# ****Internet of Things Security – Lecture 01: Introduction to IoT****

**Instructor:** Mehmoona Jabeen  
**Department of Cyber Security, Air University**

## ****Course Outline****

* Introduction to Internet of Things
* Hardware Architectures and Embedded Systems
* Embedded Operating Systems for IoT Devices
* Firmware Development and Management
* Communication Protocols for IoT
* IoT Attack Vectors and Threat Modelling
* IoT Security Analysis and Vulnerability Assessment
* IoT Application Security and Their Challenges
* IoT Data Security and Challenges
* Security Issues in Edge Computing Based IoT Architecture

**Readings:**

* Selected research articles with each lecture
* Selected chapters from specified textbooks

## ****Lecture Outline****

* What is IoT?
* Enabling Technologies
* Characteristics
* Growth and Challenges
* IoT Security Needs
* IoT Attack Surfaces and Vulnerabilities
* Common Vulnerabilities Reported
* Known Attacks in IoT

## ****What is Internet?****

* A global network of computers providing information and communication facilities
* Uses standardized communication protocols
* The Web (WWW) is one of many services of the Internet

## ****What is IoT (Internet of Things)?****

* Inter-networking of physical devices (smart devices) embedded with:
  + Electronics
  + Software
  + Sensors
  + Actuators
  + Network connectivity
* Enables data collection and exchange

**Fundamental Building Blocks of IoT:**

1. Identifiability (Recognizing Things)
2. Processing (Think and Decide)
3. Communication (Talk to Other Devices)
4. Interaction (Take Action Based on Data)

## ****Key Terminologies****

* **M2M (Machine-to-Machine Communication)**
* **CPS (Cyber Physical Systems)**
* **IoE (Internet of Everything)**

## ****IoT Growth Path****

1. Pre-Internet - Human-to-Human, Fax, SMS, Fixed/Mobile Phones
2. Internet of Contents - Web, Email, Entertainment
3. Internet of Services - Service-to-service comm using XML, JSON
4. Internet of People - Social Networking (Facebook, Twitter, Skype)
5. Internet of Things - Machine-to-Machine (Smart Metering, Smart City, Smart Home)

## ****Enabling Technologies****

* **RFID** – Identification and tracking
* **WSN (Wireless Sensor Networks)** – Sensing and monitoring
* **IPv6** – Addressing and networking
* **WPAN** – Low-power communication

## ****Pervasive Sensing/Computing****

* Massive data generation from sensors
* Controlled and actuated remotely
* Stored in local/cloud with analytics

| **Aspect** | **Examples** |
| --- | --- |
| Anytime | Driving, walking, sleeping, static |
| Anything | Healthcare sensors, jet engines, etc |
| Anyscale | Thousands of sensors in KM² |
| Anyplace | Underground metros, drones, oceans, soil, implantable, underwater |
| Anywhere | Everywhere |

## ****IoT Evolution and History****

* Already in use: Cars, Homes, Machines, Industrial Equipment
* First IoT Device: **Coke Machine (1982)** by Carnegie Mellon University

## ****Why IoT is Growing Now****

1. Low-cost, powerful microchips (e.g., STM32 F4 vs Pentium 1993)
2. Network improvements (e.g., Wi-Fi speeds)
3. IPv6 expansion (340 trillion addresses)
4. Wireless communication advances
5. Big data tools (e.g., Hadoop, Spark)
6. Affordable sensors
7. Technology convergence: Cloud, Data Analytics, Sensors, IP networks

## ****IoT Technologies Overview****

### ****Sensors****

* Types: Accelerometer, Gyroscope, Thermometer, etc.
* Factors: Size, Cost, Accuracy, Power Efficiency

### ****Networking****

* IP-based technology advantages
* IPv6 benefits with 6LoWPAN for IoT

### ****Cloud Platforms****

* **AWS IoT**, **Microsoft Azure**, **Google Cloud**, **IBM Watson**, etc.

## ****OWASP IoT Attack Surfaces & Vulnerabilities****

|  |  |
| --- | --- |
| Attack Surface | Example Vulnerabilities |
| Ecosystem Access Control | Implicit trust, lost access, poor decommissioning |
| Device Memory | Cleartext passwords, credentials |
| Physical Interfaces | Privilege escalation, insecure reset |
| Web Interfaces | SQL injection, weak/default passwords |
| Firmware | Hardcoded credentials, unsigned updates |
| Network Services | DoS, unencrypted services, vulnerable UPnP |
| Administrative Interfaces | SQL injection, XSS, default credentials |
| Local Data Storage | Unencrypted or poorly encrypted data |

## ****IoT Security Introduction****

* Attacks affect the CPS-physical interaction
* Surfaces: Cyber, Physical, Environmental, Human
* Development of detection/mitigation/recovery technologies

## ****IoT Vulnerability Reports (CVE Examples)****

* **CVE-2018-6932** – DoS via system resource exhaustion
* **CVE-2018-3619** – Data recovery via physical access
* **CVE-2018-9149** – UART insecure interface
* **CVE-2018-18653** – Bypass secure boot
* **CVE-2018-9919** – Factory backdoor via SSH

## ****IoT Exploitation and Abuse****

### ****ThingBots****

* Botnets of IoT devices used in spam, malware, and DDoS

### ****Famous Cases****

* **Proofpoint**: 100k+ household devices used in spam
* **Linux.Darlloz**: Worm using CVE-2012-1823
* **Spike Botnet**: Used 12k–15k IoT devices for DDoS
* **Wearables**: Bluetooth brute-force attacks
* **Smart Meters**: Can be used for billing fraud/blackouts
* **Mirai Botnet**, **BrickerBot**, **Cold in Finland** DDoS events

## ****IoT Security Needs****

* IPv6 expansion and DNS role
* Need for standardization
* Addressing vulnerabilities and DDoS threats

## ****Applying Internet Security to IoT****

* Mutual authentication (PKI-based)
* TLS/IPSec are complex for constrained IoT devices
* Context-aware IDS/IPS needed

## ****IoT Security Challenges****

|  |  |
| --- | --- |
| Layer | Challenges |
| Perception Layer | Cloning, Eavesdropping, Spoofing, DoS |
| Network Layer | Sybil attack, DoS, Man-in-the-Middle |
| Middleware Layer | Unauthorized access, DoS, Malicious insider |
| Application Layer | Code injection, Phishing, Sniffing, DoS |

## ****ARM Platform Security Architecture (PSA)****

* End-to-end security
* Simplifies security evaluation of IoT devices

## ****Traditional Security vs IoT****

* IoT resource constraints make traditional methods impractical
* Need for:
  + **IoT tools**
  + **IoT-specific datasets**

## ****IoT Tools****

### 1. ****IoT Traffic Generator Tool****

* Open-source, real-time simulation, latest attack generation
* Link: [GitHub IoT-Advanced-Data-Generator](https://github.com/IRIL-KICS/IoT-Advanced-Data-Generator)

### 2. ****IoT Healthcare System Dataset****

* 200+ devices
* Protocol-specific features
* Includes both normal and malicious traffic

### 3. ****IoT Firewall****

* Network-level security for constrained devices