# Three Main Areas

* **Risk Assessment:** The first step in a risk management program is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, criminal, terrorist, accidental, etc.) for a given facility/location. The ISC standard only addresses man-made threats, but individual agencies are free to expand upon the threats they consider. The assessment should examine supporting information to evaluate the relative likelihood of occurrence for each threat. For natural threats, historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to determine the credibility of the given threat. For criminal threats, the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may threaten the facility. In addition, the type of assets and/or activity located in the facility may also increase the target attractiveness in the eyes of the aggressor. The type of assets and/or activity located in the facility will also relate directly to the likelihood of various types of accidents. For example, a facility that utilizes heavy industrial machinery will be at higher risk for serious or life-threatening job-related accidents than a typical office building.
* **Vulnerability Assessment:** Once the plausible threats are identified, a vulnerability assessment must be performed. The vulnerability assessment considers the potential impact of loss from a successful attack as well as the vulnerability of the facility/location to an attack. Impact of loss is the degree to which the mission of the agency is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. These definitions may vary greatly from facility to facility. For example, the amount of time that mission capability is impaired is an important part of impact of loss. If the facility being assessed is an Air Route Traffic Control Tower, a downtime of a few minutes may be a serious impact of loss, while for a Social Security office a downtime of a few minutes would be minor. A sample set of definitions for impact of loss is provided below. These definitions are for an organization that generates revenue by serving the public.

Devastating: The facility is damaged/contaminated beyond habitable use. Most items/assets are lost, destroyed, or damaged beyond repair/restoration. The number of visitors to other facilities in the organization may be reduced by up to 75% for a limited period of time.

Severe: The facility is partially damaged/contaminated. Examples include partial structure breach resulting in weather/water, smoke, impact, or fire damage to some areas. Some items/assets in the facility are damaged beyond repair, but the facility remains mostly intact. The entire facility may be closed for a period of up to two weeks and a portion of the facility may be closed for an extended period of time (more than one month). Some assets may need to be moved to remote locations to protect them from environmental damage. The number of visitors to this and other facilities in the organization may be reduced by up to 50% for a limited period of time.

Noticeable: The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected. The number of visitors to this and other facilities in the organization may be reduced by up to 25% for a limited period of time.

Minor: The facility experiences no significant impact on operations (downtime is less than four hours) and there is no loss of major assets.

Vulnerability is defined to be a combination of the attractiveness of a facility as a target and the level of deterrence and/or defense provided by the existing countermeasures. Target attractiveness is a measure of the asset or facility in the eyes of an aggressor and is influenced by the function and/or symbolic importance of the facility. Sample definitions for vulnerability ratings are as follows:

Very High: This is a high-profile facility that provides a very attractive target for potential adversaries, and the level of deterrence and/or defense provided by the existing countermeasures is inadequate.

High: This is a high-profile regional facility or a moderate profile national facility that provides an attractive target and/or the level of deterrence and/or defense provided by the existing countermeasures is inadequate.

Moderate: This is a moderate profile facility (not well known outside the local area or region) that provides a potential target and/or the level of deterrence and/or defense provided by the existing countermeasures is marginally adequate.

Low: This is not a high-profile facility and provides a possible target and/or the level of deterrence and/or defense provided by the existing countermeasures is adequate.

* **Defence Planning:** This concept is critical to preventing or detecting future attacks. During the early stages of the lifecycle, defenders have an opportunity to detect and mitigate threats before an adversary establishes a foothold. During the later stages, incident response and mission assurance measures are used reactively.

Cyber defenders must proactively look for indicators of a pending, active, or successful cyber-attack. Telltale signs can be developed through retrospective analysis and correlation of threat characteristics observed across the cyber-attack lifecycle over time. This "learn from the past" approach, however, puts organizations at great risk if they intentionally defer remediation of compromises to learn about a cyber adversary's actions post-Exploit. One solution is to establish synthetic environments that allow cyber defenders to observe an adversary's post-Exploit activity while managing risks.

Focused sharing and collaboration. Among communities of cyber defenders, working in partnership provides a force-multiplier effect. These collaborations can greatly benefit cyber-threat intelligence analysis and strengthen cyber defenses.

# Threats

* **Data Theft** is the theft of software through the illegal copying and selling of copyrighted data or software codes in open market without permission of the owner's company. An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on darknet markets, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and audio streaming, online auctions and more. Personal health information is another frequent target for identity thieves.

Some examples of Data theft:

1. When you use a single user license for multiple user.

2. When you make duplicate CD or DVD of your software CD and sell it.

3. If any employee carries a software code made by his company and reproduces it with different name and sells it in market.

**Preventive Measures/Precautions**

1. Copyright your program code/software/data

2. Create a license agreement with your customers/users

3. Obfuscate your code.

4. Provide a trial version of your code.

5. Never share complete code/data required to run the software with a single person in your company.

6. Never allow your employees to copy/share the data/software on their personnel gadgets/emails/external drives and along with that make company devices secured to prevent data theft from the devices

7. Always assign specific duties to each employee.

8. Always make non-disclosure agreement with the employees

9. Always make inventory of the hardware/software issued to employees.

10. Train your employees and prepare them for phishing attempts and privacy breaches

* **Fraud/Forgery**: Fraud denotes any kind of practice of dishonesty of a person or a company for financial advantage. It is generally considered a well-thought-out crime by the law. On the other hand, forgery is essentially concerned with a produced or altered object. Fraud is the crime of deceiving another, which may be performed through the use of objects obtained through forgery. Forgery is a common technique in fraud schemes, where the fraudster uses forged documents in order to gain access to information or materials, they should not truly have access to. The legalities and sentencing for each is extremely nuanced, but can provide insights for your business on which steps to take to both prevent and combat existing fraud. An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts.
* **Unauthorised Access**: A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages. Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access.
* **Unauthorised Modification of data**: This offence includes the deliberate deletion or corruption of programmes or data. It also includes the introduction of viruses etc., where these result in the modification or destruction of data.

# STRIDE

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Threat** | **Definition** | **Example** |
| Authentication | **Spoofing** | Impersonating something or someone else. | Pretending to be any of billg, microsoft.com or ntdll.dll |
| Integrity | **Tampering** | Modifying data or code | Modifying a DLL on disk or DVD, or a packet as it traverses the LAN. |
| Non-repudiation | **Repudiation** | Claiming to have not performed an action. | “I didn’t send that email,” “I didn’t modify that file,” “I certainly didn’t visit that web site, dear!” |
| Confidentiality | **Information Disclosure** | Exposing information to someone not authorized to see it | Allowing someone to read the Windows source code; publishing a list of customers to a web site. |
| Availability | **Denial of Service** | Deny or degrade service to users | Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole. |
| Authorization | **Elevation of Privilege** | Gain capabilities without proper authorization | Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP. |

**Spoofing**

Most security systems rely on the identification and authentication of users. Spoofing attacks consist in using another user credentials without their knowledge. Typical spoofing threats target weak authentication mechanisms, for instance those using simple passwords, like a simple 4 digits number, or those using personal information that can be easily found, like date or place of birth.

**Tampering**

Only authorised users should be able to modify a system or the data it uses. If an attacker is able to tamper with it, it can have some consequences on the usage of the system itself, for instance if the attacker can add or remove some functional elements, or on the purpose of the system, for instance if important data is destroyed or modified.

**Repudiation**

Attackers often want to hide their malicious activity, to avoid being detected and blocked. They might therefore try to repudiate actions they have performed, for instance by erasing them from the logs, or by spoofing the credentials of another user.

**Information disclosure**

Many systems contain confidential information, and attackers often aim at getting hold of it. There are numerous examples of data breaches in the recent years.

**Denial of service**

A system is usually deployed for a particular purpose, whether it is a banking application or an integrated media management on a car. In some cases, attackers will have some interest in preventing regular users to access the system, for instance as a way to blackmail and extort money from the owner of the system (e.g., with ransomware).

**Escalation of privilege**

# TYPES OF VIRUSES

1. File-infecting Virus

A virus that attached itself to an executable program. It is also called a parasitic virus which typically infects files with .exe or .com extensions. Some file infectors can overwrite host files and others can damage your hard drive’s formatting.

2. Macro Virus

This type of virus is commonly found in programs such as Microsoft Word or Excel. These viruses are usually stored as part of a document and can spread when the files are transmitted to other computers, often through email attachments.

3. Browser Hijacker

This virus targets and alters your browser setting. It is often called a browser redirect virus because it redirects your browser to other malicious websites that you don’t have any intention of visiting. This virus can pose other threats such as changing the default home page of your browser.

4. Web Scripting Virus

A very sneaky virus that targets popular websites. What this virus does is overwrite code on a website and insert links that can install malicious software on your device. Web scripting viruses can steal your cookies and use the information to post on your behalf on the infected website.

5. Boot Sector Virus

These viruses are once common back when computers are booted from floppy disks. Today, these viruses are found distributed in forms of physical media such as external hard drives or USB. If the computer is infected with a boot sector virus, it automatically loads into the memory enabling control of your computer.

6. Polymorphic Virus

This virus has the capability to evade anti-virus programs since it can change codes every time an infected file is performed.

7. Resident Virus

A resident virus stores itself on your computer’s memory which allows it to infect files on your computer. This virus can interfere with your operating system leading to file and program corruption. Attacks file and master boot record.

8. Multipartite Virus

A type of virus that is very infectious and can easily spread on your computer system. It can infect multiple parts of a system including memory, files, and boot sector which makes it difficult to contain.

9. Non-Resident Virus

A non-resident virus is capable of infecting executable files when programs are not running. Embeds in local, removable/n/w location.

10. Metamorphic Virus

A metamorphic virus is a type of malware that is capable of changing its code and signature patterns with each iteration. Metamorphic viruses are considered to be more advanced threats than typical malware or even polymorphic viruses.

11. Stealth Virus

In computer security, a stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software. Generally, stealth describes any approach to doing something while avoiding notice.

12. Armoured Virus

A computer virus designed to be very difficult to reverse engineer and analyze. It is overly large, because it contains a large amount of misleading logic in order to foil attempts to figure out its mission.

13. Camouflage Virus

These appear harmless to antivirus software while they are not.

14. Companion Virus

A companion virus is an old type of virus that poses as a legitimate file by copying its file name but uses a different extension. It doesn't modify files.

15. Cavity Virus

A Spacefiller (Cavity) virus tries to attack devices by filling the empty spaces present in various files. That’s why this rare form of computer virus is also addressed as a Cavity Virus. Its working strategy involves using the empty sections of a file to house a virus, without altering its actual size. This also makes its detection quite impossible.

# TYPES OF TROJANS

**Backdoor Trojan**

This Trojan can create a “backdoor” on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

**Distributed Denial of Service (DDoS) attack Trojan**

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

**Downloader Trojan**

This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

**Fake AV Trojan**

This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they’re real or fake.

**Game-thief Trojan**

The losers here may be online gamers. This Trojan seeks to steal their account information.

**Infostealer Trojan**

As it sounds, this Trojan is after data on your infected computer.

**Mailfinder Trojan**

This Trojan seeks to steal the email addresses you’ve accumulated on your device.

**Ransom Trojan**

This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer’s performance.

**Remote Access Trojan**

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

**Rootkit Trojan**

A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.

**SMS Trojan**

This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

**Trojan banker**

This Trojan takes aim at your financial accounts. It’s designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

**Trojan IM**

This Trojan target instant messaging. It steals your logins and passwords on IM platforms.

**ArcBombs**

These Trojans represent special archives that are designed to behave abnormally when users try to unpack them. ArcBomb archives either freeze or seriously slow the system. Malicious archives use different techniques to achieve their goal. They may use malcrafted headers or corrupt data that lead to a malfunction of an archiver or an unpacking algorithm.

**Banking Trojans**

Banking Trojans are created to steal confidential user data such as login credentials, passwords, SMS authentication, or bank card info.

Emotet  
Discovered in 2014, Emotet was initially created to steal banking data. Spam functions and malware download options were added to later versions.

TrickBot  
Created in 2016, TrickBot is still one of the most prevalent banking Trojans.

**Droppers**

These software pieces are designed to install malware covertly. They contain other malware that is obfuscated and deeply hidden inside the dropper’s code. This is done to prevent detection by antivirus software. Many antivirus tools cannot analyze all components of droppers.

**Proxies**

These Trojans allow attackers to get anonymous access to internet websites using the victim's computer as an intermediary. Crooks use this type of viruses to send spam while hiding behind victims’ IP addresses. It acts like virus.

**Password stealing ware**

Password Stealing Ware (PSW) steals passwords from infected computers. Trojans of this type can search for passwords kept by users inside files or by web browsers. Some variants may steal software licenses and system/network passwords.

**Key Logger Trojan**

A keylogger Trojan virus is just as it sounds: a program that logs keystrokes. The danger of one infecting your computer is that it tracks every single keystroke you enter through your keyboard, including passwords and usernames.

**FTP trojan**

An FTP Trojan installs an FTP server on the victim’s machine allowing the attacker to gain access to sensitive data through the FTP Protocol. The Trojan opens port 21 and makes it accessible to the attacker or a group of individuals. Some password attacks can also be employed where only the attacker gains access to the system. The system tries to download and upload files from the victim system.

**Destructive Trojan**

An FTP Trojan installs an FTP server on the victim’s machine allowing the attacker to gain access to sensitive data through the FTP Protocol. The Trojan opens port 21 and makes it accessible to the attacker or a group of individuals. Some password attacks can also be employed where only the attacker gains access to the system. The system tries to download and upload files from the victim system.

**Security software disabler Trojan**

This Trojan horse is designed to disable security software like firewall and antivirus, enabling the attacker to use many invasion techniques to invade the victim's computer, and even to infect more than the computer.

**Spy Trojan**

A trojan-spy is a type of trojan with a wide range of capabilities, including performing keylogging, monitoring processes on the computer and stealing data from files saved on the machine.

# TYPES OF NETWORK ATTACKS

**Social Engineering Attack**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. It may lead to unauthorised access/ gain to one’s confidential information.

**Phishing Attacks**

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

**Social Phishing**

A social media phishing attack is when a hacker uses social media sites such as Facebook, Twitter, or Instagram to steal personal data. Usually this happens when a hacker posts something on friends' or colleagues' pages that they can't resist clicking on.

**Spear Phishing**

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. ... This is how it works: An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware.

**Watering Hole Attack**

Watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. Eventually, some member of the targeted group will become infected. Hacks looking for specific information may only attack users coming from a specific IP address. This also makes the hacks harder to detect and research. The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.

**Whaling**

A whaling attack is a kind of phishing scam and CEO fraud that targets high profile executives with access to highly valuable information. ... Whale phishing is generally more difficult to detect than standard phishing attacks, as these attacks often do not use malicious URLs or weaponized attachments.

**Vishing Voice**

During a vishing phone call, a scammer uses social engineering to get you to share personal information and financial details, such as account numbers and passwords. The scammer might say your account has been compromised, claim to represent your bank or law enforcement, or offer to help you install software. Warning: It's probably malware.

Vishing is just one form of phishing, which is any type of message — such as an email, text, phone call or direct-chat message — that appears to be from a trusted source, but isn’t. The goal is to steal someone's identity or money.

**Port Scanning**

A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

# DOS TYPES

**ICMP flood attack**

An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings). Normally, ICMP echo-request and echo-reply messages are used to ping a network device in order to diagnose the health and connectivity of the device and the connection between the sender and the device. By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic.

**Ping of Death**

Ping of Death (a.k.a. PoD) is a type of Denial of Service ([DoS](https://www.imperva.com/learn/application-security/denial-of-service/)) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

While PoD attacks exploit legacy weaknesses which may have been patched in target systems. However, in an unpatched system, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.

**Smurf Attack**

Smurf is a network layer distributed denial of service (DDoS) attack, named after the DDoS.Smurf malware that enables it execution.

Smurf attacks are somewhat similar to ping floods, as both are carried out by sending a slews of ICMP Echo request packets.

Unlike the regular ping flood, however, Smurf is an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast networks. It changes D+IP addresses.

**Buffer Overflow**

The most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks.

**Botnet**

A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot. ... They are also used to spread bots to recruit more computers to the botnet. Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks.

**Man in the Middle Attack**

A Man-in-the-Middle (MitM) Attack involves an attacker intruding on an existing connection, establishing himself or herself as a “man-in-the-middle”, or someone able to intercept and selectively modify all network traffic between two communicating devices.

**Session Hijacking Attack**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

**Cross Site Scripting**

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

**SQL Injection**

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

# BLUETOOTH RELATED

**Bluesnarfing**

Bluesnarfing is a type of network attack in which an attacker gains unauthorized access to a wireless device via a Bluetooth connection. Once the hacker has access to the device, they can steal sensitive user information, including personal photos, contact lists, emails, and passwords.

Once a device is compromised, hackers have access to everything on it: contact, emails, passwords, photos, and any other information. To make matters worse, they can also leave victims with costly phone bills by using their phone to tap long distance and 900-number calls.

The best way is to disable Bluetooth on your device when you’re not using it, especially in crowded public spaces, a hacker’s sweet spot. Other ways to steer clear of Bluesnarfing include:

* Switching your Bluetooth to “non-discovery” mode
* Using at least eight characters in your PIN as every digit adds approximately 10,000 more combinations required to crack it
* Never accept pairing requests from unknown users
* Require user approval for connection requests (configurable in your smartphone’s security features)
* Avoid pairing devices for the first time in public areas

**BlueJacking**

Bluejacking is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius. First, the hacker scans his surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices. Bluejacking takes advantage of a loophole in the technology's messaging options that allows a user to send unsolicited messages to other nearby Bluetooth owners. Bluejacking can’t change or delete data from a target device. The most that bluejackers can do is to annoy their targets.

The best way to safeguard against bluejacking is to turn your device’s Bluetooth functionality off when it’s not in use. Do so, especially when you’re in a public place. And if you need to use your device’s Bluetooth feature, make sure your device is not discoverable. That way, you can enjoy the benefits of the technology without having to worry about bluejacking.

Even if bluejacking is more of a prank than a threat, it is still a good practice to protect your device and hence your privacy at all times.

**Bluebugging**

Bluebugging is a type of cyber-attack done on the Bluetooth enabled devices. The attack allows the hacker to access the cell commands and infiltrate the phone calls, read and send SMS. The attack even allows any hacker to modify the contact list, connect to the internet and eavesdrop on any phone conversation and record it. The attack was developed after the onset of bluejacking and bluesnarfing.

For this attack to happen the most important condition is that the victim cell should ON and the Bluetooth should be in discoverable mode in victim cell.

If these conditions are met then the hacker first initiates the connection to the victim device. If the connection is established, then the hacker uses this connection to install the backdoor in the victim device. The backdoor then exploit several security vulnerabilities such as remote code execution vulnerability, local privilege escalation vulnerability etc. and give the unauthorized access of the victim device to the hacker.

Due to the backdoor, the hacker device remains listed in the victim cell and as a trusted device. The hacker then uses this attack to control the victim cell by entering AT commands and can even control the victim Bluetooth headset to perform malicious activities.

The attack can be prevented by:

* keeping the Bluetooth OFF when not in use.
* Reset the Bluetooth settings to take off all the devices from the trusted list.
* Set the device to the hidden, invisible or the non-discoverable mode when using the Bluetooth.
* Keep the Bluetooth off in public places, including restaurants, stores, airports, shopping malls, train stations, etc.