Lecture – 09

Intro. to Internet of Things

Dr. Ahmed Elngar
Faculty of Computers and Artificial Intelligence
Beni-Suef University

23. IoT – Security

Every connected device creates opportunities for attackers. These vulnerabilities are broad, even for a single small device. The risks posed include data transfer, device access, malfunctioning devices, and always-on/always-connected devices.

The main challenges in security remain the security limitations associated with producing low-cost devices, and the growing number of devices which creates more opportunities for attacks.

Security Spectrum

The definition of a secured device spans from the most simple measures to sophisticated designs. Security should be thought of as a spectrum of vulnerability which changes over time as threats evolve.

Security must be assessed based on user needs and implementation. Users must recognize the impact of security measures because poorly designed security creates more problems than it solves.

Example: A German report revealed hackers compromised the security system of a steel mill. They disrupted the control systems, which prevented a blast furnace from being shut down properly, resulting in massive damage. Therefore, users must understand the impact of an attack before deciding on appropriate protection.

Challenges

Beyond costs and the ubiquity of devices, other security issues plague IoT:

- **Unpredictable Behavior –** The sheer volume of deployed devices and their long list of enabling technologies means their behavior in the field can be unpredictable. A specific system may be well designed and within administration control, but there are no guarantees about how it will interact with others.
- **Device Similarity –** IoT devices are fairly uniform. They utilize the same connection technology and components. If one system or device suffers from a vulnerability, many more have the same issue.

- **Problematic Deployment –** One of the main goals of IoT remains to place advanced networks and analytics where they previously could not go. Unfortunately, this creates the problem of physically securing the devices in these strange or easily accessed places.

- **Long Device Life and Expired Support –** One of the benefits of IoT devices is longevity, however, that long life also means they may outlive their device support. Compare this to traditional systems which typically have support and upgrades long after many have stopped using them. Orphaned devices and abandonware lack the same security hardening of other systems due to the evolution of technology over time.

- **No Upgrade Support –** Many IoT devices, like many mobile and small devices, are not designed to allow upgrades or any modifications. Others offer inconvenient upgrades, which many owners ignore, or fail to notice.

- **Poor or No Transparency –** Many IoT devices fail to provide transparency with regard to their functionality. Users cannot observe or access their processes, and are left to assume how devices behave. They have no control over unwanted functions or data collection; furthermore, when a manufacturer updates the device, it may bring more unwanted functions.

- **No Alerts –** Another goal of IoT remains to provide its incredible functionality without being obtrusive. This introduces the problem of user awareness. Users do not monitor the devices or know when something goes wrong. Security breaches can persist over long periods without detection.

26. IoT – Useful Resources

The following resources offer more in-depth information on IoT development and administration. You can refer them to increase your knowledge on IoT further.

Useful IoT Websites

- Internet of Things Council – This European think tank offers the best and latest IoT information. They analyze every aspect of IoT from forecasting to discussing prototype development, and the social implications of IoT.
- LinkedIn Pulse Content – LinkedIn, described as the world's largest professional network, allows over 100 million professionals to network. It opened its publishing platform, Pulse, to the public in 2014, resulting in a wealth of valuable professional and industry information. This information includes rare insight, training media, and more related to IoT systems and technologies.
- Lynda.com IoT Videos – This online learning organization offers thousands of videos on various topics (including IoT) supplied by professionals, organizations, and individuals.
- YouTube IoT Videos – Individuals just like you produce thousands of IoT videos on YT to address particular topics not covered elsewhere, or covered poorly elsewhere. These videos use different languages, styles, and offer unique voices.

Useful IoT Literature

Building Internet of Things with the Arduino (Volume 1) by *Charalampos Doukas*	**Making Things Talk, 2nd Edition** by *Tom Igoe*	**Building Wireless Sensor Networks: with ZigBee, Xbee, Arduino, and Processing** by *Robert Faludi*
Building the Web of Things with Examples in Node.js and Raspberry Pi by *Dominique D. Guinard and Vlad M. Trifa*	**Internet of Things (A Hands-on-Approach)** by *Arshdeep Bahga and Vijay Madisetti*	**The Internet of Things in the Cloud: A Middleware Perspective** by *Honbo Zhou*