AN SAFETY INVOLVEMENTS IN IOT BASED APPLICATIONS FOR BUILDING AND FACTORY AUTOMATION

DR.SURESH NARASIMMAN[1]

FACULTY, AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

CH.SREEDHAR[1]

FACULTY, AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

M.NANDINI[2]

UG SCOLOR AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

S. RAKESH[2]

UG SCOLOR AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

Y. SHESHI PREETHAM[2]

UG SCOLOR AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

V. SAMPATH REDDY [2]

UG SCOLOR AVN INSTITUTE OF ENGINEERING AND TECHNOLOGY, HYDERABAD

OBJECTIVE

The adoption of Industry 4.0 conveys the connection of companies' assets to the Internet in order to acquire a huge amount of data that supports the creation of new services and applications that improve the efficiency and effectiveness of companies

PROBLEM STATEMENT

These paradigm rely on the adoption of Cyber Physical Systems (CPS) complemented with Internet of Things (IoT) technologies and artificial intelligence techniques. While CPS handles the control of the systems integrating both parts, hardware and software, in a networked environment of collaboration, IoT focuses on digitalize products and resources by means of placing small sensors connected to the Internet all along the system.

ABSTRACT-Industry 4.0 and Industrial Internet of Things (IIoT) are promoting the connection of millions of devices that once were seen as unconnectable, into a huge network, to be used in a large number of applications, from autonomous vehicles to industrial control systems, passing through building automation systems. These paradigm rely on the adoption of Cyber Physical Systems complemented with Internet of Things (IoT) technologies and artificial intelligence techniques. These type of systems are responsible for collecting, processing and exchanging a vast amount of data, and for that reason, it is imperative to assure data integrity and protection against malicious modifications and attacks to ensure a safe and reliable operation. Data thefts and cyber-attacks in general represent a significant danger, however, cyber-attacks on IoT systems can be specially critical due to their proximity with humans, enhancing the risk of physical damage. This paper highlights the importance of securing these systems, pursuing a safer operation, having in mind the amount of security vulnerabilities found in embedded devices. Building automation and factory automation, while seeking for solutions to improve these systems' security.

INTRODUCTION

The adoption of Industry 4.0 conveys the connection of companies' assets to the Internet in order to acquire a huge amount of data that supports the creation of new services and applications that improve the efficiency and effectiveness of companies. These paradigm rely on the adoption of Cyber Physical Systems (CPS)

complemented with Internet of Things (IoT) technologies and artificial intelligence techniques. While CPS handles the control of the systems integrating both parts, hardware and software, in a networked environment of collaboration, IoT focuses on digitalize products and resources by means of placing small sensors connected to the Internet all along the system. A great amount of communications takes place among distributed entities that exchange the huge collected data, which implies an imperative need to rely on cybersecurity requirements [1]. According to the McKinsey report [2], as the IoT grows, the possibility of threats also increases, and the cyber-risks, which in the past only affected the information technology (IT), now concerns to production systems and products, making that companies invest up to USD 500 million in cybersecurity. However, according to the data revealed by Cisco in its 2018 Annual Cybersecurity Report, this is not enough since 83% of the IoT devices are still vulnerable and 53% of all attacks resulted in damages of USD 500,000 or more [3]. Not only private companies are concerned about cybersecurity, e.g., the European Commission and the European Cyber Security Organisation (ECSO) are promoting the Horizon 2020 Cybersecurity cPPP Work Programme, where currently there are 5 open calls in cybersecurity topics [4], and the UK and German Governments published guidelines related to the topic [5]. When talking about security, it is compulsory to talk about the CIA triad: confidentiality, integrity and availability [6]. This triad is a model to design the security within an organization. It is necessary to control the access to the information (confidentiality), avoid the modification or destruction of the information (data integrity) and ensure timely access to the information (availability). These three requirements are the base of security, and can be applied to several application domains, e.g., manufacturing, logistics, building automation and smart electrical grids. Although the impact of IoT in those domains is very important, the security issues are not always one of the main concerns when implementing such solutions. In this work, the idea is primarily to analyze weaknesses in some IoT applications and try to show how we can mitigate these weaknesses by implementing simple mechanisms widely disseminate in the security literature. For this purpose, the paper considers two examples in different domains, one derived from building automation and another from factory automation, identifying several vulnerabilities and implementing some simple actions to prevent attacks that improve the security of the systems, preventing them for some of the most common attacks.

LITERATURE SURVEY:

S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008, vol. 5468, 2008, pp. 14–28. The Internet of Things is a term that has been around for several years. It was first introduced by the MIT Auto-ID Center, the precursor to the current EPCglobal organisation, and at that time stood for the vision of a world where all physical objects are tagged with an RFID transponder with a globally unique ID – the EPC or electronic product code. RFID easily allows tracking the objects, and the EPC serves as a link to data which can be queried over the Internet about each individual object. Since then, the meaning of the Internet of Things has expanded. Using sensors or sensor networks, additional information about the objects or the environment that they are in can be recorded as well. Software embedded in the objects enables data processing directly on the item, and in combination with actuators, local control loops can be implemented.

H. Lin and N. Bergmann, "Iot privacy and security challenges for smart home environments," Information, vol. 7, no. 3, p. 44, 2016. IoT security, the paper identifies key future requirements for trusted Smart Home systems. A gateway architecture is selected as the most appropriate for resource-constrained devices, and for high system availability. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automatic update of system

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015. Internet of Things (IoT) can support numerous applications and services in various domains, such as smart cities and smart homes. IoT smart objects interact with other components e.g., proxies, mobile devices, and data collectors, for management, data sharing and other activities in the context of the provided service. Sensors integrated at different places in homes, offices, and even in clothes, equipment, and utilities are used to sense and monitor owners positions, movements, required signs, valuable usage, temperature and humidity levels of rooms, etc. Along with sensing and monitoring capabilities, sensors

cooperate and communicate with themselves to deliver; share and process sensed information and help real-time decision making procedures through activate suitable alerts and actions. Often the Internet of Things (IoT) is considered as a single problem domain, with proposed solutions intended to be applied across a wide range of applications. However, the privacy and security needs of critical engineering infrastructure or sensitive commercial operations are very different to the needs of a domestic Smart Home environment. Due to internet- connected, dynamic and heterogeneous nature of smart home environment creates new security, authentication and privacy challenges.In this paper, we investigate security attacks in smart home and evaluate their impact on the overall system security. We identified security requirements and solutions in the smart home environment. Also, we have tried to provide solutions for few authentication issues.

Lin[8] explains key future requirements for trusted Smart Home systems. A gateway architecture is selected as the most appropriate for resource-constrained devices, and for high system availability. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automatic update of system software and firmware is needed to maintain on going secure system operation. Additionally, RFID (radio frequency identification) tags are seen as an IoT technology for making the location and, potentially, the status of tagged objects available on the Internet. He have explained the range of different application areas in which IoT technology is having an impact will be explored to show that IoT is not a one-size-fits-all technology set, and particular emphasis will be placed on IoT as applied to Smart Home applications. Later describes security threats and vulnerabilities in the Smart Home. He have prepared architecture supported by web-services for automatic device and network configuration and automatic system updates is our preferred approach for solving these problems. This paper presents particular challenges to security and privacy. The two main contributions of his paper are to summarize existing network techniques that can be used to secure Smart Homes, and then to present two areas of particular concern(system auto-configuration and security updates) where further work is needed

In paper[3], authors investigated security issues in the smart home environment using several scenarios. They investigated the security threats, classified these threats according to security objectives and evaluated their impact on the overall system. They identified security requirements and their solutions in the smart home environment. Based on several scenarios, they have set security goals for the smart home. Based on historical data, forecasted of security attacks (like malware, virus, etc.) that how many attacks are expected to be launched in coming five years. They describe open issues and future direction for researchers.

EXISTING SYSTEM:

In the existing work, the idea is primarily to analyse weaknesses in some IoT applications and try to show how can mitigate these weaknesses by implementing simple mechanisms widely disseminate in the security. For this purpose, delivered concepts in different domains, one derived from building automation and another from factory automation, identifying several vulnerabilities and implementing some simple actions to prevent attacks that improve the security of the systems, preventing them for some of the most common attacks.

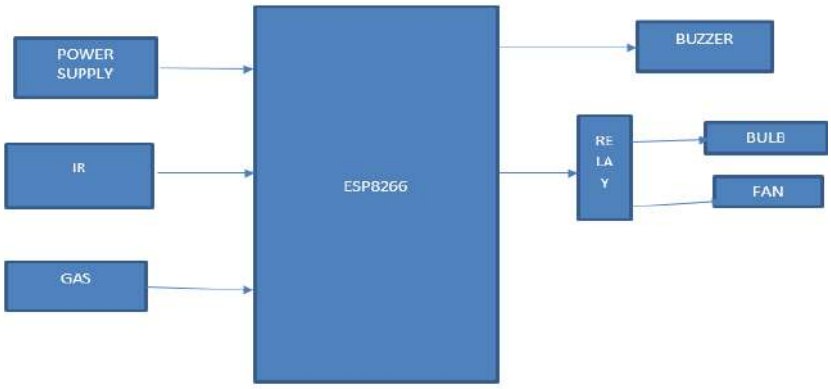
Drawbacks

- Consumes more time to find weakness
- Not efficient

PROPOSED SYSTEM:

The proposed Security in IoT based applications for Building and Factory Automation consists of embedded board which controls all the operations effectively with sensors interfaced with IOT. microcontroller which we are using to have an efficient security system in building and factories with IOT. The sensors used here are Infrared (IR) sensor which detects the obstacle, and gas sensor helps to identify the unusual gases. If any unusual happened then buzzer will make sound alert and concern persons will get message alert using GSM (Global System for Mobile Communication). The automation is done using IOT i.e. we can control any devices like motor, fan, and bulb etc. using IOT server.

IMPLEMENTATION



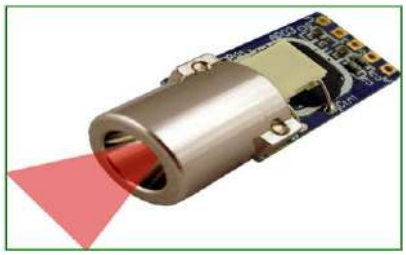
DESCRIPTION

ESP8266

The ESP8266 is a low-cost Wi-Fi microchip, with a full TCP/IP stack and microcontroller capability, produced by Espressif Systems[1] in Shanghai, China. The chip first came to the attention of Western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted.[2] The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, the chip, and the software on it, as well as to translate the Chinese documentation.[3] The ESP8285 is an ESP8266 with 1 MiB of built-in flash, allowing the building of single-chip devices capable of connecting to Wi-Fi.[4] The successors to these microcontroller chips is the ESP32 family of chips, including the pin-compatible ESP32-C3

IR SENSOR

An infrared sensor is an electronic device, that emits in order to sense some aspects of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. These types of sensors measure only infrared radiation, rather than emitting it that is called a passive IR sensor. Usually, in the infrared spectrum, all the objects radiate some form of thermal radiation. These types of radiations are invisible to our eyes, that can be detected by an infrared sensor. The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR photodiode that is sensitive to IR light of the same wavelength as that emitted by the IR LED. When IR light falls on the photodiode, the resistances and the output voltages will change in proportion to the magnitude of the IR light received.



MQ6 GAS SENSOR

The MQ-6 module is used in gas leakage detecting equipment in family and industry, This module has high sensitivity to LPG, iso-butane, propane and LNG. It can also be used to detect the presence of alcohol, cooking fumes, and cigarette smoke.The module gives out the concentration of the gases as a analog voltage equivalent to the concentration of the gases. The module also has an onboard comparator for comparing against an adjustable preset value and giving out a digital high or low.

BUZZERS

In common parlance a Buzzer is a signaling device that is not a loudspeaker. It can be mechanical, electromechanical, or electronic (a piezo transducer). BeStar produces Buzzers in every available configuration for a wide variety of applications. A Piezo transducer can produce the sound for panel mount buzzers, household goods, medical devices and even very loud sirens. When a lower frequency is required an electromagnetic buzzer can fill the need. These are very common in automotive chimes and higher end clinical diagnostic devices. The BeStar buzzer range includes self drive units with their own drive circuitry (indicators), or external drive units, which allow the designer the flexibility to create their own sound patterns.

CONCLUSIONS AND FUTURE WORK This paper discussed the importance of security on CPS and IoT devices, primarily aiming to ensure the system availability, data integrity and information confidentiality. Two case studies were considered, one related to building automation and another to factory automation, where the security issues are not usually addressed. The analysis of the test case systems allowed the identification of possible security threats that the systems are subjected to. In both cases, threats are mainly related to access to information exchanged, either sending data for remote system monitoring or between agents. Having identified the security weaknesses for both systems, simple solutions have been implemented to prevent or even eliminate potential security threats by implementing simple mechanisms widely disseminate in the security literature. Examples of such actions are keys and certificates for the MQTT broker and client, encrypted communication based on the TLS/SSL protocol, defense mechanisms, e.g., firewalls to prevent DoS or DDoS attacks, and also the JADE-S framework to encrypt data to increase security in communication between agents. Despite the fact that the attack scenarios described in this paper are relatively simple, the main objective of this work was to describe and evaluate the impact of the main vulnerabilities of building automation and factory automation solutions based on IoT technologies. Future work will be devoted to extend these basic attack scenarios to develop more complex scenarios, as well as consider more sophisticated defense mechanisms, such as the implementation of ML algorithms to detect patterns of agent interactions and attacks.

REFERENCES

[1] M. Lezzi, M. Lazoi, and A. Corallo, “Cybersecurity for industry 4.0 in the current literature: A reference framework,” Computers in Industry, vol. 103, pp. 97–110, 2018.
[2] T. Poppensieker, W. Richter, R. Riemenschnitter, and G. Scherf, “A new posture for cyberrisk in a networked world,” in Leading in a disruptive world. McKinsey&Company, 2018, ch. 3.
[3] Cisco, 2018 Annual Cybersecurity Report, 2018.
[4] ECSO, https://ecs-org.eu/cppp, accessed: 2019-07-26.
[5] D. Emm and V. Chebyshev, “Kaspersky security bulletin 2018. top security stories,” https://securelist.com/ kaspersky-security-bulletin-2018-top-security-stories/89118/, 2018.
[6] W. Stallings and L. Brown, Computer Security: Principles and Practice. Pearson, 2015.
[7] P. Leitão, A. Colombo, and S. Karnouskos, “Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges,” Computers in Industry, vol. 81, 09 2015.
[8] A. B. Chebudie, R. Minerva, and D. Rotondi, Towards a definition of the Internet of Things (IoT). IEEE, 2015.
[9] S. Haller, S. Karnouskos, and C. Schroth, “The Internet of Things in an Enterprise Context,” in Future Internet – FIS 2008, vol. 5468, 2008, pp. 14–28.
[10] H. Lin and N. Bergmann, “Iot privacy and security challenges for smart home environments,” Information, vol. 7, no. 3, p. 44, 2016.
[11] N. Naik, “Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP,” in IEEE International Systems Engineering Symposium (ISSE), 2017, pp. 1–7.
[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[13] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1–6.

