Unit 4

Malicious software's: Types of malwares (viruses, worms, trojan horse, rootkits, bots), Memory exploits - Buffer overflow, Integer overflow

Unit 5

Security in Internet-of-Things: Security implications, Mobile device security - threats and strategies

Malware	Virus
Definition: Malware is a software which is designed to get unauthorised access of a computer system, generally for a third party benefit.	**Definition:** A virus is a code which attaches itself to various files and programs which get infected in a manner that they can disrupt and corrupt a device.
The full form of Malware is Malicious Software	The full form of Virus is Vital Information Resource Under Seize
A computer system with a malware software can be repaired using an antimalware software	Antivirus is used to remove viruses from a computer device
If a malware software affects your computer device, it may: • Try to retrieve personal information • Steal data like saved cards or payment details • Initiate mining for bitcoin • Overpower its presence and execute unwanted tasks	A system attacked by a computer virus can be apprehended if: • The processing speed decreases • Too many pop-ups appear on the screen • Passwords are reset • Different programs begin to execute themselves

A Worm is a form of malware that replicates itself and can spread to different computers via Network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.

Types of malwares

Type	What It Does
Ransomware	disables victim's access to data until ransom is paid
Fileless Malware	makes changes to files that are native to the OS
Spyware	collects user activity data without their knowledge
Adware	serves unwanted advertisements
Trojans	disguises itself as desirable code
Worms	spreads through a network by replicating itself
Rootkits	gives hackers remote control of a victim's device
Keyloggers	monitors users' keystrokes
Bots	launches a broad flood of attacks
Mobile Malware	infects mobile devices
Wiper Malware	A wiper is a type of malware with a single purpose: to erase user data beyond recoverability.

Spam is unsolicited email, instant messages, or social media messages. These messages are fairly easy to spot and can be damaging if you open or respond.

Phishing is a type of online fraud that involves tricking people into providing sensitive information, such as passwords or credit card numbers, by masquerading as a trustworthy source. **Phishing can be done through email, social media or malicious websites**.

Spoofing describes a criminal who impersonates another individual or organization, with the intent to gather personal or business information.

Pharming is a malicious website that resembles a legitimate website, used to gather usernames and passwords.

- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

- **Adware:** Advertising software which can be used to spread malware.

- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

What is MITM attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

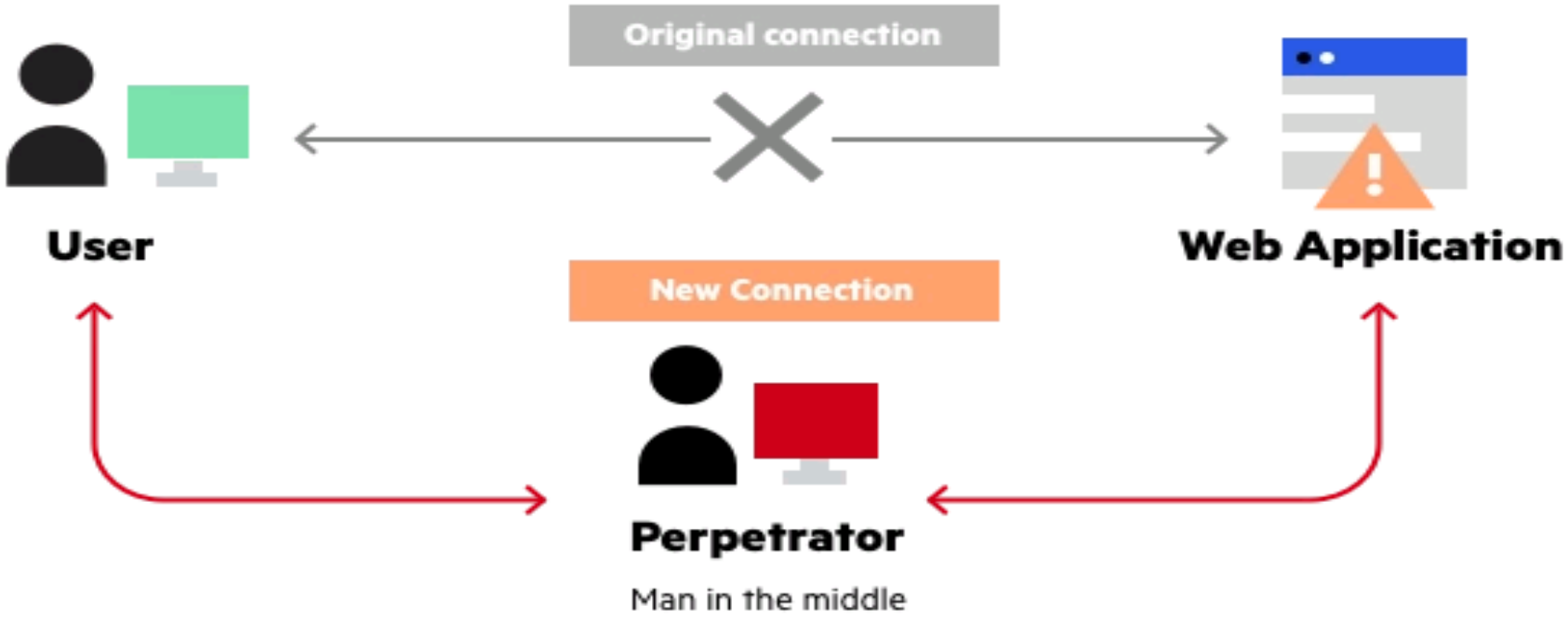
Eavesdropping attacks in the cyber security world are **when the perpetrator "listens" to and records data that is transmitted between two devices**. In simple terms, the hacker reads messages sent via, for example, an open and unsecured network.

What is cross site script attack?

Cross site scripting (XSS) is **an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website**. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.



Man in the middle attack example

What is a denial of service attack (DoS) ?

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Drive-by attacks

A drive-by attack, also known as a drive-by download attack, refers to **a cyberattack in which a malicious script causes a program to download and install itself on a user device, without explicit permission from the user**. It can happen on any user device, running any operating system.

What is SQL injection attack with example?

SQL injection, also known as SQLI, is **a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed**. This information may include any number of items, including sensitive company data, user lists or private customer details.

- **<u>Password attacks</u> are malicious ways hackers attempt to gain access to your account.**

What is a brute force attack?

A brute force attack **uses trial-and-error to guess login info, encryption keys, or find a hidden web page**. Hackers work through all possible combinations hoping to guess correctly.

Credential stuffing is **a cyberattack method in which attackers use lists of compromised user credentials to breach into a system**. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.

What is a spraying attack?

A password spraying attack is **a type of brute force attack where a hacker, much like the name implies, "sprays" an authentication server with combinations of usernames and common passwords**. Attackers often run through lists of commonly used passwords available on the web.

What is a brute force attack?

A brute force attack **uses trial-and-error to guess login info, encryption keys, or find a hidden web page**. Hackers work through all possible combinations hoping to guess correctly.

Birthday Attack

- **Birthday attack** is the one type of cryptography attack from the group of brute force attack.
- The birthday **paradox problem** was described by the higher likelihood of collisions that found among the fixed degree of permutations and random attack attempts.

What is buffer overflow attack with example?

A buffer overflow attack is **a common cyberattack that deliberately exploits a buffer overflow vulnerability where user-controlled data is written to memory**. By submitting more data than can fit in the allocated memory block, the attacker can overwrite data in other parts of memory.

Integer overflow attack

An integer overflow **occurs when you attempt to store inside an integer variable a value that is larger than the maximum value the variable can hold**.

What is Buffer Overflow

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

Buffer overflow example

What is a Buffer Overflow Attack

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

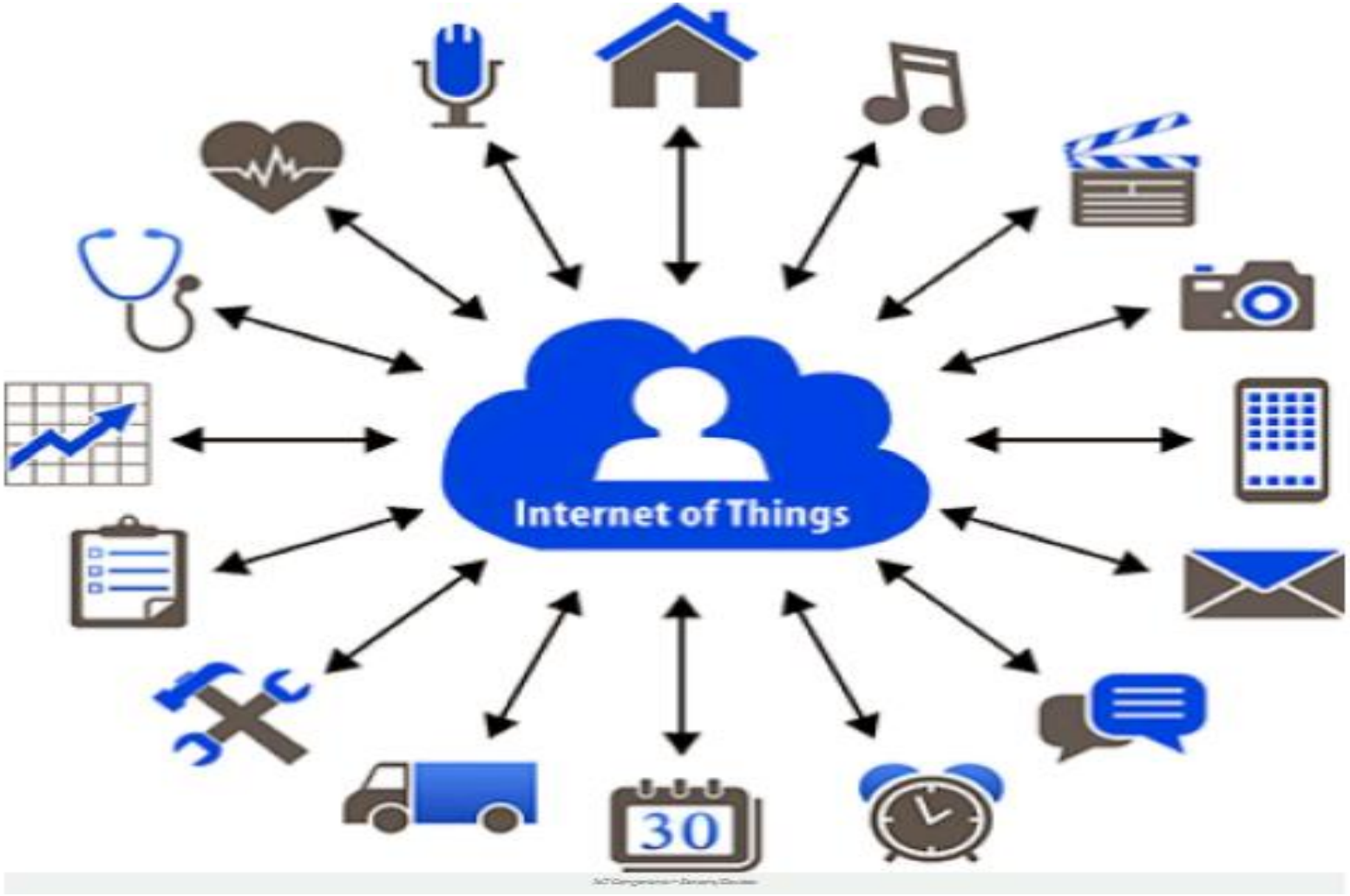
If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Types of Buffer Overflow Attacks

Stack-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.

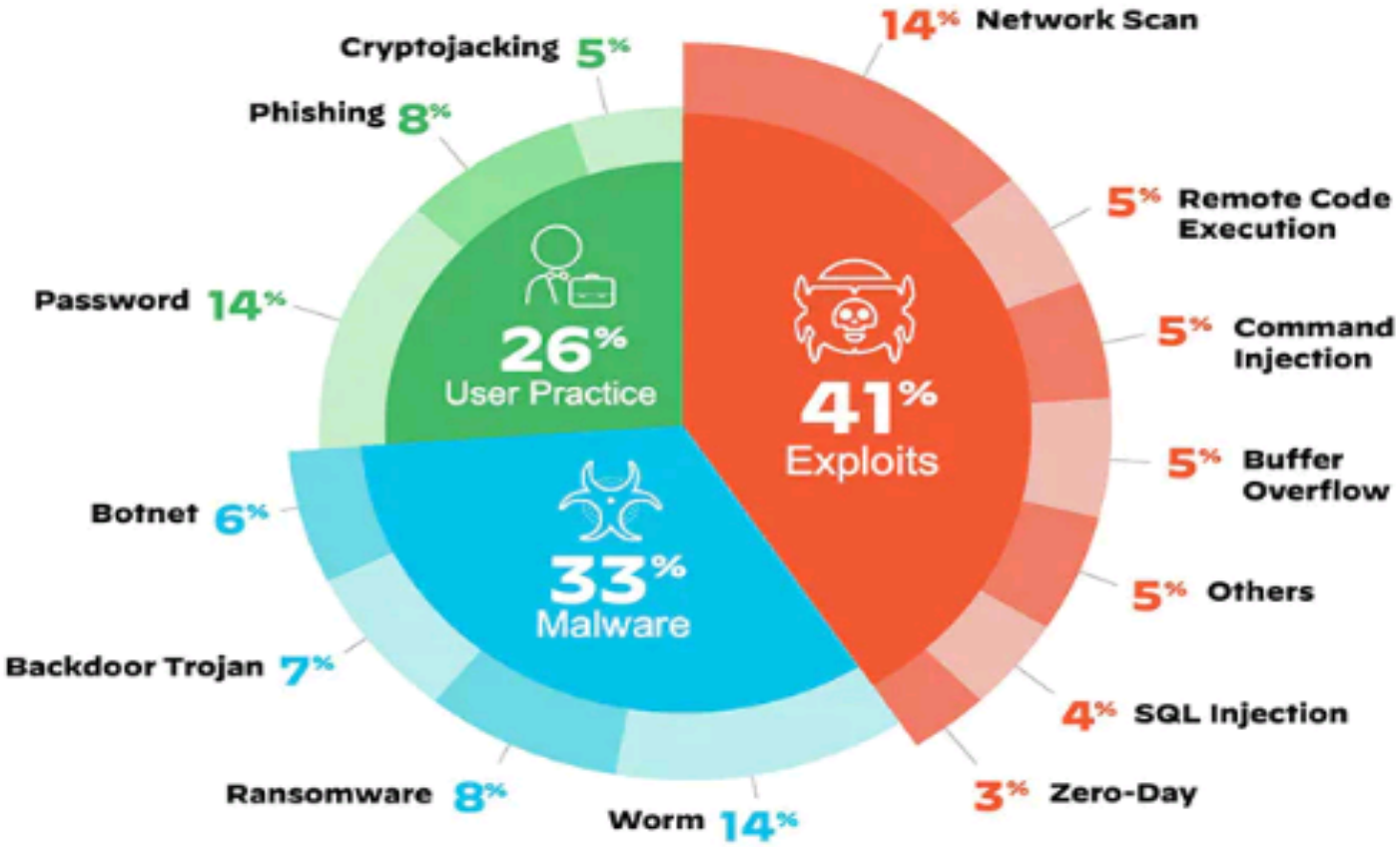
Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

- 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.



What Are the Top IoT Security Threats?

Besides using some of these time-tested attack tactics thought obsolete by modern IT-based malware prevention, peer-to-peer command-and-control (C2) communication and self-propagating IoT malware worms are two new attack tactics emerging on the IoT security horizon. IoT worms are, in fact, becoming more common than IoT botnets. Both tactics target decades-old legacy OT protocols to disrupt critical business operations in the enterprise.



What technologies have made IoT possible?

While the idea of IoT has been in existence for a long time, a collection of recent advances in a number of different technologies has made it practical.

- **Access to low-cost, low-power sensor technology.** Affordable and reliable sensors are making IoT technology possible for more manufacturers.
- **Connectivity.** A host of network protocols for the internet has made it easy to connect sensors to the cloud and to other "things" for efficient data transfer.
- **Cloud computing platforms.** The increase in the availability of cloud platforms enables both businesses and consumers to access the infrastructure they need to scale up without actually having to manage it all.
- **Machine learning and analytics.** With advances in machine learning and analytics, along with access to varied and vast amounts of data stored in the cloud, businesses can gather insights faster and more easily. The emergence of these allied technologies continues to push the boundaries of IoT and the data produced by IoT also feeds these technologies.
- **Conversational artificial intelligence (AI).** Advances in neural networks have brought natural-language processing (NLP) to IoT devices (such as digital personal assistants Alexa, Cortana, and Siri) and made them appealing, affordable, and viable for home use.

- **What is industrial IoT?**
- Industrial IoT (IIoT) refers to the application of IoT technology in industrial settings, especially with respect to instrumentation and control of sensors and devices that engage cloud technologies.
- Recently, industries have used machine-to-machine communication (M2M) to achieve wireless automation and control. But with the emergence of cloud and allied technologies (such as analytics and machine learning), industries can achieve a new automation layer and with it create new revenue and business models. IIoT is sometimes called the fourth wave of the industrial revolution, or Industry 4.0.

- Smart manufacturing
- Connected assets and preventive and predictive maintenance
- Smart power grids
- Smart cities
- Connected logistics
- Smart digital supply chains

Mobile device security - threats and strategies

- https://www.vmware.com/topics/glossary/content/mobile-device-security.html?resource=cat-681089208#cat-681089208

- https://www.ibm.com/in-en/topics/mobile-security