How to Cite:
Kiranpal Singh Virk (Dec 2020). DECODING THE ECOSYSTEM OF SYSTEM'S ATTACK SURFACE IN IOT
International Journal of Economic Perspectives,*14*(1), 237-241
Retrieved from https://ijeponline.org/index.php/journal/article

DECODING THE ECOSYSTEM OF SYSTEM'S ATTACK SURFACE IN IOT

Kiranpal Singh Virk
Assistant Professor, Department of Computer Science,
Guru Nanak Khalsa College,
Yamuna Nagar, Haryana 135001, India
{kiranpal.virk}@yahoo.com

ASBTRACT

IoT is the buzzword for the upcoming technology applied domains. Establishing an IoT ecosystem in the domains like smart homes, smart forest areas wherein animals are tagged, smart metering or smart surveillance has various issues in terms of availability of hardware and software platforms, sensing devices, power devices. In addition, IoT has security issues also as most of IoT infrastructure is placed in open periphery. Securing an IoT ecosystem is necessary as the failure to do so gives reputational impact, operative impact and legal impact for the organizations dealing in IoT implementations. One of aspect of security is the notion of attack surface. This paper is an effort in direction of understanding the concept of system's attack surface and other associated concepts of the IoT ecosystem.

Keywords: *IoT, smart, security, attack surface*

1. INTRODUCTION

The times of rather static communication in strictly controlled, closed networks for limited purposes are over, while the adoption of the Internet and other communication technologies in almost all domes- tic, economic and social sectors with new approaches for rather dynamic and open networked environments overwhelmingly progresses. Social networks, networked communities, cloud computing, Web X.0, mashups or business process design are just some of the trends that reflect the tendency towards permanent connections and permanent data collection. Today's networked systems face the challenge of various security threats, which is usually met by various protection systems against attacks from the direct system users. In an interconnected world, software with vulnerabilities presents a threat not only to individuals but also to companies and public organizations, and last but not latest to national and international cooperation.

Consider when a system is build from scratch using the traditional established life cycle models, user context may change considerably at the final stages. Under these circumstances only two options are left. First being to scrap the project, which is not viable in today's profit conscious industry. Second one is two explore the third party reliable and reusable software

Corresponding author: Kiranpal Singh Virk
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Dec 2020

components or COTS. The process of building software systems by assembling and integrating third party software components has become a strategic need in a wide variety of application areas. A software system may include one or more COTS components (products). If some requirement(s) cannot be satisfied with COTS components, then the component(s) corresponding to the given system requirement(s) may be developed in-house.

IoT applications can be considered as Service-oriented Component-based Applications that takes this scenario of component reusability a step further. Service-oriented Component-based Applications provides a framework to construct modularised applications consisting of software components that uses software services provided by other components.

2. NOTION OF ATTACK SURFACE

Various authors have suggested a notion of system's attack surface using input/output or entry/exit points of a component using Input/ Output automata model or similar techniques [1][8][9][10]. These works have considered the attack surface of software as base criteria for evaluating the security. From a set of system's resources, a sub set called system's attack surface is defined. Reducing the attack surface is one of the ways for making software more secure. Attackers exploits the system's resources like system's methods (API), channels (sockets), and data items (input streams) for attacking sandboxes.

Al-Sarayreh and Abran suggested the use of and the COSMIC generic software model suggests the use of data movement for Entry, Exit, Write and Read for measuring function size of components in a business application with humans and another 'peer' application as its functional users[11] [12].

Abran and Soubra [13] implemented the COSMIC approach on IoT application using Arduino open source. They suggested how Entry, Exit, Write and Read points are indentified and then calculated Cosmic Function Points that could be helpful in ensuring optimum battery load for continuity and quality of service in energy constrained IoT frameworks.

Multiple works[14][15][16][17] by Josef Noll suggested the multi-metric approach for measuring security, privacy and dependability in a complex system and suggested an implementation on a Smart Grid on the footprints of cyber physical systems or IoT paradigm for the special nature of security threats[18]:

- Attacks are frequently carried out by well organized groups with a commercial background (spamming, extortion, industrial espionage)
- Multi-stage attacks skilfully combine vulnerabilities on system level and organizational level information security risk analysis does often not hold for the complete life time of a product (context of product usage may change, new vulnerabilities are detected)

The notion of attack is also dependent upon the nature of IoT device. Tabulated information summarizing the various categories is shown in Table 2.1

Corresponding author: Kiranpal Singh Virk
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Dec 2020

Table 2.1 Various categorization of IoT entities

CRITERIA	CATEGORY 1	CATEGORY 2
Based upon sensing	Active – sensing with actuating capability	Passive – Only sensing capability
Based upon accessibility	Physical accessibility	Remote accessibility (e.g. buried sensors)
Device Registration	Platform-registered Devices Devices may be pre-registered by the platform as part of the platform configuration	Application-registered Devices Devices may be programmatically registered at runtime by applications.

3. RISKS OF ATTACK SURFACE

It is this reusability that poses a risk of an unidentified nature. Existing IoT application is easily extendable by adding new sensors and accordingly adding new code in the shape of a reusable software component as COTS. The reusable component added this way may expose the existing applications from within for an attack from outside.

3.1. **The internal risks** are risk arising due to design faults or implementation errors like code errors. Normally a component developed using Component Based Software Engineering principle would have well defined input and output interactions. Such interactions help in measuring the cohesion and coupling metrics of a component. Manadhata et. al. in their work have considered Input/ Output automata of a component to define its entry and exit points[1]. The empirical study conducted by Grechanik et. al. [3] suggested that majority of the interactions occur within the defined security boundaries of an application. And the topologies of the security measures and component pattern interactions were developed to suggest architecture.

3.2. **The external risks** covers the risk arising from individual unattended ES devices, communication between ES devices, information backyards like cloud databases. In most of the secured systems wherein the ES device is lying unattended on the pretext that there is a 'air gap', the security has been compromised by various attacks like Stuxnet worm attack in 2010. Mirai attack of 2016 is another indicator that in hastiness of implementation of technology wherein the remote ports with default username and password are left open to be exploited later on by the hackers. The works like [4][5] focussed upon the external risks and their mitigation by achieving access control (authorization and authentication) between a cyber physical device and the cloud storage with end-to-end communication security

Corresponding author: **Kiranpal Singh Virk**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Dec 2020

Manadhata and Wing [6][7]further suggested approach for enhancing security level by categorizing the approaches as system-centric approach and attack centric approach. In attack-centric approach, factors like behaviour, resources and capabilities of the attackers that lead to vulnerability risks. In system-centric approach system design and configurations forms the core focus area.

4. CONCLUSION

Based upon the above discussion, a framework/model could be worked upon wherein the reusable component is evaluated before its inclusion in an existing application from security point of view. The system-centric approach or the internal threat approach could be further worked upon along with COSMIC generic software model to suggest a working model for the evaluation of security.

5. REFERENCES

1. Manadhata, P. K., Kaynar, D. K. and Wing, J. M. (2007) 'A Formal Model for a System's Attack Surface'. doi: 10.21236/ADA477014.

2. Karati, A., Amin, R., Islam, S. K. H. and Choo, K. K. R. (2018) 'Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment', IEEE Transactions on Cloud Computing, pp. 1–14. doi: 10.1109/TCC.2018.2834405.

3. Grechanik, M., Perry, D. E. and Batory, D. (2006) 'A security mechanism for component-based systems', Proceedings - Fifth International Conference on Commercial-off-the-Shelf (COTS)-Based Software Systems, 2006, pp. 53–62. doi: 10.1109/ICCBSS.2006.3.

4. Karati, A., Amin, R., Islam, S. K. H. and Choo, K. K. R. (2018) 'Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment', IEEE Transactions on Cloud Computing, pp. 1–14. doi: 10.1109/TCC.2018.2834405.

5. Ragunathan R. (2012) 'A cyber–physical future', Proceedings of the IEEE, 100(Special Centennial Issue):1309–1312.

6. P. K. Manadhata and J. M. Wing (2011) 'An attack surface metric', IEEE Transactions on Software Engineering, vol. 37, no. 3, pp. 371–386.

7. R. Yesudas and R. Clarke (2013) 'A framework for risk analysis in smart grid', International Workshop on Critical Information Infrastructures Security. Springer, pp. 84–95.

8. Howard M., Pincus J., Wing J.M. (2005) 'Measuring Relative Attack Surfaces', In: Lee D.T., Shieh S.P., Tygar J.D. (eds) Computer Security in the 21st Century. Springer, Boston, MA. doi: 10.1007/0-387-24006-3_8

9. J. Szefer, E. Keller, R. B. Lee, and J. Rexford(2011) 'Eliminating the hypervisor attack surface for a more secure cloud', in Proceedings of the 18th ACM Conference on Computer and Communications Security, ser. CCS '11. ACM, pp. 401–412.

Corresponding author: Kiranpal Singh Virk
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Dec 2020

10. A. Bartel, J. Klein, Y. Le Traon, and M. Monperrus (2012) 'Automatically securing permission-based software by reducing the attack surface: An application to android', Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ser. ASE 2012. ACM, pp. 274–277.

11. Al-Sarayreh, K. T. and Abran, A. (2010) 'A generic model for the specification of software interface requirements and measurement of their functional size', 8th ACIS International Conference on Software Engineering Research, Management and Applications, SERA 2010, (October 2016), pp. 217–222. doi: 10.1109/SERA.2010.35.

12. COSMIC Measurement Manual Version 4.0.1, Common Software Measurement International Consortium, 2015.http://cosmic-sizing.org

13. Soubra H. and Abran A. (2017) ' Functional size measurement for the internet of things (IoT): an example using COSMIC and the Arduino open-source platform' , Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement (IWSM Mensura '17). ACM, New York, NY, USA, 122-128. DOI: ttps://doi.org/10.1145/3143434.3143452

14. Noll, J., Garitano, I., Fayyad, S., Asberg, E. and Abie, H. (2015) 'Measurable Security, Privacy and Dependability in Smart Grids', Journal of Cyber Security and Mobility. doi: 10.13052/jcsm2245-1439.342.

15. Fayyad, S. and Noll, J. (no date) 'Toward Objective Security Measurability and Manageability'. doi: 10.1109/HONET.2017.8102211.

16. Garitano, I., Fayyad, S. and Noll, J. (2015) 'Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems', Wireless Personal Communications. doi: 10.1007/s11277-015-2478-z.

17. Fayyad, S. and Noll, J. (2017) 'A framework for measurability of security', 2017 8th International Conference on Information and Communication Systems, ICICS 2017, (April), pp. 302–309. doi: 10.1109/IACS.2017.7921989.

18. Schieferdecker, I., Grossmann, J. and Schneider, M. (2012) 'Model-Based Security Testing', Electronic Proceedings in Theoretical Computer Science, 80(Mbt), pp. 1–12. doi: 10.4204/EPTCS.80.1.

Corresponding author: **Kiranpal Singh Virk**
Submitted: 27 Aug 2020, Revised: 09 Sep 2020, Accepted: 12 Oct 2020, Published; 30 Dec 2020