Security Evaluation of Consumer IoT Devices

Joshua Bartels, Tyler Hinrichs, Lucas Reichlinger, Logan Stranglen
University of Nebraska at Omaha

Abstract
The growing popularity of IoT devices offers consumers convenience and automation. But, at the same time, it introduces security risks that many users overlook. Our research examines smart home devices such as cameras, appliances, home automation, and entertainment systems that are vulnerable due to weak security protocols, poor update policies, and unchanged default settings. These vulnerabilities expose users to data breaches, personal data theft, and unauthorized access. Our research project develops a security-focused IoT buying guide to help consumers make informed decisions by identifying high-risk device categories, analyzing vulnerabilities like default credentials and unencrypted data, evaluating manufacturer security practices, and providing best practices for secure device management. We systematically analyzed security reports, documented vulnerabilities, disclosures, and manufacturer updates & policies to assess security weaknesses and transparency in consumer protection. Our findings highlight the need for stronger consumer awareness and proactive security measures, encouraging industry improvements in IoT security while helping users mitigate risks and protect their privacy.

Contents

1. Introduction
2. Literature Review & Research Context
3. Defining Risk Criteria
    - 3.1 Goals of Criteria
    - 3.2 Categories
    - 3.3 Criteria
4. Evaluation of IoT Security Practices
    - 4.1 Manufacturer security policies
    - 4.2 Common Security Weaknesses
    - 4.3 Case Studies
5. Rubric Score and Findings
6. Recommendations and Best Practices
7. Conclusion

---

1 Introduction

1.1 Overview of IoT devices and their growing adoption in households.

1.2 Risks associated with always-online connectivity, including data breaches and unauthorized access.

1.3 Lack of consumer awareness regarding security risks and manufacturer practices.

1.4 Objectives of this study:

- Identify security risks in IoT devices.
- Evaluate vulnerabilities and manufacturer security policies.
- Provide a consumer-oriented security rubric and best practices guide

1.5 Research Questions

- Which categories of IoT devices pose the highest security risks in home environments, and how do these vulnerabilities impact consumer privacy and safety?

- What are the most common security flaws in always-online IoT devices, and how do manufacturer security practices—such as update policies and default configurations—affect overall device security?

- What best practices can help consumers make informed purchasing decisions and securely manage IoT devices to reduce cybersecurity risks?

---

2 Literature Review

2.1 Review of existing research on IoT security vulnerabilities.

2.2 Analysis of documented breaches and cybersecurity incidents involving IoT devices.

2.3 Discussion of regulatory standards (e.g., UL Solutions, CCPA) and industry best practices.

2.4 Overview of consumer knowledge gaps in IoT security.

---

3 Defining Risk Criteria

3.1 Goals of Criteria

- Establish an objective framework for evaluating IoT device security.
- Help consumers assess risks before purchasing.
- Encourage manufacturers to adopt stronger security policies.

3.2 Categories

- Device Connectivity Requirements (Does it need constant internet access?)
- Data Handling and Storage Risks (What data is collected, and how is it stored?)
- Manufacturer Security Policies (How often are updates released? Are vulnerabilities disclosed?)
- Authentication and Access Controls (Are default credentials enforced? Multi-factor authentication available?)
- Compliance with Security Standards (Does the device meet GDPR, HIPAA, or similar security guidelines?)

3.3 Criteria

- Default security settings (Are they secure out of the box?)
- Encryption and data transmission security.
- Firmware update frequency and patching response time.
- Transparency in vulnerability disclosure.
- User access and authentication mechanisms.

---

4 Evaluation of IoT Security Practices

4.1 Manufacturer Security Policies

- Review of update policies and security patch frequency.
- Assessment of transparency in vulnerability reporting and public disclosures.
- Evaluation of bug bounty programs and consumer security guidance.

4.2 Common Security Weaknesses

- Use of default credentials and lack of forced password changes.
- Unencrypted data transmission and insecure communication protocols.
- Weak access control mechanisms.
- Cloud dependencies and privacy risks associated with data storage.

4.3 Case Studies

- Analysis of real-world IoT security incidents.
- Examination of manufacturer responses to vulnerabilities.
- Comparative study of high-risk vs. lower-risk IoT devices based on security features.

---

5 Rubric Score and Findings

5.1 Score Matrix for IoT Devices

Category	Score	Reasoning/Sources
Requires Constant Internet Connection	Yes	Reasoning
Requires Constant Connection to Company Cloud Infrastructure	No	Reasoning
Data Storage Risk Score	Hybrid	Reasoning
Data Gathering Risk Score	3	Reasoning
Company Vulnerability Remediation Score	2	Reasoning
Company Vulnerability Transparency Score	4	Reasoning

5.2 Summarized evaluation of IoT device security performance.

5.3 Comparison of security risks across different device categories.

5.4 Identification of trends in manufacturer security practices.

---

6 Recommendations and Best Practices

For Consumers

- How to select secure IoT devices.
- Best practices for configuring and managing device security.
- Importance of firmware updates and changing default settings.

For Manufacturers

- Enhancing default security settings
- Improving transparency in vulnerability reporting
- Encouraging adoption of standardized security frameworks

---

7 Conclusion

- Summary of key findings
- Emphasis on the importance of consumer awareness and industry accountability