Cyber Security in IoT communication (Internet of Things) on Smart Home

Herman Heriadi¹, Geraldi Catur Pamuji²
¹, ²Magister of Information System, Faculty of Postgraduate, Universitas Komputer Indonesia, Indonesia.
Email: *herman.75119016@mahasiswa.unikom.ac.id

Abstract. The Internet of Things (IoT) that are currently applied with the combination of smart devices that connect with each other devices over the Internet from smartphone to other household devices that are assembled in a smart home-based concept. Smart Home is one of the concepts of implementing IoT technology, which is the implementation of Software Engineering. However, in document requirements in its engineering process development, often the requirements for cyber security aspect is neglected because it is considered as a secondary requirement. Therefore, it will be done analysis process requirements on the system by specializing in the cyber security aspect. In this paper, it will be analyzed about cyber security requirements of smart home IoT communication using methodology of Security Quality Requirements Engineering (SQUARE). The methodology of cyber security requirements analysis use SQUARE methodology consisting of 9 stages consist of agreement, identification, development, and analysis. The identification and analysis that has been done also has resulted in security requirement along with the implementation required for a secure smart home system. The analysis result consists of four types of requirements such as Elicit Security Requirement, Categorize Requirement, Prioritize Requirement, and Requirement Inspection. It is very helpful in analyzing while providing recommendations to the security requirements of the system which are used to keep the availability and continuity of the software as well as the integrity of the smart home systems that are being developed.

1. Introduction

IOT has gained an appeal lately as a term for describing connections between all digital devices such as smartphones, content TV, refrigerators, lamps, smartwatches, as well as various household appliances, as well as sensors and other devices that allow it to connect to the Internet with each other. The Internet of Things (IoT) is called a concept whereby an object has the ability to transfer data over a network without requiring human or human interaction to a computer. Since the concept of IoT is implemented, start popping up devices that are accompanied by a 'smart' or 'smart' name frills. For an IoT device can do its function, it takes an operating system, which is certainly small and simple to be able to perform the desired functions. Due to memory and power limitations, many of the standard functions are trimmed, one of which is security function. As a result, the security level of IoT devices is very minimal in connection to the host Ulo send data. This is
particularly vulnerable to attack, as it is usually the data transmitted in the form of plain text to conserve the bandwidth needs and resource needs of the IoT devices [1].

The first one is 6LoWPAN security. The Institute of Electrical and Electronics Engineers (IEEE) has defined the 802.15.4 standard for wireless personal area networks (WPANs). As such, 6LoWPAN [2] is a light-weight protocol designed by the IETF to allow IPv6 packets to be transferred over IEEE 802.15.4 wireless networks. EAKES6Lo is divided into two phases to improve the security of 6LoWPAN networks.

The second is RPL security. Routing protocols are a core component of conventional networks, and this also applies to 6LoWPAN networks. RPL [3] is an optimized IPv6 routing protocol designed by IETF especially for Low power and Lossy Networks (LLNs) and is primarily used by 6LoWPAN networks. RPL is a distance-vector routing protocol, and its mapping topology is based on a Destination-Oriented Directed Acyclic Graph (DODAG) structure. A generic topology authentication scheme called Trust Anchor Interconnection Loop (TRAIL) for RPL has been presented in [4].

The last is CoAP security. CoAP [5] is a HTTP-like application layer protocol designed for constrained device networks. As there are some special requirements such as group communications in IoT networks, CoAP provides multicast support which HTTP does not have. UDP is a simpler, low-latency and connection less transport layer protocol compared with its counterpart Transmission Control Protocol (TCP). The difference between the proposed methods and the previous methods are the previous method using the transport layer for the security needs of the information system which is challenging in security systems. [6] While the proposed method which is SQUARE Methodology provide the solution from the analysis of many aspect levels not only the transport layer protocol but also the database, hardware and also the Internet used for the solution analysis. [7]

2. Methods

The methodology used in this research is the SQUARE methodology consisting of 9 stages of the process to help analyze the security needs of information systems. The 9 stages of the SQUARE methodology are (Figure 1):

- Agree on Definition
- Identify Security Goals
- Develop Artefact
- Perform Risk Assessment
- Select Elicitation Technique
- Elicit Security Requirement
- Categorize Requirement
- Prioritize Requirement
- Requirement Inspection

Figure 1. SQUARE Methodology

System security implementation requirements as well as the overall technical solutions are then researched based on the level of priority misuse case, which will provide all necessary in the framework of implementation of core components.
The interconnected nature of the Internet means that Internet resources can be attacked from any location in the world, and this makes cybersecurity the main problem. Cybersecurity covers three important things [8].

1. **Confidentiality**, is about maintaining data privacy, so only authorized users (humans and machines) can access that data.
2. **Authentication**, is about verifying that the data has not been tampered with, and that the data is verified has been sent by the author claimed.
3. **Access**, referring to only allowing authorized users to access data, the community's communication infrastructure, and computing resources, and ensuring that legitimate users are not prevented from such the access.

Cybersecurity in the IoT itself is included in the software development section. Even when it is present, these ten requirements are developed independently of the rest of the engineering activities and are not integrated with the main activities of the engineering process. As a result, a safety requirement that is for intestinal to which provides protection of services and assets is often ignored [9].

According to Curtis Coleman, the high vulnerability to an entity that has a wide network is its application. Security is much focused on antivirus and security of the jar, but the very important part of data transactions is the application and the main data [10]. Many application developers ignore the importance of security analysis needs before doing software engineering to be irony in this rapidly growing era Bluetooth. Some types of attacks on the IoT system [11]. This Model can also be used to document and analyze the security aspects of the system in terms of repair or improvisation and in the future system modification [12] (Figure 2 and Table 1).

![Figure 2. Attack on IoT Devices](image-url)
Table 1. Description of Attack on IoT Devices

| Item | Description |
|------|-------------|
| Physical Attacks | This type of attack destroys hardware components and is relatively harder to do because it requires unusual and expensive materials such as demolition chip, reconstructs layout, micro-probing, and particle-beam technology. |
| Side Channel Attacks | These attacks are based on "side channel information" which can be taken from encryption devices that are not plain text to be encrypted or cipher text generated from the encryption process. Encryption devices deliver easy-to-measure time information, power consumption statistics, and much more. Side Channel Attacks utilize some or all this information to recover the keys that the device uses. It is based on the fact that logic operations have physical characteristics that rely on input data. Examples of side channel information are time attacks, power analysis attacks, interference analysis attacks, electromagnetic attacks, and environmental attacks. |
| Cryptanalysis Attacks | These attacks are focused on the cipher text and they try to crack the encryption, which is to find the encryption key to get the plaintext. Examples of cryptanalysis attacks include a Ciphertext-only attack, a Known-plaintext attack, a Hosen-plaintext C attack, a Man-in-the-middle, etc. |
| Software Attacks | Software attacks are the primary source of security vulnerabilities in the system. The software attack exploits the vulnerability of implementation in the system via its own Communication interface. Such attacks include exploiting buffer overflows and using Program Trojan horses, worms or viruses to intentionally inject malicious code into the system. |
| Network Attacks | Wireless communication systems are vulnerable to Network Attacks due to the broadcast nature of the transmission medium. Basically, the attack is classified as an active and passive attack. Examples of passive attacks include monitor and eavesdropping, traffic analysis, complain camouflage, etc. Examples of active attacks include denial of service attacks, subversion nodes, node corruption, node capture, Node removal, corruption of messages, false nodes, routing attacks, etc. |

3. Results and Discussion

In conducting security needs analysis using SQUARE methodology, there are 9 stages that begin with Agree on Definitions, Identify Security Goals, Develop Artefact, Perform Risk Assessment, Select Elicitation Technique, Elicit Security Requirement, Categorize requirement, EXIF requirement and the last stage of requirement Inspection [1].
Stage 1: Agree on Definitions

The definition of each term to be agreed between:

a. Antivirus,
b. Authentication,
c. DoS,
d. Encryption,
e. Cryptography,
f. The DMZ.

Stage 2: Identify Security Goals

The objectives are to ensure the full and continuity of all smart home secure system services.

Security objectives:

a. Control the system utilization pen configuration
b. The guaranteed confidentiality, accuracy and integrity of data and information
c. Guaranteed availability of all system Service

Stage 3: Develop Artefact

In this stage is focused on the architecture analysis of smart home system with system architecture as described in Figure 3 and topology as described in Figure 4.

![Figure 3. Smart Home System Architecture](image)

![Figure 4. Smart Home system Architecture Topology](image)
Stage 4: Perform Risk Assessment
In this stage, risk analysis is performed qualitatively. Asset Identification is shown in Table 2. Type Security Issue is shown in Table 3. Risk Description Identify is shown in Table 4. Qualitative Risk Analysis Matrix will be shown in Table 5. The colors in each cell in Table 5 show indicators of risk level calculated from likelihood and impact.

Table 2. Asset Identification

| Assets         | Description                              |
|----------------|------------------------------------------|
| System         | Database, Smart Home application         |
| Infrastructure | Sensors, microcontrollers, LANS, PC servers |
| Other          | Internet                                 |

Table 3. Type Security Issue

| Security Issue               | Description                                         |
|------------------------------|-----------------------------------------------------|
| Databases and Applications   | Theft, destruction, data manipulation, unauthorized access, DoS, spoofing, etc. |
| Hardware devices             | Theft, damage                                       |
| Internet                     | Theft, bandwidth restriction                        |

Table 4. Risk Description Identify

| Risk Description          | Mitigation                                      | Likelihood | Impact | Risk-Level |
|---------------------------|--------------------------------------------------|------------|--------|------------|
| Damage                    | Backing up                                      | LOW        | With   | LOW        |
| Theft                     | Backing up, Port Protection                     | LOW        | HIGH   | With       |
| Data manipulation         | Encryption                                      | LOW        | HIGH   | With       |
| Unauthorized access       | Identify user restricted session, 2-factor-authentiation | With       | With   | With       |
| DoS, Spoofing             | Port Protection                                 | With       | With   | With       |

Table 5. Qualitative Risk Analysis Matrix

| Likelihood | Impact | Low   | With   | High   |
|------------|--------|-------|--------|--------|
| High       |        |       |        |        |
| With       |        |       |        |        |
| Low        |        |       |        |        |

Stage 5: Select Elicitation Technique
At this stage is selected some of the elicitation techniques in conducting analysis of security needs for smart home system, direct-to-home observation techniques for obtaining more comprehensive
information and analyzing and providing recommendations on the form of mitigation and some literature studies.

Stage 6: Elicit Security Requirement

From the observation results, analysis with the mitigations and the study of the literature, the next step is to create a list of the requirements as shown in Table 6.

Table 6. List Requirements

| No | List Requirements                                                                 |
|----|----------------------------------------------------------------------------------|
| 1  | What to do to prevent spoofing, DoS, viruses, and malware attacks                 |
|    | = Application antivirus, firewall, dan DMZ                                        |
| 2  | What to do to prevent damage, theft and data manipulation                         |
|    | = Data encryption implementation, cryptography                                     |
| 3  | What to prevent unauthorized user access                                          |
|    | = Digital signature Implementation, password encryption, hash, double authentication|

Stage 7: Categorize Requirement

From the list of requirements in the previous step, system security can be categorized as shown in Table 7.

Table 7. Categorize Requirement

| Requirement    | System level       | Software level                          | Architectural constraint         |
|----------------|--------------------|----------------------------------------|----------------------------------|
| Essential      | Cryptographic      | Implementation of data encryption and  | Implementation of DMZ and        |
|                | implementations    | password, digital signature, hash      | Firewall and double authentication|
| Non-Essential  | -                  | Antivirus usage                       | -                                |

Stage 8: Prioritize Requirement

From the categorization in the previous stage, it can be compiled the need for priority to the security of remittance system as shown in Table 8.

Table 8. Prioritize Requirements

| Requirement                                | Priority |
|--------------------------------------------|----------|
| Using an antivirus                          | LOW      |
| Implementation of cryptography, digital     | LOW      |
| signatures, and data encryption             |          |
| Password encryption implementation          | With     |
| Double authentication                       | HIGH     |
| Implementation DMZ and firewall             | HIGH     |
Stage 9: Requirement Inspection

Creating a list of categories and provide comprehensive recommendations to the architecture and policy implementation requirements of remittance system security. All existing technical solutions researched based on the level of priority misuse case, which will provide all the necessary step-by-step security and technical in the framework of implementation of core components, as shown in Table 9.

**Table 9. Requirement Inspection**

| Category | Recommendation |
|----------|----------------|
| **Goal(s)** | Protecting Smart Home Network access and data from the attacks of other parties. |
| **Requirement** | The system must meet the conditions:  
  - The system should be able to protect itself  
  - The system must detect and counteract attacks that occur  
  - The system must use firewall technology  
  - The system must have good data encryption |
| **Category** | Access Control, Encryption, Auditing, Privacy, Authentication, Survivability, Unauthorized Access |
| **Implementation** | Features that have been implemented in the system:  
  - Using antivirus  
  - Cryptographic implementations, digital signatures, and data encryption  
  - Password Encryption implementation  
  - Double authentication  
  - Implementation DMZ dan firewall |

4. Conclusion

The methodology of cyber security needs analysis used is SQUARE methodology consisting of 9 stages, which are very helpful in analyzing while providing recommendations to the security needs of the system which aims to keep the availability and continuity as well as the integrity of the smart home system. From the identification and analysis done, generated 4 security requirement for IoT communication on Smart Home. In this paper, there are still many shortcomings, such as only one-time iterations of methodologies and identification of threats that can still be dug deeper. For further research, a deeper analysis is possible to further reduce the security requirement. Further studies can use more recent methodologies so that the security requirement produced is more specific and complete.

Acknowledgment

The author would like to Prof. Dr. Ir. Eddy Soeryanto Soegoto, MT as Rector of Universitas Komputer Indonesia (UNIKOM) and Mr. Dr Yeffry Handoko Putra, ST, MT. Not forgetting the authors also would like to thank the other parties who have assisted in the completion of this paper.
References

[1] Bertino, E., Choo, K. K. R., Georgakopolous, D., & Nepal, S. 2016. Internet of Things (IoT) Smart and Secure Service Delivery. ACM Transactions on Internet Technology.

[2] Shelby, Z., & Bormann, C. 2011. 6LoWPAN: The wireless embedded Internet 43. John Wiley & Sons.

[3] Winter, T., Thubert, P., Brandt, A., Hui, J. W., Kelsey, R., Levis, P., ... & Alexander, R. K. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. rfc, 6550, pp. 1-157.

[4] Perrey, H., Lansmann, M., Uges, O., Schmidt, T. C., & Wählisch, M. 2013. TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984.

[5] Shelby, Z., Hartke, K., & Bormann, C. 2014. The Constrained Application Protocol (CoAP) Internet Engineering Task Force; Fremont, CA. USA: RFC 7252.

[6] Lin, H., & Bergmann, N. W. 2016. IoT privacy and security challenges for smart home environments. Information, 7(3), pp. 44.

[7] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. 2014. IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.

[8] O’Neill, M. 2016. Insecurity by design: Today’s IoT device security problem. Engineering, 2(1), pp. 48-49.

[9] Mead, N. R. 2007. How to compare the Security Quality Requirements Engineering (SQUARE) method with other methods (No. CMU/SEI-2007-TN-021). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

[10] L. Zhang, A. Afanasyev, J. Burke, Claffy, L. Wang, V. Jacobsan, P. Crowle, C. Papadopoulus, B. Zhang, 2014. “Named Data Networking”, In ACM SIGCOMM Computer Communication Review.

[11] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. 2011. Proposed embedded security framework for internet of things (iot). In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) (pp. 1-5). IEEE.

[12] Coleman, D., C. 2001 “Case Study: An Evolution of Putting Security into SDLC”, p. 3.