INDIVIDUAL PROJECT GUIDELINE

Report format

|  |  |
| --- | --- |
| Class | CT201HM02 |
| Student ID | B2014926 |
| Student Name | Tran Dang Khoa |
| Student Email | [Khoab2014926@student.ctu.edu.vn](mailto:Khoab2014926@student.ctu.edu.vn) |
| Submitting Date | 12-12-2023 |

1. **Area name:** New trends
2. **Title:** Survey on vulnerability analysis on Internet of Thing
3. **Purpose of study**

The purpose of conducting a survey on vulnerability analysis in the Internet of Things (IoT) serves several critical objectives:

* **Identification of Threat Landscape:**

*Understanding Vulnerabilities:* Explore and identify the diverse range of vulnerabilities that exist within the IoT ecosystem. This involves scrutinizing potential weaknesses in both hardware and software components.

* **Risk Assessment:**

*Quantifying Risks*: Evaluate and quantify the potential risks associated with identified vulnerabilities. Assess the impact these vulnerabilities could have on the confidentiality, integrity, and availability of IoT devices and systems.

* **Security Improvement:**

*Informing Countermeasures:* Provide insights into effective countermeasures and security measures to mitigate vulnerabilities. By understanding the specific threats, researchers and practitioners can develop strategies to enhance the overall security posture of IoT environments.

* **Best Practices Development:**

*Establishing Guidelines:* Contribute to the establishment of best practices and guidelines for securing IoT devices and networks. This is crucial for manufacturers, developers, and users to adopt standardized security measures.

* **Awareness and Education:**

*Educating Stakeholders*: Raise awareness among IoT stakeholders, including developers, policymakers, and end-users, about the potential risks and vulnerabilities. Education is a key component of mitigating risks as informed individuals are more likely to take proactive security measures.

* **Policy Recommendations:**

*Influencing Policies:* Provide insights that can influence the development of regulatory frameworks and policies related to IoT security. Policymakers can benefit from a comprehensive understanding of vulnerabilities to create effective legislation.

* **Continuous Improvement:**

*Facilitating Research and Development:* Foster an environment of continuous improvement by encouraging further research and development in the field of IoT security. This ensures that as technology evolves, so do the strategies for identifying and mitigating vulnerabilities.

* **Adaptation to Emerging Threats:**

*Anticipating Future Threats:* Investigate current and potential future threats to anticipate and prepare for emerging risks. This allows for proactive measures instead of reactive responses to new vulnerabilities.

* **Building Trust:**

Enhancing Consumer Trust: Establishing a secure IoT environment is crucial for building trust among consumers. Confidence in the security of IoT devices is a key factor in widespread adoption and acceptance.

* **Contributing to the Body of Knowledge:**

*Advancing Research*: Contribute to the academic and industry knowledge base by adding new insights and perspectives on vulnerability analysis in the IoT. This is essential for the growth and maturity of the field.

1. **Includion**

**4.1 The Diversity and Scale of the Internet of Things (IoT)**

*4.1.1. Diversity in IoT Devices:*

* *Sensors and Sensors*: Devices that collect data from the environment such as temperature, humidity, light.
* *Connected Devices:* Smart connectors such as smart home devices, wearables, and medical devices.
* *Control devices:* Devices capable of controlling and performing actions, from smart devices to industrial automation devices.

*4.1.2. Scale of IoT Ecosystem:*

* *Global Sensor System (GSN):* Links sensors globally to collect and share data related to the environment, weather and climate.
* *Smart Sensor Network (WSN):* A system of interconnected sensor nodes to monitor and transmit data in real time.
* *Urban Information System:* (Smart City): The rationalization of a variety of devices and sensors to manage smart city information about traffic, security and energy management.

*4.1.3. Diverse Connection Protocols:*

*MQTT (Message Queue Telemetry Transport):* Streamlines the messaging protocol for resource-mode devices.

*CoAP (Constrained Application Protocol):* Protocol specifically designed for resource-mode IoT devices.

*HTTP/HTTPS:* Used in IoT applications with high security requirements such as transmitting medical data or personal information.

*4.1.4. Combination of IoT with Other Fields:*

* *IoT and Artificial Intelligence (AI):* The integration of IoT with AI solutions helps process and analyze data intelligently and automatically.
* *IoT and Blockchain:* Information safety and security are enhanced using blockchain technology.
* *IoT and Industry 4.0:* Smart industry with high automation and management based on data from IoT devices.

*4.1.5. Global Scale of IoT:*

* *Global Connectivity*: IoT devices have the ability to connect and transmit data across national and continental borders.
* *Large-Scale Applications:* The deployment of IoT in fields such as energy, healthcare, and smart cities on a global scale.
  1. **The Importance of Risk Analysis in the Diverse and Complex Environment of IoT**

*4.2.1. Understand the Diversity and Complexity of IoT:*

* Diverse Environment:
* *Device Diversity:* IoT includes many types of devices from sensors to control devices, with diverse features and functions.
* *Connectivity:* Devices can connect via multiple protocols, from Wi-Fi to Bluetooth and LoRa, creating complex network environments.
* Complexity of IoT Ecosystem:
* Connected Ecosystem: A large ecosystem of devices, networks, and services creates a complex environment.
* Data Diversity: Diversity of data from different sources such as sensors, measurement devices, and systems.

*4.2.2. Important Features:*

* Link Interaction:
* Device Linkage: Devices in IoT often link and interact with each other, creating complex networks.
* Data Fusion: Risk analysis needs to consider how devices and data connect to ensure comprehensive security.
* Calculating Limited Resources:
* *Any Device Can Be Sinkable:* Since devices often have limited resources, the implementation of security measures must be optimized to not be burdensome.
* *Prioritize Lightweight Security:* Security solutions should focus on minimizing impact on device performance and resources.
* *Complexity of Protocols and Connection Standards:*
* *Multiple Connection Protocols*: The variety of connection protocols creates challenges in maintaining compatibility and security.
* *Security Standardization:* Common security standards are needed to ensure consistency and comprehensive security.

4.2.3. Importance of Risk Analysis:

* Shaping the Security Strategy:

*Understand Risk*: Risk analysis helps identify and understand risks for each type of device and event scenario.

* Priority Decisions:

*Risk Prioritization*: Risk analysis helps identify risks that need to be prioritized based on their potential impact and impact.

* Building Flexible Security Measures:

*Adjust for Each Case*: Risk analysis is the basis for building flexible security measures, suitable for each special situation.

*4.2.4 Continuous Reflection and Continuous Improvement:*

Is not just a one-time process but a continuous cycle to face change and new threats. Continuous Process: Risk analysis

**5. IoT Infrastructure and Architecture**

**5.1 IoT System Architecture**

*5.1.1 IoT Devices:*

* *Sensors and Data Collection Devices:* These are basic components that collect data from the surrounding environment, such as temperature, humidity, light.
* *Connectivity Devices*: Includes devices with network connectivity such as sensors, actuators, wearables, and smart appliances.
* *Control Devices:* Devices capable of taking action based on collected data, such as smart home controllers and industrial automation devices.

*5.1.2 IoT Network:*

* Sensor Networks: Used to connect sensor devices in a certain area.
* Communication Networks: Links connected devices to each other and to the Internet, including protocols such as Wi-Fi, Bluetooth, Zigbee, and LoRa.
* Database Networks: Used to store and manage data from IoT devices.

*5.1.3 IoT Server:*

* Data Collection Server: Responsible for collecting, storing, and managing data from IoT devices.
* Data Processing Server: Performs intelligent data processing, using artificial intelligence or complex algorithms to extract useful information from collected data.
* Control Server: Manage and control IoT devices based on information from collected and processed data.

**5.2 Link Protocol**

*5.2.1 Common Protocols:*

*MQTT (Message Queuing Telemetry Transport):*

* Description: Lightweight messaging protocol for communication between devices, especially devices with limited resources.
* Security Challenges: Security concerns may be related to unencrypted communications and secure certificate management.
* CoAP (Constrained Application Protocol):
* Description: Protocol designed for IoT devices with limited resources, using lightweight UDP protocol.
* Security Challenges: Faced with the risks of using unreliable protocols, security measures such as DTLS (Datagram Transport Layer Security) are needed.

*HTTP/HTTPS:*

* Description: Standard communication protocol in IoT, especially when security is a priority.
* Security Challenge: There is a need to use HTTPS to secure data transmitted over the network, but can increase resource demands.

*5.2.2 Related Security Challenges:*

*Authentication and Key Management:*

* *Challenge*: Efficient and secure authentication management, especially for devices with limited resources.
* *Challenge*: Ensure that devices have software updates to protect against new security vulnerabilities.
* *Challenge:* Protect IoT networks from cyber attacks such as DDoS and man-in-the-middle attacks.

*Access Management:*

Challenge: Ensure that only authorized people can access and control IoT devices.

*5.2.3 Security Measures:*

Data encrypt:

* Security Measures: Use encryption to protect data transmitted over the network.
* Network Authentication:
* Security Measures: Set up a network authentication process to ensure that only authorized devices can join the network.
* Firewalls and Intrusion Detection Systems (IDS):
* Security Measures: Use firewalls and intrusion detection systems to prevent and detect network attacks.

1. **Security Risks in IoT:**

**6.1 Sources of Risk**

In the diverse and complex environment of IoT, the source of risk does not come from just one source but includes many aspects, from hardware to software and from device level to system level. Here are some important sources of risk:

*6.1.1 Hardware Risks*:

Device Security Vulnerabilities: IoT devices often have limited resources, leading to the possibility of security vulnerabilities, from courses to medical devices.

Poor Quality of Equipment: Cheap or poorly manufactured equipment can create a huge safety risk.

*6.1.2 Software Risks:*

Software Vulnerabilities: The complexity of the software that controls IoT devices can create vulnerabilities, allowing attackers to conduct remote attacks.

Poor Certificate Management: Ineffective certificate management can lead to the risk of intrusion and unauthorized use.

*6.1.3 Risks From Device Level to System Level:*

Risky Interoperability: Interoperating devices can create a risk chain, where a device-level vulnerability can propagate to the system level.

Connectivity: High levels of connectivity open up many gateways for attacks, especially in the absence of strict security measures.

**6.2 Specific Examples**

*6.2.1 DDoS Attack on IoT System:*

One of the typical examples is an overlay attack on an IoT system by sending a large number of requests from thousands of connected devices. This can overload the system, impairing or stopping important services.

*6.2.2 Personal Data Intrusion Through Connected Devices:*

IoT devices, like security cameras or smart lights, can become weak points if not properly protected. Hackers can penetrate the system and collect users' personal information through these devices.

*6.2.3 Risks from Connected Medical Devices:*

In the medical field, connected devices such as heart rate monitors or step counters can be hacked to change medical information, endangering users.

1. **Risk Analysis Method**

***7.1 Risk Analysis Process***

Risk analysis in an IoT environment requires a comprehensive process, covering steps from design to implementation. Below is the detailed process:

*7.1.1 Investigation Step:*

* Collect Information: Identify and collect information about relevant IoT devices, networks, and systems.
* Identify Potential Hazards: Investigate and identify potential hazards from the device to system level.

*7.1.2 Assessment Step:*

* Severity Assessment: Determine the severity of each identified risk to prioritize treatment.
* Determine the Level of Impact: Assess the potential impact of the risk on the overall operation of the system.

*7.1.3 Mitigation Step:*

* Building a Security Strategy: Develop a security strategy based on identified and assessed risks.
* Implement Preventive Measures: Implement preventative measures to reduce risk and increase security.

7.1.4 Monitoring and Adjusting Step:

Continuous Monitoring: Perform continuous monitoring of security status to detect any changes early.

Adjust as Needed: Customize your security strategy and deploy responses based on new information and changes in the environment.

***7.2 Tools and Techniques***

*7.2.1 Risk Analysis Tool:*

* *OWASP IoT Top 10*: Used to identify and prioritize common IoT risks.
* *Security Information and Event Management (SIEM):* Monitor and report on important security events.

*7.2.2 Risk Assessment Techniques:*

* Penetration Testing (Pen Testing): Simulate attacks to identify weaknesses and security vulnerabilities.
* Code Analysis: Check source code to detect security holes and potential risks.

*7.2.3 Response Techniques:*

* *Data Encryption*: Protects data transmitted over the network and at rest.
* *Authentication Management*: Authenticate and manage user and device access rights.

*7.2.4 Monitoring and Adjustment Technology:*

* *IDS/IPS System (Intrusion Detection/Prevention Systems*): Detect and prevent attacks.
* *Network Monitoring Tools*: Manage network traffic and detect unusual activity.

This approach provides a comprehensive approach to facing risk from design to deployment and maintaining security in the evolving IoT environment.

1. **Prioritize and Minimize Risk:**

***8.1 Prioritize Risk***

To manage risk in a diverse IoT environment, a risk prioritization process is extremely important. Here are some factors that determine risk prioritization in IoT environments:

*8.1.1 Importance of Data:*

* Data Type: Prioritize sensitive data types such as personal information, medical data, and critical business data.
* Data Flows: Identify data flows critical to system operations and prioritize their protection.

*8.1.2 Impact on System Operation:*

* Severity: Assesses the severity of the risk's impact on the overall system operation.
* Resilience: Identify resilience and prioritize risks that can cause long-term damage.

*8.1.3 Interactive Links:*

* Interrelationships: Evaluate how devices interact and communicate with each other to prioritize risks affecting the network.
* Chain of Risk: Identify the chain of risk that can spread from the device level to the system level.

***8.2 Risk Mitigation Strategy***

*8.2.1 IoT Device Security:*

* *Device Encryption:* Apply encryption to data on the device to prevent unauthorized access.
* *Authentication Management*: Use strong authentication measures to protect device access.

*8.2.2 Network Security and Protocols:*

* *Use Secure Protocols:* Prioritize the use of secure protocols such as HTTPS, MQTT with TLS to protect data transmitted over the network.
* *Network Management:* Set up network management measures such as firewalls to control traffic and prevent attacks.

*8.2.3 Prevention Strategies:*

* *Update Systems Regularly:* Ensure that all devices and software are regularly updated to address new security vulnerabilities.
* *User Education:* Enhance user education so they understand and implement basic security measures.

*8.2.4 Monitoring and Evaluation:*

* *Continuous Monitoring System:* Use a monitoring system to continuously monitor activities and detect any problems early.
* *Cycle Reviews:* Perform periodic cycle reviews to ensure that the security strategy remains relevant in a changing environment.

*8.2.5 Coordination with the Security Community:*

* *Sharing Security Information:* Participate in sharing security information with the community to learn and prevent from previous incidents.
* *Security Cooperation:* Cooperate with security organizations to create a common safe environment.

A risk mitigation strategy provides a comprehensive approach, from device protection to network management and prevention through user education. This helps build a robust and secure IoT system in increasingly complex environments.

1. **Outlook and Future**

***9.1 Current Status***

Assessing the current state of security in the IoT sector is important to understand the challenges and opportunities that currently exist.

*9.1.1 Progress Achieved:*

* *Improved Security Understanding:* Due to increased risk awareness, businesses and organizations are increasingly paying attention to security in the development and deployment of IoT solutions.
* *Community Attention:* The research and industry communities are paying attention to security in IoT, creating an environment for sharing information and solutions.

*9.1.2 Challenges Still Facing:*

* *Lack of Common Standards:* The lack of common standards is a challenge, reducing compatibility and effective risk management.
* *Increasing Attacks:* IoT attacks are increasingly complex and dangerous, posing a major challenge to current security systems.
* *Interconnect Risk Management:* With the increasing interconnectivity between devices, interconnect risk management becomes complex.

***9.2 Future Trends***

Looking to the future, there are important trends that could impact the field of security in IoT.

*9.2.1 Enhanced Standardization:*

* *Common Security Standards:* Developing and adopting common security standards for IoT will help improve compatibility and reduce risk.
* *Authentication and Identity Management:* Standardizing authentication and identity management methods will help increase security.

*9.2.2 Combination of Artificial Intelligence and Security:*

* *Use of Artificial Intelligence:* The incorporation of artificial intelligence in detecting and blocking attack patterns will enhance prevention capabilities.
* *Machine Learning-Based Security:* Security solutions that use machine learning to understand and respond to new attack patterns.

*9.2.3 Basic Security and Automated Device Management:*

* *Automated Device Management:* The development of automated device management will reduce pressure and risk from users.
* *Basic Device Security:* Increasing security at the device level will be an important trend.

*9.2.4 Cooperation and Information Sharing:*

* *Industry and Government Cooperation:* Close cooperation between industry and government will help to quickly respond and prevent attacks.
* *Sharing Security Information:* Sharing security information between organizations and businesses will help the whole community prevent better.

Future trends emphasize the importance of standardization, the integration of artificial intelligence, automated equipment management, and increased collaboration to improve the ability to prevent and respond to risks in the future. The IoT environment is evolving.

1. **Conclude:**

***10.1 Key Summary***

During the research and analysis of risks in the IoT field, many important findings and results have received special attention.

*10.1.1 Current Risk Situation:*

* The diversity and scale of IoT has been clearly defined, creating a complex environment with billions of connected devices.
* Risk analysis has shown diverse sources of risk from both hardware and software, as well as from the device level to the system level.

*10.1.2 Effective Security Strategies:*

* The risk analysis process from investigation, assessment, response, to monitoring and regulation has been designed to cope with the complexity of the IoT environment.
* Tools and techniques such as penetration testing and data encryption have been proposed and used to effectively mitigate risks.

*10.1.3 Specific Examples of Risks:*

Examples of specific risks such as DDoS attacks and intrusions into personal data highlight real concerns and risks in IoT environments.

***10.2 Importance of IoT Security***

*10.2.1 Protecting User Privacy and Security:*

* IoT security is not just a business issue, but is also closely related to user privacy and personal safety.
* Improving security is about protecting not only data but also the health and safety of users.

*10.2.2 Maintaining Industry Reputation and Trust:*

* Building and maintaining the reputation of the IoT industry requires adequate investment in security.
* Consumer trust in IoT products and services depends largely on how secure they are.

*10.2.3 Shaping Industrial Development Trends*:

* IoT security is not just a technical aspect, but also shapes the overall trends and developments of the industry.
* The popularity and success of IoT depends heavily on the ability to ensure security and protection of information.

In an increasingly connected and complex environment like the IoT, improving security is not just a technical task but also a commitment to privacy and safety. The findings from this research and risk analysis provide a solid basis for building an effective security strategy and help shape a secure and trusted IoT future.

1. **Reference**

[**https://dl.acm.org/doi/10.1007/978-3-031-23020-2\_15**](https://dl.acm.org/doi/10.1007/978-3-031-23020-2_15)

[**https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9571254/**](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9571254/)