IoT Security Issues

Vladimir Dimitrov [1]

[1] *University of Sofia, 5 James Bourchier Blvd., Sofia, 1164, Bulgaria*

Abstract

IoT has a complex and multilevel architecture. This is a promise for multiple weaknesses and vulnerabilities.

The paper first presents IoT architecture and then based on it discuss the possible cybersecurity issues.

IoT architecture proposed in this paper is an attempt to combine all aspects of these systems.

Cybersecurity issues are discussed on each architecture level with a primary focus on information security.

Keywords

IoT, architecture, cybersecurity

1. IoT definition and architecture

The term IoT has been introduced for the first time by Peter T. Lewis (a speech to the Congressional Black Caucus Foundation at 15th Annual Legislative Weekend in Washington, D.C.), and published in September 1985. The definition by [1] is:

"*The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices.*"

IoT contains a huge number of endpoints (sensors, smart meters etc.) connected via public networks (internet, pervasive wireless) in "hostile" (public) environments. IoT infrastructure usually is physically controlled by multiple parties and again usually is not instrumented to detect/prevent attacks. These endpoints need to be tamper-resistant and securely managed.

Endpoints are everywhere (as smart meters, and complex like smart buildings, and smart cities etc.). They transact via public networks (IP, internet, wireless) in "hostile" (public) environments.

IoT endpoints are often cost and power constrained.

Information Systems & Grid Technologies: Fifteenth International Conference ISGT'2022, May 27–28, 2022, Sofia, Bulgaria
EMAIL: cht@fmi.uni-sofia.bg (V. Dimitrov)
ORCID: 0000-0002-7441-253X (V. Dimitrov)

The most important and IoT security challenge is endpoints to be secured against software and hardware attacks.

Endpoints combine different sensors and possibly actuators. They are at the lower architecture "instrumented" level.

Sensor data generated by the endpoints are transmitted for real time data integration. Integrated data are used for decision support at the higher architecture levels. Following the taken decisions, the actuators may be activated.

Integrated data are transmitted for data modeling and analytics too. Analyzed data usually are visualized for decision support in possibly intelligent manner.

All these data transmissions must occurs in a secure reliable infrastructure.

Some purpose oriented IoT structuring is based on the concepts of Smarter Energy, Smarter Buildings, Smarter Healthcare, Smarter Transportation etc. Below the common IoT architecture is discussed with illustrations mainly from Smarter Energy.

IoT security is infrastructure security plus enterprise security.

IoT architecture by [2] can be layered as follows:

- **Perception layer** interconnects devices, sensors and actuators (machines, smart devices) to IoT.
- **Connectivity/Transport layer** transfers data via Personal Area Network, Local Area Network, Wireless Local Area Network, Campus Area Network, Metropolitan Area Network, Wide Area Network, Storage-Area Network, System-Area Network, Passive Optical Local Area Network, Enterprise Private Network, and Virtual Private Network. Protocols used at this layer are:
  - TCP/IP, UDP/IP.
  - LAN, WAN.
  - Data Distribution Service (DDS) – a machine-to-machine real-time messaging framework.
  - Advanced Message Queuing Protocol (AMQP) – protocols for servers based on peer-to-peer connections.
  - Constrained Application Protocol (CoAP) – protocols for constrained devices (low power and memory).
  - Message Queue Telemetry Transport (MQTT) – messaging protocol standards for low-powered devices using TCP/IP.
- **Edge Computing layer** (pre)processes information at the edge (near the device information collection) to decrease information delay. As example 5G vs 4G – the last one has no Edge Computing layer.
- **Processing layer** captures, stores, and processes data. It functionality can be defined in:
  - Data Accumulation that selects essential data from device data streams.
  - Data Abstraction that collects data from IoT and non-IoT systems, vir-

tualizes data to be accessible from one single point, and manages raw data in multiple forms.

- **Application layer** processes and analyzes data to gather business intelligence.
- **Business layer** derives information for decision-making analysis.
- **Security layer** covers all aspects of protecting the whole IoT architecture. Cybersecurity aspects at this level are:
  - Device Security;
  - Cloud Security;
  - Connection Security.

Cybersecurity issues are discussed in the next sections layer by layer.

2. Perception layer

At the Perception layer, endpoint (advanced) sensors transfer its raw data to an aggregator (poletop collector, meter concentrator, collection engine, transmission-monitoring equipment, substation remote monitoring equipment) via RF mesh.

Possible security issues here can be:

- Device (meter) authentication;
- Device (meter) secure boot and provisioning;
- Collector secure boot and provisioning;
- Data encryption / decryption;
- Device (meter) and collector event generation and routing.

Devices usually are cheaper ignoring cybersecurity designed to achieve mainly low power and low memory consumption. There are many device vendors using their own private protocols.

Communications with the aggregator are usually Bluetooth, RF- or Wi-Fi-based.

This layer can be structured in Personal Area Networks and further in Home Area Networks. Sometimes local structuring is extended in the building at Entrance Area Network and Building Area Network or Smart Home, Smart Building, and Smart City.

Some elements and standards of Advanced Metering Infrastructure (AMI) (part of Smarter Energy) are:

- LMS/DRMS: Load Management / Demand Response Management System;
- MDMS: Meter Data Management System;
- RF: 900MHz band radio frequency meter mesh network;
- ANSI C12.19: Meter table data format;
- ANSI C12.22: Application layer protocol for meter operations;

- DLMS: Device Language Messaging Specification;
- COSEM: Companion Specification for Energy Metering.

Typical threads for AMI are:

- **Cheating Customer threat**: Only valid meters have to be identified and registered with AMI network. Meter-tampering events must be handled. Cheating customer threat is a consequence of low levels of funding, moderate commitment. There may be some attempt to perform the types of physical attacks that have been used in the past against conventional meters, but these will be quickly detected through monitoring of electric use in real-time. The more likely attacks against advanced meters will be similar to the attacks against broadband modems. These will include accessing the advanced meter configuration through cyber means and even modification of the advanced meter firmware. Just as in the cable modem un-capper world described in the references, the threat will arise from small groups who combine talents and knowledge to develop tools to modify advanced meters for consumers.
- **COTS Power Pilfering Tools threat**: Firmware must be attested on initial boot. Its updates have to be applied only after attestation. Firmware integrity must be queried against baseline measurements.
- **Network Attacks**: IP enabled collector must be free from malware. It must be accessible only under strict access control. Security events must be handled.

3. Connectivity/Transport layer

Connectivity in network terms can be defined as Home Area Network, Neighbor Area Network, Access Network, Backhaul Network, Office Network, and Extranet – integrated communication networks.

Home Area Network connects in-home devices as smart appliances, personal computers, in-home displays, load control devices, electric vehicle outlets etc.

Neighbor Area Network connects smart meters as electric meters, gas meters, water meters etc.

Access Network connects substation and grid devices as switches, reclosers, condition sensors, voltage controllers etc.

Backhaul Network and Office Network connect mobile devices as ruggedized laptops, handheld data devices, cell phones etc.

Extranet connects distributed resources as solar panels, wind turbines, energy storage, combined heat and power, etc.

Common thread here are the **network attacks**. Head-end have to be protected from DOS attacks, scrub XML traffic for SQL injection, malformed XML attacks.

Connectivity deals with system integration platforms consisting of computing infrastructure (servers, storage and backups), systems management (security management, system and network management), and application integration (business process management, messaging and Web services).

Intelligent applications management deals with warehouse management system, call management, network analytics, geographic information system, meter data collection, asset management, order management system, customer information systems, meter data management systems, load control, environmental management system, document management system etc.

Intelligent presentations deal with customer Web, customer mobile devices, display device interface, employee portal / dashboard, paper bills etc.

4. Edge Computing layer

The Edge Computing Infrastructure (ECI) is placed near to device information collection. There is no widely accepted definition of the term "Edge Computing". ECI is called sometimes Meter Head End.

For some authors, ECI is placed in front of the datacenter collecting IoT data. It collects data from pole mounted cell relay collectors using the network fabric. ECI is behind a firewall protecting it from WAN (Internet) threads. ECI transmits the data to the next Application layer via secured network (internal, protected). The Application layer is protected in depth with another firewall.

For other authors, ECI is distributed in the field. The only difference is that ECI is connected to the Application layer using public Internet connections. It is possible these connections to be organized in Virtual Public Network (VPN).

The purpose of Edge Computing is to booster the query response times by preprocessing the data near to the data collectors and further to transmit preprocessed data faster to the Application layer.

Edge Computing consists of Data Aggregators and Data Collectors.

Specific thread for this layer is the **reverse engineered meter**. To fight this thread must be established trust with the meters.

Another specific thread is the **insider threat**. Must be established control on who has access to meter, under what conditions, and throttle meter disconnects. The insider can use the AMI to increase peak usage, thereby creating increased demand for generation power, possibly via the spot market, but certainly at a higher price point than would otherwise occur. Thus, the colluding generation provider will make more money that they have to be shared with the insider. The last one in this case would be described as having low funding (they want to make money, not spend it), low goal intensity. High stealth (insiders require stealth to succeed and to avoid being caught), high physical access (they are insiders, after all), low cyber skills (they are far more likely to misuse the system than to de-

velop cyberattacks), an implementation time in months, and a cyber organization size in ones.

The other threads are originated from the network fabric.

5. Application layer

Applications layer consists of applications that are common and control the whole IoT system. Some of these applications support Business Intelligence effort on the Business layer – prepare data for it.

Some applications on this layer are:

- Advanced metering control and data management system;
- Distributed Control Systems or SCADA (Supervisory Control and Data Acquisition);
- Meter Data Management Systems (MDMS);
- Demand Response Management Systems (DRMS);
- Local Management Systems (LMS).

Most of the problems at this layer are well known and traditionally well managed.

Some specific threads are:

- **Privacy loss threat**. Consumer privacy has to be protected. Privacy data have to be shared on the base only need-to-know elements of meter data.
- **Insider threat**. Accuracy of billed meter data have to be in the focus. Database access shared with third party service providers has to be monitored.

6. Business layer

Business intelligence layer deals with decision support systems at middle and high management levels. It includes systems from the categories MIS, DSS, ESS.

There is no specifics threads burdened by IoT.

7. Security layer

Cybersecurity is more focused on intelligent and interconnected areas. IoT demands this focus to be extended on the instrumented area.

There are many challenges to securing the lower layers of the stack:

- One vendor does not own all the pieces;
- There are many players and standards;
- Solutions are constrained by cost, power, etc.

Topics covered at this layer are security intelligence and analytics, governance, risk management, and compliance management.

Traditional cyber security is:

- more mature end-to-end security;
- requirements fit well-defined pattern;
- carrier class communication;
- more standardized control points;
- limited controlled exposure;
- less variance in operating systems and network protocols.

IoT security is:

- Geographically dispersed sensors remote from data center are more susceptible to attacks.
- Heterogeneous technologies and proprietary protocols between sensors and devices, non-carrier class communication, and control points that are not always standardized and secure.
- Endpoints often built in embedded systems with non-traditional OS, where normal security functions may not exist.
- Cost-conscious endpoint vendors often cut corners for security (example: factory-set cryptographic keys in electric meters).
- Unique non-traditional operating systems; not enough memory; low margins of selling.
- Computing deeply embedded in controllers, sitting in different environments.
- Highly automated, optimized functions within endpoints.

For critical infrastructure, the nation-state or terrorist threat is very important to be under permanent investigation. Although utilities cannot counter nation-state or terrorist threats on their own, their security improvements for other threats can help the government in countering these threats. These threats would attack AMI with intent to cause effects outside of the AMI system, probably effects centered on the bulk electric grid. The high-level threat will have all of the access of the customer and insider threat, so defenses against these would help counter the high-level threat. In addition, the high-level threat may have access in ways different from those threats discussed earlier.

High assurance is defined as compelling evidence that the system or component delivers its services in a manner that satisfies certain critical properties, including the following:

- **Security**. The system prevents unauthorized disclosure, modification, and access to sensitive information, as well as any loss of service caused by an intentional act.
- **Safety**. Assurance that the system will operate within a specified environment without resulting in unacceptable risk.
- **Fault tolerance**. The system guarantees a certain quality of service despite faults such as hardware, workload, or environmental anomalies.

- **Timeliness**. The system delivers its outputs within a usable timeframe. Of the critical properties listed here, timeliness requirements are the most likely to conflict with security requirements: security mechanisms will tend to slow down a system, thus interfering with time requirements.

From technical point of view, security is based on the trust. What are trust issues for IoT?

- Can I trust that this code has not been tampered in any way by its developer or by someone else?
- Can I trust that the user of this code will employ it within its design envelope?
- Can I trust that the user of this code will not reverse engineer the code?
- Can I trust that this code will execute as designed?
- Can I trust that the execution of this code will not leak any information that should not be revealed?
- Can I trust that the execution of this code will not harm or disrupt other processing that is being executed in the same environment?
- Can I trust that the methods and assets by which the information was collected, processed, and otherwise transformed were executed in a way that preserved the integrity and accuracy of the information?
- At what point does the amount and integration of data or code effect a change in my integrity evaluation and trustworthiness assessments?

Embedded systems growing in complexity. Security is paramount since the controller does not change often security into these is an afterthought. Devices must be able to recover from unknown threats and sometimes they cannot reboot.

Perimeter is being extended. Traditional embedded systems are sitting outside your perimeter. How do to have cyber-resiliency beyond the perimeter.

Operationally, we need data from these devices. We cannot just reimage these devices. Somehow, we have to rely on this sensor. So, connectivity is needed to it – to read the data. Evolution of security is moving from traditional IT network/application world to embedded security world.

Examples of embedded security: Luxury car – 100 MLOC; 787 Boeing Dreamliner: 6.5M, UAV – Launch/Recovery and Mission Control. Remote users are very vulnerable to cyber-attacks.

Embedded systems security runs a close parallel to the mobile security domain, Android is 11MLOCs- significant increase in attacks.

8. Summary

IoT cybersecurity is a complex effort. The different architecture levels have different specifics, risks and threads. Therefore, different approaches have to be implemented to achieve desired security levels.

Today, IoT hugely penetrates in all areas of everyday life and cybersecurity of these systems is one of the biggest problems.

9. Acknowledgements

This paper is prepared with the support of MIRACle: Mechatronics, Innovation, Robotics, Automation, Clean technologies – Establishment and development of a Center for Competence in Mechatronics and Clean Technologies – Laboratory Intelligent Urban Environment, funded by the Operational Program Science and Education for smart growth 2014-2020, Project BG 05M2OP001-1.002-0011.

10. References

[1] Chetan, Sharma, Correcting the IoT History, 2022. URL: http://www.chetansharma.com/correcting-the-iot-history.

[2] Ajay, Sarangam, 7 IOT Layers That You Should Know in 2021, 2022. URL: https://www.jigsawacademy.com/4-layers-of-the-internet-of-things.