Supplemental Material

ANONYMOUS AUTHOR(S)

A Guidelines

The list of guidelines we studied in our stratified sample is given in Table 1.

Table 1. Table of guidelines reviewed.

No.	Code Name	Citation	No.	Code Name	Citation
1	AMZN-20XX	[18]	14	JPN-ITPA-2017	[32]
2	AUS-IoTA-2016	[30]	15	MSFT-2017	[33]
3	BG-20XX	[19]	16	NIST-2021	[34]
4	CIS-2015	[20]	17	NZMI-2020	[35]
5	CSA-2016	[22]	18	OWASP-2018	[36]
6	CSA-2017	[21]	19	SGP-2020	[37]
7	ENISA-2017	[24]	20	TCG-2015	[39]
8	GFCE-2019	[25]	21	TT-2017	[38]
9	HS-2015	[26]	22	UK-2018	[40]
10	IEEE-2017	[29]	23	US-CoC-2017	[41]
11	IIC-2019	[27]	24	US-DOJ-2017	[23]
12	IOTSF-2021	[31]	25	WRS-2016	[42]
13	ITIC-20XX	[28]	-	-	-

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.

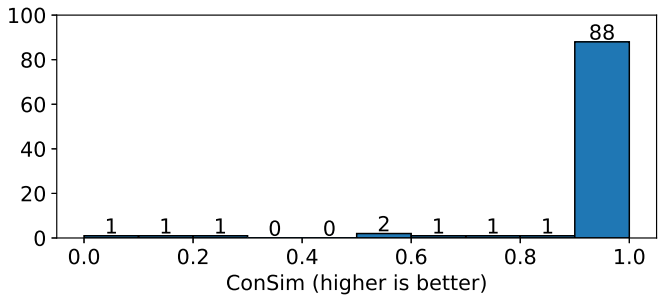

Fig. 1. Mismatch analysis based on conceptual similarity. All 88 in the rightmost bucket have a perfect match.

Table 2 gives the top 10 recommendations by frequency across guidelines.

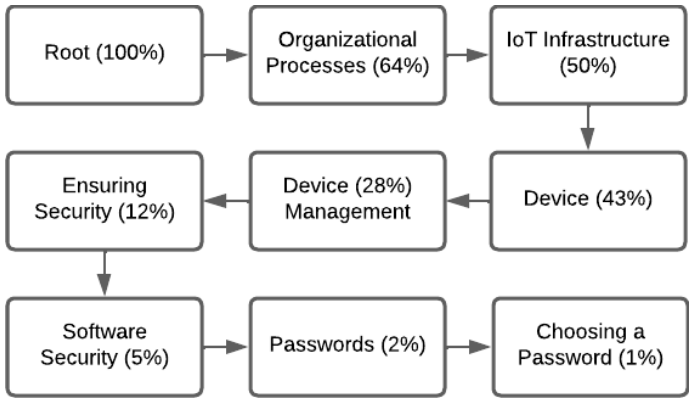

Fig. 2. Path by choosing the child category with the most recommendations. Each category includes the percentage of all recommendations that all of their child categories contain. Recommendations come under *Choosing a Password*, which is a leaf category.

Table 2. 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 News Stories

The list of news storied analyzed is in Table 3.

Table 3. Table of news stories analyzed.

No.	Code Name	Citation	No.	Code Name	Citation
1	'Dangerous Stuff': Hackers Tried To Poison Water Supply of Florida Town	[15]	10	The Myth of the Hacker-Proof Voting Machine	[9]
2	Pipeline Attack Yields Urgent Lessons About US Cybersecurity	[16]	11	Hackers Could Use Smart Displays to Spy on Meetings	[12]
3	Security News This Week: Hackers Found a Freaky New Way to Kill Your Car	[13]	12	Watch a Drone Take Over a Nearby Smart TV	[14]
4	Decades-Old Code Is Putting Millions of Critical Devices at Risk	[11]	13	A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever	[1]
5	An Easy Way for Hackers to Remotely Burn Industrial Motors	[7]	14	An Easy Way for Hackers to Remotely Burn Industrial Motors	[4]
6	Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid	[5]	15	Watch a Hacker Hijack a Capsule Hotel's Lights, Fans, and Beds	[17]
7	Hackers Remotely Kill a Jeep on a Highway	[3]	16	Xfinity's Security System Flaws Open Homes to Thieves	[6]
8	Hackers Cut a Corvette's Brakes Via a Common Car Gadget	[2]	17	Hacker Warns Radioactivity Sensors Can Be Spoofed Or Disabled	[8]
9	Strava Fitness App Can Reveal Military Sites, Analysts Say	[10]	-	-	-

D 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.

E Contradictions

Contradictions are noted in Table 4.

Table 4. Contradicting recommendation pairs.

No.	Recommendation 1	Recommendation 2
1	Avoid words or phrases that include personal details in passwords. (363) [19]	Use a phrase that is long and personal for passwords that most people don't know about you. E.g. IHateBrownSnails. (368) [19]
2	Use different administrator users and passwords and grant granular permissions. (126) [22]	Forbid the deployment of back doors or admin accounts as part of released products. (1078) [39]
3	[Devices should] limit admin capabilities to a local interface only. (851) [30]	Forbid the deployment of back doors or admin accounts as part of released products. (1078) [39]

F CVE and News Story Collection Methods

F.1 CVE Dataset Construction Methodology

The goal of CVE analysis is to study if specific CVEs could have been prevented by following the recommendations in our taxonomy. Incidental vulnerabilities for which no prevention assurance can be achieved (e.g., buffer overflows) are irrelevant to this analysis. Thus, to sort CVEs, we define the following two categories of CVEs:

- **Design flaw:** We define a design issue vulnerability as any missing security features by design for which the implementor made a conscious decision. Following is an example of a design issue CVE: *An issue was discovered in AvertX Autofocus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 ... They do not require users to change the default password for the admin account* [**?**].
- **Implementation issue:** These issues are mostly incidental – for which the implementor did not make a conscious decision during the development (*i.e.* implementation) of the product. An example implementation issue CVE: *IBM Watson IoT Message Gateway 2.0.0.x, 5.0.0.0, 5.0.0.1, and 5.0.0.2 is vulnerable to a buffer overflow, caused by improper bounds checking when ...* [**?**].

CVE Collection. CVE analysis requires a set of IoT-related CVEs, which in turn requires a set of IoT-related keywords to search for them [1]. To gather the set of keywords, we collected survey papers published from 2017-2022 in the journals: (1) *IoT Journal*, (2) *ACM Computing Surveys*, (3) *Transactions on Software Engineering*, and (4) *Transactions on Dependable and Secure Computing*. We included any paper whose title matched "survey", "security|privacy" and "IoT|internet of things", resulting in 4 papers. We read through the 4 matching survey papers and extracted any terms related to (1) IoT vulnerabilities, (2) IoT devices or products, and (3) IoT software packages and libraries, which resulted in a collection of 36 keywords. Using these 36 keywords, we searched the CVE database for CVEs from 2011-2022 that match $\geq$ 1 keyword in their description. We then extracted the names of IoT-related companies from these CVEs and determine the names of their IoT-related products with CVEs. Finally, we use pairs of company names plus product lines

[1] A trial run using keywords from IoT literature review papers did not yield a rich corpus of IoT CVEs.

to serve as the keywords to search the CVE database, filtering out CVEs for non-IoT products produced by each company. This ensures that our final list of CVEs has wide coverage while only containing IoT-related CVEs. The resulting list contained 2500 CVEs from 61 companies. However, the distribution of CVEs is heavily skewed by large vendors like Apple and Qualcomm, as seen in Figure 3. Therefore, we used stratified random sampling, where each stratum is a company, to randomly choose up to 4 CVEs per company. Our final list contained 158 IoT CVEs.

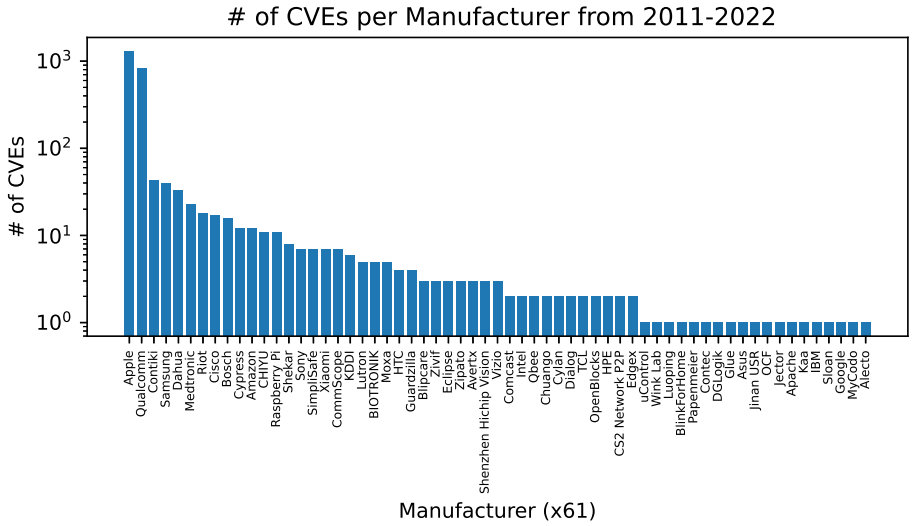

Fig. 3. IoT-related CVEs were identified through our multi-stage CVE database search. The vast majority of these are from Apple's iOS-based OSes like WatchOS and tvOS (1307 Apple CVEs), and Qualcomm's SnapDragon product line (830 Qualcomm CVEs). When applying our taxonomy to CVEs, we used stratified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

CVE Preparation. First, we categorize the CVEs into design and implementation issues as defined earlier, which resulted in 103 design issue CVEs. For better generalization, we also categorized the CVEs into the following seven application domains, expanding the categories from [**?**] based on our observations: (1) Consumer product, (2) Commercial product, (3) Industrial product, (4) Medical product, (5) Automotive product, (6) Critical infrastructure, and (7) SW/HW component. These categorizations were done by one author and validated by an independent author.

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.

F.2 News Dataset Construction Methodology

News collection. Following the methods of an IoT failure study [**?**], we compiled IoT security failures reported by reputable news sources: *WIRED* and *The New York Times*. In order to maintain reproducibility, we used Google News to search both sources. We used a condensed list of search terms from phrases used for the CVE search. [2] Specifically, we conducted a pilot search to eliminate

[2]Search Terms: "iot, cyber-physical system, cyber security fail, autonomous, smart, Fitbit, embedded device, robot, wearable, industrial control, router, sensors".

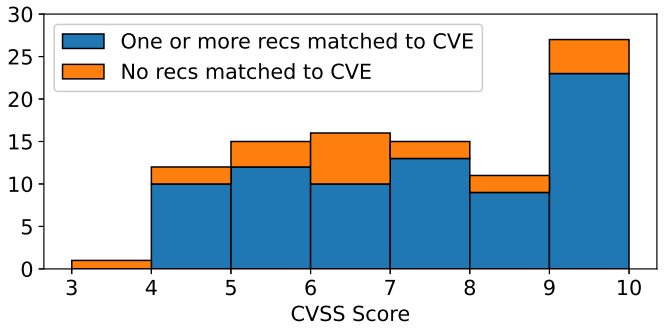

Fig. 4. Number of CVEs with a certain CVSS score. The mean CVSS score for CVEs with one or more specific-recommendations matched to it is 7.5/10 and the mean CVSS score for CVEs with no matches is 7.0/10, both of which are equivalent to a qualitative rating of high severity [?].

phrases that did not yield results, and condensed common terms across multiple phrases. We also added general terms such as, "autonomous", "cyber-physical system", and "cyber security fail" to collect a wider set of news data. We used this list of search terms and limited the search from January 2015 to October 2021 [3]. With this search criterion, we collected a corpus of IoT security failures. The results were filtered for articles describing a security failure, first by title and then by content. The article with greater detail was used, when multiple articles described the same failure. Sources referenced in the articles were also reviewed for supplementary information.

Our search criteria yielded a total of 1400+ results of news articles, out of which we identified 28 IoT security failure articles. However, we discarded 11 of the articles due to insufficient information. Of the remaining 17 news articles, 4 were reported by *The New York Times* and 13 by *WIRED*.

News dataset preparation. By following the CVE analysis method, we categorized news articles based on application domains as follows: (1) consumer products (5 failure events), (2) critical infrastructures (5 events), (3) automotive (3 events), (4) industrial products (2 events), (5) HW/SW components (2 events). From each article, we identified the sources and repair recommendations for the failure, as reported by the journalists. Two authors independently performed the article analysis to reduce bias. While reaching an agreement, the authors did not disagree, but there were additional identifications. Across the 17 articles, there were 33 sources of failure and 29 repair recommendations; most articles listed multiple sources of failure and multiple repair recommendations.

G Taxonomy Visualization Tool

[3]Google News Search Syntax: "[SearchTerm] site:[SourceWebsite] after:[StartDate: Year-Month-Day] before:[EndDate: Year-Month-Day]."

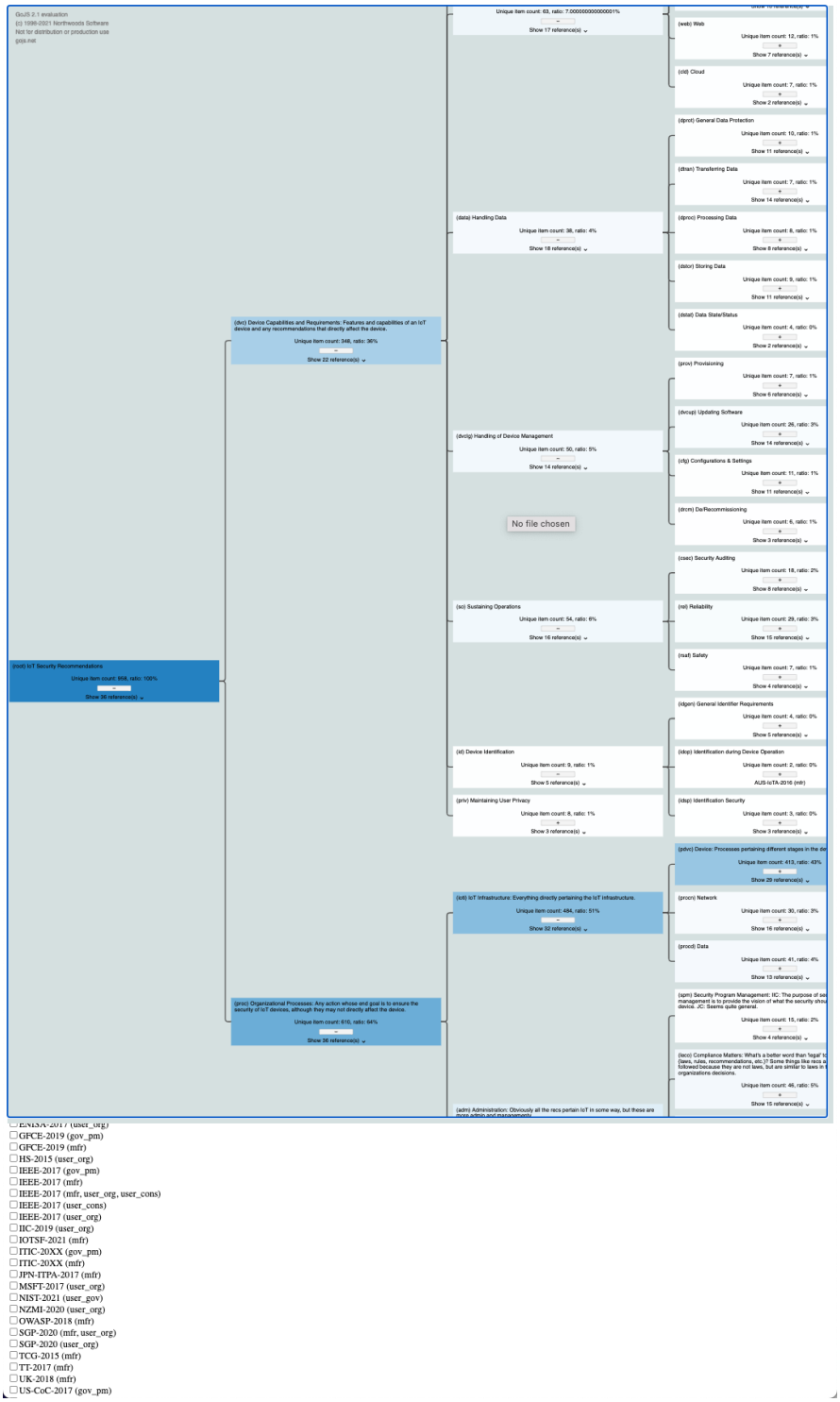

Fig. 5. Screenshot of data visualization tool with categories expanded to level 3. Working on code release for exploration.

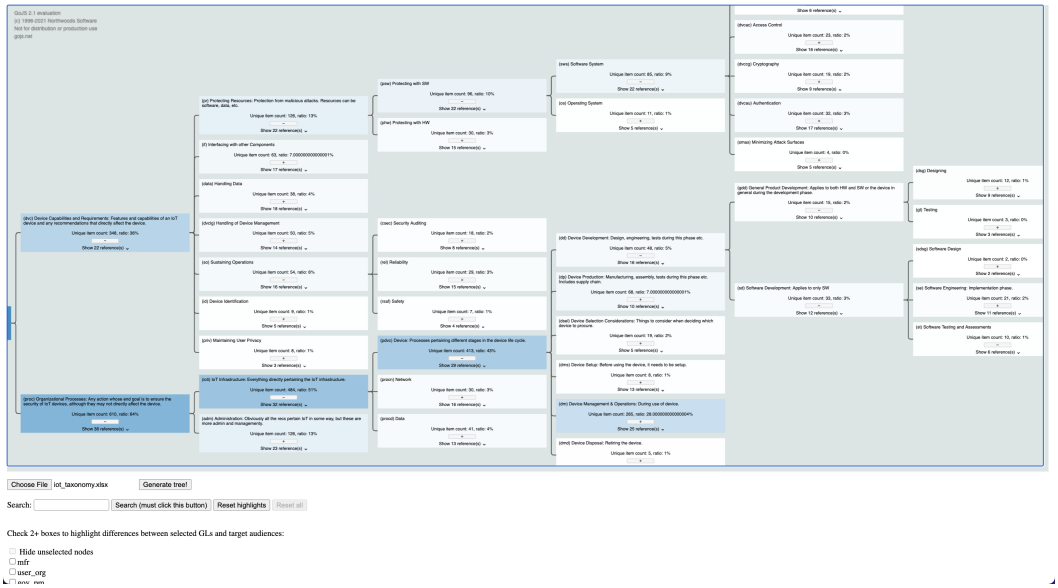

Fig. 6. Screenshot of data visualization tool with randomly chosen categories expanded. Working on code release for exploration.

References

[1] 2015. A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/. Accessed: 2022.

[2] 2015. Hackers Cut a Corvette's Brakes Via a Common Car Gadget. http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/. Accessed: 2022.

[3] 2015. Hackers Remotely Kill a Jeep on a Highway. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed: 2022.

[4] 2016. An Easy Way for Hackers to Remotely Burn Industrial Motors. https://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/. Accessed: 2022.

[5] 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed: 2022.

[6] 2016. Xfinity's Security System Flaws Open Homes to Thieves. https://www.wired.com/2016/01/xfinitys-security-system-flaws-open-homes-to-thieves/. Accessed: 2022.

[7] 2016. Your DVR Didn't Take Down the Internet—Yet. https://www.wired.com/2016/10/internet-outage-webcam-dvr-botnet/. Accessed: 2022.

[8] 2017. Hacker Warns Radioactivity Sensors Can Be Spoofed Or Disabled. https://www.wired.com/story/radioactivity-sensor-hacks/. Accessed: 2022.

[9] 2018. The Myth of the Hacker-Proof Voting Machine. https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html. Accessed: 2022.

[10] 2018. Strava Fitness App Can Reveal Military Sites, Analysts Say. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html. Accessed: 2022.

[11] 2019. Decades-Old Code Is Putting Millions of Critical Devices at Risk. https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/. Accessed: 2022.

[12] 2019. Hackers Could Use Smart Displays to Spy on Meetings. https://www.wired.com/story/dten-video-conferencing-vulnerabilities/. Accessed: 2022.

[13] 2019. Security News This Week: Hackers Found a Freaky New Way to Kill Your Car. https://www.wired.com/story/car-hacking-biometric-database-security-roundup/. Accessed: 2022.

[14] 2019. Watch a Drone Take Over a Nearby Smart TV. https://www.wired.com/story/smart-tv-drone-hack/. Accessed: 2022.

[15] 2021. 'Dangerous Stuff': Hackers Tried To Poison Water Supply of Florida Town. https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html. Accessed: 2022.
[16] 2021. Pipeline Attack Yields Urgent Lessons About US Cybersecurity. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Accessed: 2022.
[17] 2021. Watch a Hacker Hijack a Capsule Hotel's Lights, Fans, and Beds. https://www.wired.com/story/capsule-hotel-hack-lights-fan-bed/. Accessed: 2022.
[18] Amazon. 20XX. The ultimate IoT security best practices guide. https://pages.awscloud.com/rs/112-TZM-766/images/IoT_Security_Best_Practices_Guide_design_v3.1.pdf. Accessed: 2022.
[19] BullGuard. 20XX. Consumer Guide to the Internet of Things. https://www.bullguard.com/marketingfiles/ext/web/IoT-Consumer_Guide.pdf. Accessed: 2022.
[20] Center for Internet Security. 2015. Internet of Things Security Companion to the CIS Critical Security Controls. https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf. Accessed: 2022.
[21] Cloud Security Alliance. 2017. Observations and Recommendations on Connected Vehicle Security. https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/connected-vehicle-security.pdf. Accessed: 2022.
[22] Cloud Security Alliance - Securing Smart Cities. 2016. Cyber Security Guidelines for Smart City Technology Adoption. https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf. Accessed: 2022.
[23] Department of Justice. 2017. Securing Your "Internet of Things" Devices. https://www.justice.gov/criminal-ccips/page/file/984001/download. Accessed: 2022.
[24] European Union Agency for Network and Information Security. 2017. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/@@download/fullReport. Accessed: 2022.
[25] Global Forum on Cyber Expertise. 2019. Internet of Things (IoT) Security GFCE Global Good Practices. https://cybilportal.org/wp-content/uploads/2019/10/GFCE-GGP-IoT.pdf. Accessed: 2022.
[26] Help Systems. 2015. Securing Enterprise Data in the Ever Connected Internet of Things. https://static.helpsystems.com/globalscape/pdfs/guides/gs-securing-enterprise-data-ever-connected-internet-things-gd.pdf. Accessed: 2022.
[27] Industry IoT Consortium. 2019. IoT SMM Practitioner's Guide. https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf. Accessed: 2022.
[28] Information Technology Industry Council. 20XX. IoT Security Policy Principles. https://www.itic.org/policy/ITIIoTSecurityPolicyPrinciples.pdf. Accessed: 2022.
[29] Institute of Electrical and Electronics Engineers. 2017. INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES. https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf. Accessed: 2022.
[30] IoT Alliance Australia. 2016. INTERNET OF THINGS SECURITY GUIDELINE'. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.0.pdf. Accessed: 2022.
[31] IoT Security Foundation. 2021. IoT Security Assurance Framework. https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf. Accessed: 2022.
[32] Japan Information-technology Promotion Agency. 2017. Guidance for Practice Regarding "IoT Safety/Security Development Guidelines". https://www.ipa.go.jp/files/000063228.pdf. Accessed: 2022.
[33] Microsoft. 2017. Evaluating Your IoT Security. https://download.microsoft.com/download/D/3/9/D3948E3C-D5DC-474E-B22F-81BA8ED7A446/Evaluating_Your_IOT_Security_whitepaper_EN_US.pdf. Accessed: 2022.
[34] National Institute of Standards and Technology. 2021. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf. Accessed: 2022.
[35] Nozomi Networks. 2020. The IT Pro's Guide to OT/IoT Security. https://www.exclusive-networks.com/ae/wp-content/uploads/sites/30/2021/02/Nozomi-Networks-IT-Pro-Guide-1.pdf. Accessed: 2022.
[36] Open Web Application Security Project . 2018. OWASP IoT Top 10. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf. Accessed: 2022.
[37] Singapore Infocomm Media Development Authority. 2020. Internet of Things (IoT) Cyber Security Guide. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf?la=en. Accessed: 2022.

[38] TechTarget. 2017. Prevent Enterprise IoT Security Challenges. https://cdn.ttgtmedia.com/digitalguide/images/Misc/EA-Marketing/Eguides/Prevent-Enterprise-IoT-Security-Challenges.pdf. Accessed: 2022.

[39] Trusted Computing Group. 2015. Guidance for Securing IoT Using TCG Technology. https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf. Accessed: 2022.

[40] UK Department of Digital, Culture, Media, & Sport. 2018. Code of Practice for Consumer IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf. Accessed: 2022.

[41] US Chamber of Commerce. 2017. THE IOT REVOLUTION AND OUR DIGITAL SECURITY: Principles for IoT Security. https://scglegal.com/wp-content/uploads/2018/02/2017-Denver-TR-1550-PP-The.IoT_.Revolution..Our_.Digital.Security.Final-002-WILEY-REIN.pdf. Accessed: 2022.

[42] Wind River Systems. 2016. Internet of Things Security Is More Challenging Than Cybersecurity. https://events.windriver.com/wrcd01/wrcm/2016/10/IoT-Security-Is-More-Challenging-Than-Cybersecurity-White-Paper-2.pdf. Accessed: 2022.