

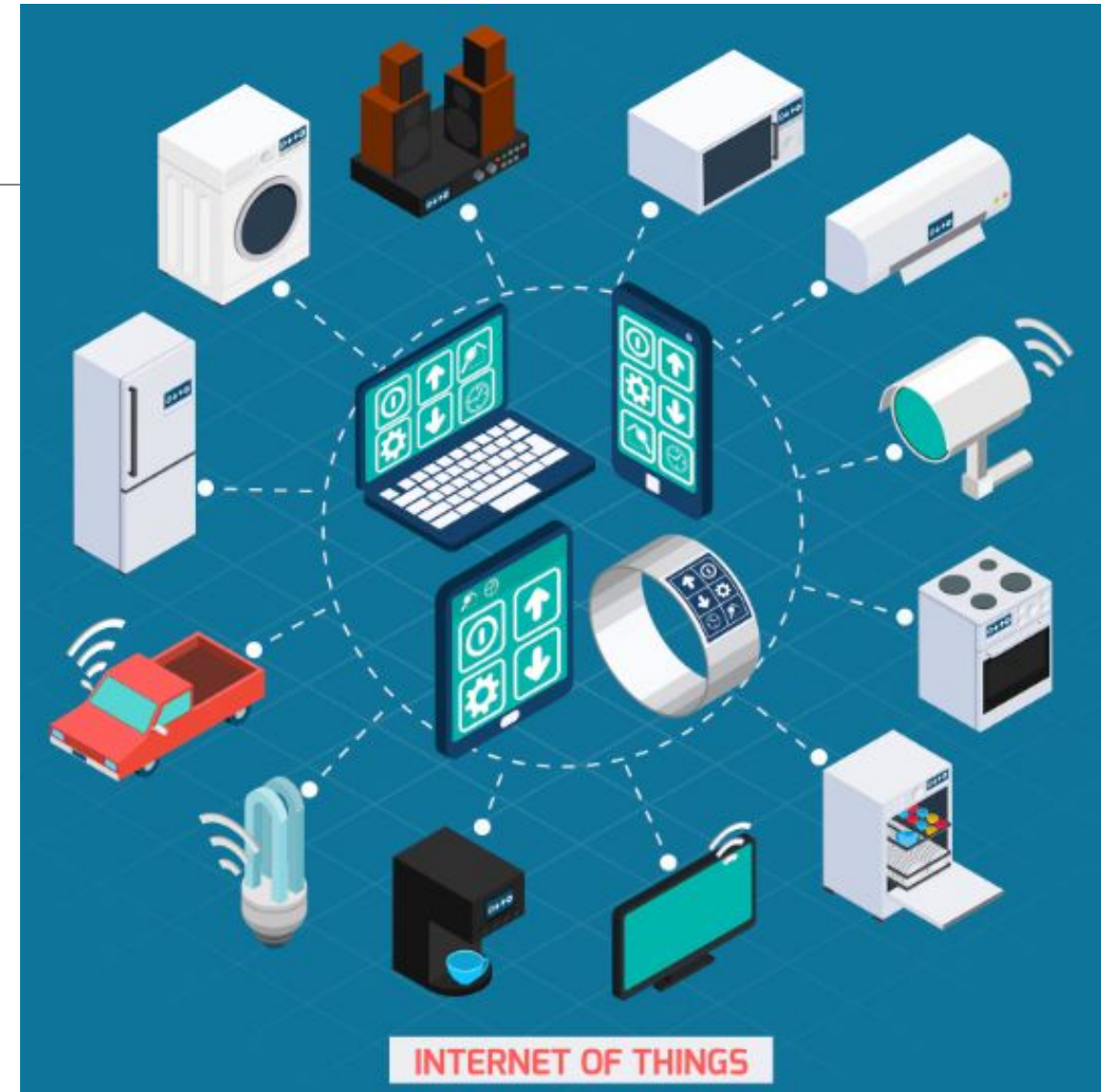
IOT Device Security

TRUST IS THE NEW CURRENCY OF IOT

By **Sumera Farooq**
Project Engineer
CDAC Mohali

Overview

- Introduction to IOT security
- Key IOT security challenges
- Real Life Example
- Common IOT attacks
- Security measures for IOT devices



What does IOT mean?

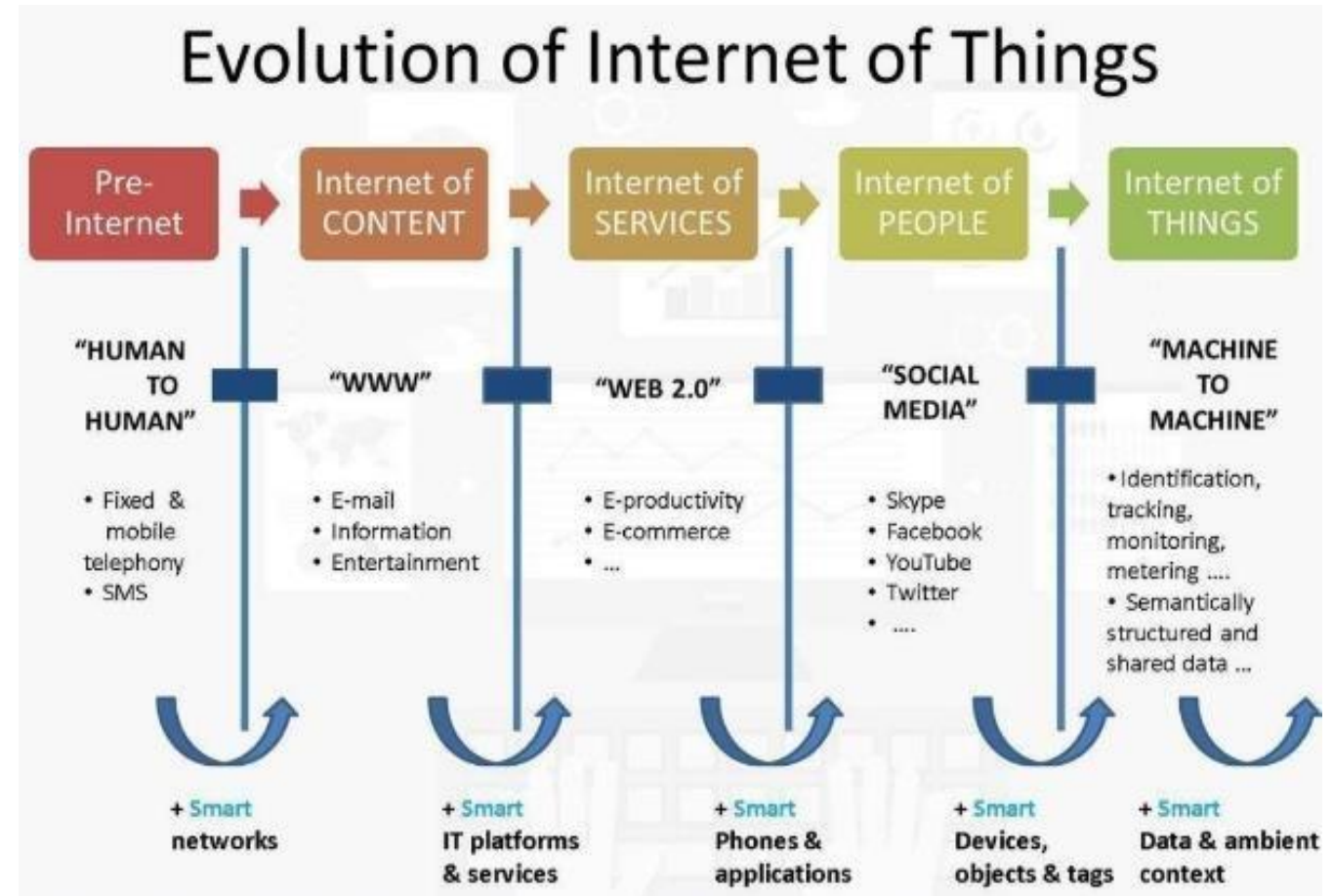
anytime, anyplace, anything in connectivity.

- ❖ The **Internet of Things (IoT)** connects ordinary objects to other objects and applications in the cloud, making them intelligent and interactive. Such "smart" devices make our lives richer and healthier and help to optimize the use of scarce resources
- ❖ A "**thing**" can be any physical entity that is given a unique identity and the ability to communicate or interact with other devices over a network. **Examples** of "things" include vehicles, appliances, industrial machines, wearable devices, and more.
- ❖ **Sensors** embedded in **physical objects** include temperature sensors, motion sensors, light sensors, humidity sensors, GPS sensors, and more.



Evolution & Revolution of IOT

The internet evolved from connecting people → to sharing content → to enabling services → to connecting people socially → and now to connecting machines directly, which is the essence of IoT.

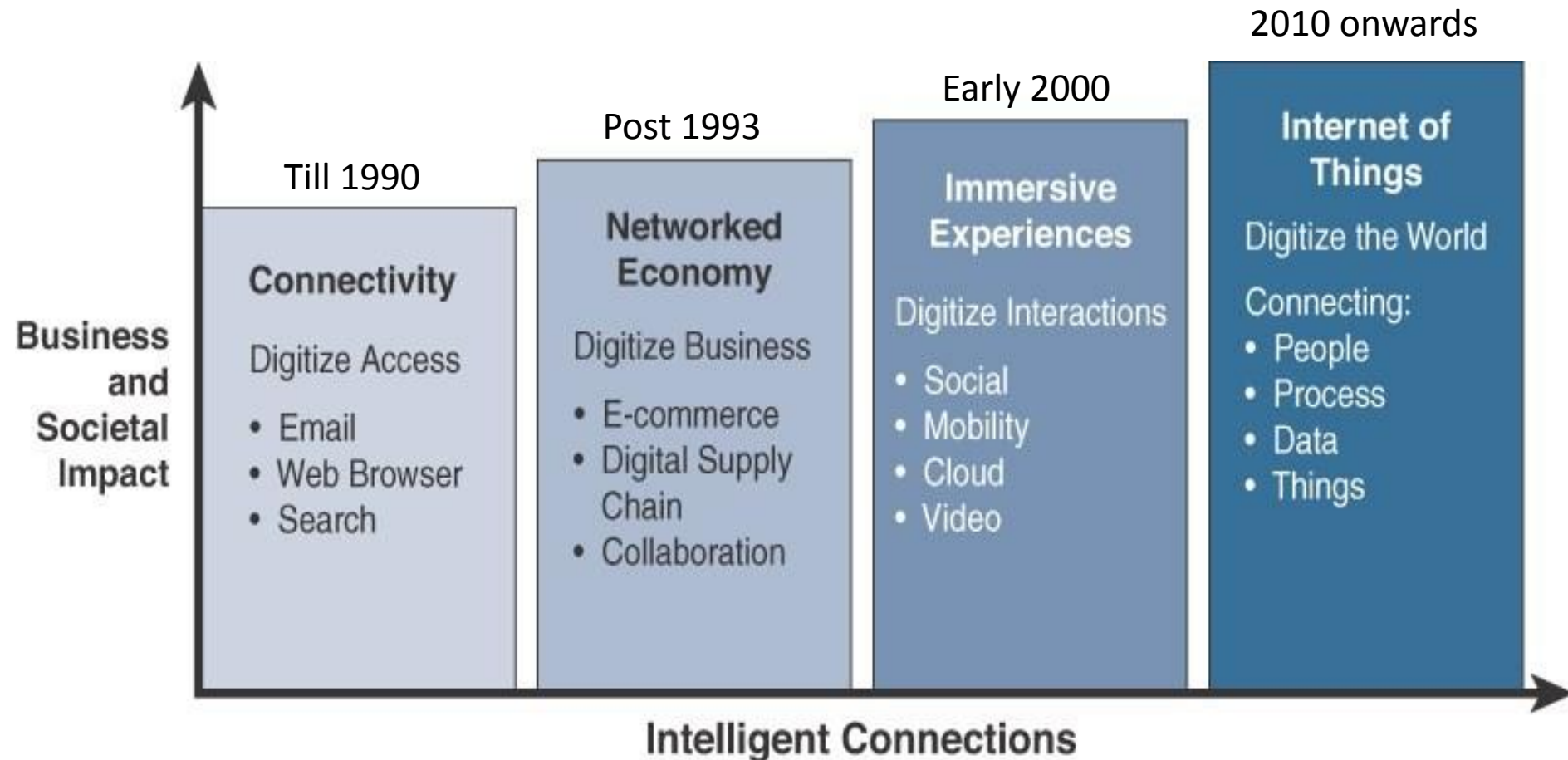


The Creation of the "Internet of Things"

- Coined by **Kevin Ashton** in 1999 during his tenure at Procter & Gamble.
- Ashton's work involved improving supply chain efficiency.
- Term emerged to describe a revolutionary concept of connecting objects to the internet.
- Term went beyond its initial context, reshaping technology and industries.



Brief History



Four Key Components of IOT

1. Sensing (Devices & Sensors)

“eyes and ears” of IoT

IoT devices use sensors to **collect data** from the physical environment (temperature, motion, location, heart rate, humidity, etc.).

2. Network Connectivity

The data collected must be **transmitted** to other devices, servers, or the cloud.

Short-range

Long-range/low-power

3. Data Processing (Edge/Cloud Computing)

Once data is transmitted, it must be **analyzed and processed**.

On the device itself (Edge Computing) → faster, less bandwidth.

In the Cloud → powerful analytics, big data, AI/ML.

4. User Interface (Application Layer)

The final step is where insights are made **usable for humans**.

A **mobile app** (to control your smart AC).

A **dashboard** (showing factory machine health).

Automated **alerts/notifications**.



1

Sensors

Collecting data



2

Connectivity

Sending data to cloud



3

Data Processing

Making data useful



4

User Interface

Delivering information to user

Sense → Connect → Process → Act

Advantages of IOT



1. Automation & Control

Devices can work automatically with minimal human intervention.

2. Efficiency & Productivity

Saves time and resources by automating repetitive tasks.

3. Data Collection & Insights

Continuous monitoring provides valuable data for decision-making.

4. Cost Savings

Energy-efficient systems lower utility bills.

5. Improved Safety & Security

IoT-enabled cameras, alarms, and sensors ensure better security.

6. Better Quality of Life

Smart homes, smart healthcare, smart transport → more convenience and comfort.

Disadvantages of IoT



1. Security Risks

Billions of connected devices increase the attack surface.

2. Privacy Concerns

IoT devices collect sensitive personal data.

3. Complexity & Compatibility

Different devices, networks, and protocols may not work together smoothly.

4. High Initial Costs

Smart devices and IoT infrastructure can be expensive to deploy.

5. Data Overload

Massive amounts of data need strong processing and storage.

6. Dependency on Internet

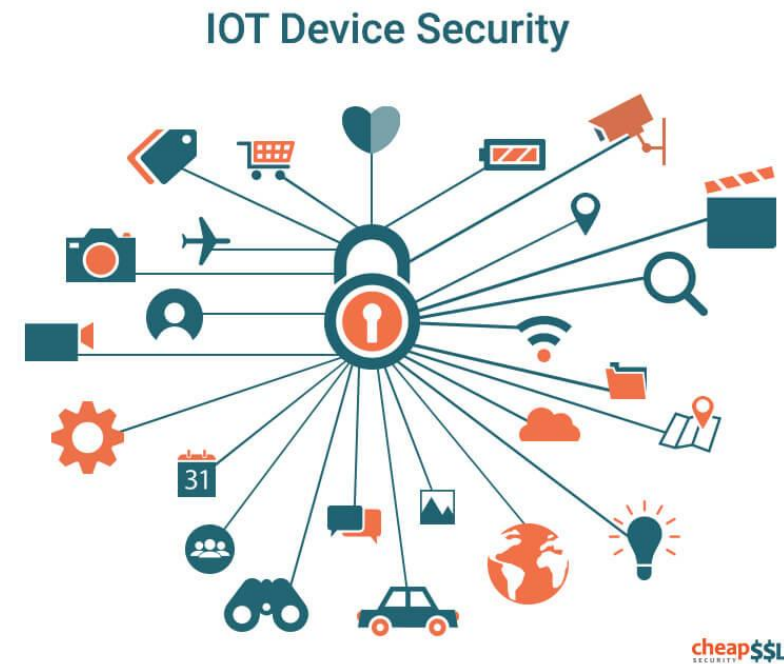
If the network goes down, devices may fail to function properly.

Modern Applications

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection
- Water flow monitoring
- Security
- Traffic monitoring
- Wearables
- Smart door lock protection system
- Robots and Drones
- Healthcare and Hospitals, Telemedicine applications
- Biochip Transponders (For animals in farms)
- Heart monitoring implants (Example Pacemaker)
- Agriculture
- Industry

IOT SECURITY

IoT Security is the set of principles, methods, and technologies ensuring that IoT devices, their communications, and their ecosystems are **confidential, integrity-protected, and available** (the classic CIA triad), and also ensuring **safety** (because many IoT systems interact with the physical world).



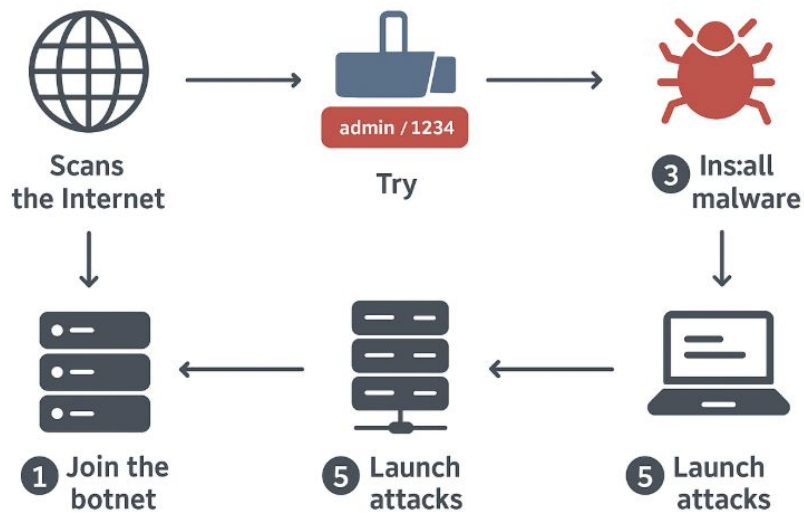
Why it's critical now

- The number of IoT devices is exploding (tens of billions globally) → **attack surface is huge.**
- Many IoT devices are deployed in **poorly controlled**, remote, or unmonitored settings (e.g. sensors in the field, consumer homes).
- IoT devices often have limited compute, memory, power, and cost constraints, making it harder to embed strong security. Because IoT devices often link to critical systems (e.g. industrial, healthcare, utilities), their compromise can have serious physical or societal impact (not just data breaches).
- Attackers increasingly use IoT devices as entry points into networks or as building blocks (e.g. botnets) for larger attacks.

So securing IoT is not optional—it must be built in throughout the lifecycle.

MIRAI Botnet

HOW THE MIRAI BOTNET WORKED



Mirai exploited weak/default passwords and open services on internet-connected devices to build a giant army of infected devices and use them to attack websites — the fix is basic hygiene: change defaults, update firmware, and isolate IoT devices.

How MIRAI Botnet Worked

Scan the Internet: Mirai looked for devices that were connected to the internet and listening on common ports (like Telnet).

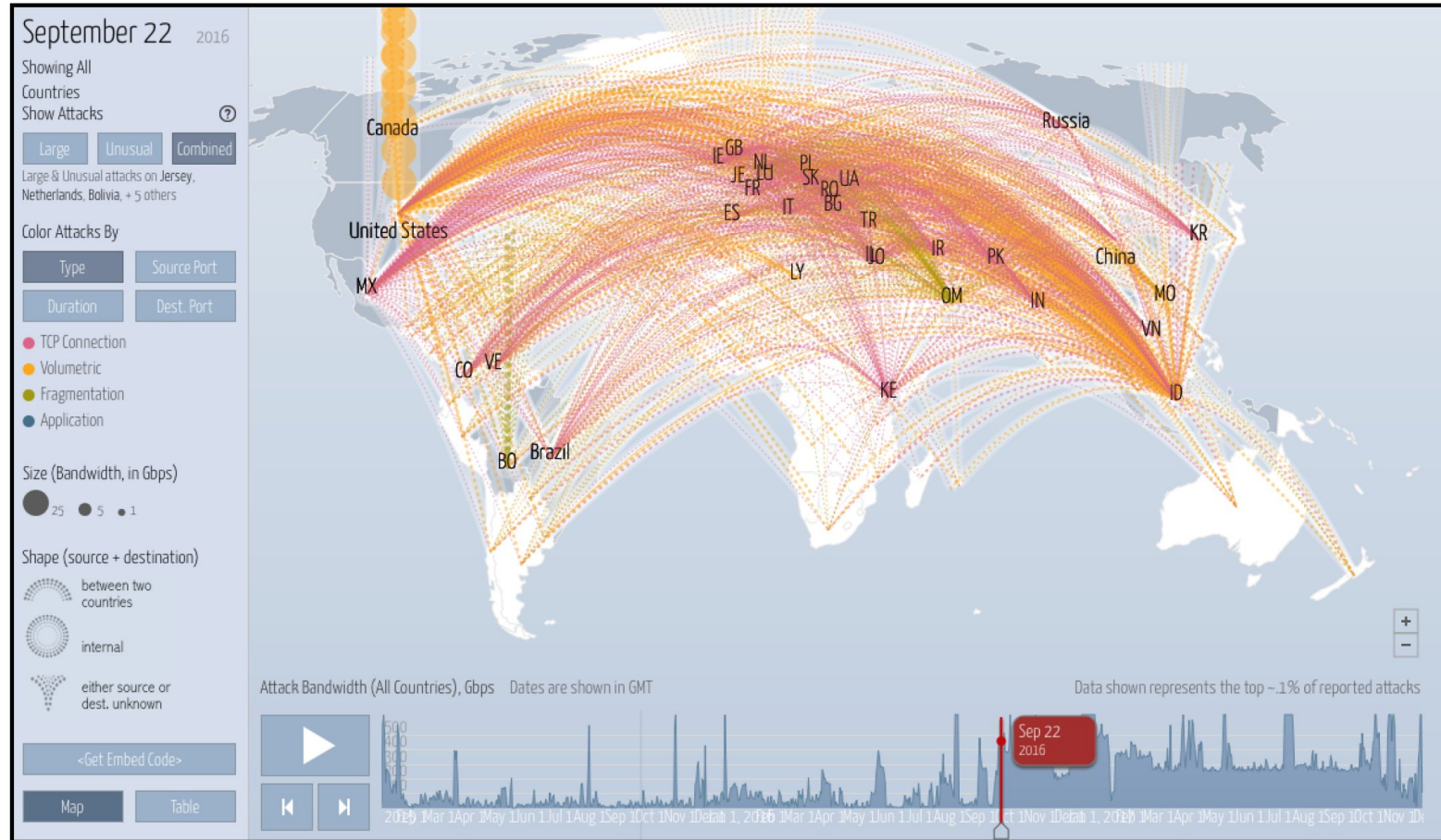
Try default passwords: For each device it found, Mirai tried a long list of common usernames and passwords (things like admin/admin) that manufacturers sometimes ship as defaults.

Log in and install itself: If the device accepted one of those usernames/passwords, Mirai logged in, downloaded the malware, and installed it on the device.

Join the botnet: The infected device connected back to the attacker's control server and awaited commands.

Launch attacks: When commanded, the attacker made all those infected devices send massive amounts of traffic to a chosen target — this is a Distributed Denial of Service (DDoS) attack, which can make a website or service unusable.

Real time screen shot captured during attack



Challenges

Security
How to ensure robust and lifelong security in IoT products and services?

Interoperability and Standards
The voluntary use of open, interoperable, and widely available standards as technical building blocks for IoT devices will deliver greater benefits.



Privacy

Strategies need to be developed that promote transparency, fairness, and user choice in data collection and handling.

Regulatory, Legal, and Rights Issues

The rapid rate of change in IoT technology could outpace the ability of associated policy, legal, and regulatory structures to adapt.

Emerging Economy and Development Issues

In order for the benefits of the IoT to be truly global, the unique needs and challenges of implementation in less-developed regions will need to be addressed.

Key IoT Security Challenges

- 1. Massive Attack Surface** Billions of IoT devices (CCTV cameras, wearables, smart meters, cars, etc.) are connected.
- 2. Weak Authentication & Authorization** Many IoT devices still use **default passwords** (like "admin/1234"). Lack of proper **multi-factor authentication** makes devices easy to compromise.
- 3. Data Privacy Concerns** IoT devices continuously collect sensitive data (health, location, voice, video). Unauthorized access or misuse can lead to identity theft, surveillance, or profiling.
- 4. Insecure Network Communication** Many devices transmit data **without encryption** (plain text). This makes it easy for attackers to perform **man-in-the-middle (MITM)** attacks.
- 5. Limited Device Resources** IoT devices have **low processing power, memory, and battery**. Running advanced security features (like firewalls, intrusion detection, or strong encryption) is difficult.

Contd...

6. Unpatched Vulnerabilities

Manufacturers often don't provide timely **security updates** or firmware patches. Hackers exploit outdated systems (e.g., Mirai botnet exploited unsecured cameras).

7. Physical Security Risks

Many IoT devices are deployed in public areas (traffic sensors, ATMs, cameras). Attackers can physically tamper with devices to extract data or install malware.

8. Supply Chain Risks

Components are sourced from different vendors. Malicious chips, backdoors, or compromised firmware can be introduced before the device is even sold.

9. Scalability of Security

Security mechanisms that work for a few devices may fail when scaled to millions. Managing credentials, updates, and monitoring at scale is a huge challenge.

Common IoT Attacks

Botnets / DDoS attacks

- Attackers compromise many IoT devices and use them to generate massive traffic to a target, overwhelming it (Distributed Denial of Service). The **Mirai** botnet is a classic example: it scanned for devices with default credentials (telnet) and conscripted them for DDoS.

Man-in-the-Middle (MITM) / Eavesdropping / Sniffing

- Intercept communications between devices, gateways, or cloud and either passively monitor or alter the data in flight. If protocols are not encrypted or properly authenticated, attackers can inject commands or corrupt data.

Spoofing / Identity / Replay Attacks

- An attacker may masquerade as a legitimate device, sensor, or gateway. Replay attacks reuse previously captured valid messages (e.g. commands) to trick the system.

Firmware / Software Exploits / Code Injection

- Vulnerabilities in firmware or application code (buffer overflows, injection points) are exploited to run malicious code or gain control.

Sensor / Side-Channel Attacks

- Using side information (e.g. power consumption, electromagnetic emanations, timing, thermal traces) to infer secrets (e.g. cryptographic keys).

Contd...

Denial of Service (DoS) / Resource Exhaustion

- Overwhelm limited-capability devices with requests or force them into a state of continuously trying to respond, draining battery or CPU. Jamming attacks (in wireless environments) can also block or degrade communications.

Supply Chain Attacks / Hardware Backdoors

- Malicious modifications or embedded backdoors during manufacturing, or insertion of malicious firmware before deployment. Attackers may also compromise the update infrastructure (e.g., push malicious updates).

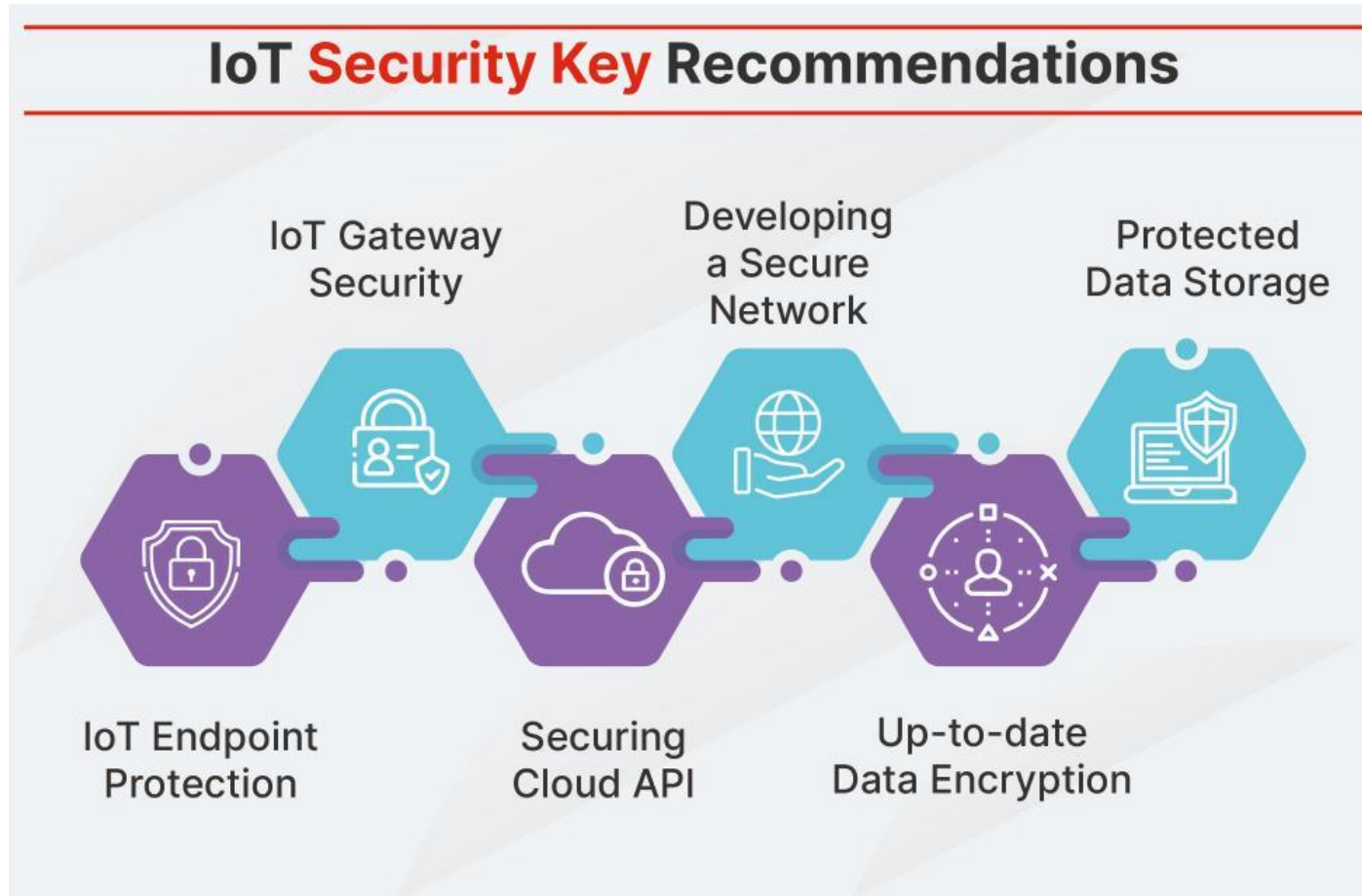
Data / Privacy Attacks

- Unauthorized access (or leakage) of sensor data, personal information, or control commands. Integrity attacks that manipulate data to mislead applications or operators.

Ransomware / Extortion Attacks

- In more sophisticated environments, attackers may encrypt or lock control systems (e.g. in OT / IoT contexts) to force ransom. OT/IoT ransomware is becoming more prevalent, especially targeting critical infrastructure.

IOT Security Key Recommendation



IOT Security 6-Key Recommendation

IoT Endpoint Protection

Secure device ports (TCP, UDP, wireless)

Block unencrypted communication

Prevent code injection & malware

Full visibility of connected devices

IoT Gateway Security

Use **Secure Web Gateway (SWG)**

Features: app control, HTTPS/SSL inspection, URL filtering

Stop malware & unauthorized access

Secure remote/cloud connections with VPN & monitoring

Securing Cloud APIs

APIs = bridge between IoT & cloud → must be secured

Use authentication, encryption, tokens, API gateways

Prevent large-scale data breaches

Example: REST APIs secure data transfer between devices & servers

IOT Security 6-Key Recommendation

Secure Network Development

Deploy firewalls & MFA (multi-factor authentication)

Allow only verified devices on the network

Protect authentication keys, update antivirus/antimalware

Continuous monitoring of network activity

Up-to-Date Data Encryption

Encrypt data in motion (device ↔ internet)

Symmetric encryption
→ single key

Asymmetric encryption
→ public + private keys (more secure)

Stronger defense against eavesdropping & replay attacks

Protected Data Storage

Secure sensitive info (financial, personal, biometric)

Updated antivirus, antimalware & scanning tools

Real-time threat monitoring + alerts

Centralized console for visibility & control

IoT Emerging Trends

5G-powered IoT – Faster, low-latency connectivity enabling smart cities, autonomous vehicles, and industrial IoT.

AI + IoT (AIoT) – Smarter decision-making with predictive analytics, anomaly detection, and automation.

Edge Computing – Data processed closer to devices for real-time insights and reduced cloud dependency.

IoT Security Enhancements – Stronger endpoint protection, blockchain-based authentication, and zero-trust models.

Wearable & Healthcare IoT – Smart health monitoring, remote patient care, and wellness tracking.

Sustainable IoT – Energy-efficient devices and IoT solutions for smart grids, agriculture, and climate monitoring.

IOT Future Directions

Hyperconnected Smart Cities – Seamless integration of IoT in traffic, utilities, waste, and safety systems.

Autonomous IoT Systems – Self-learning IoT networks powered by AI/ML.

Quantum IoT (QIoT) – Leveraging quantum computing for stronger IoT security and faster data analysis.

Interoperability Standards – Universal IoT protocols for device compatibility across industries.

Human-Centric IoT – Focus on user privacy, accessibility, and ethical IoT use.

Safety Measures for Common IoT Users

Change Default Passwords

Most IoT devices come with weak default passwords (like “admin123”).

What to do: Always set a strong, unique password for each device.

Example: If someone hacks your Wi-Fi camera using the default password, they can spy on your home.

Keep Devices Updated

Manufacturers release security updates to fix vulnerabilities.

What to do: Turn on automatic updates or check regularly.

Example: Outdated smart TVs may get infected by malware that spreads across your Wi-Fi.

Use Secure Wi-Fi

IoT devices connect through your home Wi-Fi, so if Wi-Fi is weak, all devices are at risk.

What to do: Use **WPA3** or **WPA2 encryption**, set a strong Wi-Fi password, and avoid public Wi-Fi.

Example: A hacker in your neighborhood could connect to your Wi-Fi if it's open and control your smart door lock.

Safety Measures Contd...

Separate IoT Network

Many routers allow a “guest network.” Use that for IoT devices.

What to do: Keep your laptop/phone on one network and IoT devices on another.

Example: If a smart bulb gets hacked, it won't affect your banking app on the laptop.

Turn Off When Not in Use

Idle devices still consume data and remain hackable.

What to do: Switch off IoT devices when not needed (like smart plugs, cameras).

Example: A baby monitor left on 24/7 could be hijacked by attackers to listen inside your home.

Be Careful with Permissions

Many IoT apps ask for location, contacts, or camera access unnecessarily.

What to do: Give only the permissions required.

Example: A smart torch app asking for microphone access may be spying.

Safety Measures Contd...

Use Two-Factor Authentication (2FA)

Extra layer of protection for accounts connected to IoT devices.

Example: If your smart lock app is hacked, the hacker still can't log in without your OTP.

Install Security Software

Use antivirus and firewall on your home Wi-Fi or smartphone controlling IoT.

Example: Prevents malicious apps from stealing IoT login details.

Stay Aware

Learn about recent IoT scams (like fake apps or malicious firmware updates).

Example: Fake Alexa apps on app stores steal login details from careless users.

Key Takeaway Points: IoT Safety for Everyone

1. **Change Default Passwords**
 - Set a strong, unique password
 2. **Keep Devices Updated**
 - Enable automatic updates
 3. **Use Secure Wi-Fi**
 - Use WPA3 or WPA2 encryption
 4. **Separate IoT Network**
 - Use a guest network for IoT devices
 5. **Turn Off When Not in Use**
 - Switch off idle devices
 6. **Be Careful with Permissions**
 - Grant only necessary permissions
 7. **Use Two-Factor Authentication**
 - Add an extra layer of protection
 8. **Check Privacy Policies**
 - Prefer brands with transparent policies
 9. **Stay Aware**
 - Learn about latest IoT scams & risks
-

Q & A

Thank You