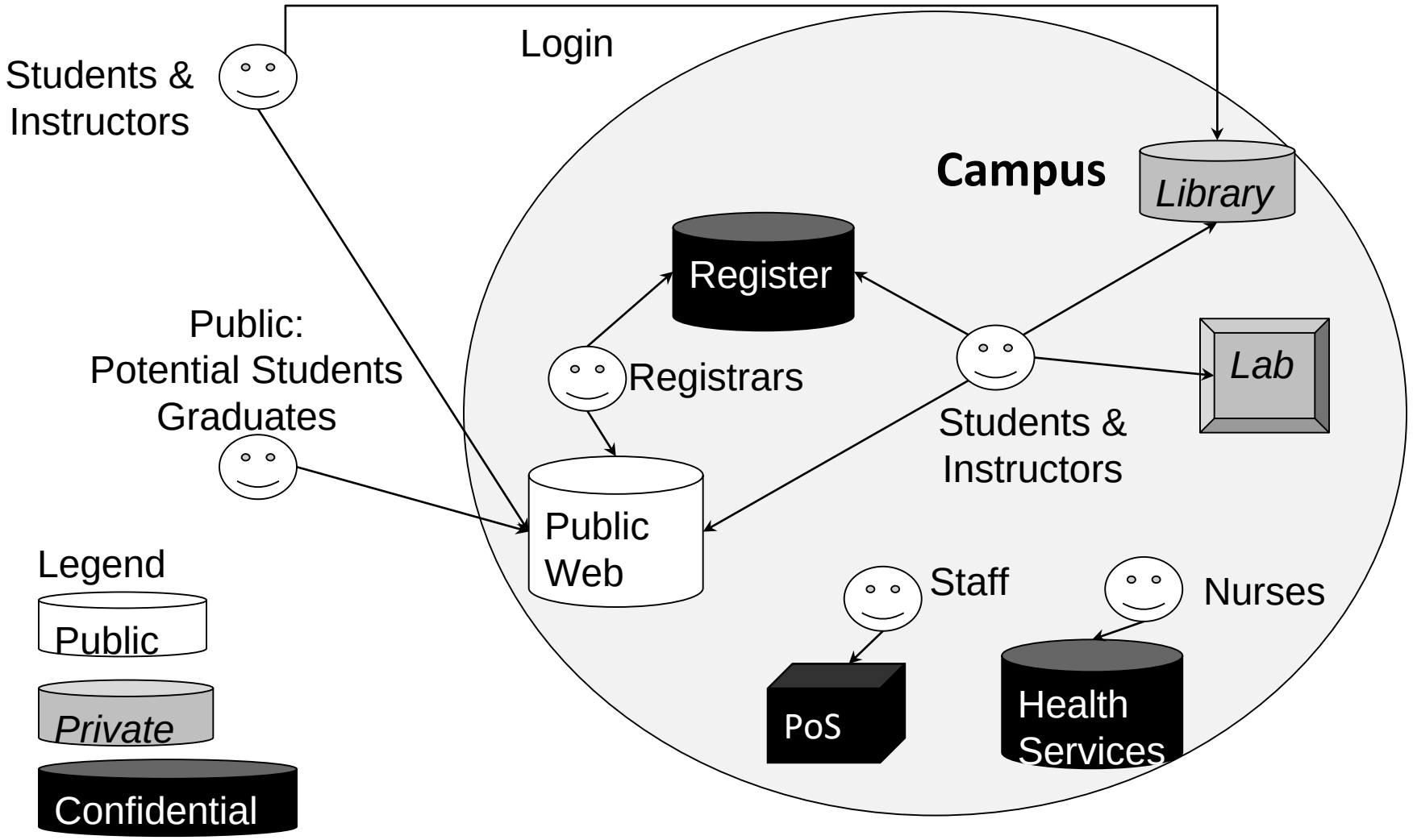
Niche Players: focus on a small segment, or are unfocused and do not out-innovate or outperform others

Challengers: execute well today or may dominate a large segment, but do not demonstrate an understanding of market direction

Firewalls – Next Generation

Packet Filter FW
IDS/IPS
Application Control
Anti Virus
Anti Bot
SSL inspection
DLP
…

Informal Path of Logical Access



Determine Services

Service (e.g., web, sales database)	Source (e.g., home, world, local computer)
Registration	Registrars: On campus
Library databases	On campus students and staff. Off-campus requires login
Health Services	On campus: nurses office
External (Internet) web services	On campus: Campus labs, dorms, faculty offices

Allocate Network Zones

Zone	Services	Zone Description
Internet		This zone is external to the organization.
DMZ	Web, Email, DNS	This zone houses services that the public are allowed to access in our network.
Wireless Network	Wireless local employees	This zone connects wireless/laptop employees/students (and crackers) to our internal network. They have wide access.
Private Server Zone	DBs	This zone hosts our student learning databases, faculty servers, and student servers.
Confidential Zone	Payment card, health, grades info	This highly-secure zone hosts databases with payment and other confidential (protected by law) information.
Private User Zone	Wired staff/ students	This zone hosts our wired/fixed employee/classroom computer terminals.

Define Controls

Zone	Service	Required Controls
DMZ	Web, Email, DNS	Hacking: Intrusion Prevention System, Monitor alarm logs, Anti-virus software within Email package.
Wireless Network	Wireless local users	Confidentiality: WPA2 Encryption Authentication: WPA2 Authentication
Private Server Zone	Classroom software, Faculty & student storage.	Confidentiality: Secure Web (HTTPS), Secure Protocols (SSH, SFTP). Authentication: Single Sign-on through Radius Hacking: Monitor alarm logs

Data Privacy

Confidentiality: Unauthorized parties cannot access information

(->Secret Key Encryption)

Authenticity: Ensures claimed sender = actual sender.

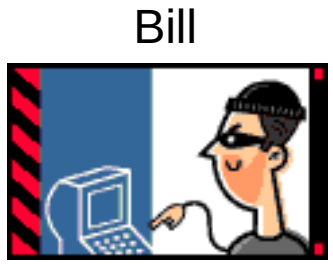
(->Public Key Encryption)

Integrity: Ensures the message is not modified in transmission.

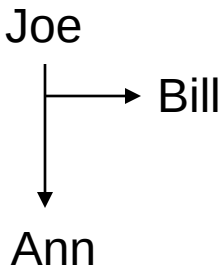
(->Hashing)

Nonrepudiation: Ensures sender cannot later deny sending message.

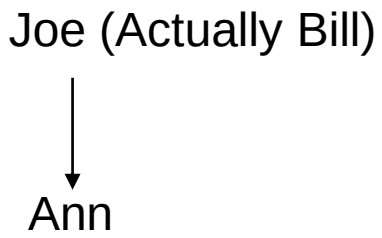
(->Digital Signature)



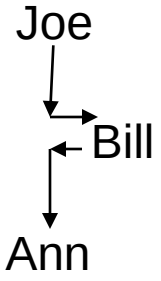
Confidentiality



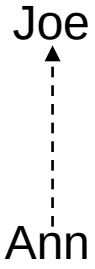
Authenticity



Integrity



Non-Repudiation



Confidentiality:

Encryption – Secret Key

Examples: DES, AES

Sender, Receiver have IDENTICAL keys

Plaintext = Decrypt(K_{secret}, Encrypt(K_{secret},Plaintext))

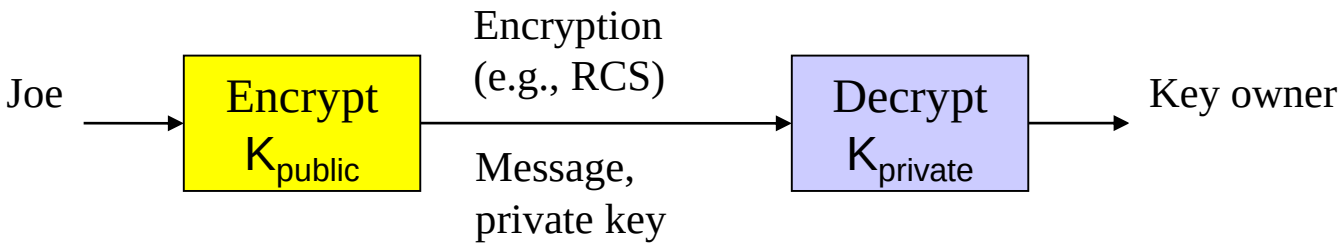
Confidentiality, Authentication, Non-Repudiation

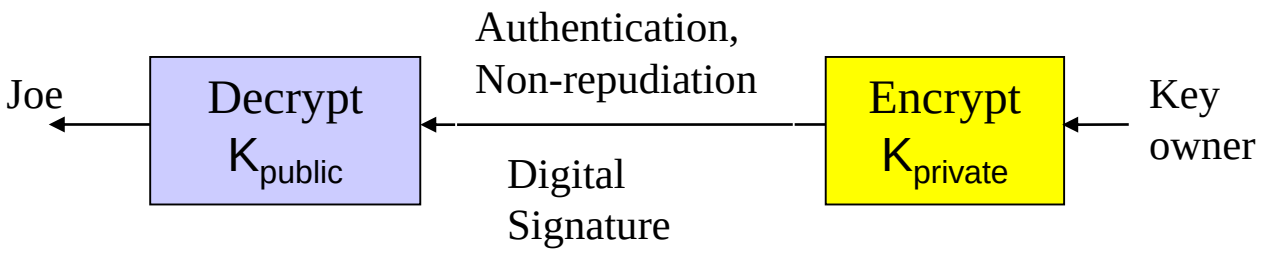
Public Key Encryption

Examples: RSA, ECC, Quantum

Sender, Receiver have Complimentary Keys

Plaintext = Decrypt(k_{PRIV}, Encrypt(k_{PUB},Plaintext))



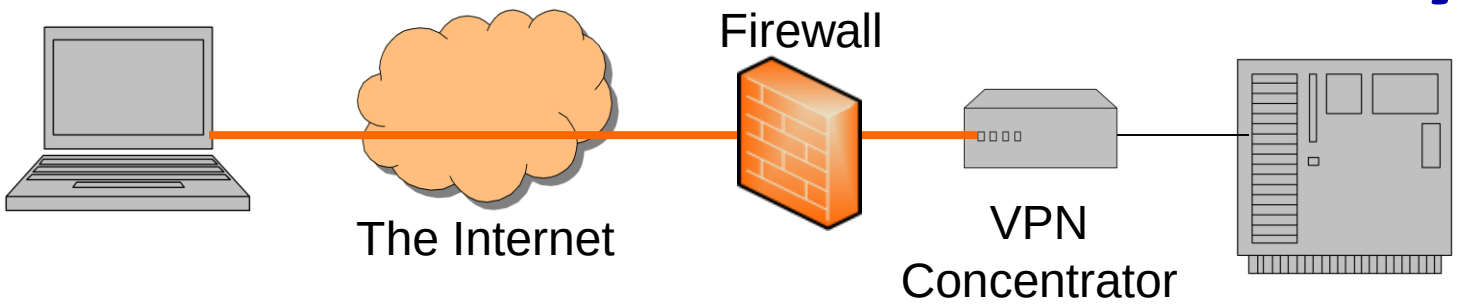


Plaintext = Decrypt(k_{PUB}, Encrypt(k_{PRIV},Plaintext))

PK enc. is processor-intensive, and not useful for long term data communications sessions. Therefore, it is often used to change a Secret key(session key) between two endpoints, and then Secret key is used to enc. data.

Confidentiality:

Remote Access Security



Virtual Private Network (VPN): encrypted point-to-point path between two nodes, often implemented with IPSec

Can authenticate and encrypt data through Internet (red line)

Easy to use and inexpensive

Difficult to troubleshoot

Susceptible to malicious software and unauthorized actions

Often router or firewall is the VPN endpoint

Integrity:

Hash Functions

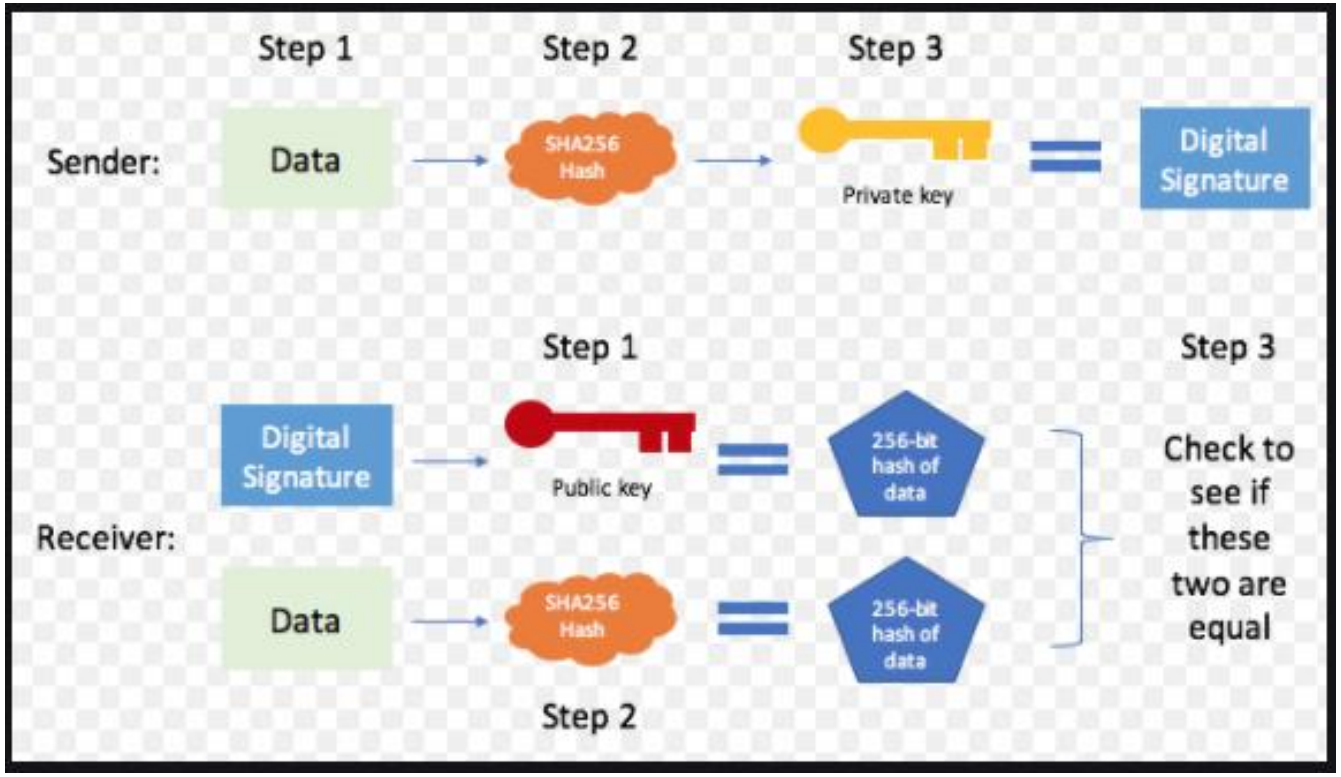
Examples: SHA-2, SHA-3

Ensures the message was not modified during transmission

H = Hash Algorithm

H=Hashed Value

Non-Repudiation:
Digital Signature



Public key algorithm

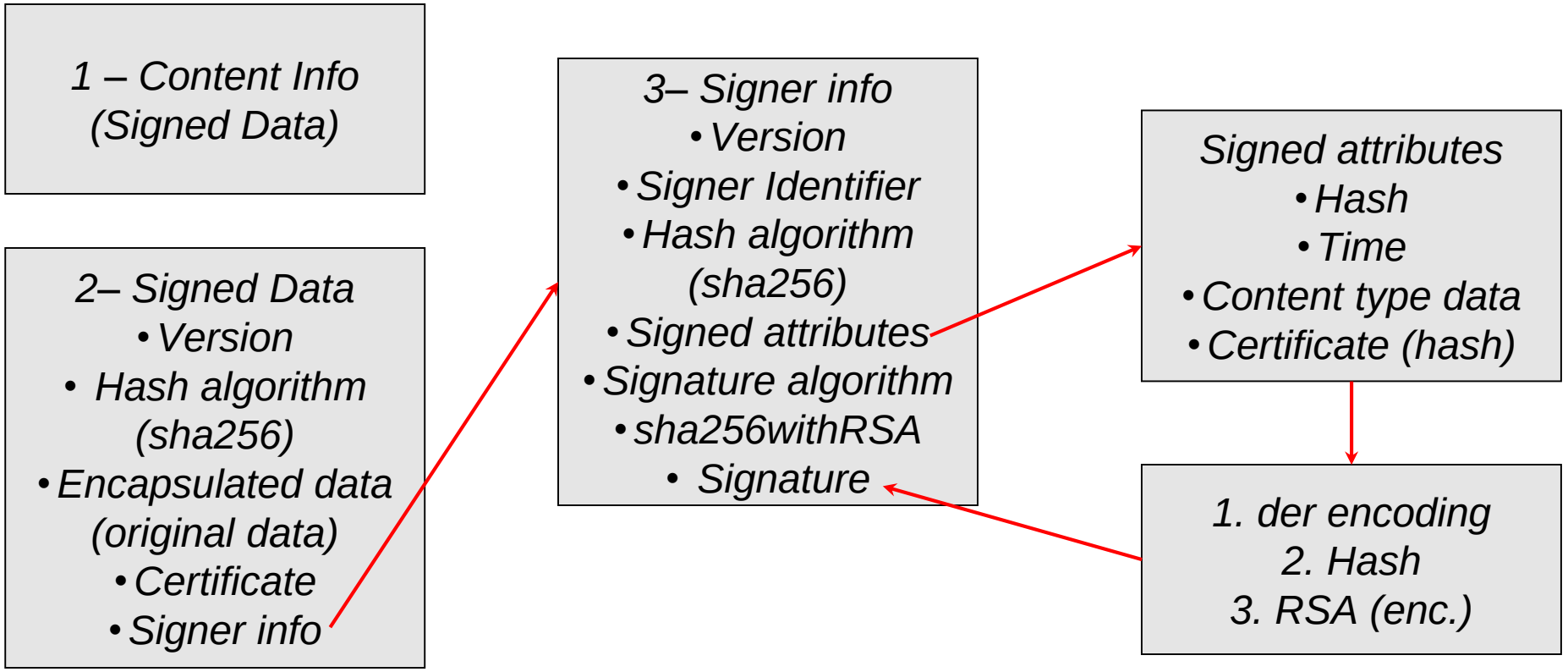
Verifies integrity of data

Verifies identity of sender: non-repudiation

Non-Repudiation:

Digital Signature

X.509 public key infrastructure (PKI)



Authentication:

Public Key Infrastructure (PKI)

7. Tom confirms Sue's DS

Tom

5. Tom requests Sue's DC □
6. CA sends Sue's DC □

Certificate Authority (CA)

Digital Certificate
User: Sue
Public Key: 2456

4. Sue sends Tom message signed with Digital Signature

3. Send approved Digital Certificates

Sue

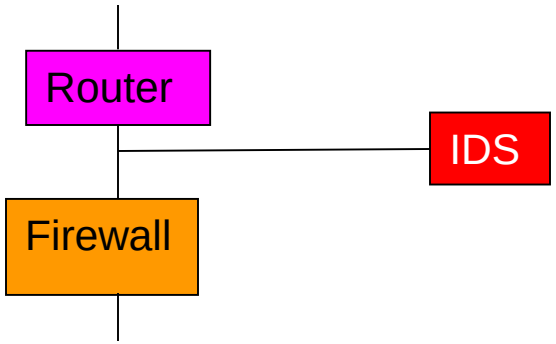
1. Sue registers with CA through RA

Register(Owner, Public Key)

2. **Registration Authority** (RA) verifies owners

Hacking Defense:

Intrusion Detection/Prevention Systems (IDS or IPS)

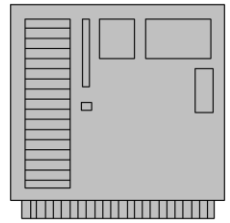


Network IDS=NIDS

Examines packets for attacks

Can find worms, viruses, or defined attacks

Warns administrator of attack



Host IDS=HIDS

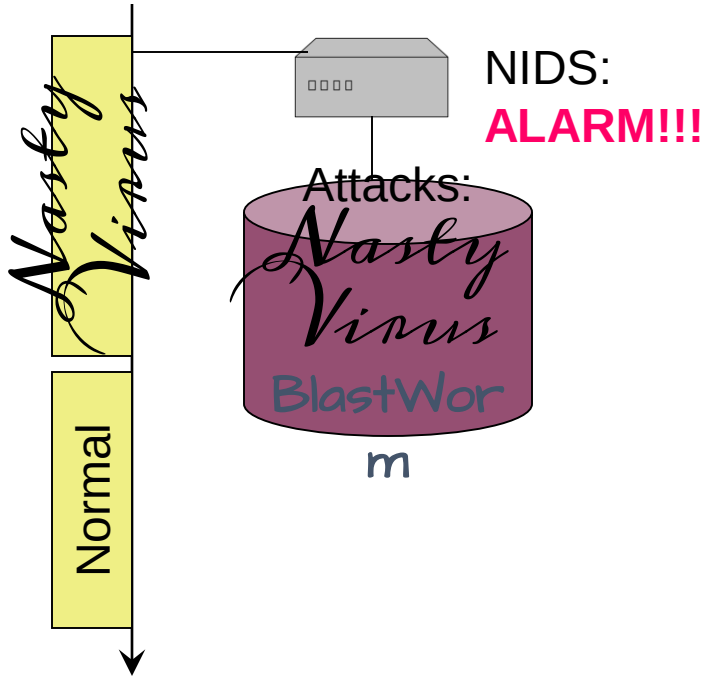
Examines actions or resources for attacks

Recognize unusual or inappropriate behavior

E.g., Detect modification or deletion of special files

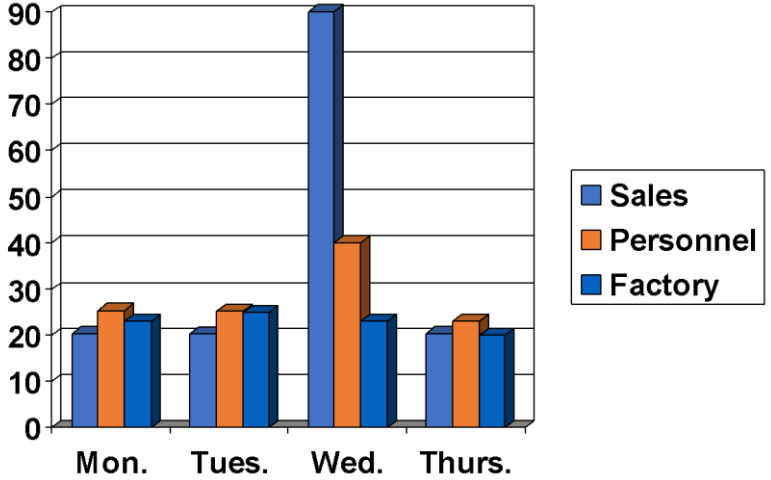
Hacking Defense:

IDS/IPS Intelligence Systems



Signature-Based:

Specific patterns are recognized as attacks



Statistical-Based:

The expected behavior of the system is understood

If variations occur, they may be attacks (or maybe not)

Neural Networks:

Statistical-Based with self-learning (or artificial intelligence)

Recognizes patterns

Hacking Defense:
IDS/IPS

Commercial

- Cisco
- Intel Security (McAfee)
- Trend Micro (Tipping Point)

Open Source

- Snort
- Suricata

Hacking Defense:
WAF

SQL injection
Cross-site scripting
Local File Inclusion
Remote File Inclusion
Remote Code Execusion
PHP Code Inclusion
….

Hacking Defense:

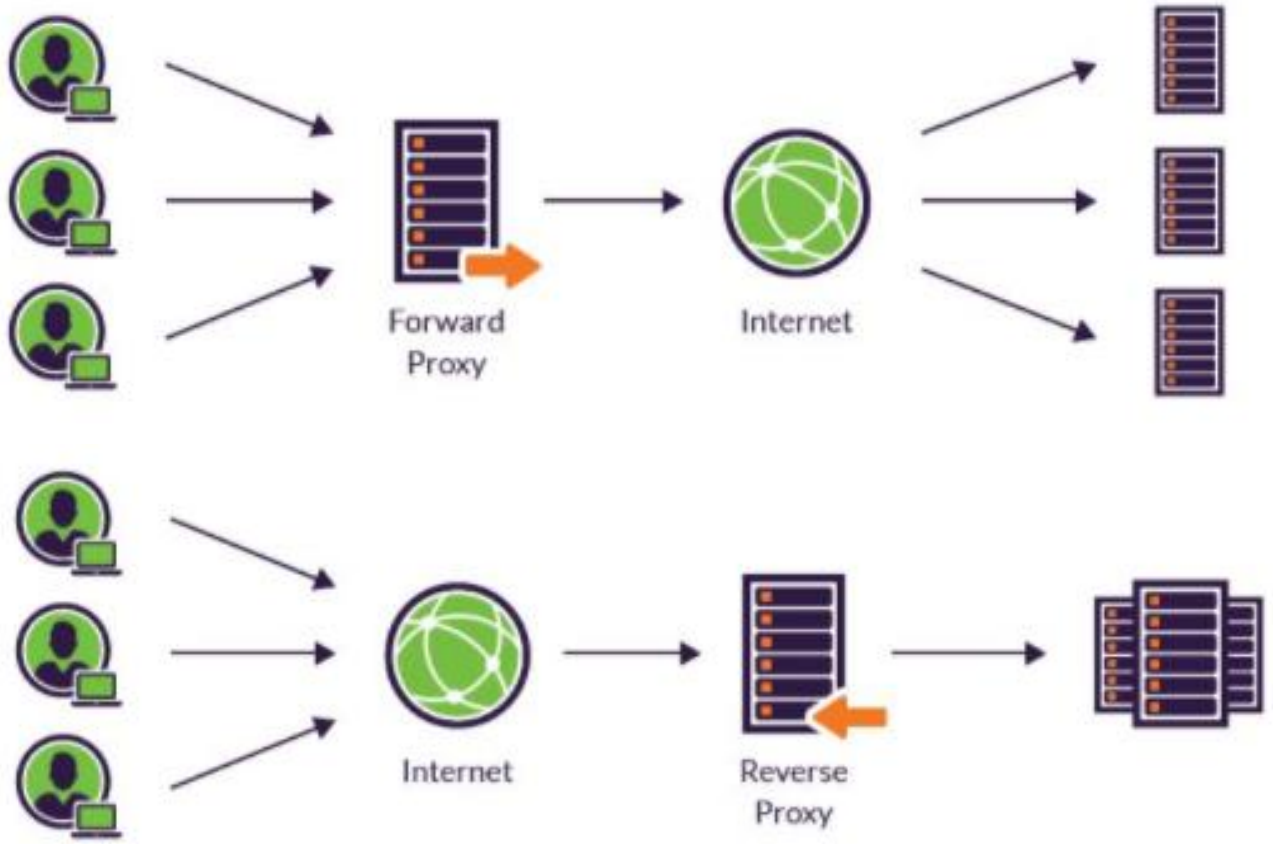
WAF

Commercial
- Imperva
- F5
- Akamai

Open Source
- ModSecurity
- IronBee

Hacking Defense:

Web Proxy (Web Gateway)



A forward proxy server: a web server that acts as a gateway between a client application (e.g. a browser), and the real server.

makes requests to the real server on behalf of the client, two purposes: to filter requests (monitor, block) and improve performance (caching external site content).

A reverse proxy server: pass on requests from web clients to web servers; load balancing, IP masking, traffic scrubbing (DDoS mitigation, wep app sec), content caching-rapid content delivery

Hacking Defense:
Web Proxy

Commercial
- Symantec
- Zscaler

Open Source
- Squid
- Varnish

Hacking Defense:

Honeypot & Honeynet

Honeypot: A system with a special software application which appears easy to break into

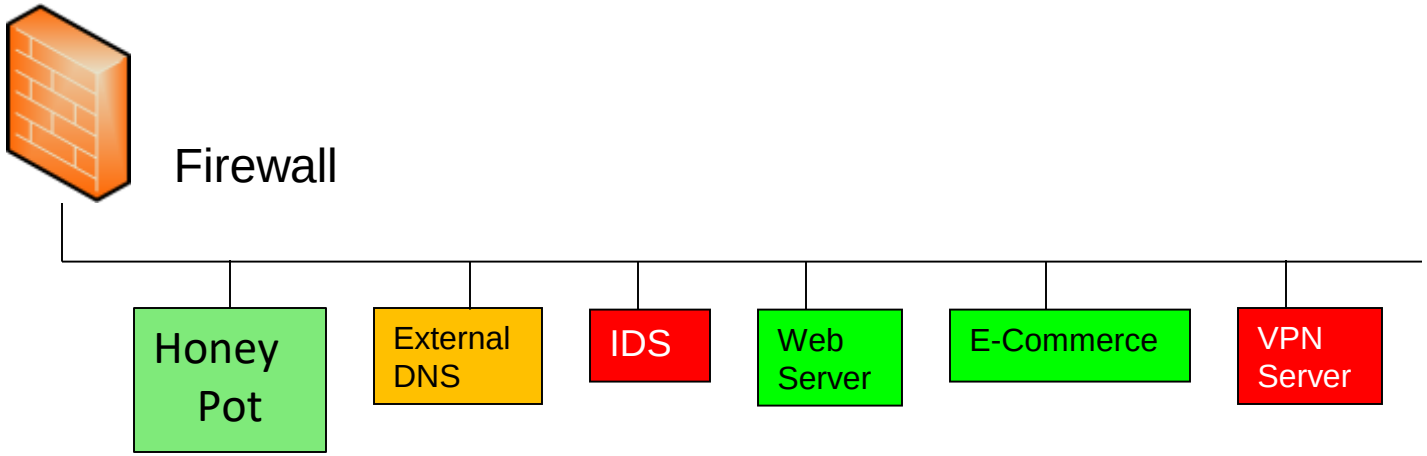
Honeynet: A network which appears easy to break into

Purpose: Catch attackers

All traffic going to honeypot/net is suspicious

If successfully penetrated, can launch further attacks

Must be carefully monitored



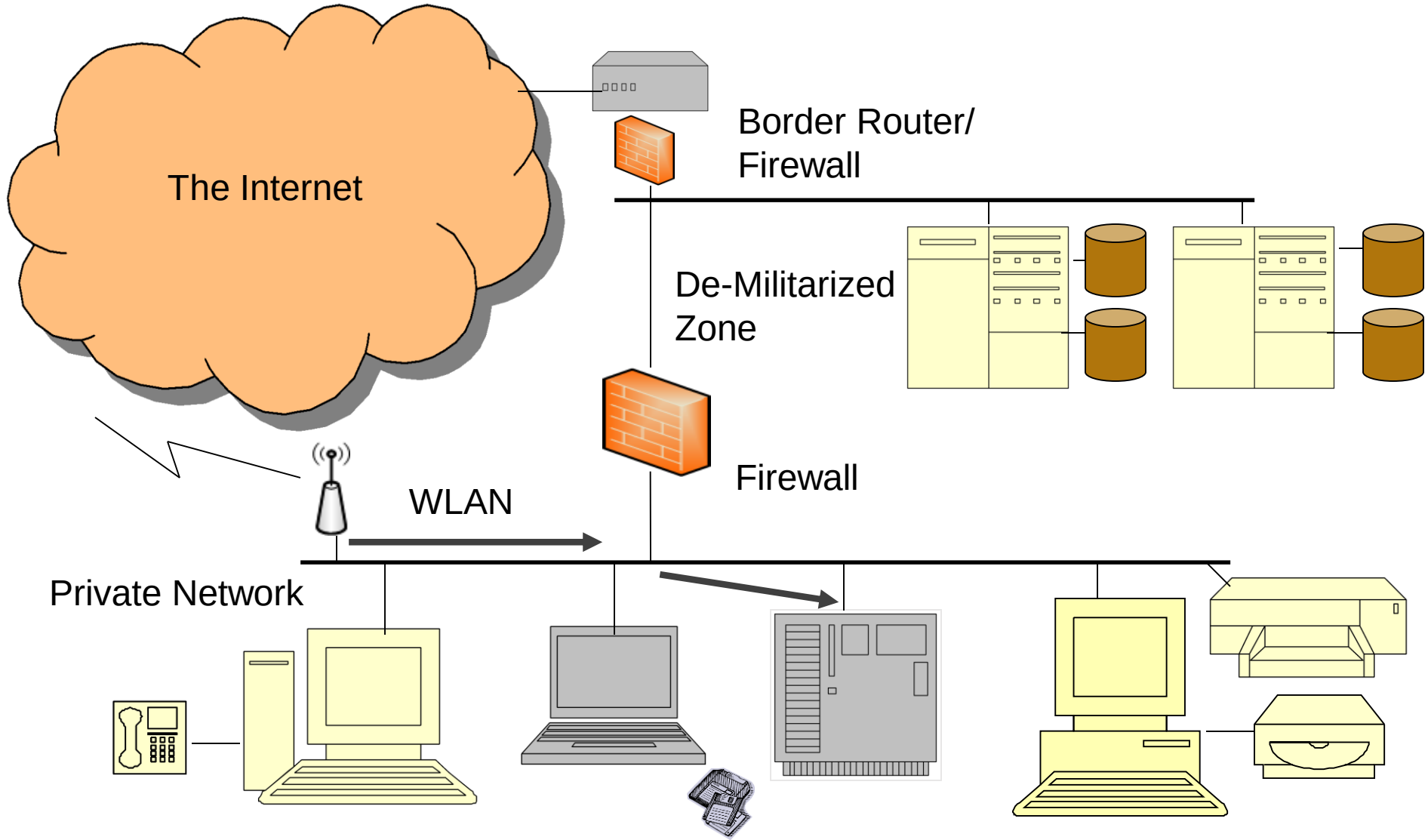
Hacking Defense:

Vulnerability Assessment

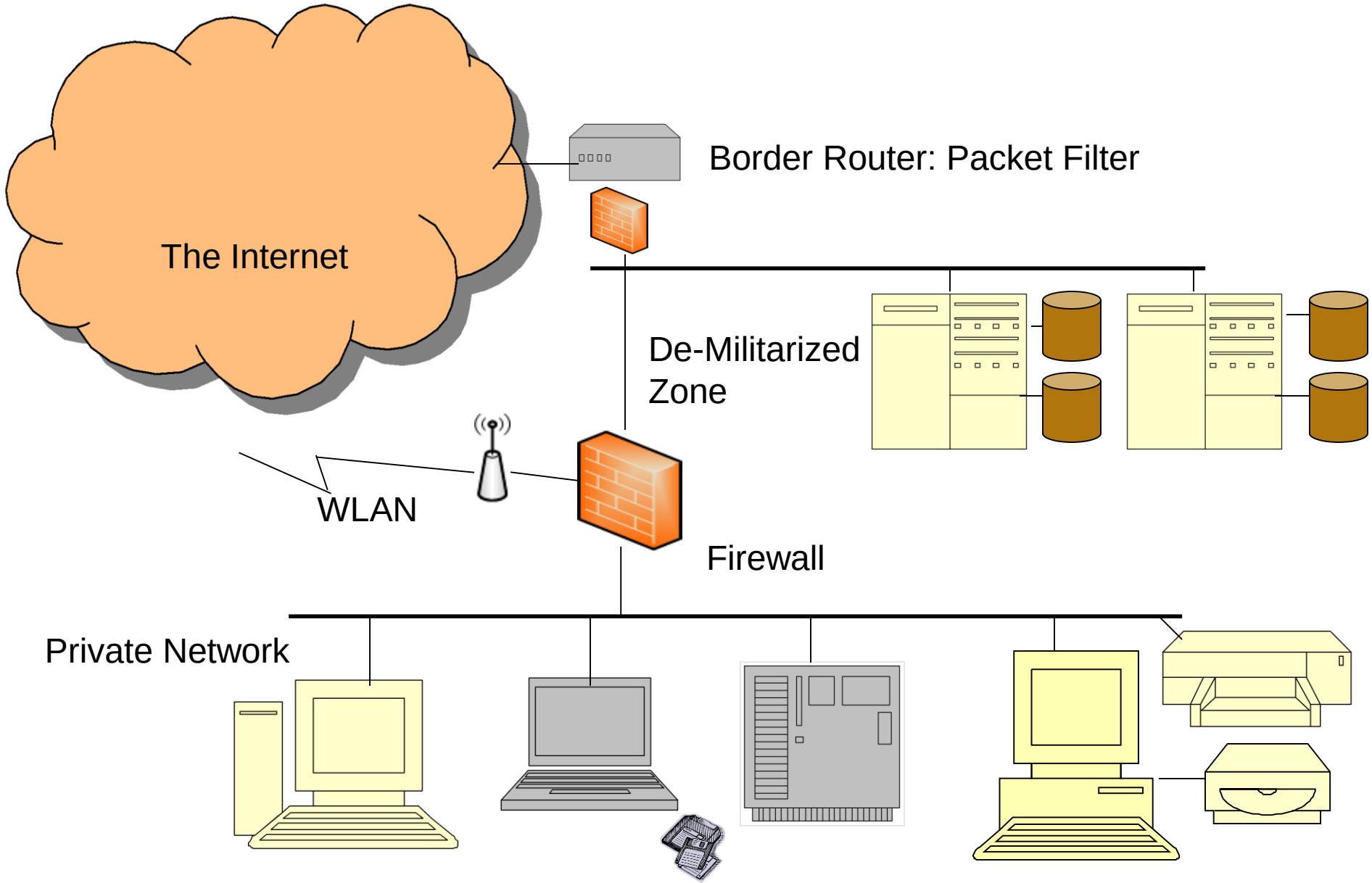
* Scan servers, work stations, and control devices for vulnerabilities
* Open services, patching, configuration weaknesses
* Testing controls for effectiveness
* Adherence to policy & standards
* Penetration testing

Path of Logical Access

How would access control be improved?



Protecting the Network



End User Security Systems

Host FW
Host IPS
Anti Virus, Endpoint Security Systems
Endpoint Detection and Response (EDR)
DLP
Sandbox
Application Control
Encryption

...