REVIEW ON VULNERABLITIES AND ATTACKS IN EMBEDDED SYSTEM

KATAKAM GEETHANJALI[1], BALAM KALYANI[2]
[1]*Assistant Professor, Department of Electronics and Communication Engineering,*
[2] *Assistant Professor, Department of Electronics and Communication Engineering*
[1,2]*Keshav Memorial College of Engineering, Ibrahimpatnam, R.R Dist [India].*

ABSTRACT: Embedded systems are the main thrust for technological advancement in numerous spaces, for example, car, medical care, and modern control in the arising post-PC time. As an ever increasing number of computational and organized gadgets are coordinated into all parts of our lives in an unavoidable and "undetectable" way, security becomes basic for the steadfastness of all savvy or clever frameworks based upon these installed systems. In this paper, we direct an orderly survey of the existing dangers and weaknesses in implanted systems based on open accessible information. In addition, we derive an embedded systems attack taxonomy from the data. We imagine that the discoveries in this paper give an important knowledge of the danger scene confronting embedded systems. The information can be utilized for a superior comprehension and the ID of safety gambles in framework examination and plan.

KEYWORDS: security, Common vulnerabilities and exposure

I INTRODUCTION

An embedded system is a figuring framework incorporated into a bigger framework, intended for devoted capabilities. It comprises of a blend of equipment, programming, and alternatively mechanical parts. As a result, any computing system other than a general-purpose PC or mainframe computer is included in the definition [1]. Frequently they are Cyber Physical Systems (CPS) because of the mix of calculation and actual cycles [2]. The modern pattern shows that they are the main thrust in numerous application spaces that form brilliant or smart systems, including regions like car gadgets, aeronautics, customer hardware, rail routes, broadcast communications, and medical services [3]. Security is a significant issue in light of the jobs of implanted frameworks in numerous mission and wellbeing basic systems. It has been demonstrated that cyber system attacks result in physical harm [4]. Notwithstanding, contrasting with

traditional IT frameworks, security of installed frameworks is no greater because of unfortunate security plan and execution and the trouble of nonstop fixing [5]. Albeit many methodologies have been proposed in the past to get implanted frameworks [6], [7], different realities for example, arrangement scale, asset impediments, the trouble of actual security, and cost thought all make it very testing to get them [8], especially for gadgets with controller, support and activity capabilities. Having an exhaustive view and comprehension of an assailants ability, for example knowing the adversary, is essential for security designing of implanted frameworks. Security examination, secure plan and advancement should consider the full range of the danger scene to recognize security necessities, improve and apply security controls inside the limit of requirements. In this paper, we conduct a systematic review of existing threats and vulnerabilities. We focus on two sets of data, i.e., the exposures of attacks on embedded systems in security conferences and literature, and the published vulnerabilities specific to embedded systems. Based on the data, we derive an attack taxonomy to systematically identify and classify common attacks against embedded systems. We envision that the comprehensive knowledge of attacks and their implications will contribute to savvy design decisions for mission and safety critical systems.

II ATTACKS ON EMMBEDED SYSTEMS

This part records a few instances of assaults against inserted gadgets and systems and investigates the assailants capabilities and their suggestions. Albeit not far reaching, in our view, the models are extremely delegate and cover a expansive scope of utilization areas like modern frameworks, interchanges, and buyer gadgets. [23] presents a timetable for basic embedded system. Noteworthy assaults date back to the 1982 and the quantity of assaults have been expanding beginning around 2001. [24] presents weaknesses what's more, potential adventures of key administration in remote gadgets. For instance, one of the gadgets is transported with a graphical UI with default values to arrange the gadget. The execution of the connection point creates a passphrase which is subsequently used to create the AES key. In any case, the Pseudo Arbitrary Number Generator is cultivated by the srand() function

utilizing the ongoing time and generator itself is the rand() capability. Thus, the assailant is fit for computing the passphrase and the encryption key and can catch all communication on the objective remote organization. [25] illustrates remote assaults against SCADA gadgets utilizing the ModBus convention. The weakness took advantage of is inside the plan of the convention: it needs encryption and verification. Accordingly, a gadget double-dealing can be effortlessly accomplished with a cautiously created bundle. The operating system's hard-coded credentials can be used to attack RuggedCom devices [26]. The default account is available in the framework to help secret key recuperation, so can not be impaired. However, this account can be used by attackers who know the MAC address to connect to the device and take full control of it.[27] introduced numerous assaults against satellite communication frameworks beginning starting from the earliest stage. In one of the assault situations, the man-machine connection point of the plane installed SATCOM unit requires overseer secret word for confined setups and control components. The generation calculation utilizes the gadget chronic number (can be found imprinted on the gadget) in addition to a hard-coded string, which makes it simple to figure the secret phrase. Subsequently the aggressor approaches to all setups and can incapacitate basic parts connected with the security of the airplane. [28] implemented a rogue satellite system carrier. Their strategy permits the assailant to turn into an ill-conceived client of administrations gave. Right off the bat, the assailant should choose its objective, a fake satellite. Then, the aggressor direct his recieving wire toward the objective and looks for unused, lawful recurrence for clients. On the off chance that such a recurrence is found, the assailant is allowed to send and get as he wishes. In any case, the aggressor actually needs to keep away from identification: He must precisely comply with the operator packet's requests while sniffing packets sent to legitimate clients. As expressed in their discussions, the strategy works since regardless of whether the satellite backings encryption, turning it on makes execution drop essentially. Subsequently, administrators switch it off in light of the fact that it is the help clients pay for, not the security of the assistance. [30] presents an assault against a shrewd home mechanization

gadget, the Home Indoor regulator. Squeezing a button for 10 minutes on the gadget starts a worldwide reset. Subsequently, there is a humble window during which the gadget acknowledges code from USB sticks associated with it and utilizations that code for booting with no cryptographic minds the code. This flaw allows an adversary to install an SSH server and gain access to the user's home network. Be that as it may, actual access is expected to the gadget to send off the assault, so either the aggressor needs to break into the house or compromise the gadget during transport. [31] presents physical and remote assault surfaces in vehicles. For instance, the verification convention between the Telematics Unit and the middle depends on a test reaction components. Notwithstanding, the arbitrary number generator is cultivated with a similar steady each time it is introduced. Accordingly, a noticed reaction bundle can be replayed by the assailant to confirm himself as the Telematics Call Center, getting full command over the vehicle. A potential assault against a remote home robotization gadget is introduced in [32] which is utilized for controlling power plugs. The execution of the Home Organization Convention contains a cradle flood which can be utilized to execute erratic code on the gadget. Since the gadget controls the electrical plug to any gadget truly associated with it, the aggressor has the capacity to harm the associated gadget. The D-Connection DIR-815 Remote N Double Band Switch contains an order infusion weakness which permits the aggressor to get remote access to the gadget as exhibited by [33]. The packet parsing process is the source of the flaw: strings inside backticks are thought of orders and executed on the switch. [34] examines a contextual investigation of malevolent firmware refreshes to a HP-RFU (Far off Firmware Update) LaserJet printer. The weakness which empowers this assault comes from the way that the printer needs to acknowledge printing position in an unauthenticated way (as directed by the norm) and that the firmware is refreshed by printing to the memory. Subsequently, an assailant can send a printing position to the gadget, training it to refresh its firmware with the malevolent code gave. [35] talks about assaults against a firecrackers control framework. The convention utilized by the framework gives no encryption, nor validation, which permits the assailant to sniff bundles and in this manner gain proficiency with the addresses of

every gadget. Presently, the aggressor could hang tight for the administrator to arm the framework, the aggressor can right away send the computerized arm and fire orders. The framework will quickly fire its fireworks stacks and may cause actual mischief to the administrator. The assault can be mechanized also, since erratic Python code can be transferred to the gadgets. [36] shows various assaults against an robotized outer defibrillator. For instance, there is a buffer overflow flaw in the firmware upgrade software that comes with the device. This flaw could let arbitrary code run. Another weakness is the utilization of CRC as a computerized signature. Consolidating these two weaknesses permits the aggressor to hurt patients by setting shock conventions and shock qualities or send off a cyberattack against the IT system in which the gadget is conveyed

IV ATTACK TAXONOMY FOR EMMBEDED SYSTEMS

Examining CVE information was a significant test in our work. The CVE data set has in excess of 60,000 records, in which just a little part is pertinent to installed gadgets. CVE records don't contain meta-data that would make it simple to distinguish which records are connected with implanted frameworks. In order to locate and extract the relevant subset, we used heuristics. In particular, we put in place a script that compared CVE records to a whitelist and a blacklist of keywords that we had created. Only entries whose textual description contained at least one word from our whitelist but no word from our blacklist were selected. Our script recognized 4936 applicable CVE records, which was still infeasible to peruse and dissect physically. What's more, the set of chosen CVE records was very one-sided as in a huge subset of the records was connected with gadgets created by few embedded device producers. Fig 1 states the common attack scenarios

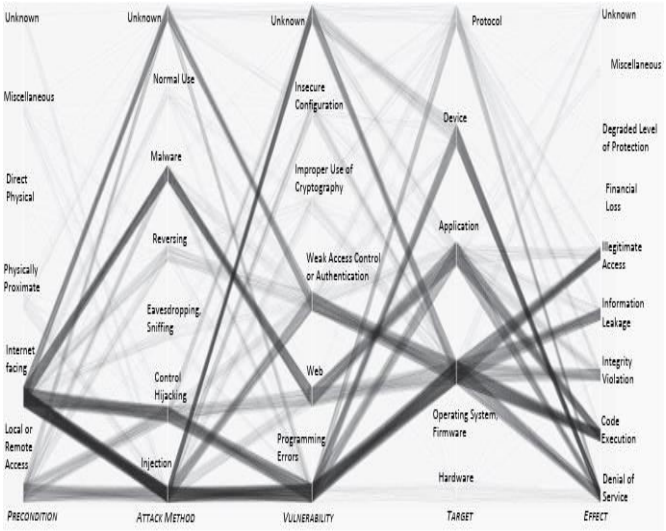

Fig 1 : Common attack scenarios

V CONCLUSION

This paper gives a complete outline of embedded systems security by depicting the two assaults and weaknesses. It empowers us to make an assault scientific classification which we utilized to characterize and depict normal assault situations against installed frameworks. The assault scientific categorization determined in this paper gives data on how an inserted framework can be attached. Besides, the organized information can help investigation furthermore, plan of frameworks including or in view of implanted gadgets during framework improvement lifecycle. The introduced assault scientific categorization likewise assists us with determining patterns in implanted framework security. Taking into account the assaults what's more, weaknesses talked about in this paper and the new patterns in machine-to-machine correspondences, as we would see it, Web confronting gadgets will keep on experiencing most of assaults. Additionally, our taxonomy's vulnerabilities and errors are comparable to those found in conventional IT systems. However, these problems can already be solved with the help of traditional IT systems' tools and solutions. We anticipate that the solutions will be implemented in customized embedded systems to meet the requirements of this industry. This scientific categorization is created inside an enormous scope research project tending to implanted frameworks security for wellbeing and crucial frameworks. Our following stage will be to further approve the scientific categorization in practical settings through various use cases drove by industry. In addition, the scientific categorization and the knowledge will be applied to security examination of digital physical frameworks to recognize and identify dangers in an orderly manner with decreased blunder and vulnerability

REFERENCES

[1] F. Vahid and T. Givargis, “Embedded system design: A unified hardware/software approach, Department of Computer Science and Engineering University of California, 1999.

[2] E. A. Lee, “Computing foundations and practice for cyber-physical systems: A preliminary report, University of California, Berkeley, Tech.Rep. UCB/EECS-2007-72, 2007.

[3] P. Marwedel, Embedded system design: Embedded systems foundations of cyber-physical systems. Springer Science & Business Media, 2010.

[4] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon, Security & Privacy, IEEE, vol. 9, no. 3, pp. 49–51, 2011.

[5] B. Schneier, "Security risks of embedded systems, https: //www.schneier.com/blog/archives/2014/01/security risks 9.html, January 2014.

[6] S. Parameswaran and T. Wolf, "Embedded systems security- an overview, Design Automation for Embedded Systems, vol. 12, no. 3, pp. 173–183, 2008.

[7]D. Kleidermacher and M. Kleidermacher, Embedded systems security: practical methods for safe and secure software and systems development. Elsevier, 2012.

[8] D. N. Serpanos and A. G. Voyiatzis, "Security challenges in embedded systems, ACM Transactions on Embedded Computing Systems (TECS), vol. 12, no. 1s, p. 66, 2013.

[9] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, and S. Moderator Ravi, "Security as a new dimension in embedded system design, in Proceedings of the 41st annual Design Automation Conference. ACM, 2004, pp. 753–760.

[10] P. Koopman, "Embedded system security, Computer, vol. 37, no. 7, pp. 95–97, 2004.

[11] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges, ACM Transactions on Embedded Computing Systems (TECS), vol. 3, no. 3, pp. 461–491, 2004.

[12] H. Holm, M. Ekstedt, and D. Andersson, "Empirical analysis of system level vulnerability metrics through actual attacks, Dependable and Secure Computing, IEEE Tran. on, vol. 9, no. 6, pp. 825–837, 2012.

[13] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world, in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 833–844.

[14] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares, in Proceedings of the 23rd USENIX Security Symposium. San Diego, CA, USA: USENIX Association, 2014, pp. 95–110.[Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-costin.pdf

[15] European Union Agency for Network and Information Security (ENISA), "Existing indicent taxonomies.

[16] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "Avoidit: A cyber attack taxonomy, University of Memphis, Technical Report CS-09-003, 2009. [Online]. Available: http://si.lopesgazzani.com.br/docentes/marcio/SegApp/CyberAttack Taxonomy IEEE Mag.pdf

[17] T. L. Nielsen, J. Abildskov, P. M. Harper, I. Papaeconomou, and R. Gani, "The capec database, Journal of Chemical & Engineering Data, vol. 46, no. 5, pp. 1041–1044, 2001.

[18] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks, Computers and Security, vol. 24, no. 1, pp. 31– 43, 2005. [Online]. Available:http://www.sciencedirect.com/science/article/pii/S0167404804001804

[19] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems, in (iThings/CPSCom'11, Washington, DC, USA, 2011.

[20] A. Dessiatnikoff, Y. Deswarte, E. Alata, and V. Nicomette, "Potential attacks on onboard aerospace systems, IEEE Security and Privacy, vol. 10, no. 4, pp. 71–74, Jul. 2012. [Online]. Available: http: //dx.doi.org/10.1109/MSP.2012.104

[21] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Szti panovits, "Taxonomy for description of cross-domain attacks on cps, in

Proceedings of the 2Nd ACM International Conference on High Condence Networked Systems, ser. HiCoNS 13. New York, NY,USA: ACM, 2013, pp. 135–142.
[22] MITRE Corporation, “Common Vulnerabilities and Exposures, https: //cve.mitre.org/, 1999-2015.
[23] M. Keefe, increase “Timeline: steadily Available: in Critical past infrastructure decade, 2012. Attacks [Online].http://www.computerworld.com/article/2493205/security0/ timeline--critical-infrastructure-attacks-increase-steadily-in-past-decade.html
[24] L. Apa and C. M. Penagos, “Compromising Industrial Facilities from 40 Miles Away , ser. BlackHat, 2013.
[25] E. Forner and B. Meixell, Out of Control: SCADA Device Exploitation, Cimation, 2013. [Online]. Available: https://media.blackhat.com/us-13/ US-13-Forner-Out-of-Control-Demonstrating-SCADA-WP.pdf
[26] J. W. Clarke, “RuggedCom-Backdoor Accounts in my SCADA net work? You dont say... http://seclists.org/fulldisclosure/2012/Apr/277, April 2012.
[27] R. Santamarta, SATCOM Terminals: Hacking by Air, Sea, and Land, IOActive, Inc., 2014. [Online]. Available:https://www.defcon.org/images/defcon-22/dc-22 presentations/Cerrudo/ DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf Exploiting
[28] J. Geovedi and R. Irayndi, “Hacking a bird in the sky: satellite trust relationship, 2008. [Online]. Available: http://www.sliim-projects.eu/docs/Hacking/D1T1-Jim Geovedi-Hacking a Bird in the Sky 2.0.pdf
[29] A. Costin and A. Francillon, “Ghost in the air(traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices, 2012. [Online]. Available: http://s3.eurecom.fr/docs/bh12us costin.pdf
[30] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, “Smart nest thermos stat: A smart syp in your home, ser. Black Hat, 2014.
[31] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces, in Proceedings of the 20th USENIX Conference on Security, ser. SEC11. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6.
[32] “Hacking the d-link dsp-w215 smart plug, http://www.devttys0.com/2014/05/hacking-the-d-link-dsp-w215-smart-plug/, /DEV/TTYS0, May 2014.
[33] Z. Cutlip, “Dlink dir-815 upnp command injection, http://shadow-file.blogspot.hu/2013/02/dlink-dir-815-upnp-command-injection.html, February 2012.
[34] A. Cui, M. Costello, and S. J. Stolfo, “When firmware modifications attack: A case study of embedded exploitation, in Proceedings of NDSS Symposium 2013, 2013.
[35] A. Costin and A. Francillon, “Short paper: A dangerous pyrotechnic composition: Fireworks, embedded wireless and insecurity-by-design, in Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks, ser. WiSec 14. New York, NY, USA: ACM, 2014, pp. 57–62.
[36] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song, “Take two software updates and see me in the morning:The case for software security evaluations of medical devices, in Proceedings of the 2Nd USENIX Conference on Health Security and Privacy, ser.

HealthSec11. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6.
[37] "CVE Details. [Online]. Available: http://www.cvedetails.com/.