JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-13, May 2019 E-ISSN: 2347-2693

Vulnerabilities, Threats and Attacks on SCADA, Mobile Networks and in IoT

Latha. P[1*], Andhe Pallavi[2]

[1,2] Dept. of Electronics and Instrumentation Engineering, RNS Institute of Technology, VTU, Bengaluru, India

[*]Corresponding Author: ashamanjunatha@yahoo.com, Tel.: 9538104144

DOI: https://doi.org/10.26438/ijcse/v7si13.1015 | Available online at: www.ijcseonline.org

Abstract— Ever since the emergence of 1G in mobile technology, evolution of new mobile generations have introduced various protocols and interfaces, high data transmission capacity making way for different vulnerabilities which allows for launch of attacks on network components. Performance of mobile networks and security is of a major concern.

Industrial networks and automation networks were isolated in a physical sense until the emergence of Supervisory Control and Data Acquisition (SCADA). Simplicity, more productivity, reduction in downtime for system adjustments are some advantages with the industrial networks going public on internet. The result is the increase in the number of attack vectors on the SCADA system.

IoT to define is a transformative approach providing numerous services over internet. Integrating the existing smart devices to the internet introduces security issues, threat of cyber attacks and crime. In this paper, we discuss the various vulnerabilities, threats and attacks on these three systems namely Mobile networks, SCADA systems, and IoT systems.

Keywords— Mobile networks, Mobile network security, SCADA systems, Internet of Things, security, vulnerabilities.

I. INTRODUCTION

Over the recent decades, mobile capability has expanded drastically and is expected to interconnect more than 30 billion devices by 2020. After 1G, 2G evolution gave more efficiency in data services and spectrum efficiency. 3G gives mobile broadband experience with high speed for data transmission. 4G architecture allows to deliver more capacity and better broadband experiences. It allows for seamless interoperability among different network technologies thereby increasing the security issues.

Several research papers[4]-[13] have reported the mobile network vulnerabilities against various threats such as Eavesdropping, interface flooding and Unauthorized data access, Malicious insider, Theft of service etc. Some of the attacks reported in 4G include signaling Denial of Service (DoS) attacks, Jamming based DoS attacks, Man-In-The- Middle(MITM) attacks, Spoofing attacks etc. Traffic redirection and Resynchronization attacks in LTE are reported in [14] and [15].

Physical layer security have also been reviewed in [15] and [16]-[18]. In [15] investigation on physical layer security threats of Worldwide Interoperability for Microwave Access(WiMax) and LTE and threats related to protocol stacks, network interfaces are done. [19] and [20] also reviews the threats and attacks on mobile devices. Author in [1] has focused on IP-based attacks, jamming and signaling attacks in the 4G networks.

A threat is the ability to gain unauthorized access to information, manipulate information and reduce the

system to unreliable or unusable state. Mobile core Several research papers[4]-[13] have reported the mobile network vulnerabilities against various threats such as Eavesdropping, interface flooding and Unauthorized data access, Malicious insider, Theft of service etc. Some of the attacks reported in

4G include signaling Denial of Service (DoS) attacks, Jamming based DoS attacks, Man-In-The-Middle(MITM) attacks, Spoofing attacks etc. Traffic redirection and Resynchronization attacks in LTE are reported in [14] and [15].

Physical layer security have also been reviewed in [12],13], [15] and [10]-[12]. In [15] investigation on physical layer security threats of Worldwide Interoperability for Microwave Access(WiMax) and LTE and threats related to protocol stacks, network interfaces are done. [19] and [20] also reviews the threats and attacks on mobile devices. Author in [1] has focused on IP-based attacks, jamming and signaling attacks in the 4G networks.

A threat is the ability to gain unauthorized access to information, manipulate information and reduce the system to unreliable or unusable state. Mobile core networks in 2G and 3G were not threat prone due to use of SS7. But in 4G and beyond technologies, the use of Diameter Signaling protocol for billing data, subscriber authentication, roaming etc are more vulnerable to various attacks.

Currently, the computing power, storage capacity of smart devices have improved with the reduction in the size of the smart device. Also the number of these devices connected to internet to provide service has increased. IoT provides an advantage of combining sensing, authentication, identification, computing so that information access is possible at any time. This has led to the increase in the potential threats and possible attacks against security of the system.

Section II contains the Classification of Attacks in Mobile Networks, Section III contains the Attacks on SCADA systems and Section IV discusses the IoT reference model from CISCO and discusses the vulnerabilities in IoT

II. CLASSIFICATION OF ATTACKS IN MOBILE NETWORKS

Attacks on the mobile networks are classified into four
groups namely
The first group is the threat from Internet.
Physical access to network entities is the second group. The third group being the Mobile device based attack. The last group is the Insider attacks.

These attacks can be the result from threats, which are classified into five groups namely
Loss of Availability, Loss of Confidentiality, Loss of Integrity,
Loss of Control and
Theft of Service.

In [21] and [22] discusses that the 4G mobile network attacks can be a result of failure in security requirements namely-
Application Security
Network Access Security
User Security
Network area Security
QoS maintenance and Physical Layer Security

Application Security relates to software, hardware and OS
integrity.
Network Access Security relates to Confidentiality, Authentication and Integrity
User Security relates to User Identity and authorization. Network area Security relates to confidentiality and Mobile Equipment location authentication.
QoS maintenance relates to the security provided against
Denial of Service attack.
Physical Layer Security relates to tampering resistance. Attack entry points in 4G mobile networks are
Access network Compromised smart mobile devices external 3rd party networks and Backhaul and core networks

III. ATTACKS ON SCADA SYSTEMS

Paper [21] discusses the SCADA exploitation over two decades. In [22,[23],[24],[25],[26] authors have reviewed the current attack vectors on SCADA systems and their counter measures. From the common vulnerabilities and exposures found online, the largest vulnerability group is the Remote Code execution, then Denial of Service and Injection attacks.

Attacks at PLC level

PLC's interact and operate with devices in the physical world and so various attacks on these PLC's will have a great impact on the physical entities. Attacks on PLC's are classified as Code Execution where malicious code is executed without authorization

Data Extraction where information is disclosed without authentication DoS where service is partially or fully degraded

Privilege Escalation is obtaining unauthorized privileges on the system

Attacks at Fieldbus-Level

Various fieldbus protocols such as Modbus[27],

FlexRay[28], Profinet[29] have inherent security flaws. An attacker can access the bus and either extract or inject messages into the systems. Man-In-The-Middle(MITM) and DoS are few such attacks.

Wireless system attacks

Some of the wireless protocols commonly used in industries

are Bluetooth[30], ZigBee[31], Radio Frequency Identifier(RFID)[43]etc. These protocols are encrypted, but they can be broken rendering the system unprotected. The encryption key can be easily recovered when ZigBee is configured in default mode.

Relay attacks are another problem in wireless networks. Using Bluetooth or RFID, the attacker can capture a packet and introduce it at another place in the network.

Spoofing and Impersonation also exists in wireless systems. In spoofing, an attacker enters the system in disguise and participate in the communication.

In Impersonation, an attacker claims to be an identity who he is not.

Attacker can jam the system with flooding of data resulting in Jamming attacks

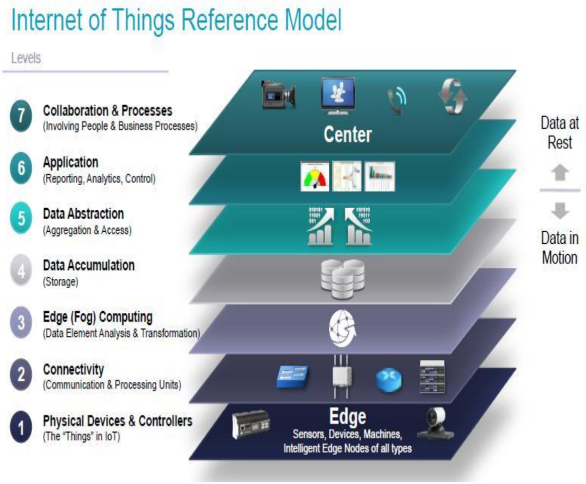
Attacks at Physical-Layer level

Attacks at this layer is most difficult. These attacks have great levels of inflicting damage to the system. Securing physical layer access is a critical task for industry.

In [31] the cyber attack vectors possible on SCADA systems are discussed. The threats are categorized as Software side threats, Hardware side threats and Communication sided threats. Unauthorized access to the physical location of SCADA damages the operational procedure.

IV. IOT REFERENCE MODEL FROM CISCO

Cisco's seven–level model is a widely accepted IoT reference model. In this model, the data flow is bidirectional. Figure 1 shows the CISCO IoT reference model

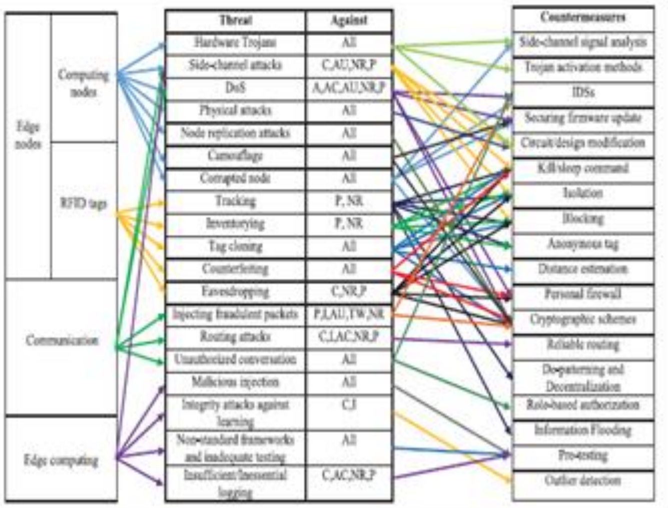

Internet of Things Reference Model
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion

Level-1 Edge devices: This consists of sensors, RFID

readers, controllers etc.
Level-2 Communication: where the components communicate between first and third levels and also among themselves
Level-3 Edge computing or Fog computing: Here the data processing is initiated. Here basic signal processing algorithms are implemented. The resources of the nodes decide the amount of computations
Level-4 Data accumulation: This level stores the unused data for future analysis through filtering, selective storing etc.
Level-5 Data abstraction: This level stores data for further processing and efficiency. The main tasks include normalization, De normalization and consolidating of data and indexing
Level-6 Applications: It looks into data or information interpretation. The software cooperates with data abstraction and data accumulation levels.
Level-7 Users and centers: It is the top level of IoT. Users run the application for their data available.
As per CIA-triad, IoT security are broken into three categories namely integrity, confidentiality and availability.

IoT Vulnerabilities
In [32] various security requirements to be met by a smart
thing are discussed. Security attack happens when any one of the security requirements are not met. The author discusses the vulnerabilities and attacks at each level of the edge side layer namely edge nodes, communication and edge computing.
This paper also discusses extensively on the various attacks and the counter measures. Figure 2 shows the attacks and the counter measures.

The attacks at the first level (edge nodes) include the hardware Trojan, Denial of Service etc. The types of attacks in DoS are Battery draining
Sleep deprivation and
Outage attacks which are discussed in detail. Other possible attacks at this layer are Tampering
Camouflage
Malicious node.



Attacks against RFID Tags are Eavesdropping
Tag Cloning Tampering/Physical Attacks Counterfeiting.

The second level (Communication) attacks include
Eavesdropping
Side-Channel Attacks
Dos Attacks
Routing Attacks and
Unauthorized conversation.

The third level(Edge computing level) attacks are Malicious Injection Integrity attacks against machine learning, Insufficient logging etc.

Open research problems
4G mobile network attacks viz., Dos and DDos and Jamming attacks are still an open issue.

V. CONCLUSION AND FUTURE SCOPE

Security issues in the mobile networks has been reviewed in this paper. Securing mobile networks and its protection is a major concern.
Since the emergence of IoT, various threats and attacks against security has increased drastically. This paper has tried to summarize on the security attacks in the mobile networks, SCADA systems and IoT. Given the wide range of applications, these threats are to be addressed aggressively.

REFERENCES

[1] SILVÈRE MAVOUNGOU1, GEORGES KADDOUM1, (Member, IEEE), MOSTAFA TAHA2, (Member, IEEE), AND GEORGES MATAR1 “*Survey on Threats and Attacks on Mobile Networks”* IEEE Access, Year: 2016 , Volume: 4, Page s: 4543 – 4572,IEEE Journals & Magazines

[2] A. Kumar, Y. Liu, J. Sengupta, and Divya. (Dec. 2010). “*Evolution of Mobile Wireless Communication Networks: 1G to 4G*.” [Online]. Available: http://www.iject.org/pdf/amit.pdf

[3] M. O§ul and S. Bakt_r, ``*Practical attacks on mobile cellular networks and possible counter measures,'' Future Internet*, vol. 5, no. 4, pp.474_489, 2013. [Online]. Available: http://www.mdpi.com/1999- 5903/5/4/474

[4] Y. Zheng, D. He, X. Tang, and H.Wang, ``*AKA and authorization scheme for 4G mobile networks based on trusted mobile platform,''* in *Proc. 5th Int. Conf. Inf. Commun. Signal Process.*, 2005, pp. 976_980.

[5] X. Li and Y. Wang, ``*Security enhanced authentication and key agreement protocol for LTE/SAE network,*'' in *Proc. 7th Int. Conf. Wireless*

[6] *Commun., Netw. Mobile Comput. (WiCOM)*, Sep. 2011, pp. 1_4.

[7] M. Liyanage and A. Gurtov, ``*Secured VPN models for LTE backhaul networks,''* in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2012,pp. 1_5.

[8] C.-K. Han and H.-K. Choi, ``*Security analysis of handover key management in 4G LTE/SAE networks,'' IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457_468, Feb. 2014.

[9] D. Yu and W. Wen, ``*Non-access-stratum request attack in E- UTRAN,''* in *Proc. Comput., Commun. Appl. Conf. (ComComAp)*, Jan.2012, pp. 48_53.

[10] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, ``*Effects of signaling attacks on LTE networks,''* in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl.Workshops (WAINA)*, Mar. 2013, pp. 499_504.

[11] R. Bassil, I. H. Elhajj, A. Chehab, and A. kayssi, ``*A resource reservation attack against LTE networks,''* in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2013, pp. 262_268.

[12] S. Park, S. Kim, J. Oh, M. Noh, and C. Im, ``*Threats and countermeasures on a 4G mobile network,''* in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2014, pp. 538_541.

[13] R. P. Jover, J. Lackey, and A. Raghavan, ``*Enhancing the security of LTE networks against jamming attacks,'' EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1_14, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1186/1687-417X-2014-7 C. Shahriar *et al.*, ``*PHY- layer resiliency in OFDM communications: A tutorial'' IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292_314,1st Quart., 2015

[14] Y. Park and T. Park, ``*A survey of security threats on 4G networks,''* in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1_6.

[15] B. Matt and C. Li, ``*A survey of the security and threats of the IMTadvanced requirements for 4G standards,''* in *Proc. IEEE Conf. Anthol.*, Jan. 2013, pp. 1_5.

[16] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, ``*Detection and mitigation of uplink control channel jamming in LTE,''* in *Proc. IEEE Military Commun. Conf.*, Oct. 2014, pp. 1187_1194.

[17] Y. Zou, J. Zhu, X. Wang, and L. Hanzo. (May 2015). “*A survey on wireless security: Technical challenges, recent advances and future trends*." [Online]. Available: https://arxiv.org/pdf/1505.07919.pdf

[18] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, ``*LTE/LTE-A jamming, spoo_ng, and snif_ng: Threat assessment and mitigation,'' IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54_61, Apr. 2016.

[19] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, ``*Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices,''* in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 96_111.

[20] M. La Polla, F. Martinelli, and D. Sgandurra, ``*A survey on security for mobile devices,'' IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446_471, 1st Quart., 2013.

[21] R. Muraleedharan and L. A. Osadciw, ``*Increasing QoS and security in 4G networks using cognitive intelligence*,'' in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1_6.

[22] C. B. Sankaran, ``*Network access security in next-generation 3GPP systems: A tutorial,'' IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84_91, Feb. 2009.

[23] Simon Duque Ant´on, Daniel Fraunholz, Christoph Lipps, Frederic Pohl, Marc Zimmermann and Hans D. Schotten, “*Two Decades of SCADA Exploitation: A Brief History*”, 2017 IEEE Conference on Application, Information and Network Security (AINS), 978-1-5386- 0725-1/17

[24] V. M. Igure, S. A. Laughter, and R. D. Williams, “*Security issues in scada networks,*” *Computers & Security*, vol. 25, pp. 498–506, 2006.

[25] B. Zhu, A. Joseph, and S. Sastry, “*A taxonomy of cyber attacks on scada systems*,” 2011 International Conference on Internet of Things and 4thInternational Conference on Cyber, Physical and Social Computing, pp. 380–388, 2011.

[26] P. S. Motta Pires and Oliveira, Luiz Affonso H. G., “*Security aspects of scada and corporate network interconnection: An overview*,” 2006,

International Conference on Dependability of Computer Systems, pp.127–134, 2006.

[27] J. Caswell, "*A survey of industrial control systems security*," 2011. [Online]. Available: https://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/

[28] B. Meixell and E. Forner, "*Out of control: Demonstrating scada exploitation,"* Las Vegas, July 2013. [Online]. Available: https://www.blackhat.com/us-13/

[29] MODICON Inc., 1996. [Online]. Available: http://www.modbus.org/docs/PI MBUS 300.pdf

[30]FlexRay Consortium, "*Flexray communications system protocol specification version 3.0.1*," 2010. [Online]. Available: https://svn.ipd.kit.edu/nlrp/public/FlexRay/FlexRay%E2%84%A2%20Proto col%20Specification%20Version%203.0.1.pdf

[29] PROFIBUS, "*Profinet specification*," 2017. [Online]. Available: http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-io-secification/display

[30] Bluetooth SIG, "Specification of the bluetooth system," 2010. [Online]. Available: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiY76 but3UAhWDWBoKHXnARUQFggpMAA&url=https%3A%2F%2Fwww.bluetooth.org%2Fdocman%2Fhandlers%2Fdownloaddoc.ashx%3Fdoc id%3D229737&usg=AFQjCNFY1IFeFAAWwimnoaWMsIRZQvPDSw&cad=rja [31] ZigBee Alliance, "*Zigbee specification*," 2004. [Online].

[32] *Arsalan Mosenia ; Niraj K. Jha, "A Comprehensive Study of ", IEEE Transactions on Emerging Topics in Computing, year: 2017 , Volume: 5 , Issue: 4 , Page s: 586 – 602, IEEE Journals & Magazines* *Security of Internet-of-Things*

AUTHORS PROFILE

Mrs. Latha P is currently pursuing Ph.D. in VTU, Belagavi. She is working as an Asst. Prof. in RNSIT, Bengaluru. She is having 10 years Experience in Teaching and 2 years research experience. Her area of research interest includes Data Security, Error Control Coding, Cross layer design and IoT

Dr. Andhe Pallavi is heading the Department of Electronics and Instrumentation at RNS Institute of Technology. She has 22 years of teaching experience. Her areas of research interest include Information Theory and Error Control Coding, Digital Signal Processing and Microcontrollers.