

Security Threats, Vulnerabilities, and Controls

Types of Malware

Malware Type	Description
Virus	A piece of code that spreads from one device to another by attaching itself to other files. The code executes when the carrier files is opened. Often, they pave the way for other attacks, send data to the attacker, or corrupt or destroy data.
Worm	A piece of code that spreads from one device to another without attaching itself to another file. Often, they pave the way for other attacks, send data to the attacker, or corrupt or destroy data.
Trojan horse	A software attack that paves the way for other attacks. Social engineering is involved, since the user must be tricked into running the Trojan horse software.
Logic bomb	A piece of code that sits dormant on a target device until it is triggered by a specific event, such as a date. Then, the logic bomb "detonates," and performs the actions it was programmed to do, such as erasing and corrupting data on the target system.

Types of Malware

Malware Type	Description
Spyware	Surreptitiously installed malicious software that tracks and reports the usage of a target system, or to collect other data the author wants to obtain, such as web browsing history, personal information, banking and other financial information, and user names and passwords.
Adware	Software that automatically displays or downloads advertisements when it is used. While not all adware is malicious, many adware programs have been associated with spyware and other types of malicious software.
Rootkit	Code that takes control of a system at the lowest levels. Rootkits often attempt to hide themselves from monitoring or detection, and modify low-level system files when integrating themselves into a system.
Ransomware	Malicious code that restricts access to a user's device or the data stored on it until the victim pays the attacker to remove the restriction. Ransomware is often implemented as a Trojan horse and can use file encryption to restrict access to data.
Spam	Spam is an email-based threat that presents advertising materials, promotional content, or get-rich-quick schemes to users. The messages can quickly fill a user's inbox and cause storage issues. Spam can also carry malicious code and other types of malware.

Malware & Virus Overview

- <https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>
- Differences between Malware, Trojans, Worms.
 - <https://youtu.be/n8mbzU0X2nQ>
- European Institute for Computer Anti-Virus Research (EICAR)
 - Anti Malware Test File
 - <https://www.eicar.org/download-anti-malware-testfile/>
- Batch File Example (Warning: Do Not type this in!)

```
@echo off
cd C:Documents and SettingsusernameDesktop
:loop
md %RANDOM%
goto loop
```

Social Engineering

- Deception and trickery to convince users to part with sensitive data
- Human factors and not technological
- Takes advantage of users trust, especially if they are not technically aware.
- Exploiting peoples desire to be helpful and “nice” and trusting and not be embarrassed.

Social Engineering

- Shoulder Surfing – looking over a persons shoulder
- Spoofing -pretending to be someone else for identity concealment
- Impersonation – attacker pretends to be someone and asks for the information required. Impersonation.
- Tail gating
- Hoax – normally email to trick user to perform undesired actions

Social Engineering

- Phishing – Email based social engineering. Emails appear to come from a reputable source, designed to get a users information
- Vishing – to get users information when they use services such as VoIP. Also called voice phishing.
- Whaling – A form of Phishing to target individuals with wealth. Also called spear Phishing.
- Spam – Categorised as social engineering!

Phishing Example

From PayPal <Ebay@ebay.co.uk>★

Subject **Log in to PayPal to resolve a limitation on your account !**

To swaraj★



Dear customer,

We received a request to reset the password associated with your account.
This request was generated by a user from IP address 82.30.120.166 clicking the "Forgot Password" . If you did not request to have your password reset,


Please take advantage of our verification process and decrease your fraud risks

What you can do to minimise fraudulent transactions?

- 1.Download the attached document and open it in a secure browser .
- 2.Follow the instructions.

Thank you,

Copyright 2014 . All rights reserved Email ID PP85942

▶  1 attachment: Document-PayPal.html size unknown

Types of Attack

Attack Type	Description
Zero day attack	Exploits a previously unknown vulnerability in an application or OS.
Brute force attack	Uses password-cracking software to try every possible alphanumeric combination.
Dictionary attack	Automates password guessing by comparing encrypted passwords against a list of possible values.
Eavesdropping or sniffing attack	Uses special monitoring software to intercept private network communications, either to steal the content of the communication itself or to obtain user names and passwords for future software attacks.
Man-in-the-middle attack	A form of eavesdropping where the attacker makes an independent connection between two victims and relays information between the victims as if they are directly communicating over a closed connection, when in reality the attacker is controlling the information that travels between the victims.

Types of Attack

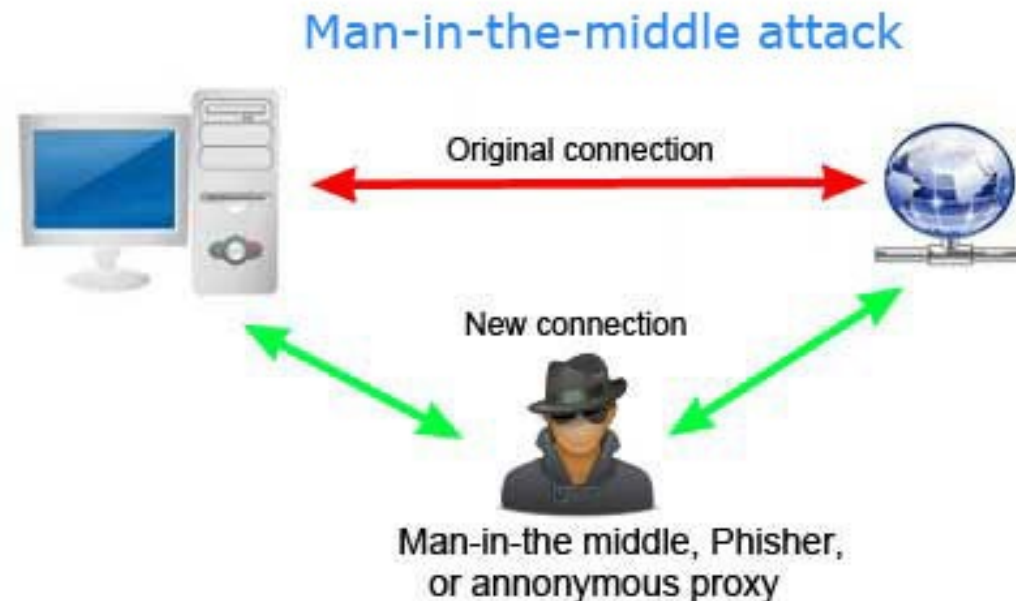
- Spoofing Attack
 - <https://www.malwarebytes.com/spoofing>
 - The person masquerades as someone else.
- Keyloggers
 - Software or Hardware that records the key presses on a PC
- Rootkits
 - Ability to hide malicious SW from the Operating System
 - Designed to fool anti virus / malware software
- SQL Injection
 - Structured Query Language
 - Inserted into URL's
 - To prevent – Back end sanitisation.

Common Software Threats

- Ransomware
 - 24 June 2019
 - <https://www.bbc.co.uk/news/av/technology-48707033/ransomware-cyber-attacks-are-targeting-large-companies-and-demanding-huge-payments>
- **Backups are Critical**

Man in the middle (On Path Attack)

- an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other



Man-in-the-Middle Attack Example

Jack
Victim 1

Peter
Man in the
Middle

Jill
Victim 2

Send over your key

Send over your key

Peter sends his
own key to Jack

Jill sends her key to Jack

Jack sends his account
number as 123456789

Peter sends Jill his account
number 987654321

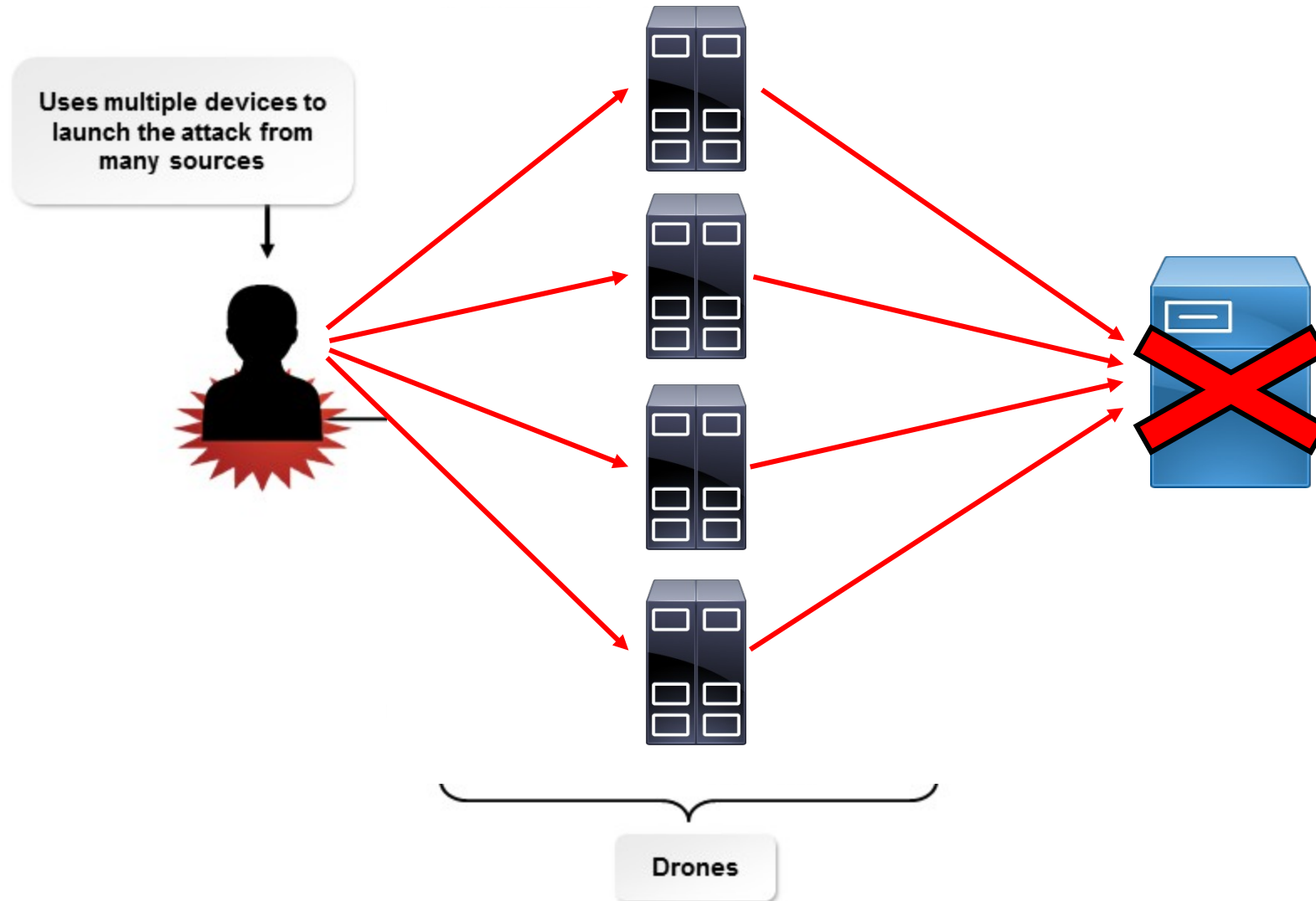
Jill sends money to
the wrong account

The MITM
attack
is complete

Zombies and Botnets

- Denial of Service Attack
 - ICMP based
 - Ping
- Distributed Denial of Service (DDoS) attack
 - Multiple devices to attack a source simultaneously
 - Uses software called a Zombie or Drone
 - Botnets are a collection of programs that communicate with others similar programs to perform tasks
 - Forged IP addresses
 - Reflective (or smurf) – Uses a third party server to respond to false addresses
 - Amplified – Small request to a third party server that makes large response to victim
 - DNS queries can be used in this way

Zombies and Botnets



Symptoms

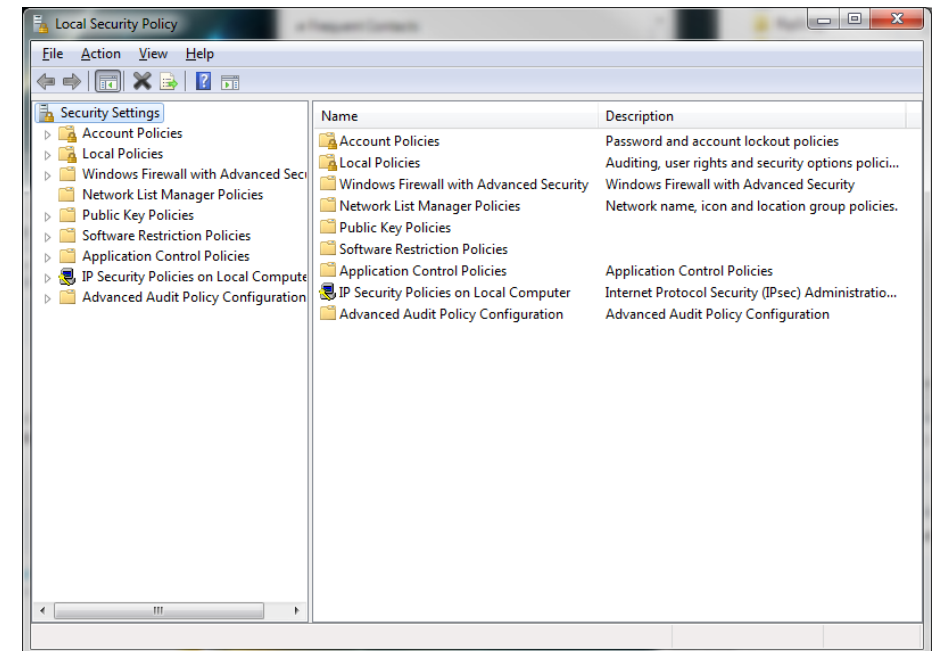
- Programs load more slowly
- Unusual files appear
- Files start to disappear
- Program size changes
- Browser plays up
- System shuts down
- Excessive HD activity
- Access limited
- System doesn't reboot
- All of the above!

Non Compliant Systems

- Any system that doesn't have permission to connect to the network
- A system that doesn't meet the minimum security requirements.
 - Use windows security policies to enforce compliance
- Windows Security Policies
 - Configuration settings to control overall security
 - Local Security Policy is a subset of the comprehensive local policy object

Windows Security Policies

- Active Directory
 - Uses LDAP (Lightweight Directory Access Protocol)
- Microsoft Management Console (MMC)



Windows Security Policies

- Active Directory
 - Uses LDAP (Lightweight Directory Access Protocol)
- Domain
 - Hierarchical collection of security objects
 - Users, computers, policies
 - Named with DNS convention
 - Organisational Units
 - Allows objects to be grouped together

Security Best Practices

Practice	Description
Manage user authentication	<ul style="list-style-type: none">• Change the default user account name and password on each device.• Require all users to create strong passwords and to protect those passwords.• When necessary, implement multifactor authentication, including smart cards or biometric authentication systems.
Install updates and patches	<ul style="list-style-type: none">• Install the latest OS service packs and security updates.• Install the latest application patches for OS utilities and web browsers, not just third-party applications.
Manage user accounts	<ul style="list-style-type: none">• Use policy settings to disable guest and other unneeded accounts.• Restrict user permissions.
Educate users	<ul style="list-style-type: none">• Train users to recognize and avoid hoaxes, phishing attacks, and potential sources of malware.
Apply device security measures	<ul style="list-style-type: none">• Implement antivirus software.• Block pop-ups in web browsers.• Install and configure firewalls.• Use warning messages and banners at user login.• Disable the autorun feature for external storage devices.• Enable screen locks for idle systems.• Enable automatic OS updates.• Limit the shared resources available on a system.

Violations of Security Best Practices

- Follow your organisations security policy
- Notify the user of non-compliant systems.
- Automatically install patches and updates to bring systems into compliance.
- Test for malware, and then install or update antimalware software.

Security Incident Reports

- Security Incident Management
 - Practices and procedures on managing an incident
 - Goal is to contain an incident
 - Minimise the damage
 - Requirement to log and report all incidents with actions taken

Security Incident Reports

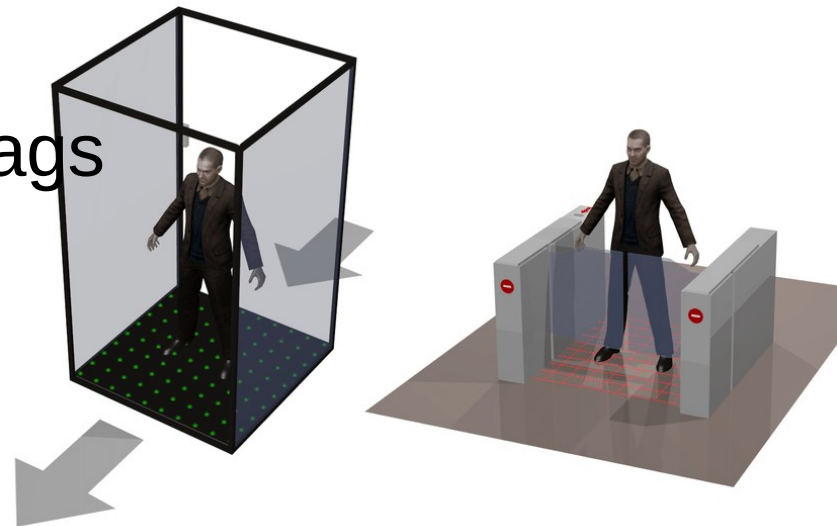
- Type of incident
- Severity of incident
 - How many people/devices affected?
 - Work stoppage?
 - Data lost or compromised?
- Names of those involved
 - Titles
 - Phone numbers
 - Email addresses
- Full description of the incident
- Actions taken to mitigate the incident

General Security Controls

- Safeguards and methods to avoid, counteract, or minimize security risks.
- Categories:
 - Physical controls (Fences, doors, locks etc)
 - Procedural controls (Incident response processes, management oversight, security awareness, training)
 - Digital controls (User Authentication, AV Software, Firewalls)
 - Legal, regulatory, and compliance controls (Privacy laws, policies and clauses)

Physical Security

- Implementing controls to restrict physical access to facilities.
- Mantrap (also called Access Control Vestibule)
 - Prevents tailgating
 - Two controlled doors
 - Commonly uses RFID tags



Physical Security

- Identification badges used to provide proof of access
 - Often RFID (Passive)
 - Problems when stolen/lost
 - Provides an audit of access
- Video Surveillance
 - Backbone of physical security
 - Fixed or PTZ (Pan Tilt Zoom)
 - Coaxial Connection (legacy)
 - Can use media converter to make IP camera
 - Ethernet Connected
 - Ethernet allows PoE devices
 - Allows VLAN isolation
 - ANPR
- Motion Detector
 - Commonly Passive Infra Red (PIR)



Physical Security

- Implementing controls to restrict physical access to facilities.
- Increasing or assuring infrastructure elements:
 - Electrical power
 - Data networks
 - Fire suppression
- Protecting against:
 - Facilities intrusion
 - Electrical grid failure
 - Fire
 - Personnel illnesses
 - Data network interruptions

Physical Security Measure	Description
Locking doors	<ul style="list-style-type: none">• Lock and key: restriction on duplicate keys.• Combination/cipher locks.• Electronic door locks with ID cards.• Biometric door locks.• Hardware locks to secure portable items and file cabinets.
Mantraps	Two sets of interlocking doors inside a small space, where the first set of doors must close before the second set opens.
Logging and visitor access	Entry control roster: <ul style="list-style-type: none">• Name and company represented.• Date, time of entry, and time of departure.• Reason for visit.• Contact person within the organization.
Identification systems	<ul style="list-style-type: none">• Badges.• Key fobs.• Smart cards.
Video surveillance	<ul style="list-style-type: none">• Deter unauthorized access.• Assist in prosecuting unauthorized access.• Cameras strategically placed.• Data stored safely.

Physical Security Measure	Description
Security guards	Human security guards, armed or unarmed, can be placed in front of and around a location to protect it. They can monitor critical checkpoints and verify identification, allow or disallow access, and log physical entry occurrences. They also provide a visual deterrent and can apply their own knowledge and intuition to potential security breaches.
Physical barriers	The location of highly secure resources, such as a server room, should not have windows or be visible from the outside of a building. This creates a more secure barrier from the outside. Other types of physical barriers, such as privacy filters, can be implemented to restrict viewing of a user's computer display.
Cable locks	Laptops and other devices that can easily be removed should be secured to a stationary object by using a cable lock.
Securing physical documents	Physical documents such as printed output should be kept in a locked cabinet or drawer when not in use. Passwords should never be written down on a physical paper where it could be seen. When a document is not longer needed, it should be shredded. For highly sensitive physical documents, the pages should be placed in a locked recycling bin.
Biometrics	A biometric lock is a lock that is activated by biometric features, such as a fingerprint, voice, retina, or signature. Biometric locks make it more difficult for someone to counterfeit the key used to open the lock.
Alarms	Alarms activated by an unauthorized access attempt require a quick response. Locally stationed security guards or police may respond to alarms. These responding individuals may trigger access control devices in the facility to automatically lock.

Digital Security

- Information or data that is created, stored, and transmitted in digital form is adequately protected.
- Prevention methods:
 - Antivirus software
 - Anti-spyware software
 - Firewalls
 - User authentication and strong passwords
 - Directory permissions

Antivirus and Anti-malware

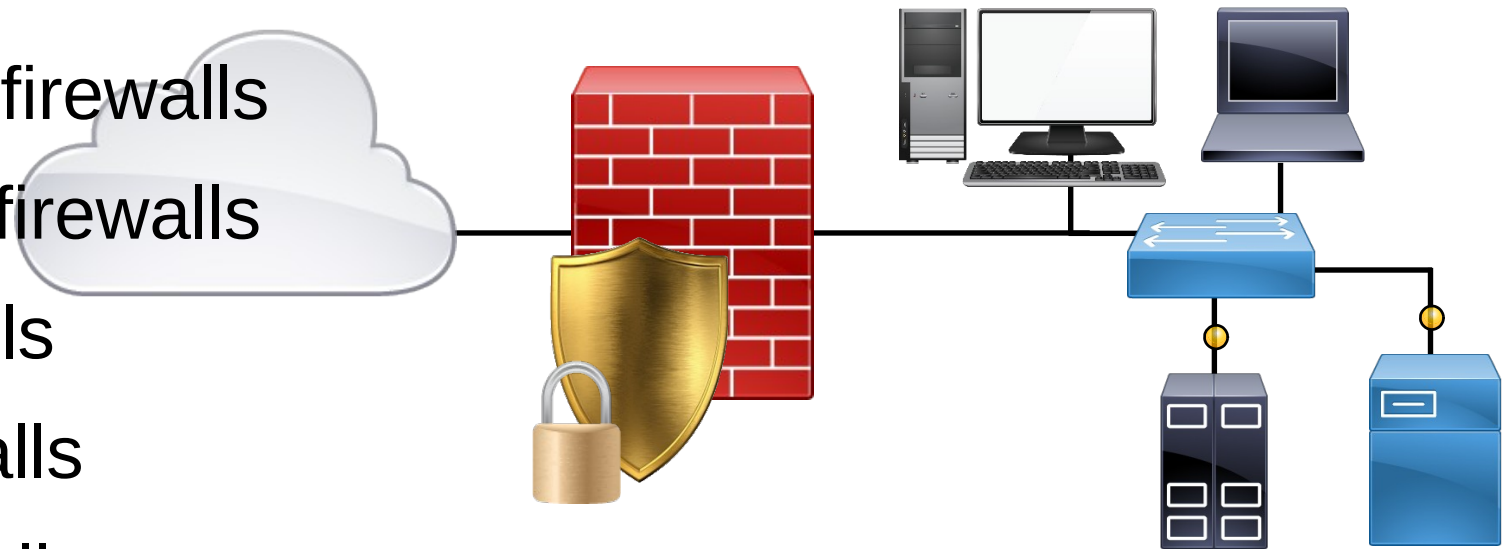
- Scans files for:
 - Executable code that matches known signatures or definitions.
 - Activity associated with malware.
- When threat is identified, files are quarantined and cleaned.
- Keep signature and definition files current.
- Keep engine software current.

Antivirus and Antimalware

- An application installed on a system to protect it and to scan for viruses, worms and trojans
- Looks for pattern (characteristics) or suspicious activity (accessing certain files)
- Over 20,000 known viruses, worms, bombs
- New ones added daily – esp targeting Windows
- Definition file needs to be kept uptodate
- Should not be installed more than once on any machine

Firewalls

- Protect computers and networks by filtering out unauthorized traffic.
- Types:
 - Host (personal) firewalls
 - Network-based firewalls
 - Software firewalls
 - Hardware firewalls
 - Windows Firewall



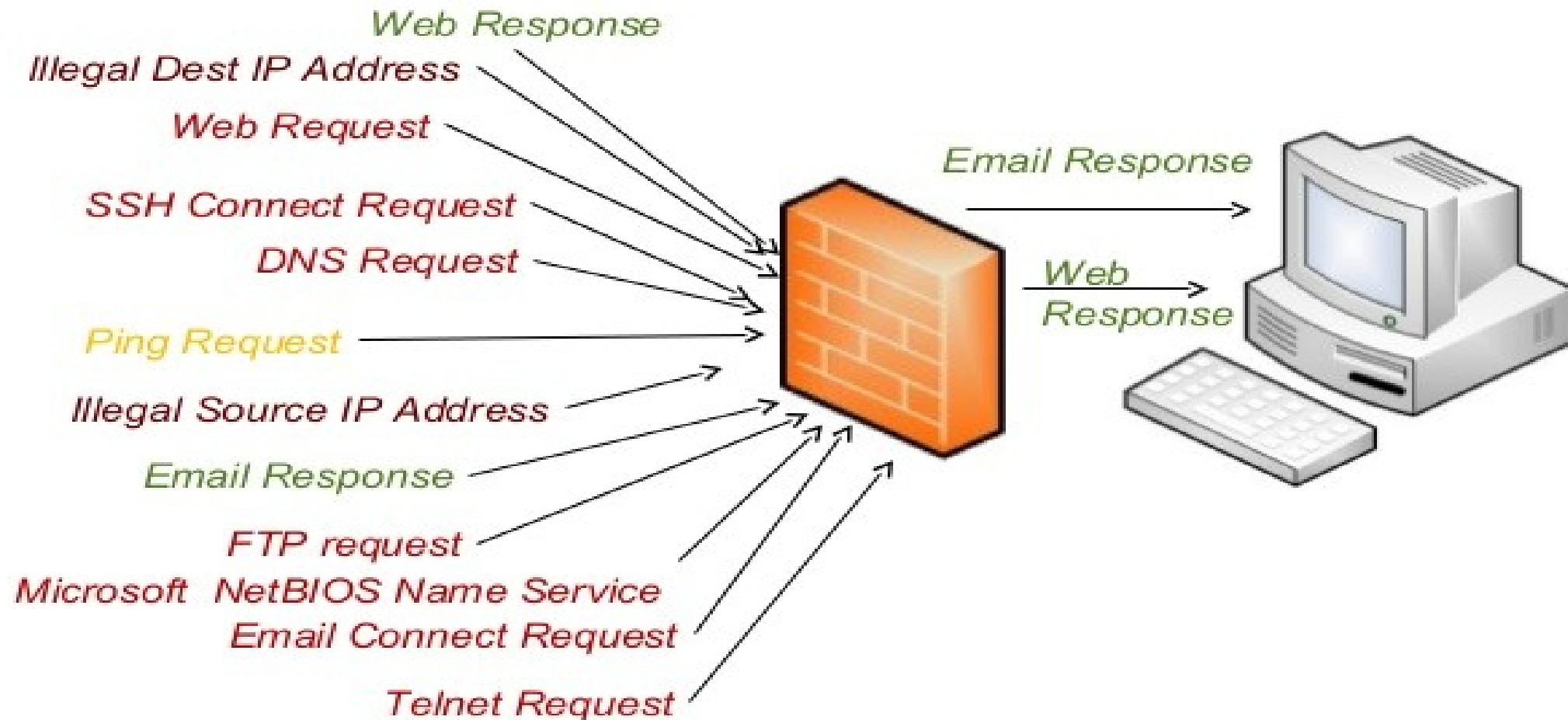
Firewalls

- Purpose is to isolate 2 networks
- Stand alone or built in to another device (e.g router)
- Implemented as Hardware appliance or Software (e.g Windows)
- Deployed in three ways
 - Packet Filter
 - Proxy Firewall
 - Stateful Inspection Firewall

Firewalls – Packet Filter

- Blocks traffic based on type of application and port used
- Not content of packet
- E.g Web traffic on port 80, Telnet on port 23
- Firewall can be customised as needed to block specific ports
- Default is to deny access to all ports

Packet Filter Firewall



Stateful Inspection Firewalls

- Keeps records (a table) of where packets came from/went to and makes decision on this
- So can deny packets that were NOT requested by the internal network
- Vulnerable to DDOS attacks which flood the state table

User Authentication Methods

- User name and password
- Biometrics
- Tokens
- Multifactor authentication
- Mutual authentication
- User Access Process
 - Identification – The claim of identity (Normally username and password)
 - Authentication – Verification of the claim
 - Authorisation – Action taken as a result of the claim

Password Strength

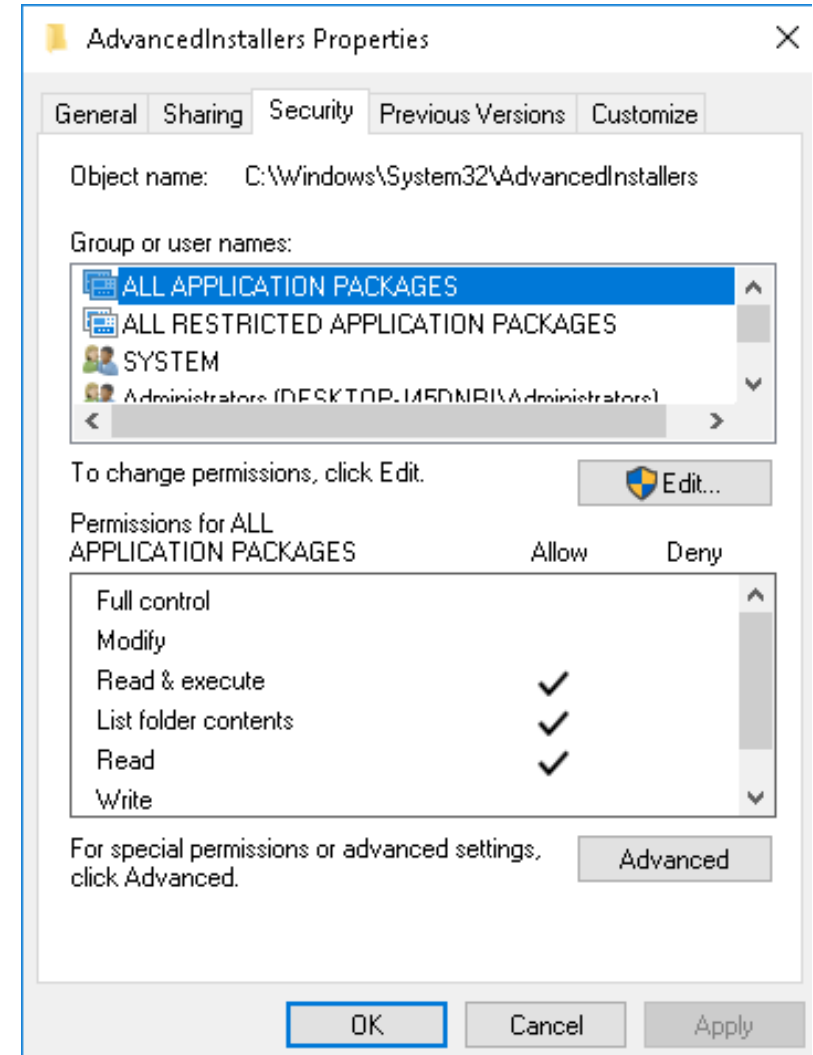
- Minimum and maximum length.
- Required characters: letters, numbers, and symbols.
- Forbidden character strings: user name, personal information, and words.
- Frequency for changing passwords.
- Whether or not passwords can be reused.

Network Security Measures

- Directory permissions
- VPNs
- Port disabling
- ACLs

Directory Permissions

- File Level Permissions
 - NTFS partitions only
- Share Level Permissions
- Permissions at File and share level
 - Windows environments
- Linux
 - Read, Write and Delete valid local and Shares



Linux Permissions

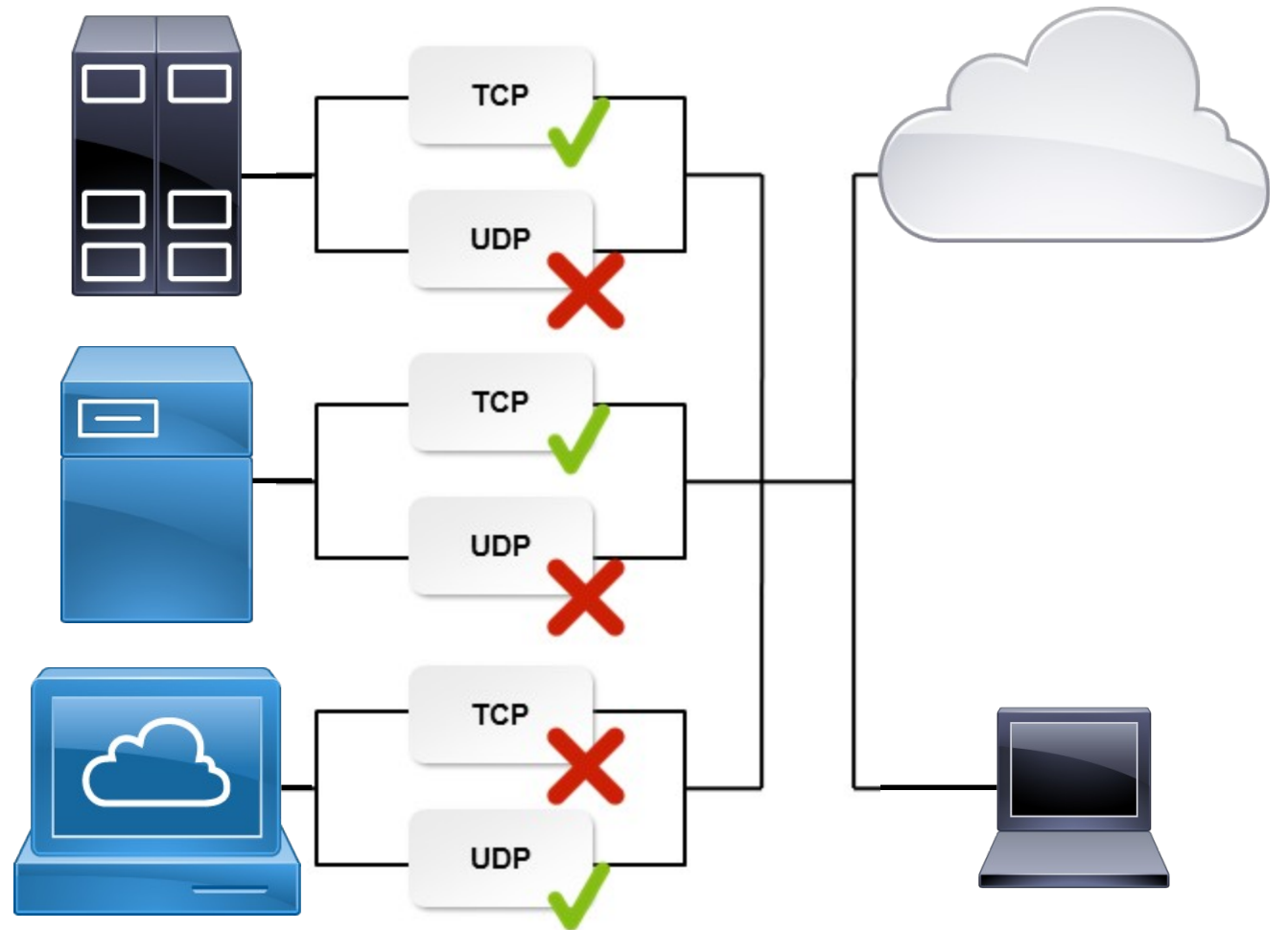
- (R)ead
 - View file content
 - See whats in the directory
- (W)rite
 - Modify the file contents
 - Create and Delete directory contents
- E(x)ecute
 - Run the file
 - Move into the directory. When combined with Read, you can see a long listing of the contents of the directory

VPN's

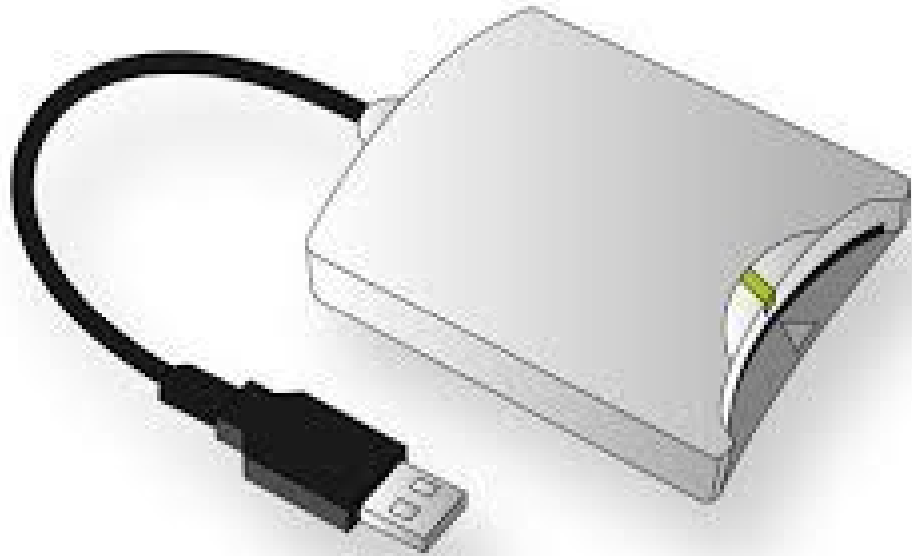
- Private networks/connection are secure but expensive and may not be available where you want to use it
- Public network (BT phone service, Internet) is cheap and everywhere BUT not private/secure
- So you need virtual solution - behaves like it's a private secure connection but its actually public.
- Done by placing private data inside packets (encapsulation) that can travel in public network
- This is called Tunnelling (PPTP, L2TP etc)
- Can connect individual to LAN or two LANS
- The remote end APPEARS to be connected to local
- So you can transfer files,
- Needs special hardware or software

Port Disabling / Port Filtering

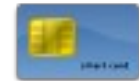
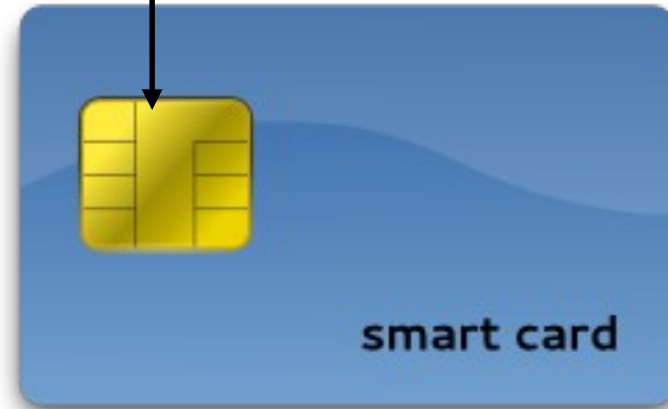
- Used in firewalls
- Device Hardening



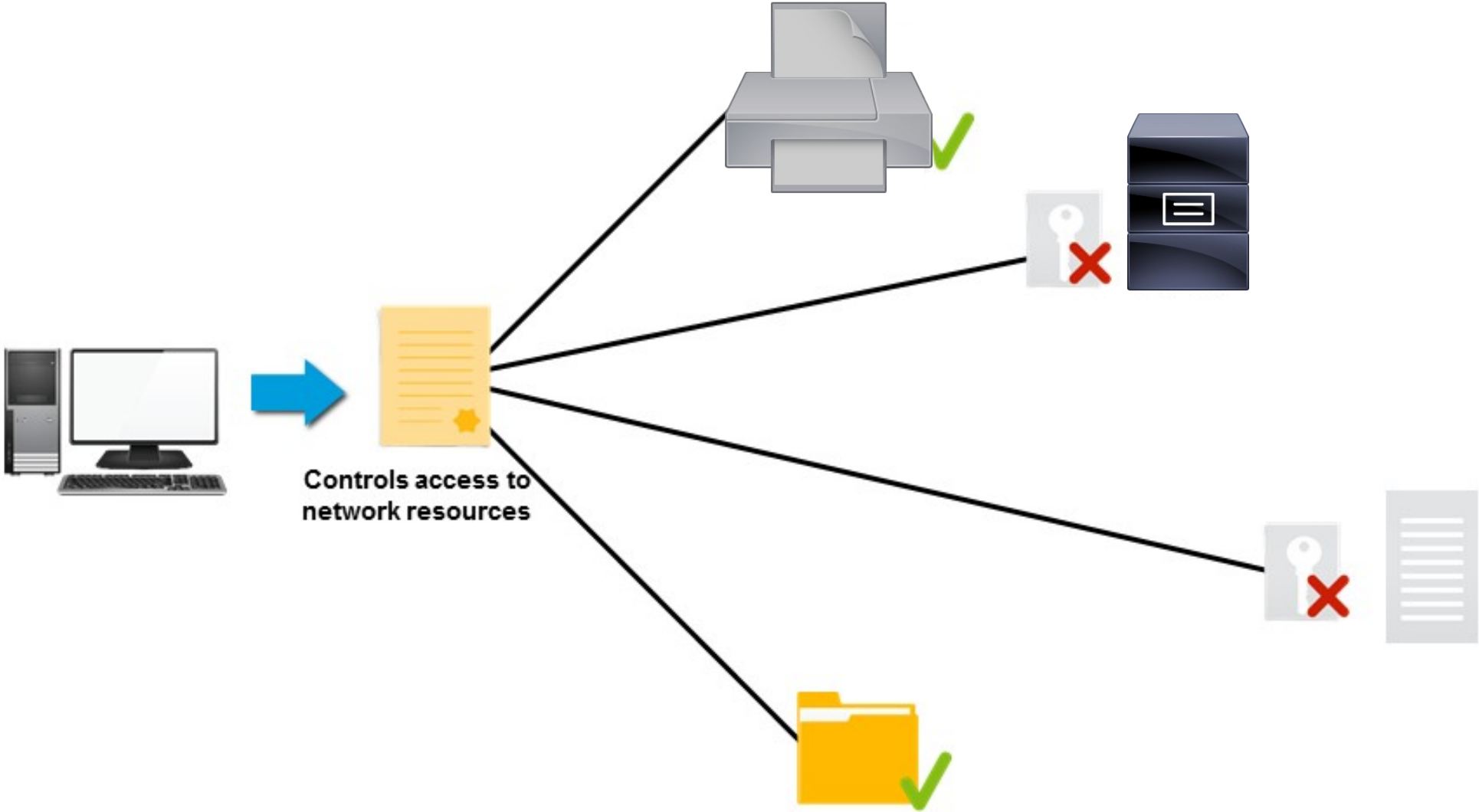
Smart Cards



Smart memory chip



ACLs (Access Control Lists)



Email Filtering

- Checking and filtering out suspicious email E.g spam filter
- Based on some rules - blocked senders, domains, IP addresses, ISP, content patterns
- Automatic removal of folders
- Rules need to be managed – kept updated
- Not 100%
- Can have false positives – need to check junk folder

Software Sources

- Known sources:
 - Vendor
 - App store
- Beware of piracy and embedded malware in untrusted software.

Mobile Security Controls

- All the same threats as PCs and laptops
- Loss
- Theft
- Physical damage

Mobile Security Controls

Security Control	Description
Enable screen lock and passcode settings	The screen lock option on all mobile devices should be enabled with a passcode, and strict requirements on when the device will be locked.
Configure device encryption	When available, all mobile devices should be configured to use data encryption to protect company-specific and personal data that may be stored and accessed on the device.
Require remote wipes	When available, configure mobile devices to support removing and permanently deleting sensitive data from the device if it is lost or stolen.
Enable location services and applications	Use GPS services to protect and track mobile devices that may be lost or stolen.
Enable remote backup	At a minimum, use the remote backup services available through the mobile device's OS.
Install antivirus software	Organizations that allow mobile devices to connect to the network and transfer data should require that antivirus apps get installed to prevent unauthorized access to data, systems, and resources.
Install updates and patches	Verify that devices are set up to automatically install updates from the manufacturer.

Data Destruction and Disposal Methods

- Physical Destruction
 - Shredding
 - Burning
 - Drilling
 - Smashing
 - Degaussing
 - Electromagnetic waves

Data Destruction and Disposal Methods

- Recycling or Repurposing
 - Consider formatting hard disks or using a disk wipe utility.
 - Install remote wiping software on portable devices.
 - Check hard disks after sanitizing to ensure that data was removed.
- Low Level Formatting
 - Writes to each track and sector
- High Level Formatting (Standard Formatting)
 - OS function to clean and write file system
 - Can perform a disk check to identify bad areas

Destruction / Disposal

- Formatting (reuses), sanitation (wiping), destruction
- Standard - e,g FORMAT command, OS level
- Low level Format – by manufacturer, not OS dependent
- Sanitation (wipe clean)
- Can be built in by vendor, or use HDDERASE
- Commercial wipers - not 100%
- Overwrite - put 0s everywhere
- Physical Destruction (of HDD, USB, CDs)
- Mechanical shredders
- drill and hammer, Grinding
- Electromagnetic (Degaussing)
- Incineration
- Get proof of disposal - certificate