Ministry of Education
Government of India

G20 भारत 2023 INDIA

Azadi Ka Amrit Mahotsav

एन सी ई आर टी NCERT

Indian Cyber Crime Coordination Centre

Online training on

Internet of Things (IoT) and Mobile Security

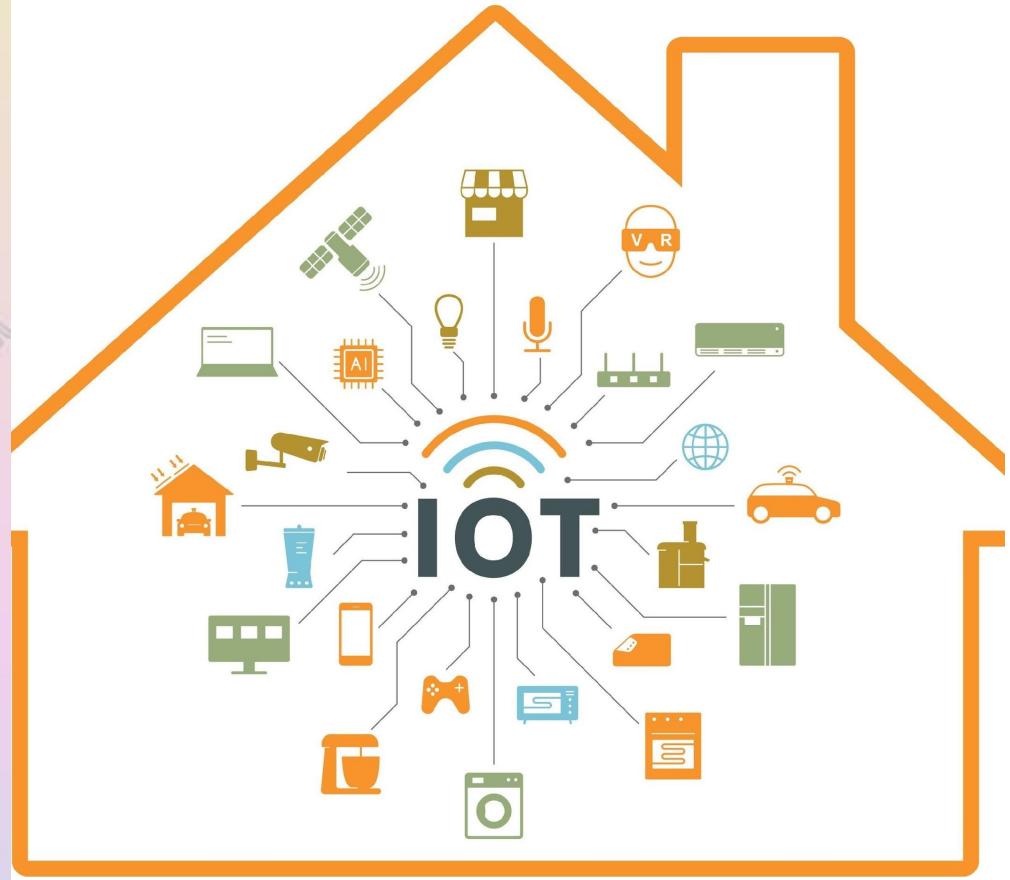
Organized by CIET-NCERT in collaboration with I4C, MHA

5 Sep, 2023 4:00 pm-5:00 pm

Day 2: Cybersecurity Risks with Internet of Things (IoT)

Dr. Deepak Kumar
Sr. Cyber Intelligence and Digital Forensic Professional
I4C, MHA

Mr. Davinder Kumar
Consultant
I4C, MHA



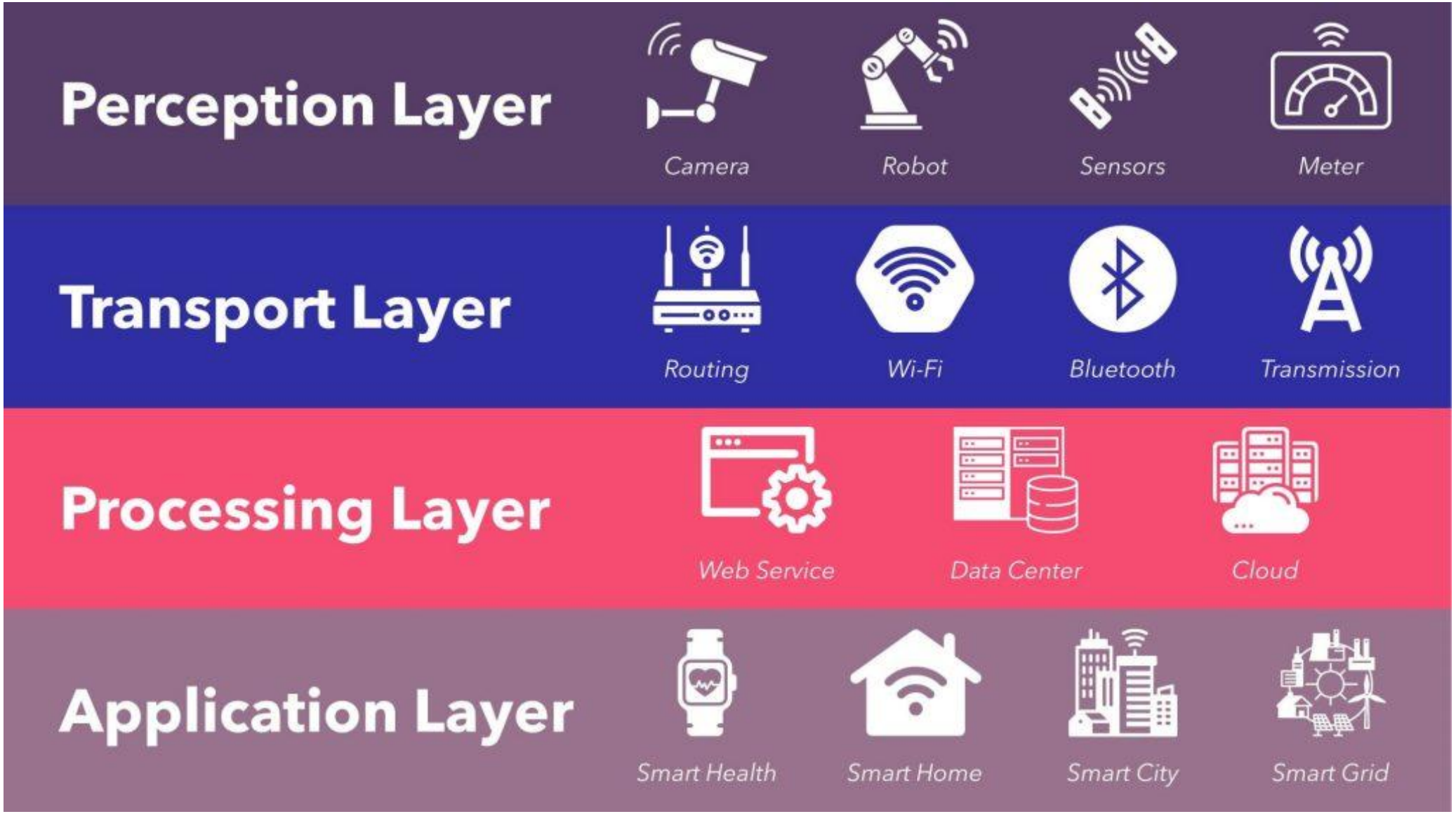
A **vulnerability** is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by a threat.

A **threat** is a potential for a threat agent to exploit a vulnerability.

A **risk** is the potential for loss when the threat happens.

Vulnerability x Threat = Risk

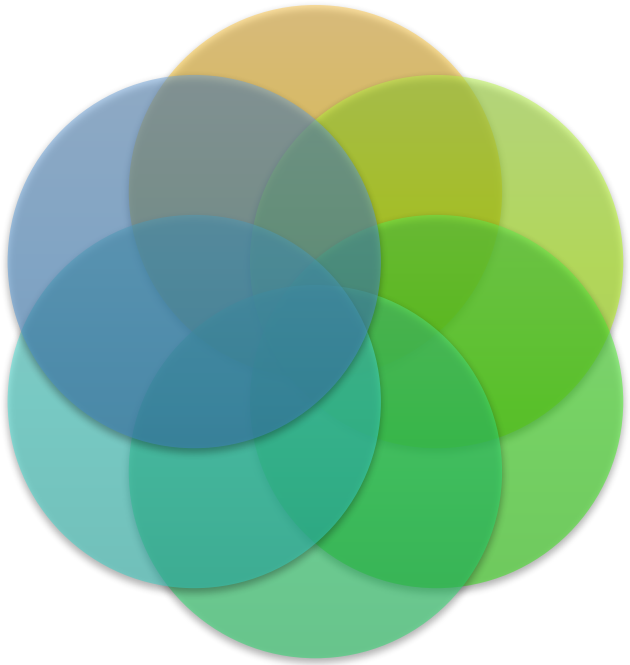
IoT Architecture



Risks of IoT Devices

Cyber criminals an access your heating and lighting system to find out if you are away from home.

Espionage: Hackers can opt to carry out a campaign where the end goal is the prolonged monitoring or surveillance of a home



Access your password or even your bank account through the information you shared with a digital assistant like Alexa and Google Assistant.

Use your devices as BOTs to deliver computing power for DDoS attack, click fraud, password cracking, or send out spam or mine cryptocurrency.

Break-in: The hackers can monitor residents using IP cameras installed in the house.

Get into your network through an IoT device and launch a ransomware attack making your IoT smart home unusable, unless you pay.

Risks of IoT Devices

Device	Functions	Actions hackers can take once compromised
Smart robot vacuum cleaner	• Conduct automatic and scheduled cleaning • Provide several cleaning modes for users to choose from, such as wet mopping and dry sweeping • Take anti-twining and anti-dropping maneuvers • Map the home's layout automatically • Recharge automatically when low on power	• Steal the home layout • Monitor room activities remotely • Attack users or residents using the vacuum's stored water • Dirty the home by deliberately creating a mess
Smart lock	• Lock and unlock through a simple icon tap on a mobile device or web interface • Unlock even without a physical key • Record permanent and temporary users and set access schedules for specified days and times • Turn on forced entry alarms to warn users of possible break-ins • Automatically lock after being unlocked for a specified period of time	• Unlock for intruders to enter the home or facility • Lock out users or residents and block the house remotely • Change the lock password remotely • Turn on the alarm when no break-in or intrusion occurred

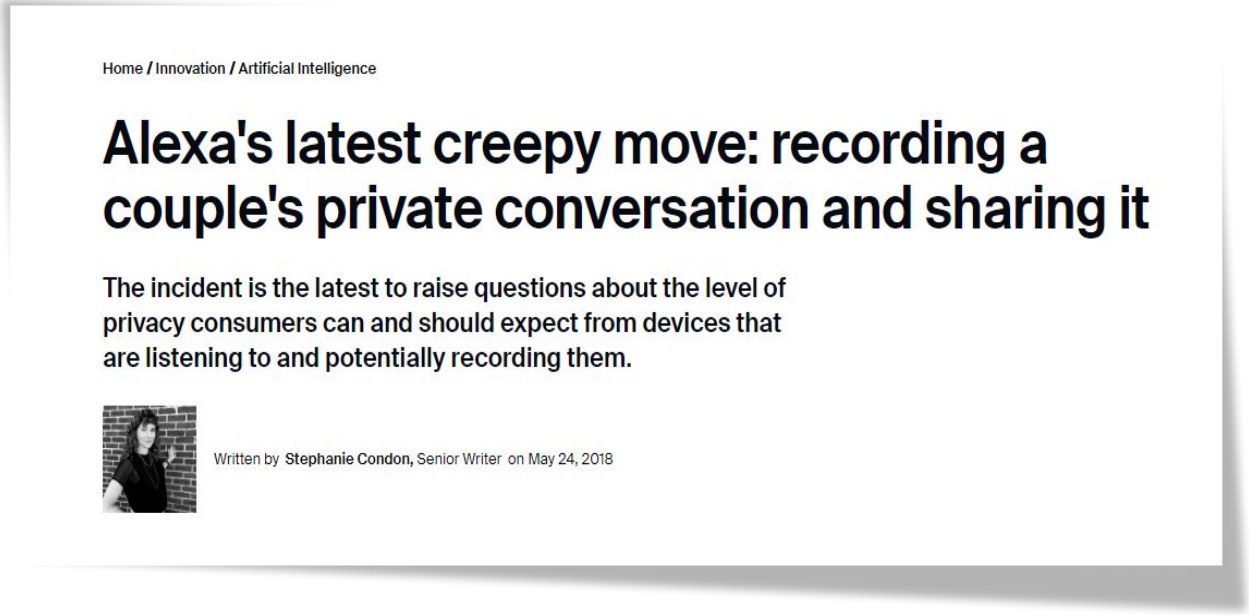
Risks of IoT Devices

Device	Functions	Actions hackers can take once compromised
Smart bulb	• Be controllable by a mobile app or a virtual assistant • Let users select from various lighting colors • Turn on or off as scheduled	• Turn the light on or off at unpredictable times • Turn all of the lights on in the home or facility to overload the power system • Flash lights as quickly as possible to blind people or cause seizures in people with photosensitive epilepsy
Smart coffee machine	• Brew coffee based on a set timer or remote command • Brew higher-quality coffee while giving users more control over the process • Be controllable and configurable through mobile apps	• Disrupt the brewing process • Stop the machine's function completely • Brew coffee continuously even when there are no more coffee beans loaded in the machine
Smartwatch	• Monitor the user's heart rate • Track the user's activity • Send out reminders and alarms • Provide a fitness tracker • Allow users to reply to messages and	• Spoof the user's smartphone from the smartwatch • Steal the user's health data • Send fake text messages from the smartwatch

Risks of IoT Devices

Device	Functions	Actions hackers can take once compromised
Home gateway	• Serve as the entry point to the internet • Connect devices through Wi-Fi or other wireless protocols • Perform device control • Provide gateway functions like WAN-to-LAN bridging, Network Address Translation (NAT), IPv4 and IPv6 forwarding, wireless access point (WAP) management, and Voice over IP (VoIP) processing	• Connect to a fake or malicious URL to download malware • Steal credentials or personally identifiable information (PII) through the gateway • Control connected devices remotely from the gateway by either disabling device functions or meddling with them • Block or modify connections to redirect them toward hidden malicious behaviors
Voice-activated home automation device	• Reduce human effort and errors, thus increasing efficiency • Turn devices on or off based on voice commands • Run tasks based on an AI-enabled voice recognition system • Provide the connected virtual assistant data when commanded by its user	• Play voice commands at strategic times to cause inconvenience for residents or users, like "brew coffee at 3 a.m." or "turn on all lights at 4 a.m." • Order unwanted stocks by voice commands • Steal voice data as credentials for use in other voice command systems

Risks of IoT Devices



Home / Innovation / Artificial Intelligence

Alexa's latest creepy move: recording a couple's private conversation and sharing it

The incident is the latest to raise questions about the level of privacy consumers can and should expect from devices that are listening to and potentially recording them.

Written by **Stephanie Condon,** Senior Writer on May 24, 2018

Amazon explained to ZDNet how it all happened: "Echo woke up due to a word in background conversation sounding like 'Alexa,' the company said in a statement. "Then, the subsequent conversation was heard as a 'send message' request. At which point, Alexa said out loud 'To whom?' At which point, the background conversation was interpreted as a name in the customers contact list. Alexa then asked out loud, '[contact name], right?' Alexa then interpreted background conversation as 'right'. As unlikely as this string of events is, we are evaluating options to make this case even less likely."

Apply the CIA Triad to Internet of Things Product Design and Security

ELEMENTS OF THE AUGMENTED CIA TRIAD

Confidentiality:

Confidentiality entails the protection of personal data from access by unauthorized parties. It addresses user privacy concerns and ensures that the data collected in IoT-enabled environments, transmitted over networks, and stored on servers is reliable. Protecting the confidentiality of user information requires assessing data sensitivity, defining access levels, and managing file permissions. Methods of ensuring the confidentiality of data include access control lists, volume encryption, and management of UNIX and Linux file permissions.

Nonrepudiation:

Nonrepudiation refers to identifying document sources and ensuring the validity of digital signatures. It provides irrefutable proof of online transactions.

Authentication:

Authentication ensures that devices in an IoT environment are trusted. Authentication methods include digital certificates, two-factor authentication, and hardware authentication. Secure hash algorithms are sometimes used to authenticate a transaction. It is typically the role of IT administrators to determine the appropriate controls for user access.

Availability:

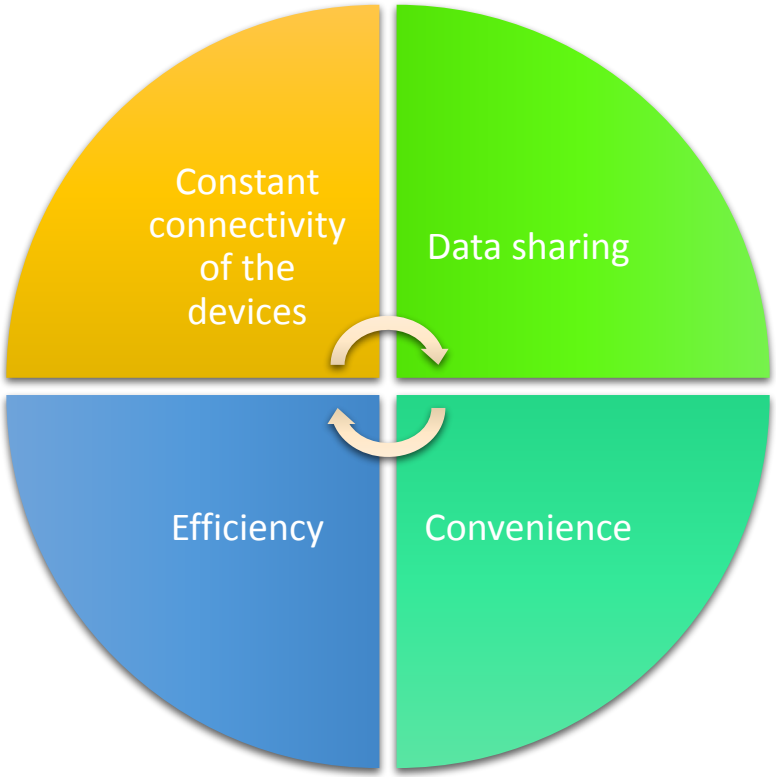
Data availability applies to the authentication mechanisms, internet-connected apps, and access channels linked to IoT environments. In most cases, IoT services and data must be available at all times. Availability is affected by access speeds when devices transmit and receive data. An IoT system's data can become unavailable or the entire system might go offline for an extended period due to faulty hardware, power outages, oversights in security, or problems with the IoT architecture, for example.

Integrity:

Integrity refers to protecting IoT data against modification, deletion, or alteration from their original form. Parties that have access to IoT-enabled environments can lose their access rights if they violate data integrity standards.

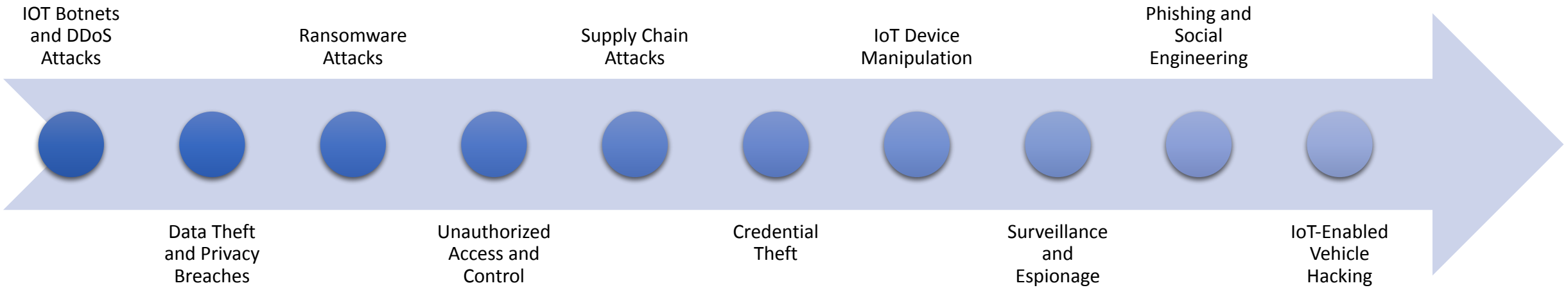
Code Validation:

Many software products and services are used in IoT environments. Some companies write custom code for IoT devices and software products to meet specific business requirements. Attackers may discover code base vulnerabilities in these IoT products and sell their findings to third parties on the dark web. Proper code validation is therefore an essential part of checking for and correcting vulnerabilities (ISBuzz Staff, 2015).



- Including poor data protection
- Poor password protection
- Unpatched devices
- Poor IoT device management
- IoT skill gaps

IoT-related cybercrimes



IoT Cyber Risks

Weak Authentication and Authorization:

Many IoT devices have weak or default usernames and passwords, making them vulnerable to brute force attacks. Additionally, they may lack robust authorization mechanisms, allowing unauthorized access to sensitive data or control over the device.

Lack of Encryption:

IoT devices often transmit data over networks without proper encryption, leaving data vulnerable to interception and tampering. This is especially concerning when dealing with personal or sensitive information.

Firmware and Software Vulnerabilities:

Manufacturers may not provide regular updates and patches for IoT devices, leaving them exposed to known vulnerabilities. Hackers can exploit these vulnerabilities to gain access to devices or compromise their functionality.

Inadequate Device Management:

Managing and securing a large number of IoT devices can be challenging. Organizations may not have effective processes in place for monitoring and updating devices, leading to security gaps.

Data Privacy Concerns:

IoT devices collect vast amounts of data, often without users' explicit consent or knowledge. This data can be mishandled, leading to privacy breaches and potential misuse.

IoT cyber risks

Physical Security: IoT devices deployed in physical environments may be physically accessible to attackers. Tampering with or stealing these devices can compromise security.

DDoS Attacks: IoT devices can be hijacked and used as part of botnets to launch Distributed Denial of Service (DDoS) attacks on other systems or networks.

Interoperability Issues: IoT devices from different manufacturers may not always work seamlessly together, potentially leading to security vulnerabilities when attempting to integrate them into a larger IoT ecosystem.

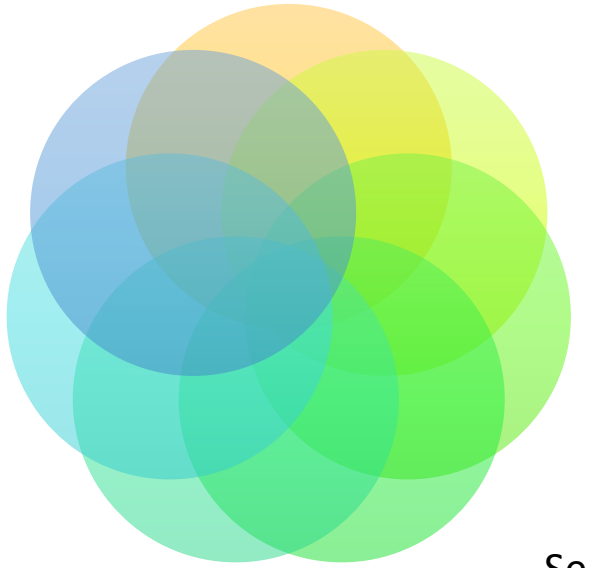
Supply Chain Risks: Compromised or counterfeit IoT components during the manufacturing and distribution process can introduce vulnerabilities into devices before they even reach the end user.

Legacy Devices: Older IoT devices may lack modern security features and cannot be easily updated or replaced, leaving them susceptible to attacks.

IoT cyber risks Mitigation

Change default passwords and usernames on IoT devices.

Educate users and employees about IoT security best practices.



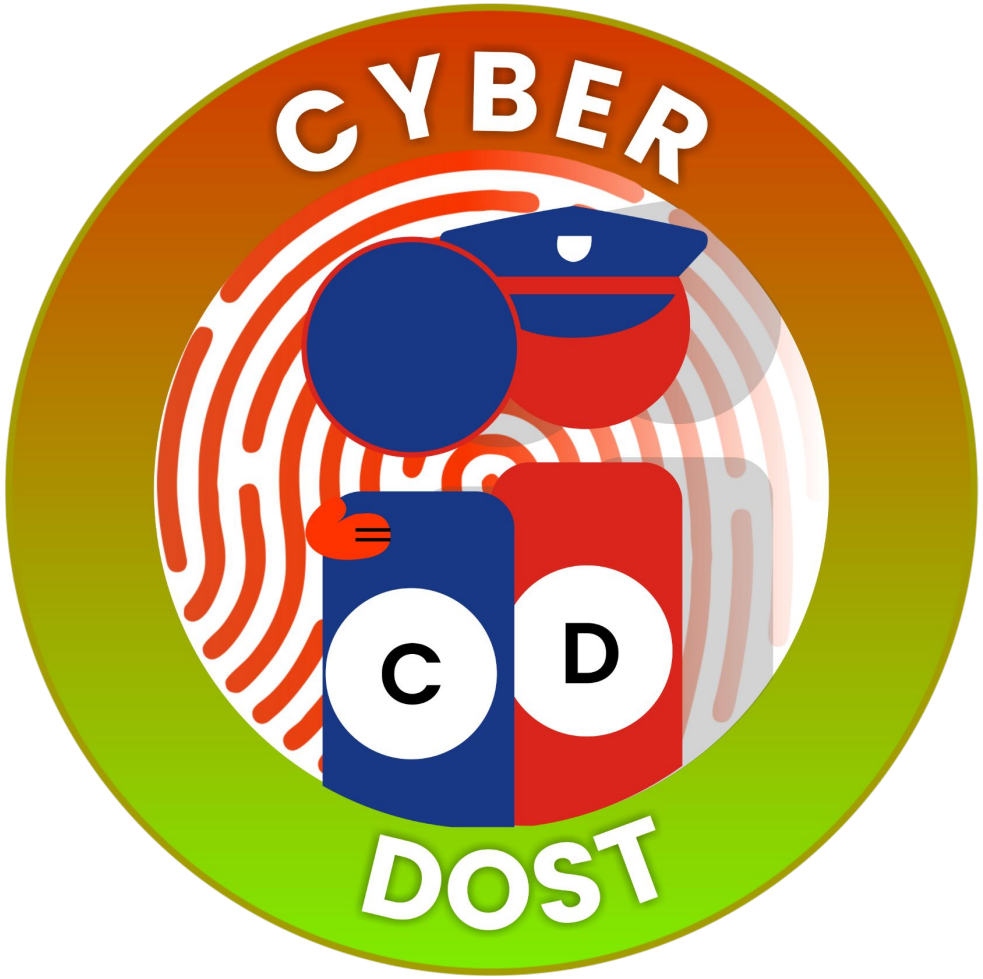
Regularly update device firmware and software.

Establish and enforce IoT security policies.

Implement strong encryption and authentication mechanisms.

Monitor network traffic for unusual activity.

Segment IoT devices from critical networks when possible.



Follow *CyberDost* on social media

- Get the latest Cyber Safety Tips
- Learn about various types of Scam Alerts
- Get updates on National and International Cyber news
- Learn about the achievements in the attempt to make the nation cyber safe
- Become a Cyber Volunteer and share the CyberDost content with your community
- Do your bit to stay vigilant and stay cyber safe!

@cyberdosti4c @CyberDosti4c @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c @cyberdost @cyberdost