On the Contents and Utility of IoT Cybersecurity Guidelines (Appendix)

JESSE CHEN, University of Arizona, USA
DHARUN ANANDAYUVARAJ, Purdue University, USA
JAMES C. DAVIS, Purdue University, USA
SAZZADUR RAHAMAN, University of Arizona, USA

Cybersecurity concerns of Internet of Things (IoT) devices and infrastructure are growing each year. In response, organizations worldwide have published IoT security guidelines to protect their citizens and customers by providing recommendations on the development and operation of IoT systems. While these guidelines are being adopted, *e.g.* by US federal contractors, their content and merits have not been critically examined. Specifically, we do not know what topics and recommendations they cover and their effectiveness at preventing real-world IoT failures.

In this paper, we address these gaps through a qualitative study of guidelines. We collect 142 IoT cybersecurity guidelines and sample them for recommendations until reaching saturation at 25 guidelines. From the resulting 958 unique recommendations, we iteratively develop a hierarchical taxonomy following grounded theory coding principles and study the guidelines' comprehensiveness. In addition, we evaluate the actionability and specificity of each recommendation and match recommendations to CVEs and security failures in the news they can prevent. We report that: (1) Each guideline has gaps in its topic coverage and comprehensiveness; (2) 87.2% recommendations are actionable and 38.7% recommendations can prevent specific threats; and (3) although the union of the guidelines mitigates all 17 of the failures from our news stories corpus, 21% of the CVEs evade the guidelines. In summary, we report shortcomings in each guideline's depth and breadth, but as a whole they address major security issues.

CCS Concepts: • **General and reference** → **Empirical studies**; • **Security and privacy** → **Software security engineering**; **Security requirements**.

Additional Key Words and Phrases: IoT security, security guidelines, security recommendations, security best practices, security advice, taxonomy

ACM Reference Format:
Jesse Chen, Dharun Anandayuvaraj, James C. Davis, and Sazzadur Rahaman. 2024. On the Contents and Utility of IoT Cybersecurity Guidelines (Appendix). *Proc. ACM Softw. Eng.* 1, FSE, Article 63 (July 2024), 7 pages. https://doi.org/10.1145/3660770

Authors' addresses: Jesse Chen, University of Arizona, Tucson, USA, jessechen@arizona.edu; Dharun Anandayuvaraj, Purdue University, West Lafayette, USA, dananday@purdue.edu; James C. Davis, Purdue University, West Lafayette, USA, davisjam@purdue.edu; Sazzadur Rahaman, University of Arizona, Tucson, USA, sazz@cs.arizona.edu.

ACM 2994-970X/2024/7-ART63
https://doi.org/10.1145/3660770

A GENERAL

The list of guidelines we studied in our stratified sample and extracted recommendations are both listed in "iot_taxonomy.xlsx".

B RECOMMENDATIONS

Figure 2 shows an example path up to level 8 by recursively choosing the child category with the most recommendations. Figure 1 shows the ConSim histogram of our Taxonomy validation.

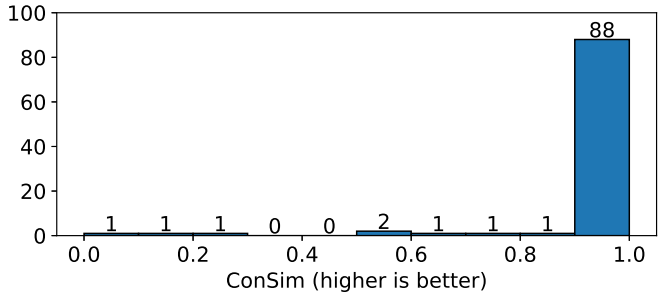

Fig. 1. Mismatch analysis based on conceptual similarity. All 88 in the rightmost bucket have a perfect match.

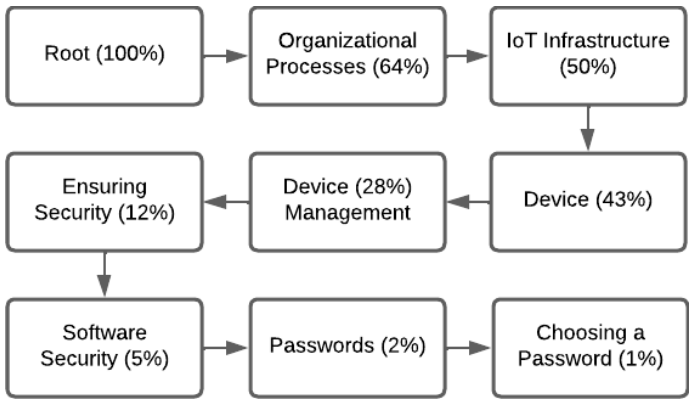

Fig. 2. Path by choosing the child category with the most recommendations. Each category includes the percentage of all recommendations that all of their child categories contain. Recommendations come under *Choosing a Password*, which is a leaf category.

Table 1 gives the top 10 recommendations by frequency across guidelines.

Table 1. Top 10 recommendations by guideline reference counts.

No.	Count	Recommendation
1	11	Encrypt data in transit.
2	9	Device firmware/software should only be modifiable with the proper digital signature.
3	8	Anti-tampering capabilities: Devices should have a mechanism to prevent tampering by unauthorized sources.
4	7	Strong cryptography to protect data at rest
5	7	Default accounts and passwords should be changed.
6	6	Keep software updated
7	6	Communicate securely
8	6	Validate input data
9	6	Device should operate on the principle of least privilege.
10	6	Physical security also needs to be put in place.

C STUDENT STUDY SURVEY

Each student reviewed 15 recommendations. For each recommendation, they answered the following 5 questions:

Question 1: Did you fully understand the recommendation?
(a) Yes.
(b) No.

Question 2a: Do you think the recommendation can prevent a specific security issue (e.g. threat, vulnerability, or attack-surface) if executed correctly?
(a) Yes.
(b) No.

Question 2b: How confident are you about your answer to the previous question?
(a) Very confident.
(b) Somewhat confident.
(c) Not confident.

Question 3a: Do you think the recommendation is concrete enough to be actionable? Recall that recommendations are "actionable" if you know what action to take after reading it (knowing how to do it is a different story).
(a) Yes.
(b) No.

Question 3b: How confident are you about your answer to the previous question?
(a) Very confident.
(b) Somewhat confident.
(c) Not confident.

D CONTRADICTIONS

Contradictions are noted in Table 2.

Table 2. Contradicting recommendation pairs.

No.	Recommendation 1	Recommendation 2
1	Avoid words or phrases that include personal details in passwords. (363) [2]	Use a phrase that is long and personal for passwords that most people don't know about you. E.g. IHateBrownSnails. (368) [2]
2	Use different administrator users and passwords and grant granular permissions. (126) [3]	Forbid the deployment of back doors or admin accounts as part of released products. (1078) [5]
3	[Devices should] limit admin capabilities to a local interface only. (851) [4]	Forbid the deployment of back doors or admin accounts as part of released products. (1078) [5]

E CVES

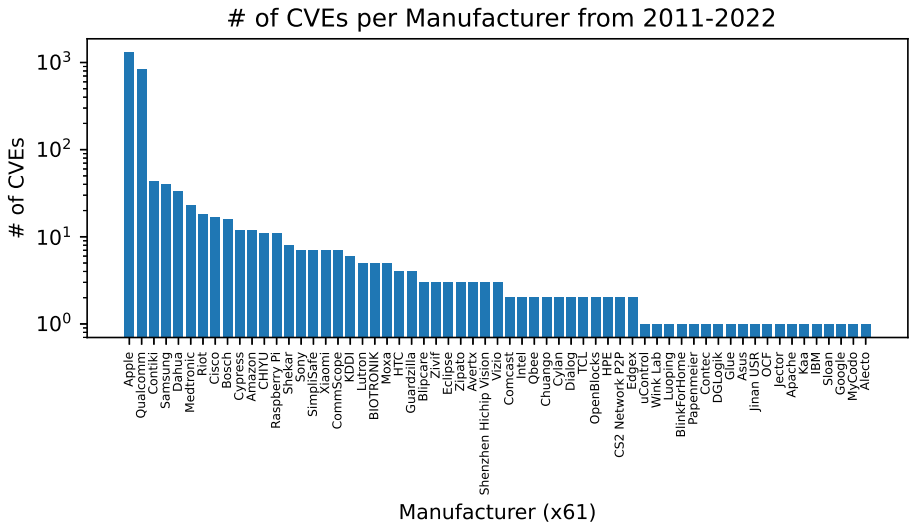

Fig. 3. IoT-related CVEs were identified through our multi-stage CVE database search. The vast majority of these are from Apple's iOS-based OSes like WatchOS and tvOS (1307 Apple CVEs), and Qualcomm's SnapDragon product line (830 Qualcomm CVEs). When applying our taxonomy to CVEs, we used stratified sampling by the company to avoid bias by failure modes specific to a particular company.

CVE summary by CVSS and coverage. Figure 4 shows the distribution of CVEs by CVSS score, also noting the proportion of CVEs that had associated recommendations.

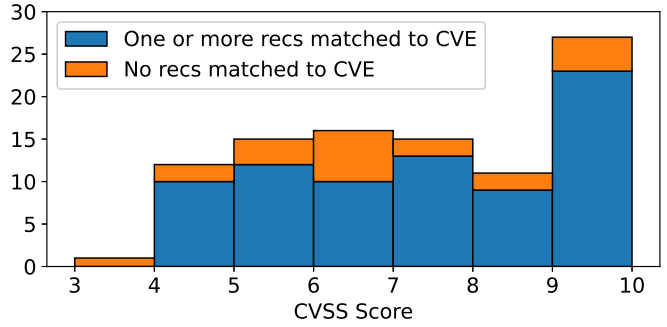

Fig. 4. Number of CVEs with a certain CVSS score. The mean CVSS score for CVEs with one or more specific-recommendations matched to it is 7.5/10 and the mean CVSS score for CVEs with no matches is 7.0/10, both of which are equivalent to a qualitative rating of high severity [1].

F TAXONOMY VISUALIZATION TOOL

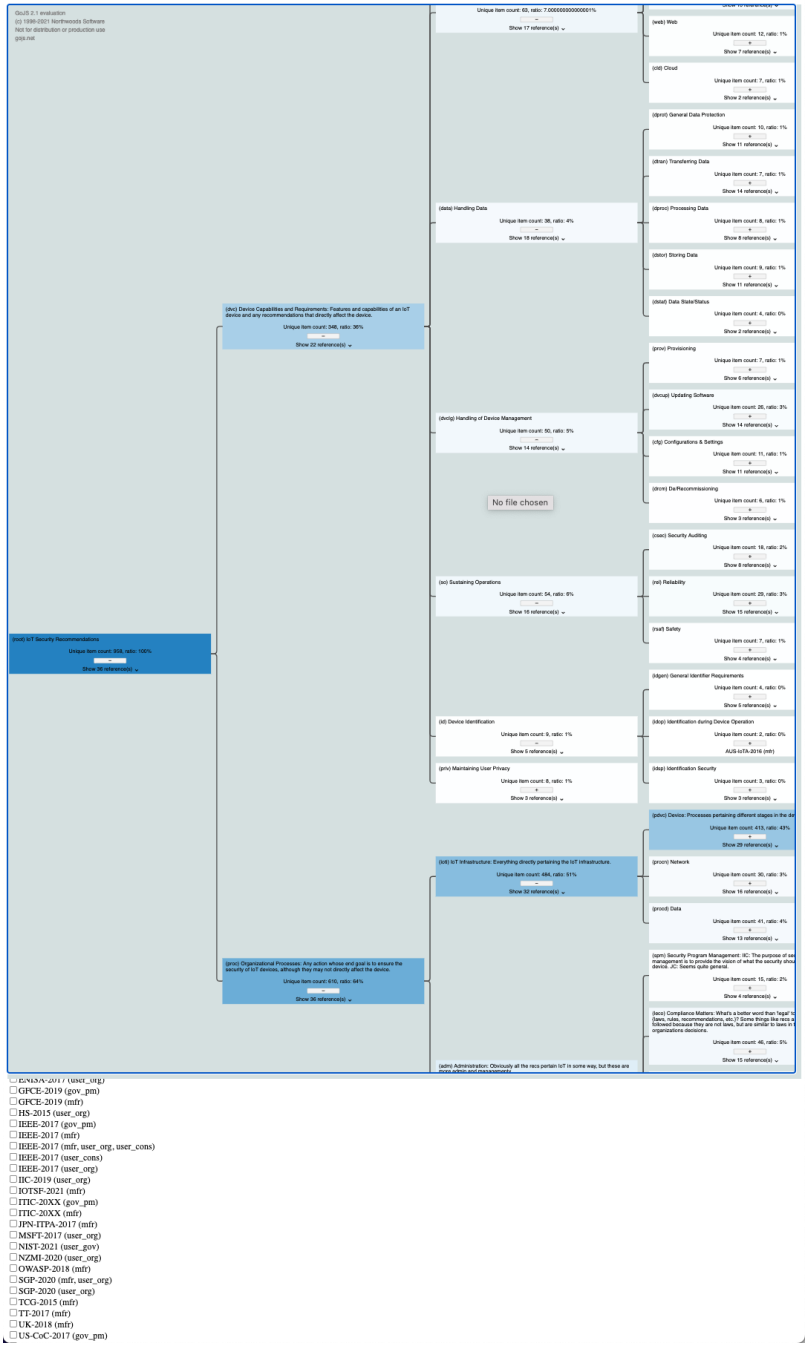

Fig. 5. Screenshot of data visualization tool with categories expanded to level 3. Working on code release for exploration.

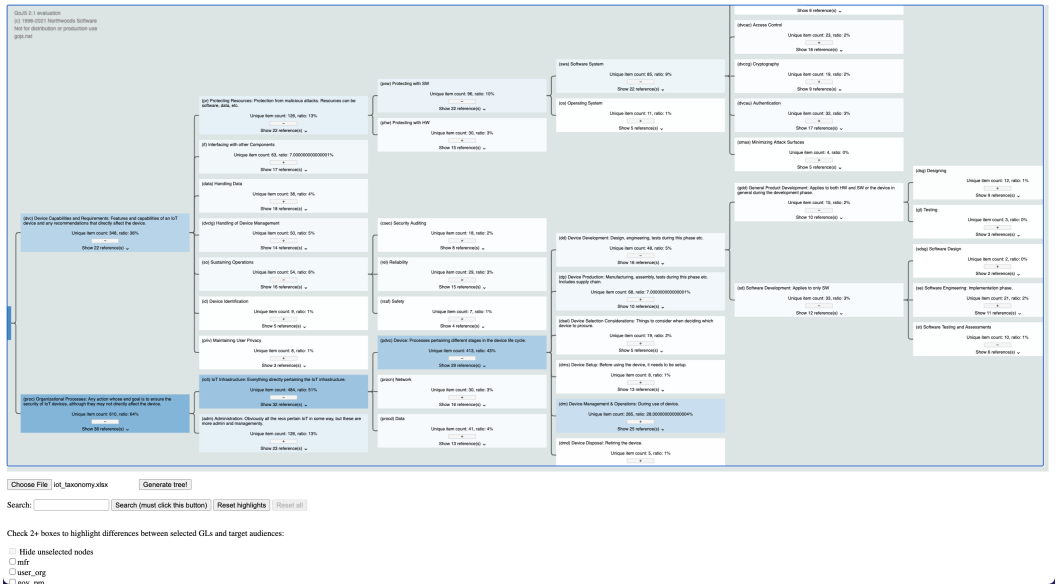

Fig. 6. Screenshot of data visualization tool with randomly chosen categories expanded. Working on code release for exploration.

REFERENCES

[1] [n. d.]. CVSS v3.1 Specification Document. https://www.first.org/cvss/specification-document. Accessed: 2023.
[2] BullGuard. 20XX. Consumer Guide to the Internet of Things. Accessed: 2022.
[3] Cloud Security Alliance et al. 2016. Cyber Security Guidelines for Smart City Technology Adoption. Accessed: 2022.
[4] IoT Alliance Australia. 2016. Internet of Things Security Guideline. Accessed: 2022.
[5] Trusted Computing Group. 2015. Guidance for Securing IoT Using TCG Technology. Accessed: 2022.

Received 2023-09-28; accepted 2024-04-16