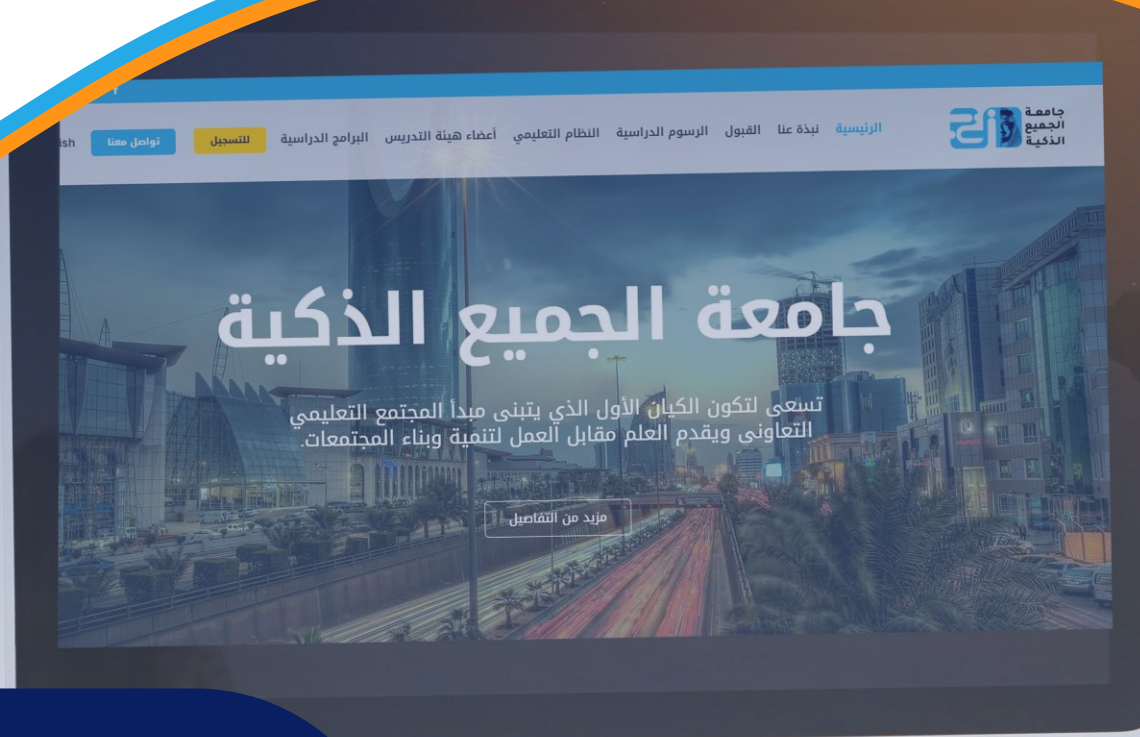




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

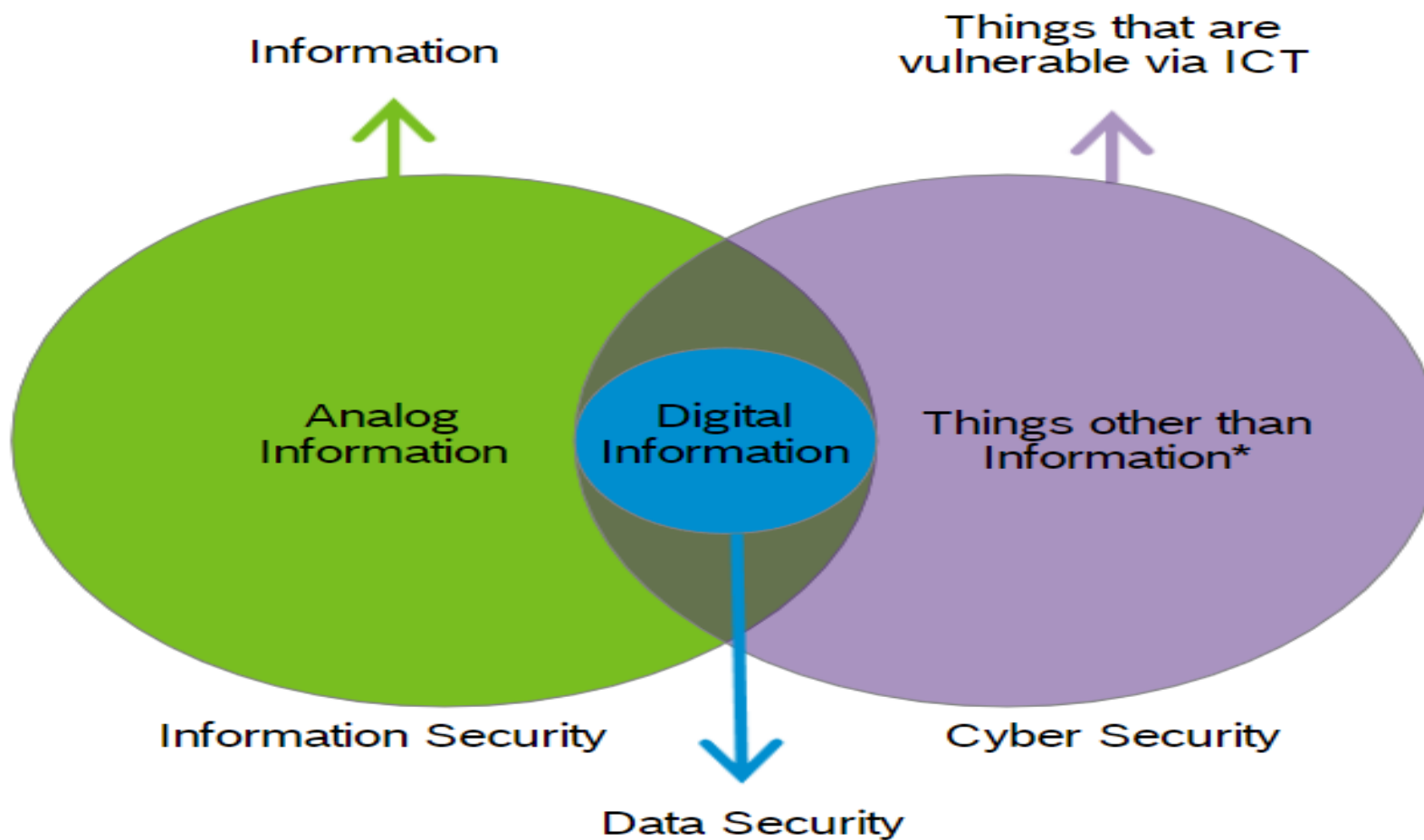


IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 4

IoT in Cybersecurity

Chapter 4

INTRO TO CYBER ATTACKS



Cyber Attacks may be categorized as followed :

Cyber Security



Refers to a body of technologies, processes and practices designed to protect networks, computers, programs & data from attacks, damage or unauthorized access.

Information Security



Sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption modifications, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form data may take.

Data Security



Refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. It deals with physical data such as encryption techniques.

1. Gaining or attempting to gain unauthorized access to a computer system or its data.
2. Unwanted disruption or denial of service attacks including the takedown of the entire website.
3. Installation of viruses or malicious code (malware) on a computer system.
4. Unauthorized use of a computer system for processing or storing data.
5. Inappropriate use of computer systems by employees or former employees.
6. Change to the characteristics of a computer system's hardware, firmware, or software without the owner's knowledge, instruction, or consent.



The widely accepted security model is the CIA triad with three key principles that can be implemented in any kind of organization.

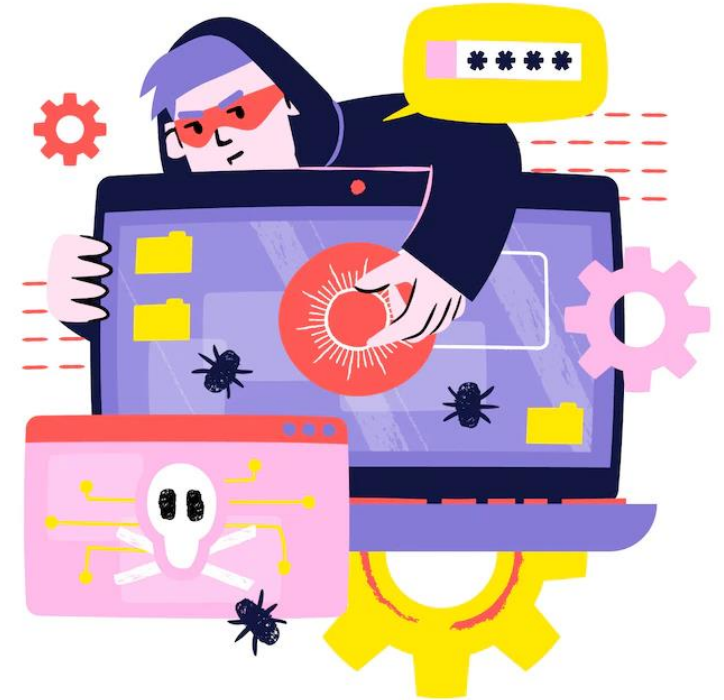
1. Confidentiality: A loss of confidentiality is the unauthorized disclosure of information.
2. Integrity: A loss of integrity is the unauthorized modification or destruction of information.
3. Availability: A loss of availability is the disruption of access to or use of information or an information system.

If any one of the three is non-compliant it may have serious consequences.



1. Ransomware: In a ransomware attack, you suddenly get a message stating that all data on your phone or computer is now encrypted, denying you access to your own data. With ransomware, the perpetrator will tell you that they will turn the data back over to you and not release it to the public if you pay a fee. This can range from nominal to hundreds of thousands of dollars. The problem here is that you're dealing with an admitted criminal and paying the ransom doesn't guarantee that you'll actually get your data back or that they won't release it later.

Many companies hire risk management solution companies to avoid the release or deletion of important or compromising materials.



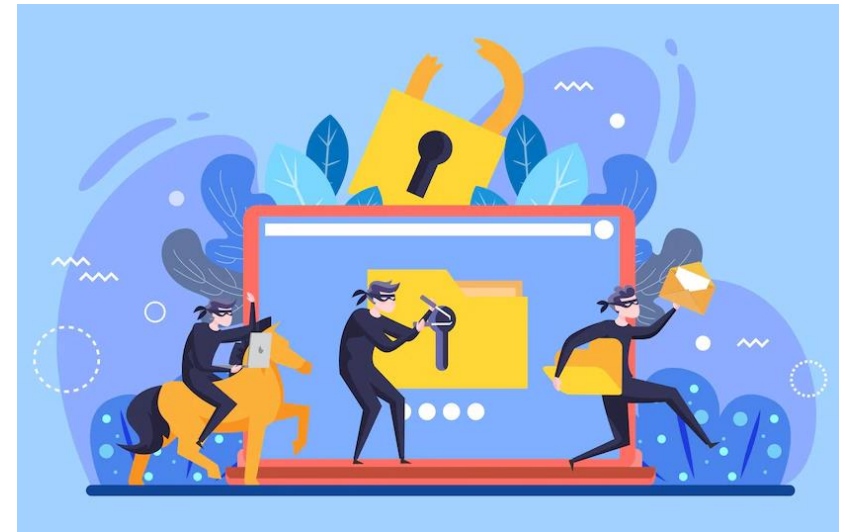
2. Password Guessing (**Brute-force attack**) : Some companies leave passwords for computers on Post-It notes, allowing anyone to access them, which could have meddling employees accessing the files somewhere else. Many people are hacked simply because their passwords was too easy or guessable. This type of breach is called a **brute-force attack** and is a very common method amongst hackers. People often use passwords like the name of their street, their pet's name, or their birthday, which can make hacking into their accounts easy.

It goes without saying that if someone has your password, they can go into your files and find any type of sensitive information on your company they desire.



3. Recording Keyloggers: Cybercriminals can insert or email you malware called keyloggers that can record what you're typing onto your computer. The data is passed back to the hackers and used to access sensitive data. This can happen at your place of employment, or on your personal computer. When this happens, they record everything you are typing – regardless of whether or not the characters appear on the screen. This makes it easy for the perpetrator to gather passwords, credit card numbers, and sensitive information you might enter into a database like names, health data, or pretty much anything else.

This can be used against your company easily, as they will immediately have your passwords as well as company credit card information. They will then use these to find and possibly release sensitive company information.



Chapter 4

DATA SECURITY ATTACKS

4. Phishing: Phishing attacks come from third-party hackers who create sites that look incredibly genuine. For example, they may make a site that mirrors PayPal, and ask you to log into the site for a necessary change. If you log in it without realizing that you're not simply logging in to your account, you can end up giving the hacker your password. This scheme is common at universities. Students will often get emails from a third party posing as the school asking them to confirm their login details. Once they do, the hacker then has their login details to do anything they please with them. We've also seen phishing attacks target Microsoft 365 applications, most notably Exchange Online.

Again, a phishing scheme can compromise the safety of any sensitive information you or your company possess.

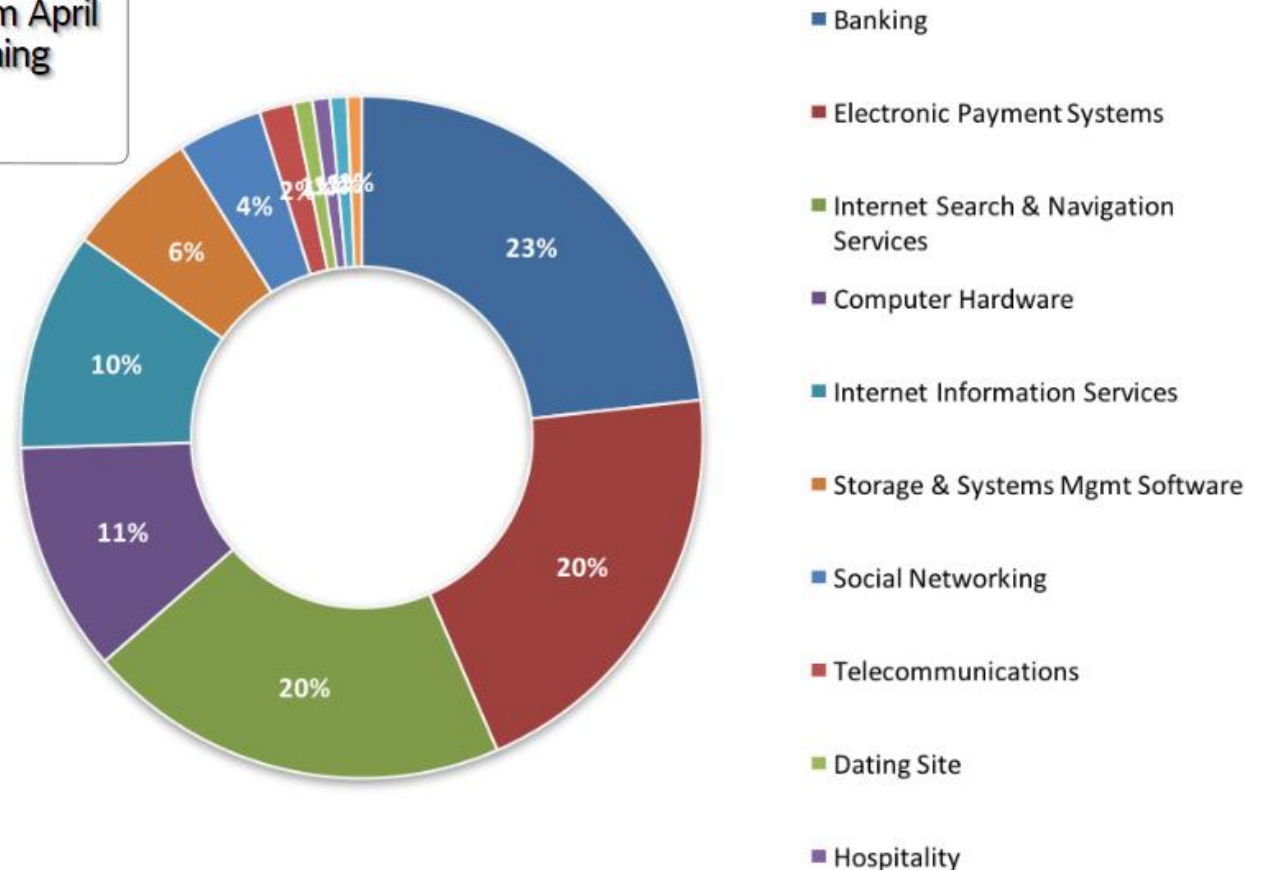


Chapter 4

DATA SECURITY ATTACKS

To give you an idea about phishing, here are some statistics from April 2017 on the top 20 phishing targets.

Top 20 Phishing Targets



5. Malware or viruses: Malware or viruses are sent to people with the goal of wiping their computer of all data. This can be harmful to any company, especially those who rely on their data. For example, if a malware virus was sent to a hospital, it could wipe the data of thousands of patients. This could result in a very serious situation, delaying treatment or even meaning the death of some of those inside the hospital.

In order to prevent these types of viruses, don't click on anything you aren't sure where it is from. Some companies who require that clients or potential clients email them things will ask them not to attach anything but place it in the body of the email. This prevents them from accidentally clicking on anything that could potentially erase a server.

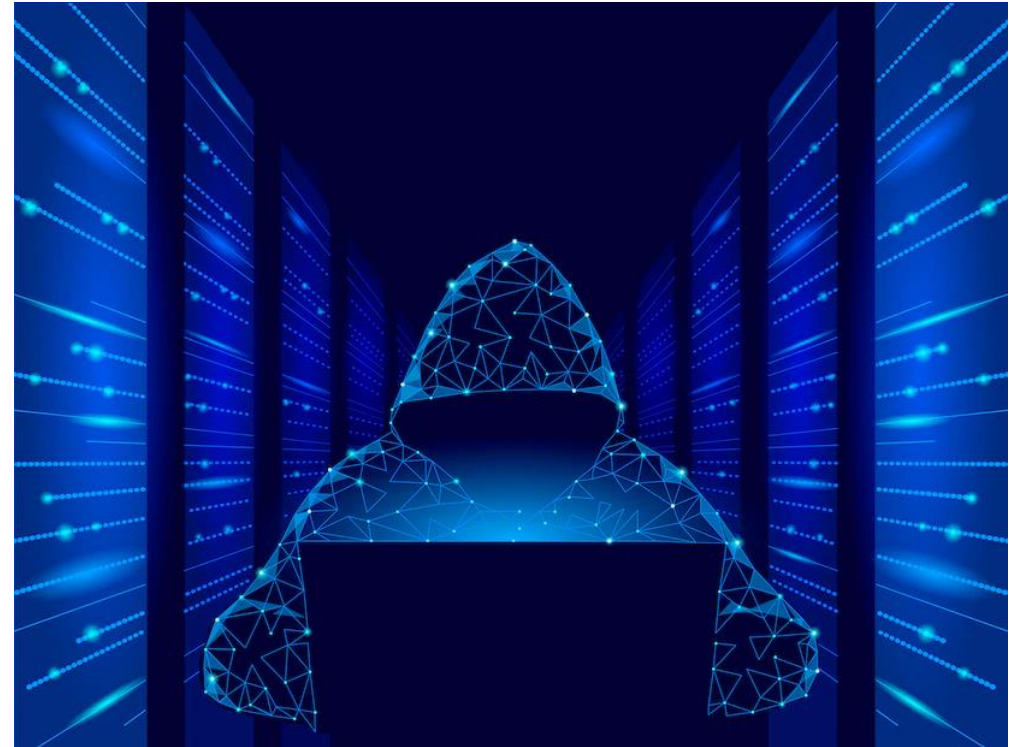


6. Distributed Denial-Of-Service (DDoS): This attack tends to only target larger companies and is often a form of protest. For example, if vigilante justice trolls, like Anonymous, decide that they do not like the way a pharmaceutical company is running and feel it is taking advantage of patients, they can launch a denial-of-service attack. A distributed denial-of-service attack is when the attack is launched from multiple sources simultaneously. With this type of attack, they will make it impossible for those at work to sign into the system. If sites are unreachable due to all the traffic from the attack, customers are unable to access the company's services. While the data isn't necessarily lost, they force the company to shut down while they deal with the security breach, potentially losing business.

This type of attack does not often happen to individuals, as it takes a large amount of resources and a very coordinated attack.



7. DoS Attack: A cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the internet.



Chapter 4

WHO IS A HACKER?



Black Hats

Uses hacking skills for evil purposes without permission



White Hats

Uses hacking skills for good, with permission, known as "Ethical"



Gray Hats

In between Black and White, sometimes good and sometimes BAD



Suicide Hacker

Uses hacking skills with no concern of being caught



Script Kiddies

Derogatory term: no skills must use tools and copy attacks



Cyber Terrorists

Uses hacking skills for evil. motivated by religious or political beliefs to create fear



State sponsored Hackers

Works for a Government or Military entity



Hacktivist

Hacking with an agenda, usually politically motivated

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems via the internet or another computer network.

Modern Encryption Algorithms:

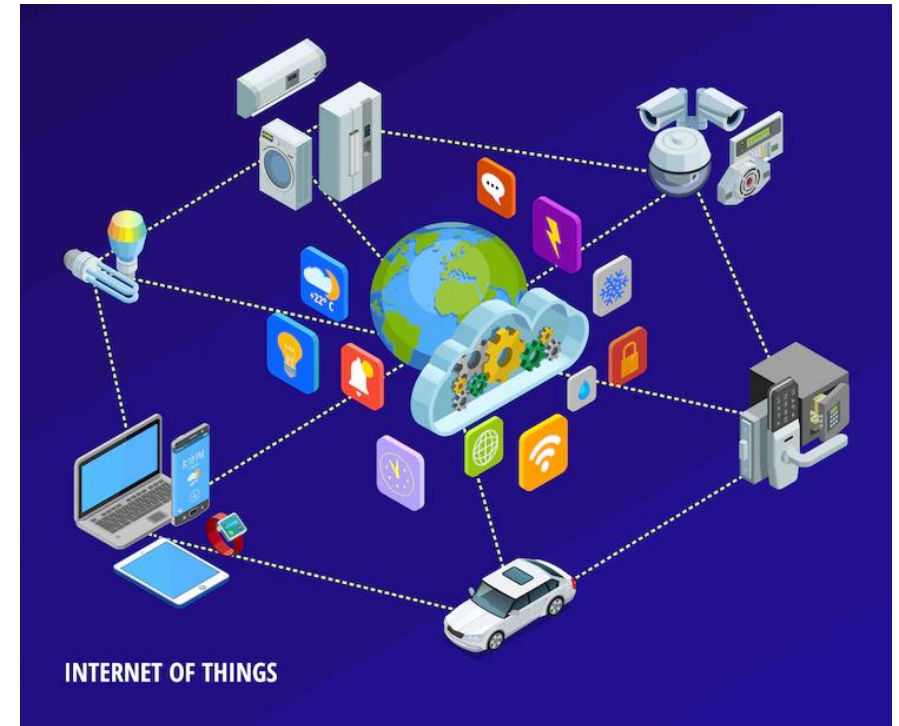
1. Authentication: The origin of the message can be verified.
2. Integrity: Proof that the contents of a message have not been changed since it was sent.
3. Nonrepudiation: The sender of a message cannot deny sending the message.
4. Access Control: Access to an object requires access to the associated crypto keys in many systems (e.g login)



Chapter 4

INTERNET OF THINGS

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. Oracle has a network of device partners.



Chapter 4

IMPORTANCE OF IOT

Over the past few years, IoT has become one of the most important technologies of the 21st century. Now that we can connect everyday objects—kitchen appliances, cars, thermostats, baby monitors—to the internet via embedded devices, seamless communication is possible between people, processes, and things. By means of low-cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. In this hyperconnected world, digital systems can record, monitor, and adjust each interaction between connected things.

The physical world meets the digital world—and they cooperate.



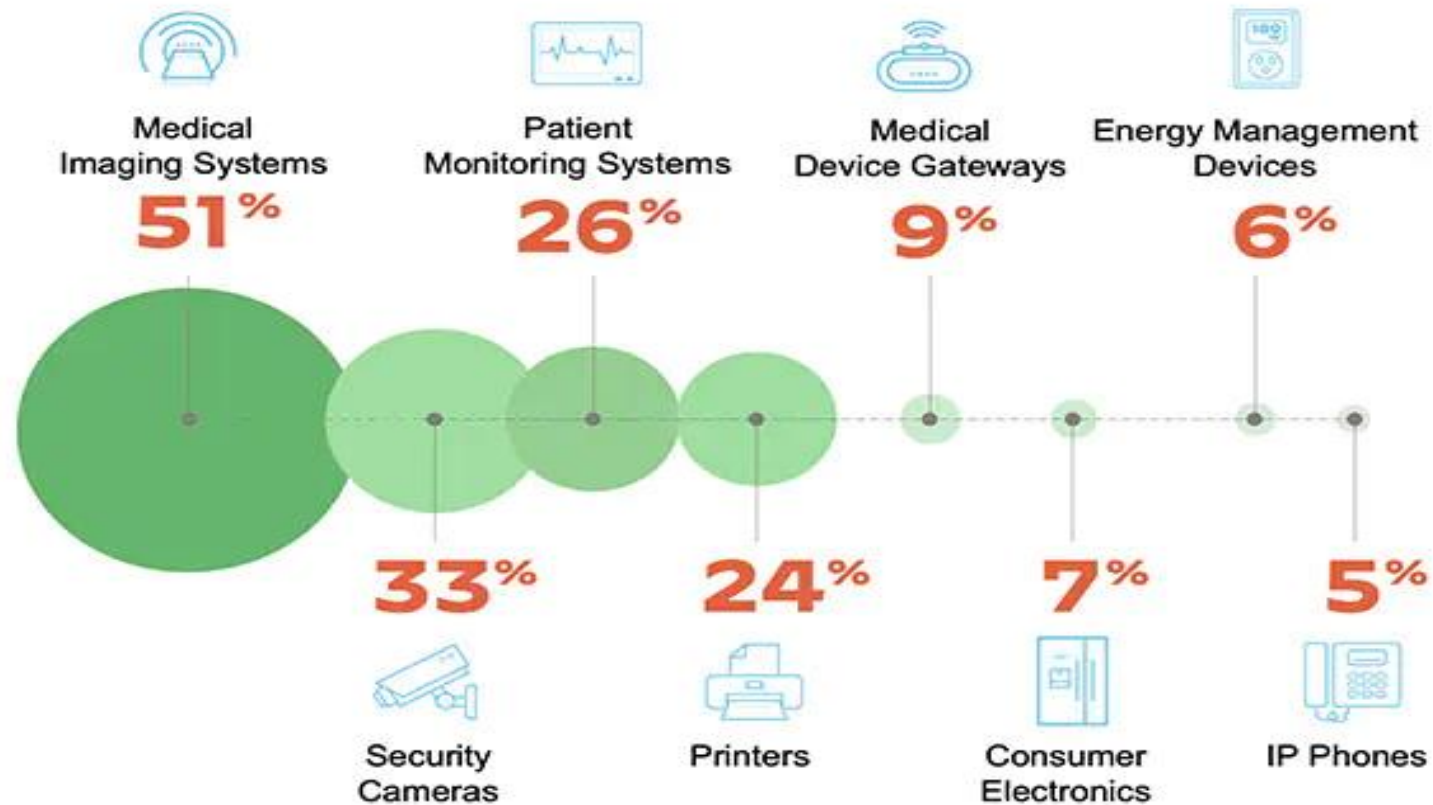
The overarching challenge for security in IoT is that as large volumes of diverse IoT devices continue to connect to the network, a dramatic expansion of the attack surface is happening in parallel. Ultimately the entire network security posture is diminished to the level of integrity and protection offered to the least secure device.

Security teams are now faced with new and escalating challenges that are unique to IoT security, including:

- Inventory – not having clear visibility and context for what IoT devices are in the network and how to securely manage new devices.
- Threats – lack of well-embedded security into IoT device operating systems that are hard or impossible to patch.
- Data volume – overseeing vast amounts of data generated from both managed and unmanaged IoT devices.

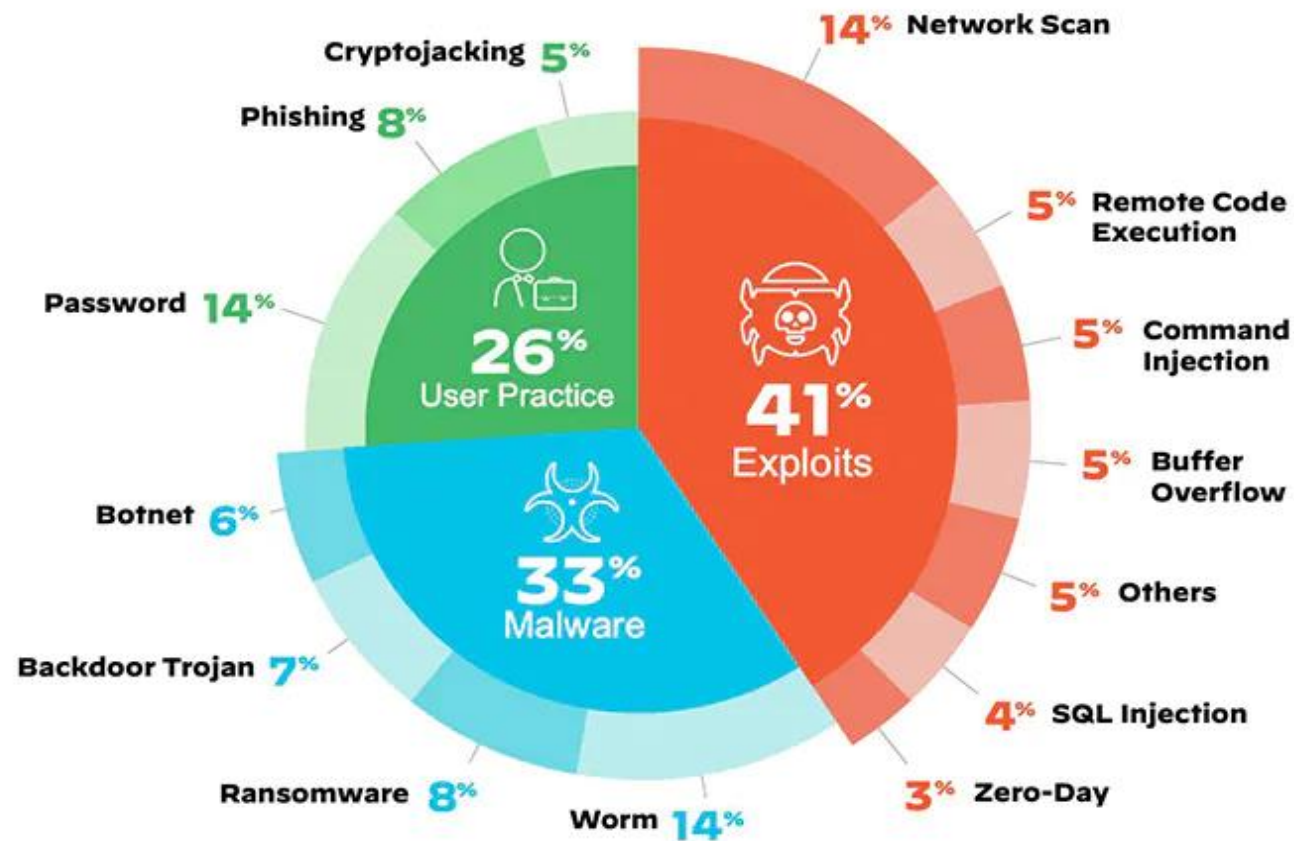
- Ownership – new risks associated with the management of IoT devices by disparate teams within the organization.
- Diversity – the sheer diversity of IoT devices in terms of their limitless forms and functions.
- Operations – the unification crisis wherein IoT devices are critical to core operations yet difficult for IT to integrate into the core security posture.

IoT Devices with Highest Share of Security Issues



Chapter 4

TOP IOT THREATS



1. Unsecure Communications

One of the biggest risks associated with IoT is unsecure communications. Data transmissions between devices is susceptible to interception by third parties. This could allow threat actors to gain access to sensitive information, like user passwords or credit card numbers.

Security Controls: Leverage encryption to protect data in transit, whenever possible. If you are unable to encrypt data in transit, then try to isolate the network in which the device resides. Segmentation will help reduce attack vector associated with the device. Organizations can use BeyondTrust's Privileged Remote Access to consolidate the access to these segmented networks in a secure and encrypted manner.



2. Lack of IoT Security Updates

Once a device is released, it's up to the manufacturer to provide updates to address new security risks. However, many IoT / IIoT manufacturers do not release timely updates. Many manufacturers stop releasing updates altogether after a certain point. This leaves IoT devices vulnerable to attack from known security flaws.

Security Controls: To protect against this, businesses should only use devices from manufacturers who have a good track record of releasing timely updates. To offset this risk, it is important your vulnerability management system is capable of scanning IoT devices, so be sure to add them to your list of devices that are scanned. If you are unable to automate device patching, then attempt to fingerprint the devices as best you can. If there are no facilities enabled for you to install the patch, then at least you will know the potential vulnerabilities associated with the device. Then, you can take other mitigating actions to protect it.

3. Insufficient Authentication and Password Hygiene

Insufficient authentication hygiene means the device lacks adequate measures to verify users are who they claim to be. This could allow external attackers, as well as insider threat actors, to access IoT endpoints and systems that should be off-limits.

Security Controls: To protect against this threat, businesses should use strong authentication methods, like two-factor authentication or biometrics. In addition, drive access to IoT devices through a secure centralized infrastructure access solution like Privileged Remote Access. Also implement a method for:

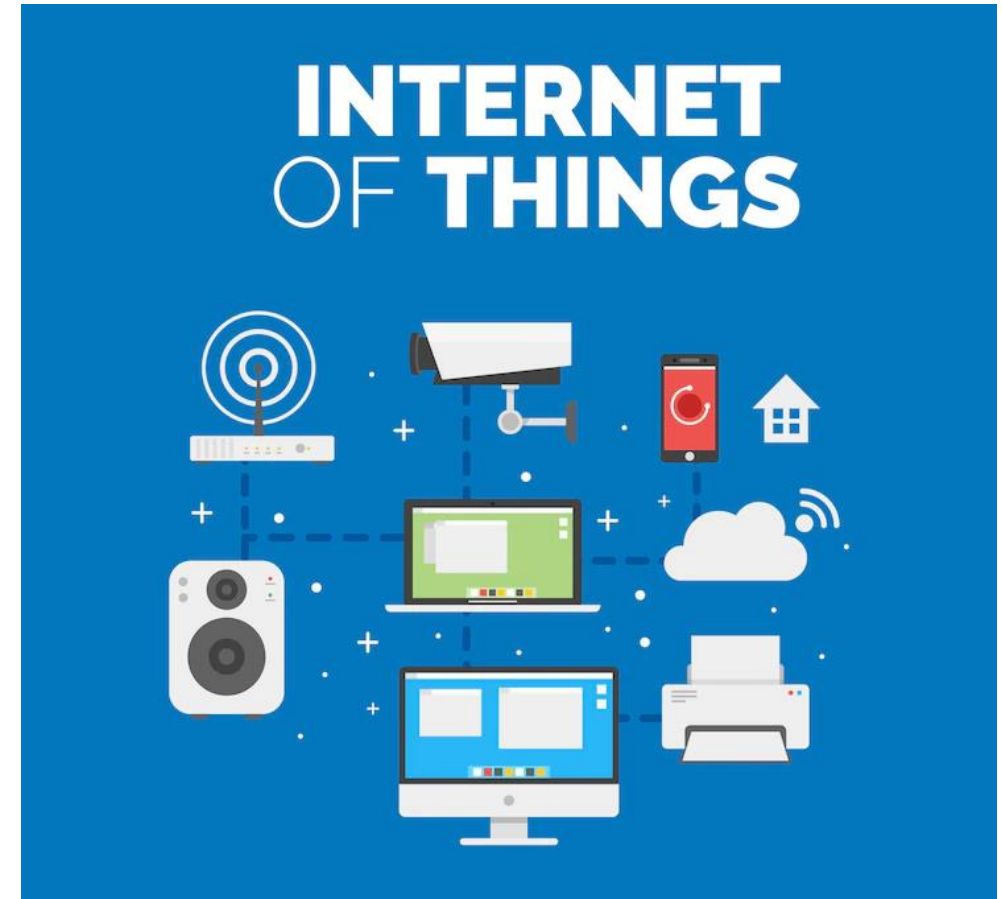
- a) discovering new IoT devices as they are added to your network, and
- b) rotating the passwords associated with the accounts on the device.



Chapter 4

IOT VULNERABILITY ATTACKS

Almost all devices have one or more privileged accounts that are part of the operating system. You can use a solution like BeyondTrust Password Safe to discover, onboard, and systematically manage these passwords. But since IoT devices usually have very lightweight operating systems, it's not possible to install an agent on the device to enforce security policies for accounts. So, you need to take other steps, like network segmentation and good password hygiene, to protect your IoT devices.



Abbreviations and terms

Vulnerability

A vulnerability is a flaw in a system, or in some software within the system, that could provide an attacker with a way to bypass the security infrastructure of the host operating system or of the software itself. It isn't an open door but rather a weakness which if attacked could provide a way in.

Exploit

The act of trying to turn a vulnerability (a weakness) into an actual way to breach a system.

Threat

Refers to the hypothetical event wherein a hacker uses the vulnerability.

Exploiting system vulnerabilities

Exploiting means modifying system or application features which are outside the original purpose of the developer. This therefore makes it possible to steal and share intellectual data which can lead to business loss.

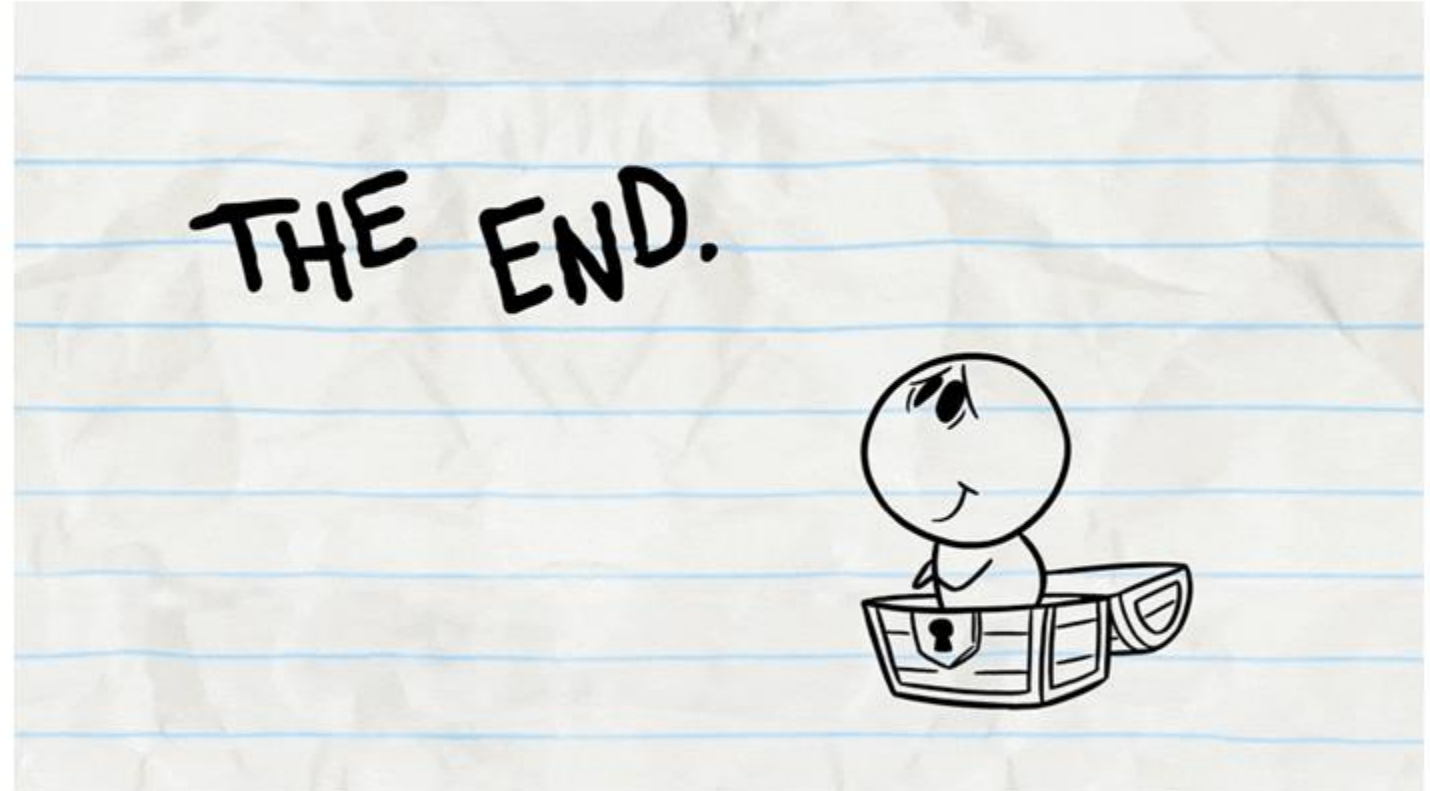
Abbreviations and terms

Sensitive data	Is defined as information that is protected against unwarranted disclosure.
Ciphertext	Plaintext is what you have before encryption, and ciphertext is the encrypted result.
Book Ciphers	A book cipher is a cipher in which the key is some aspect of a book or other piece of text.
Encryption Machines	A series of electro-mechanical rotor cipher machines developed and used in the early- to mid-20th century to protect communication.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY