Article

Not peer-reviewed version

S3: Security Score System

Dalton Valadares *, Danilo Santos, Angelo Perkusich

Posted Date: 12 December 2023

doi: 10.20944/preprints202312.0776.v1

Keywords: data security; security comparison; vulnerabilities; CVSS

Article

S3: Security Score System

Dalton Cézane Gomes Valadares [1,2,*], Danilo Freire de Souza Santos [2] and Angelo Perkusich [2]

[1] Federal Institute of Pernambuco (IFPE), Caruaru, Pernambuco
[2] VIRTUS RDI Center, Federal University of Campina Grande, Campina Grande, Brazil; danilo.santos@virtus.ufcg.edu.br (D.F.d.S.S.); perkusic@virtus.ufcg.edu.br (A.P.)
* Correspondence: dalton.valadares@virtus.ufcg.edu.br

Abstract: Security in the Internet of Things (IoT) is a critical concern due to the growing number of connected devices and the limited resources to implement robust security mechanisms in most of them. Adopting standard assessment frameworks, such as CVSS (Common Vulnerability Score System), allows for systematic vulnerability assessment. At the same time, CVE (Common Vulnerabilities and Exposures) records provide unique identifiers for known security issues, making it easier to share information. However, comparing security solutions is still challenging due to the diverse nature of IoT devices and the ever-evolving threat landscape, requiring continual innovation and collaboration between stakeholders. Furthermore, there still needs to be a simple way to compare technologies and solutions, taking into account the security provided by them. In this sense, in this article, we propose a tool for calculating a security score based on the CVSS index of each existing vulnerability in a given technology. We explain how the tool performs the calculation, discuss some challenges and propose improvements for future work.

Keywords: data security; security comparison; vulnerabilities; CVSS

I. Introduction

Data security in the Internet of Things (IoT) is a growing concern as more connected devices are deployed across different industries. The IoT devices' diverse and interconnected nature creates a complex landscape, making them susceptible to cyber threats [1–3]. Thus, data protection is essential to ensure user privacy, prevent malicious attacks and maintain system integrity. Measures such as robust cryptography, device authentication, regular software updates, and continuous monitoring are critical to strengthening IoT security [4]. Furthermore, collaboration between manufacturers, governments, and cybersecurity experts is essential to address the ever-evolving challenges in this field. For instance, ETSI (European Telecommunications Standards Institute) and NIST (National Institute of Standards and Technology) have proposed technical recommendations for cyber security in Consumer IoT devices [5–7] and general IoT [8,9].

IoT security is a key concern because of the vulnerabilities in this rapidly expanding ecosystem. According to the ISO/IEC 29147:2018 standard [10], a vulnerability is a behavior or set of conditions existing in a product, system, service, or component that violates an implicit or explicit security policy. A vulnerability can be considered a weakness or exposure with a security impact and can be exploited by attackers to compromise confidentiality, integrity, availability, or other security properties.

IoT devices are subject to various cyber threats due to factors like improper configurations, lack of security standards, weak identity and access management, and design flaws. Additionally, many IoT devices have limited resources (e.g., processing, memory, and storage), hampering to implement robust security measures. This characteristic can open loopholes for attacks such as unauthorized access, data interception, denial of service, and privacy invasions. Exploiting these vulnerabilities can have serious consequences, such as compromising critical infrastructure, personal data breaches, and even physical security risks. Therefore, it is critical to address and mitigate these vulnerabilities by implementing robust security practices and developing solutions that ensure the integrity, confidentiality, and availability of IoT devices and the data they collect and transmit.

 doi:10.20944/preprints202312.0776.v1

To manage vulnerabilities in the cybersecurity scenario, two tools are crucial to classify and track existing vulnerabilities in systems and devices: CVSS (Common Vulnerability Scoring System) [11,12] and CVE (Common Vulnerabilities and Exposures) [13,14]. CVSS is a standardized system that allows to assess the vulnerabilities' severity based on metrics such as impact, exploitation, and attack complexity [15]. It assigns a numerical score to indicate how critical the vulnerability is, helping to prioritize their fixes and mitigate risks. In contrast, the CVE is a public dictionary that provides unique identifiers (CVE IDs) for each known vulnerability. Each CVE ID is a unique entry for a specific vulnerability, allowing organizations, researchers, and cybersecurity professionals to share information about threats, facilitating collaboration and coordination in responses to security incidents. Together, CVSS and CVE play a critical role in securing systems and sharing information about known vulnerabilities throughout the security community.

There are some databases that catalog known vulnerabilities along with their CVSS scores [16]. One of the most widely recognized is the NVD (National Vulnerability Database) [17], maintained by NIST (National Institute of Standards and Technology) in the United States. NVD is an authoritative source that gathers detailed information about software security vulnerabilities, assigning CVSS scores to help assess the severity of each vulnerability. In addition to the NVD, there is also the CNVD (China National Vulnerability Database) [18], maintained by a Chinese government institution, which has its own vulnerability identifier, similar to the CVE, and the JVNDB (Japan Vulnerability Notes Database) [19], which stores the vulnerabilities in Japanese and is maintained by a national agency in Japan, just to cite a few.

Considering only vulnerabilities in IoT technologies and devices, there is the VARIoT database (Vulnerability and Attack Repository for IoT) [20]. VARIot is a European collaborative research project that focuses on IoT security. The project aims to develop a comprehensive framework for IoT security that includes the identification of vulnerabilities and attacks, as well as the development of countermeasures to mitigate them. The project is a partnership among several European universities and research institutions. VARIoT database gathers specific IoT vulnerabilities from other data sources such as NVD and CNVD.

Although there are security frameworks and tools for risk management, we could not find a tool in the literature that makes it possible to assign a security score and thus compare technologies and solutions. Thus, in this article, we propose a tool to assign a security score: the S3 (Security Score System). S3 considers the CVSS values assigned to a technology's vulnerabilities and uses the VARIoT database to obtain such information. With S3, it is possible to compare technologies and solutions considering security.

The main contributions of this work are:

- we propose a tool to compare technologies and solutions considering security requirements;
- we implement the tool considering a primary way to calculate the security score (sesco).

The remainder of this paper is organized as follows: Section II brings a brief explanation of the CVSS; Section III presents the related work that consider security frameworks or risk assessment proposals; Section IV describes the S3 tool, presenting how it works, describing two use cases, and discussing some challenges; Section V ends this work, summarizing the proposal and suggesting future work.

II. Background: Common Vulnerability Score System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a framework used to assess the severity and potential impact of security vulnerabilities [11,12]. It provides a standardized method for evaluating and communicating the characteristics of vulnerabilities in software and systems. CVSS assigns a numerical score to vulnerabilities based on a set of metrics that measure the vulnerability's characteristics [4]. These metrics include factors such as the exploitability of the vulnerability, the impact it could have on the confidentiality, integrity, and availability of the affected system, and other

 doi:10.20944/preprints202312.0776.v1

environmental factors. CVSS scores is used by security professionals, system administrators, and organizations to assess the risks associated with vulnerabilities and prioritize their remediation efforts. They provide a common language for describing vulnerabilities and facilitate communication among different parties involved in vulnerability management.

The CVSS framework consists of three versions: CVSSv1, CVSSv2, and CVSSv3. The latest version, CVSSv3, is the most used and provides a more comprehensive and accurate assessment of vulnerabilities. CVSSv3 calculates a base score, temporal score, and environmental score for a vulnerability. The base score represents the intrinsic qualities of the vulnerability, including its severity and impact. The temporal score considers factors that may change over time, such as the availability of patches or the prevalence of exploits. The environmental score considers the specific characteristics of the affected system or organization, such as its value or criticality. The CVSS scoring system ranges from 0 to 10, with higher scores indicating more severe vulnerabilities. The scores are divided into different severity levels, such as Low (0.0-3.9), Medium (4.0-6.9), High (7.0-8.9), and Critical (9.0-10.0). These severity levels help users prioritize and understand the potential impact of vulnerabilities.

The criteria for assigning a vulnerability score are defined by metric groups. There are three groups of metrics, namely: base metrics, temporal metrics and environmental metrics. The base metrics are the mandatory group needed to get a result. Although fulfilling the requirements of the other metric groups will help to obtain a more effective result, they are not mandatory. In the base metrics, we have two subgroups: exploitability and impact. Basically, exploitability deals with the technical means by which the vulnerability can be exploited, and the impact represents the consequence for the impacted component. The temporal metrics symbolize the characteristics of a vulnerability that may change over time, while the environmental metrics are those characteristics of a vulnerability that are relevant and unique to a specific user's environment. Following we present a brief description of the involved metrics.

A. Base Metrics

The base group is divided in 8 metrics, described as follows.

The **Attack Vector** is a metric that describes how easy it is for an attacker to access the vulnerability. The score will be higher the more remote an attacker can access it, for example: a vulnerability that requires an attacker to be physically present will receive a lower AV score than one that can be accessed over a network.

The **Attack Complexity** metric describes the conditions beyond an attacker's control that must exist to exploit the vulnerability. The score is higher for less complex attacks.

The **Required Privileges** metric describes the level of privileges an attacker must have before successfully exploiting the vulnerability. The base score is higher if no privileges are required.

The **User Interaction** metric captures the requirement of a human user, other than the attacker, for a successful attack.

The **Scope** metric checks whether a vulnerability in a vulnerable component affects features in components beyond its security scope. The base score is higher when a scope change occurs.

The **Confidentiality** metric measures the impact on the confidentiality of vulnerable resources. Confidentiality refers to limiting access and disclosure of information to authorized users only, as well as preventing access or disclosure to unauthorized users. The base score is higher when the loss to the impacted component is higher.

The **Integrity** metric measures the integrity impact of a successfully exploited vulnerability. Integrity refers to the reliability and veracity of information. The base score is higher when the consequence for the impacted component is higher.

Availability is a metric to calculate the availability of affected services.

 doi:10.20944/preprints202312.0776.v1

B. Time Metrics

As previously mentioned, temporal metrics are used to analyze the characteristics of a vulnerability that may change over time. Below we describe the metrics of this group.

The **Exploration Maturity** reflects the likelihood that a vulnerability will actually be exploited, based on exploit techniques. The **Remediation Level** is basically the problem-solving level. The **Report Confidence** metric measures the degree of confidence that the vulnerability exists and the credibility of known technical details.

C. Environmental Metrics

As stated earlier, environmental metrics consist of the characteristics of a vulnerability that are relevant and unique to a specific user's environment. This group considers a modified version of the base metrics, and confidentiality, integrity and availability requirements.

The **Modified Base Metrics** allow the analyst to override individual baseline metrics based on specific characteristics of a user's environment. For example, confidentiality might be compromised in an administrator environment, which would lead to high risks, but in a user environment, the risks would be lower.

The **Confidentiality, Integrity, and Availability requirements** allow to customize the CVSS score considering the importance of each of these security properties for the affected technology.

III. Related Work

In this section, we review some related works in the field of security scoring systems and cybersecurity evaluation tools.

Peter Mell [21] presented a domain-agnostic technique for generating scoring systems. The method involves expert comparisons of elements from a domain, resulting in a directed acyclic graph that orders the equivalency sets. While the approach demonstrated usability in the security domain, the accuracy of the generated scoring systems and consistency among multiple expert encodings were not formally proven.

Benz and Chatterjee [22] introduced the Small and Medium Enterprise Cybersecurity Evaluation Tool (CET). The CET is a 35-question online survey based on the NIST framework, empowering SMEs (Small and Medium-sized Enterprises) to self-rate their cybersecurity maturity and prioritize improvements. The authors evaluated the tool's effectiveness through pilot studies, enabling better cybersecurity posture and fostering a security-conscious environment.

Alwari et al. [23] systematically analyzed home-based IoT devices, utilizing an abstract model for insights. The study evaluated 45 IoT devices, publicly sharing findings and evaluation data to encourage collaboration and further research in IoT systems.

Alsubaei et al. [24] presented the Internet of Medical Things Security Assessment Framework (IoMT-SAF) for enhancing security in medical IoT (IoMT) solutions. IoMT-SAF offers a detailed assessment based on ontological scenarios, catering to different stakeholders and emerging technologies.

Boakye-Boaten et al. [25] presented a risk assessment tool designed for substation environments by incorporating stages of the ISM (Information Security Management) process. The tool allows for comprehensive profiling of substation devices, considering unique identification, classification, type, and functional influence to determine their criticality level. The tool's output includes color-coded representations of device criticality and visualizations of their functional influence within the substation. This information aids in understanding potential security risks and the impact of device compromise, facilitating informed decision-making to enhance security.

While these works provided valuable contributions to security and evaluation in their respective domains, none explicitly introduced a tool for calculating a security score, as demonstrated in our

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0776.v1

work. Our introduced tool stands apart with its focus on quantifying security measures, providing a clear security score for IoT technologies and solutions.

IV. S3 - Security Score System

To enable technologies or solutions to be compared in terms of security, S3 assumes that vulnerabilities weaken the security of a device, product, or system/service. As mentioned in the ISO/IEC 29147:2018 standard [10], attackers can exploit vulnerabilities to carry out attacks, harming security properties. Thus, we can assume that the more vulnerabilities a device or system/service has, the more susceptible to attacks it will be, i.e., we can consider that, in this case, the security level is weaker. Analogously, we can also consider that the higher the CVSS of a vulnerability, the lower the security.

Therefore, to calculate the Security Score (SeSco), S3 considers all existing vulnerabilities in each technology and uses the CVSS of each vulnerability. Having the CVSS of all vulnerabilities for each technology, S3 calculates the average of the CVSS scores and then calculates the ten's complement. Thus, for example, if a technology has three vulnerabilities with CVSS scores equal to 7.5, 6.5, and 8.6, the calculated SeSco will be equal to 2.47.

The first version of the S3 calculator uses the VARIoT database, which gathers vulnerabilities specific to devices and technologies related to IoT scenarios. As we needed to handle the return of queries using the VARIoT API and we would be dependent on the latency of the search performed, we decided to make a local replica of the database. In general, the tool has the communication flow presented in Figure 1 and works as follows:

1. The user types the technology for which they want to calculate the security score (sesco);
2. The S3 tool searches for vulnerabilities known for the informed technology;
3. An average is calculated considering all the CVSS scores from the technology vulnerabilities;
4. Finally, the tool calculates the ten's complement with the average of the CVSSs from the vulnerabilities.

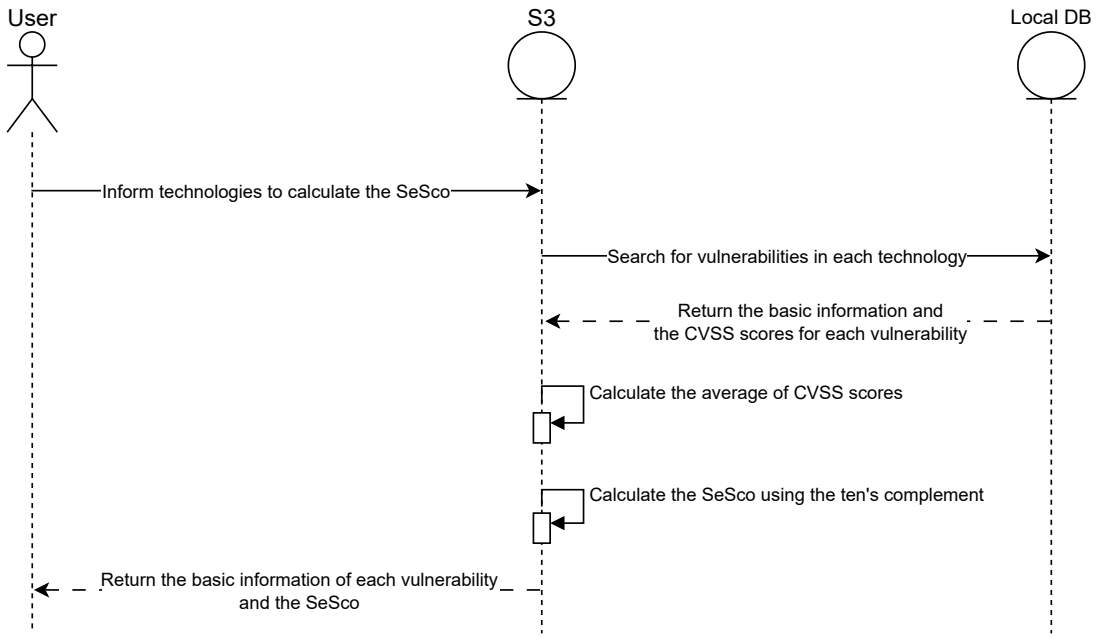

Figure 1. S3 Communication Flow.

In addition to the security scores for technologies and solutions, the tool also provides basic information about each vulnerability cataloged for technologies. This information can help users who decide to adopt such technologies in mitigating vulnerabilities.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0776.v1

A. Use Case 1 - Comparing technologies

The first usage scenario is when a developer or a team of developers needs to implement a system that handles sensitive data and therefore has security requirements. In this case, the developer(s) may be in doubt about which technologies to use and, in this sense, may make the decision based on the security level of the technologies. For example, if he/she is in doubt between three programming languages (e.g., PHP, Java, or Ruby), the decision could be the one with the fewest vulnerabilities. The same can be applied to decide on other technologies, such as DBMS and frameworks. Figure 2 exhibits this use case, demonstrating a comparison between three programming languages (PHP, Java, and Ruby).

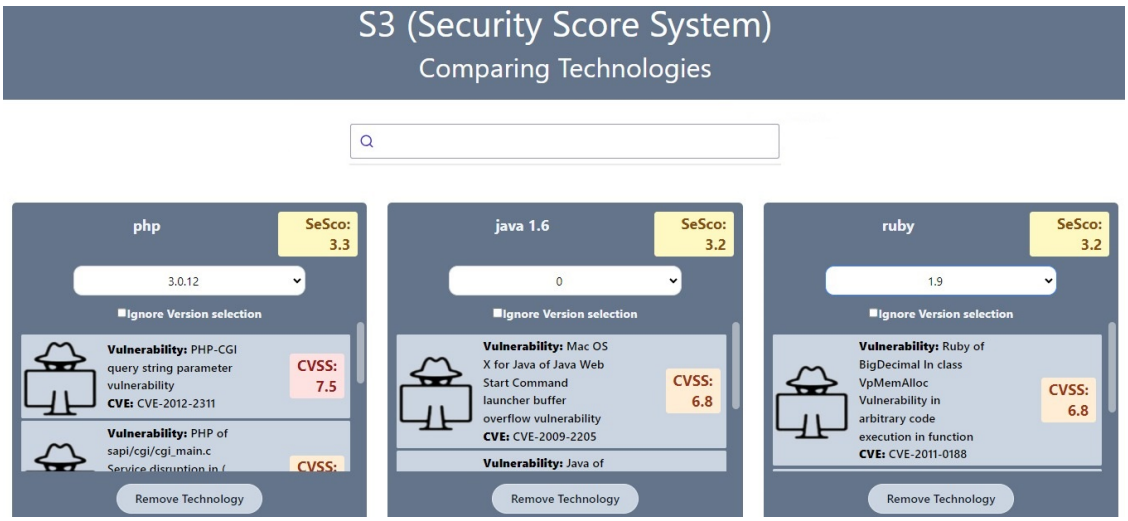

Figure 2. S3 - Comparing security scores.

B. Use Case 2 - Comparing solutions

The second usage scenario considers someone who needs to make a decision on the adoption of a system and has data security as one of the main requirements. For this, the user must obtain the list of technologies used in each solution. With this, he/she inserts each technology into the S3 tool, and it will be in charge of researching the vulnerabilities for each technology, obtaining the CVSS of each vulnerability, calculating the average of all CVSS, and, finally, calculating the equivalent security score (SeSco). The tool can display only the SeSco for just one solution, or it can display the scores for more than one solution simultaneously, in case the user is interested in comparing solutions. Figure 3 shows a comparison among two solutions: Solution 1, with a SeSco of 3.8, and Solution 2, with a SeSco of 3.5. Figure 4 shows the screen where we can select a technology for comparing solutions.

Figure 3. S3 - Comparing solutions.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 December 2023 doi:10.20944/preprints202312.0776.v1

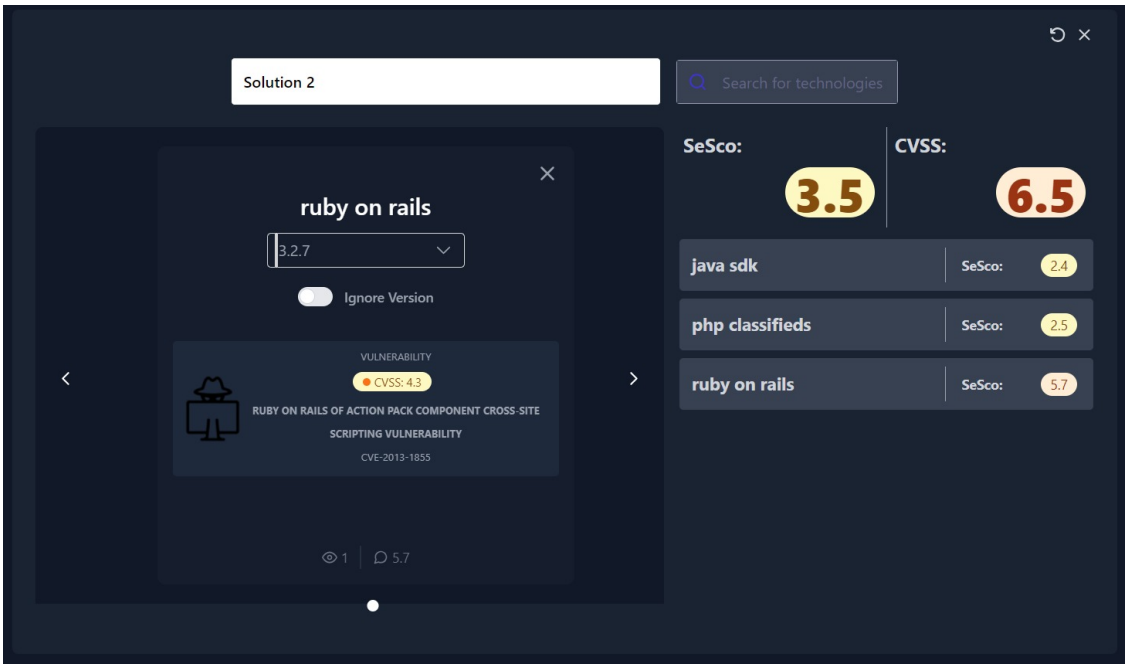

Figure 4. S3 - Comparing solutions.

C. Threats to Validity

We consider that using only CVSS scores may not be the best approach for calculating the SeSco. With the use of the tool, we intend to analyze the inclusion of other variables in an attempt to make the calculation more accurate and fair. For example, a CVSS value can be nullified if the vulnerability has been mitigated during the implementation of a multi-technology solution, or a value could be subtracted from that specific CVSS if the vulnerability has been only partially mitigated.

Furthermore, we know that new vulnerabilities, such as zero-day vulnerabilities, can be discovered at any moment. A zero-day vulnerability is a vulnerability that has been discovered but not yet addressed/mitigated by the vendors/developers [26,27], which can lead to what is called a zero-day exploit. Therefore, they are considered high-risk. As such vulnerabilities are new and may not be cataloged, they will not have CVSS. Thus, S3 may include some way of considering zero-day vulnerabilities, either using a standard CVSS or allowing the user to define a value that he/she deems appropriate, given the available knowledge about the vulnerability.

Finally, it does not seem fair that a technology with only one vulnerability and a high CVSS value has a lower security score than a technology with many vulnerabilities but a lower average CVSS value. For example, a technology X could have a vulnerability with CVSS 8 and a technology Y could have four vulnerabilities with CVSS values equal to 7, 6, 5, and 7. In this case, technology X would have a SeSco equal to 2, while technology Y would have a SeSco equal to 3.75. Therefore, we will also evaluate including a factor that considers the number of vulnerabilities in the technology for the SeSco calculation.

The S3 tool has a lot to evolve, mainly in the way of calculating the security score. However, we intend to evolve it as it happened with CVSS, whose initial version was released in February 2005 and, 18 years later (today), is releasing its 4th version [28].

V. Conclusion

In the general context of data security in the Internet of Things, in this work, we presented a tool that calculates a security score (SeSco) based on the CVSS score of the existing vulnerabilities in technologies. This tool can help in decision-making processes when someone needs to decide among different technologies to implement software components that have security requirements. In addition to enabling the SeSco calculation for a specific technology, the tool enables the calculation for a solution

 doi:10.20944/preprints202312.0776.v1

involving different technologies. In this case, the tool considers the CVSS of all vulnerabilities from all technologies used to implement the solution. It is also possible to compare technologies or solutions.

For future work, we want to include other vulnerability databases in addition to the specific IoT database the tool is using (VARIoT). For example, the S3 tool can include the base of NIST (NIST Vulnerability Database - NVD). With this, the tool will serve generic scenarios, not just IoT. Furthermore, we intend to improve the SeSco calculation to consider zero-day vulnerabilities and/or other variables related to the security of the technologies. We also want to include some factor that allows the calculation considering the number of existing vulnerabilities and not just the CVSS values. Finally, we can analyze integrating S3 into other existing security tools, such as a risk management system.

References

1. Simsek, I.; Rathgeb, E.P. Zero-Knowledge and Identity-Based Authentication and Key Exchange for Internet of Things. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 283–288. doi:10.1109/WF-IoT.2019.8767235.
2. da Silva, L.P.; Nascimento, B.S.; Dias, R.A.M.P.; Mendonça, D.S. A Comprehensive Approach for Applying Threat Modeling to Internet of Things Systems. 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), 2022, pp. 01–06. doi:10.1109/WF-IoT54382.2022.10152291.
3. Valadares, D.C.G.; Sobrinho, Á.; Will, N.C.; Gorgônio, K.C.; Perkusich, A. Trusted and only Trusted. That is the Access! Advanced Information Networking and Applications; Barolli, L., Ed.; Springer International Publishing: Cham, 2023; pp. 490–503.
4. Valadares, D.C.G.; Will, N.C.; Sobrinho, Á.Á.C.C.; Lima, A.C.D.; Morais, I.S.; Santos, D.F.S. Security Challenges and Recommendations in 5G-IoT Scenarios. Advanced Information Networking and Applications; Barolli, L., Ed.; Springer International Publishing: Cham, 2023; pp. 558–573.
5. (ETSI), E.T.S.I. Cyber Security for Consumer Internet of Things: Baseline Requirements, 2020.
6. (ETSI), E.T.S.I. Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements, 2021.
7. (ETSI), E.T.S.I. Guide to Cyber Security for Consumer Internet of Things, 2022.
8. of Standards, N.I.; (NIST), T. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, 2019. doi:10.6028/NIST.IR.8228.
9. of Standards, N.I.; (NIST), T. IoT Device Cybersecurity Capability Core Baseline, 2020. doi:10.6028/NIST.IR.8259A.
10. ISO, *ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure*, International Organization for Standardization (ISO) Std., 2018.
11. Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S. A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS. *ACM Comput. Surv.* **2020**, *53*. doi:10.1145/3381038.
12. Anand, P.; Singh, Y.; Selwal, A.; Singh, P.; Ghafoor, K. IVQFIoT: Intelligent vulnerability quantification framework for scoring internet of things vulnerabilities. *Expert Systems* **2021**, *39*. doi:10.1111/exsy.12829.
13. Bhandari, G.; Naseer, A.; Moonen, L. CVEfixes: Automated Collection of Vulnerabilities and Their Fixes from Open-Source Software. Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering; Association for Computing Machinery: New York, NY, USA, 2021; PROMISE 2021, p. 30–39. doi:10.1145/3475960.3475985.
14. Lim, J.; Lau, Y.L.; Ming Chan, L.K.; Tristan Paul Goo, J.M.; Zhang, H.; Zhang, Z.; Guo, H. CVE Records of Known Exploited Vulnerabilities. 8th International Conference on Computer and Communication Systems (ICCCS), 2023, pp. 738–743. doi:10.1109/ICCCS57501.2023.10150856.
15. Common Vulnerability Scoring System v3.1: Specification Document. https://www.first.org/cvss/v3.1/specification-document, 2023.
16. Rytel, M.; Felkner, A.; Janiszewski, M. Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources. *Sensors* **2020**, *20*. doi:10.3390/s20215969.
17. National Vulnerability Database. https://nvd.nist.gov/, 2023.
18. China National Vulnerability Database. https://www.cnvd.org.cn/, 2023.
19. JVN iPedia. https://jvndb.jvn.jp/en/, 2023.

20. Janiszewski, M.; Felkner, A.; Lewandowski, P.; Rytel, M.; Romanowski, H. Automatic Actionable Information Processing and Trust Management towards Safer Internet of Things. *Sensors* **2021**, *21*. doi:10.3390/s21134359.
21. Mell, P. The Generation of Software Security Scoring Systems Leveraging Human Expert Opinion. 2022 IEEE 29th Annual Software Technology Conference (STC), 2022, pp. 116–124. doi:10.1109/STC55697.2022.00023.
22. Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons* **2020**, *63*, 531–540. doi:https://doi.org/10.1016/j.bushor.2020.03.010.
23. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1362–1380. doi:10.1109/SP.2019.00013.
24. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things* **2019**, *8*, 100123. doi:https://doi.org/10.1016/j.iot.2019.100123.
25. Boakye-Boateng, K.; Ghorbani, A.A.; Lashkari, A.H. RiskISM: A Risk Assessment Tool for Substations. 2021 IEEE 9th International Conference on Smart City and Informatization (iSCI), 2021, pp. 23–30. doi:10.1109/iSCI53438.2021.00013.
26. Singh, U.K.; Joshi, C.; Kanellopoulos, D. A framework for zero-day vulnerabilities detection and prioritization. *Journal of Information Security and Applications* **2019**, *46*, 164–172. doi:https://doi.org/10.1016/j.jisa.2019.03.011.
27. Peppes, N.; Alexakis, T.; Adamopoulou, E.; Demestichas, K. The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers. *Sensors* **2023**, *23*. doi:10.3390/s23020900.
28. Common Vulnerability Scoring System Version 4.0. https://www.first.org/cvss/v4-0/, 2023.