Springer Link

Security Challenges in IoT Cyber World

Security in Smart Cities: Models, Applications, and Challenges pp 171-191 | Cite as

- Chintan Patel (1)
- Nishant Doshi (1) Email author (doshinikki2004@gmail.com)

1. Department of Computer Science and Engineering, Pandit Deendayal Petroleum University, , Gandhinagar, India

Chapter
First Online: 05 November 2018

Part of the Lecture Notes in Intelligent Transportation and Infrastructure book series (LNITI)

Abstract

Internet of Things (IoT) has created revolutionary impact in the world of technology and social life of billions of people. “Things” in the IoT refer to the real world objects which gets cognitive and communicative capabilities with the help of smart sensors, cameras and other devices. Indeed, IoT is implanting its footprint in each domain (i.e. health care, transportation, electric grid, agriculture, retail, manufacturing) to make it smart. Like, smart health care uses smart wearable devices equipped with smart sensors and tracking systems to provide live connectivity between patient, doctor and hospitals. Similarly, intelligent transport provides quick response in the accident or other hazardous situations. Smart grid provides complete information about usage of electricity and controlling of power supply. Agriculture monitoring and irrigation of waters and fertilizer using smart agriculture can save lots of time and energy of the farmers. Smart retail and transport can help to track quality of food, to generate easy billing and to provide product recommendation to the customers based on their past shopping habits. Thus, IoT creates big comfort for the businesses, government and peoples in their work of day-to-day life. With the advancement in the comfort, IoT come up with many serious technological challenges. Reliable and secure implementation of IoT application is most important aspect for the long time adaption of IoT. Availability of internet connected tracking devices and environment capturing sensors keep track of personal life of people at the same time it transfer it via internet to the cloud. So to assure security triangle CIA (Confidentiality, Integrity and Availability) to the people is major challenge for the researchers and developers. Recent attacks using concept of ransomware, in which attackers was seeking bitcoins to enable blocked services has created big financial damage to many people. In this chapter, we have discussed major security challenges for

the IoT, major cyber threats, attacks and remedies on various IoT parts and applications. Importance of role and requirement of light weight cryptography in the IoT is also discussed in this chapter.

Keywords

IoT Cyber security Ransomware Confidentiality Integrity Machine learning Industry 4.0 Smart grid Smart agriculture

This work was completed with the support of our Family, Friends and Guide.

Notes

Acknowledgements

We are thankful to editors of this book who have taken their keen interest in our chapter proposal and support us in each stage. We also thankful to reviewers who given their comments for improvement of this chapter. Many thanks to all well wishers and supporters.

References

1. Kevin A (2009) That 'Internet of Things' Thing. RFID J. Eprint: http://www.rfidjournal.com/articles/pdf?4986 (http://www.rfidjournal.com/articles/pdf?4986)
2. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a Survey. Comput Netw 54(15):2787–2805. ISSN: 1389-1286. https://doi.org/10.1016/j.comnet.2010.05.010 (https://doi.org/10.1016/j.comnet.2010.05.010) CrossRef (https://doi.org/10.1016/j.comnet.2010.05.010) Google Scholar (http://scholar.google.com/scholar_lookup?title=The%20Internet%20of%20Things%3A%20A%20survey&author=Luigi.%20Atzori&author=Antonio.%20Iera&author=Giacomo.%20Morabito&journal=Computer%20Networks&volume=54&issue=15&pages=2787-2805&publication_year=2010)
3. Jamoussi B (2005) Executive summary on "The internet of things". eprint: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf (https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf)
4. Li S, Xu LD, Zhao S (2015) The internet of things: a survey. Inf Syst Frontiers 17(2):243–259. ISSN: 1387-3326. https://doi.org/10.1007/s10796-014-9492-7 (https://doi.org/10.1007/s10796-014-9492-7)

CrossRef (https://doi.org/10.1007/s10796-014-9492-7)
Google Scholar (http://scholar.google.com/scholar_lookup?title=The%20internet%20of%20things%3A%20a%20survey&author=Shancang.%20Li&author=Li%20Da.%20Xu&author=Shanshan.%20Zhao&journal=Information%20Systems%20Frontiers&volume=17&issue=2&pages=243-259&publication_year=2014)

5. Statista (2016) IOT Statistics by statista https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/) (visited on 01/13/2018)

6. Carsten M (2017) Security and privacy in the internet of things. J Cyber Policy 2(2):155–184. eprint: https://doi.org/10.1080/23738871.2017.1366536 (https://doi.org/10.1080/23738871.2017.1366536)
CrossRef (https://doi.org/10.1080/23738871.2017.1366536)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Security%20and%20privacy%20in%20the%20internet%20of%20things&author=Carsten.%20Maple&journal=Journal%20of%20Cyber%20Policy&volume=2&issue=2&pages=155-184&publication_year=2017)

7. Al-Fuqaha A et al (2015) Internet of things: a survey on enabling technologies, Protocols, and Applications. IEEE Commun Surveys Tutorials 17(4):2347–2376. ISSn: 1553-877X. https://doi.org/10.1109/COMST.2015.2444095 (https://doi.org/10.1109/COMST.2015.2444095)
CrossRef (https://doi.org/10.1109/COMST.2015.2444095)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Internet%20of%20Things%3A%20A%20Survey%20on%20Enabling%20Technologies%2C%20Protocols%2C%20and%20Applications&author=Ala.%20Al-Fuqaha&author=Mohsen.%20Guizani&author=Mehdi.%20Mohammadi&author=Mohammed.%20Aledhari&author=Moussa.%20Ayyash&journal=IEEE%20Communications%20Surveys%20%26%20Tutorials&volume=17&issue=4&pages=2347-2376&publication_year=2015)

8. Xu LD, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Informatics 10(4):2233–2243. ISSN: 1551-3203. https://doi.org/10.1109/TII.2014.2300753 (https://doi.org/10.1109/TII.2014.2300753)
CrossRef (https://doi.org/10.1109/TII.2014.2300753)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Internet%20of%20Things%20in%20Industries%3A%20A%20Survey&author=Li%20Da.%20Xu&author=Wu.%20He&author=Shancang.%20Li&journal=IEEE%20Transactions%20on%20Industrial%20Informatics&volume=10&issue=4&pages=2233-2243&publication_year=2014)

9. Alam M, Ferreira J, Fonseca J (2016) Introduction to intelligent transportation systems. In: Alam M, Ferreira J, Fonseca J (eds) Intelligent transportation systems: dependable vehicular communications for improved road safety. Springer International Publishing, Cham, pp 1–17. ISBN 978-3-319-28183-4. https://doi.org/10.1007/978-3-319-28183-4_1 (https://doi.org/10.1007/978-3-319-28183-4_1)
CrossRef (https://doi.org/10.1007/978-3-319-28183-4)

Google Scholar (http://scholar.google.com/scholar_lookup?title=Introduction%20to%20Intelligent%20Transportation%20Systems&author=Muhammad.%20Alam&author=Joaquim.%20Ferreira&author=Jos%C3%A9.%20Fonseca&pages=1-17&publication_year=2016)

10. Zhang J et al (2011) Data-driven intelligent transportation systems: a Survey. IEEE Trans Intell Transport Syst 12(4):1624–1639. ISSN: 1524-9050. https://doi.org/10.1109/TITS.2011.2158001 (https://doi.org/10.1109/TITS.2011.2158001)
CrossRef (https://doi.org/10.1109/TITS.2011.2158001)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Data-Driven%20Intelligent%20Transportation%20Systems%3A%20A%20Survey&author=Junping.%20Zhang&author=Fei-Yue.%20Wang&author=Kunfeng.%20Wang&author=Wei-Hua.%20Lin&author=Xin.%20Xu&author=Cheng.%20Chen&journal=IEEE%20Transactions%20on%20Intelligent%20Transportation%20Systems&volume=12&issue=4&pages=1624-1639&publication_year=2011)

11. Baig MM, Gholamhosseini H (2013) Smart Health Monitoring systems: an overview of design and modeling. J Med Syst 37(2):9898. ISSN: 1573-689X. https://doi.org/10.1007/s10916-012-9898-z (https://doi.org/10.1007/s10916-012-9898-z)

12. Smart hospitals security and resilience for smart health service and infrastructures. In: (2016). Eprint: https://doi.org/10.2824/28801 (https://doi.org/10.2824/28801)

13. Alam MR, Reaz MBI, Ali MAM (2012) A Review of Smart homes past, present, and future. IEEE Trans Syst Man, and Cyber Part C (Appl and Rev) 42(6):1190–1203. ISSN: 1094-6977. https://doi.org/10.1109/TSMCC.2012.2189204 (https://doi.org/10.1109/TSMCC.2012.2189204)
CrossRef (https://doi.org/10.1109/TSMCC.2012.2189204)
Google Scholar (http://scholar.google.com/scholar_lookup?title=A%20Review%20of%20Smart%20Homes%E2%80%94Past%2C%20Present%2C%20and%20Future&author=Muhammad%20Raisul.%20Alam&author=Mamun%20Bin%20Ibne.%20Reaz&author=Mohd%20Alauddin%20Mohd.%20Ali&journal=IEEE%20Transactions%20on%20Systems%2C%20Man%2C%20and%20Cybernetics%2C%20Part%20C%20%28Applications%20and%20Reviews%29&volume=42&issue=6&pages=1190-1203&publication_year=2012)

14. Khan M, Silva BN, Han K (2016) Internet of Things Based Energy Aware Smart Home Control System. IEEE Access 4:7556–7566. ISSN: 2169-3536. https://doi.org/10.1109/ACCESS.2016.2621752 (https://doi.org/10.1109/ACCESS.2016.2621752)
CrossRef (https://doi.org/10.1109/ACCESS.2016.2621752)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Internet%20of%20Things%20Based%20Energy%20Aware%20Smart%20Home%20Control%20System&author=Murad.%20Khan&author=Bhagya%20Nathali.%20Silva&author=Kijun.%20Han&journal=IEEE%20Access&volume=4&pages=7556-7566&publication_year=2016)

15. Fang X et al (2012) Smart grid : the new and improved power grid: a survey. IEEE Commun Surveys Tutorials 14(4):944–980. ISSN: 1553-877X.

https://doi.org/10.1109/SURV.2011.101911.00087 (https://doi.org/10.1109/SURV.2011.101911.00087)
CrossRef (https://doi.org/10.1109/SURV.2011.101911.00087)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Smart%20Grid%20%E2%80%94%20The%20New%20and%20Improved%20Power%20Grid%3A%20A%20Survey&author=Xi.%20Fang&author=Satyajayant.%20Misra&author=Guoliang.%20Xue&author=Dejun.%20Yang&journal=IEEE%20Communications%20Surveys%20%26%20Tutorials&volume=14&issue=4&pages=944-980&publication_year=2012)

16. Mei S, Chen L (2013) Recent advances on smart grid technology and renewable energy integration. Sci China Technol Sci 56(12):3040–3048. ISSN: 1869-1900. https://doi.org/10.1007/s11431-013-5414-z (https://doi.org/10.1007/s11431-013-5414-z)
CrossRef (https://doi.org/10.1007/s11431-013-5414-z)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Recent%20advances%20on%20smart%20grid%20technology%20and%20renewable%20energy%20integration&author=ShengWei.%20Mei&author=LaiJun.%20Chen&journal=Science%20China%20Technological%20Sciences&volume=56&issue=12&pages=3040-3048&publication_year=2013)

17. Benzi F et al (2011) Electricity smart meters interfacing the households. IEEE Trans Ind Electron 58(10):4487–4494. ISSN: 0278-0046. https://doi.org/10.1109/TIE.2011.2107713 (https://doi.org/10.1109/TIE.2011.2107713)
CrossRef (https://doi.org/10.1109/TIE.2011.2107713)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Electricity%20Smart%20Meters%20Interfacing%20the%20Households&author=F..%20Benzi&author=N..%20Anglani&author=E..%20Bassi&author=L..%20Frosini&journal=IEEE%20Transactions%20on%20Industrial%20Electronics&volume=58&issue=10&pages=4487-4494&publication_year=2011)

18. Alahakoon D, Yu X (2016) Smart electricity meter data intelligence for future energy systems: a survey. IEEE Trans Ind Informatics 12(1):425–436. ISSN: 1551-3203. https://doi.org/10.1109/TII.2015.2414355 (https://doi.org/10.1109/TII.2015.2414355)
CrossRef (https://doi.org/10.1109/TII.2015.2414355)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Smart%20Electricity%20Meter%20Data%20Intelligence%20for%20Future%20Energy%20Systems%3A%20A%20Survey&author=Damminda.%20Alahakoon&author=Xinghuo.%20Yu&journal=IEEE%20Transactions%20on%20Industrial%20Informatics&volume=12&issue=1&pages=425-436&publication_year=2016)

19. Haverkort BR, Zimmermann A (2017) Smart industry: how ICT will change the game. IEEE Internet Comput 21(1):8–10. ISSN: 1089-7801. https://doi.org/10.1109/MIC.2017.22 (https://doi.org/10.1109/MIC.2017.22)
CrossRef (https://doi.org/10.1109/MIC.2017.22)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Smart%20Industry%3A%20How%20ICT%20Will%20Change%20the%20Game%21&author=Boudewijn%20R..%20Haverkort&author=Armin.%20Zimmermann&journal=IEEE%20Internet%20Computing&volume=21&issue=1&pages=8-10&publication_year=2017)

20. The internet of things reference model (2014) eprint: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4 (http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)

21. Khan R, Khan SU, Zaheer R, Khan S (2012) Future Internet: The internet of things architecture, possible applications and key challenges. In 2012 10th International Conference on Frontiers of Information Technology, pp 257–260. https://doi.org/10.1109/FIT.2012.53 (https://doi.org/10.1109/FIT.2012.53)

22. Yang Z et al (2011) Study and application on the architecture and key technologies for IOT. In: 2011 International Conference on Multimedia Technology. pp. 747–751. https://doi.org/10.1109/ICMT.2011.6002149 (https://doi.org/10.1109/ICMT.2011.6002149)

23. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng
Google Scholar (https://scholar.google.com/scholar?q=Sethi%20P%2C%20Sarangi%20SR%20%282017%29%20Internet%20of%20things%3A%20architectures%2C%20protocols%2C%20and%20applications.%20J%20Electr%20Comput%20Eng)

24. Ray PP (2016) A survey on internet of things architectures. J King Saud University - Comput Inf Sci ISSN: 1319-1578. https://doi.org/10.1016/j.jksuci.2016.10.003 (https://doi.org/10.1016/j.jksuci.2016.10.003). URL: http://www.sciencedirect.com/science/article/pii/S1319157816300799 (http://www.sciencedirect.com/science/article/pii/S1319157816300799)
CrossRef (https://doi.org/10.1016/j.jksuci.2016.10.003)
Google Scholar (http://scholar.google.com/scholar_lookup?title=A%20survey%20on%20Internet%20of%20Things%20architectures&author=P.P..%20Ray&journal=Journal%20of%20King%20Saud%20University%20-%20Computer%20and%20Information%20Sciences&volume=30&issue=3&pages=291-319&publication_year=2018)

25. Mosenia A, Jha NK (2017) A Comprehensive Study of Security of Internet-of-Things. IEEE Trans Emerging Topics in Comput 5(4):586–602. https://doi.org/10.1109/TETC.2016.2606384 (https://doi.org/10.1109/TETC.2016.2606384)
CrossRef (https://doi.org/10.1109/TETC.2016.2606384)
Google Scholar (http://scholar.google.com/scholar_lookup?title=A%20Comprehensive%20Study%20of%20Security%20of%20Internet-of-Things&author=Arsalan.%20Mosenia&author=Niraj%20K..%20Jha&journal=IEEE%20Transactions%20on%20Emerging%20Topics%20in%20Computing&volume=5&issue=4&pages=586-602&publication_year=2017)

26. Elmaghraby AS, Losavio MM (2014) Cyber security challenges in Smart Cities: safety, security and privacy. J Adv Res 5(4):491–497. ISSN: 2090-1232. https://doi.org/10.1016/j.jare.2014.02.006 (https://doi.org/10.1016/j.jare.2014.02.006). URL: http://www.sciencedirect.com/science/article/pii/S2090123214000290 (http://www.sciencedirect.com/science/article/pii/S2090123214000290)
CrossRef (https://doi.org/10.1016/j.jare.2014.02.006)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Cyber%20security%20challenges%20in%20Smart%20Cities%3A%20Safety

%2C%20security%20and%20privacy&author=Adel%20S..%20Elmaghraby&author=Michael%20M..%20Losavio&journal=Journal%20of%20Advanced%20Research&volume=5&issue=4&pages=491-497&publication_year=2014)

27. Zeadally S, Isaac JT, Baig Z (2016) Security attacks and solutions in electronic health (E-health) systems. J Med Syst 40(12):1–12. ISSN: 0148-5598. https://doi.org/10.1007/s10916-016-0597-z (https://doi.org/10.1007/s10916-016-0597-z)

28. Sfar AR et al (2017) A roadmap for security challenges in the internet of things. Digital Commun and Networks (2017). ISSN: 2352-8648. https://doi.org/10.1016/j.dcan.2017.04.003 (https://doi.org/10.1016/j.dcan.2017.04.003). URL: http://www.sciencedirect.com/science/article/pii/S2352864817300214 (http://www.sciencedirect.com/science/article/pii/S2352864817300214) CrossRef (https://doi.org/10.1016/j.dcan.2017.04.003) Google Scholar (http://scholar.google.com/scholar_lookup?title=A%20roadmap%20for%20security%20challenges%20in%20the%20Internet%20of%20Things&author=Arbia.%20Riahi%20Sfar&author=Enrico.%20Natalizio&author=Yacine.%20Challal&author=Zied.%20Chtourou&journal=Digital%20Communications%20and%20Networks&volume=4&issue=2&pages=118-137&publication_year=2018)

29. Rodosek GD, Golling M (2013) Cyber security: challenges and application areas. In: Essig M et al (eds) Supply chain safety management: security and robustness in logistics. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp 179–197. ISBN 978-3-642-32021-7. https://doi.org/10.1007/978-3-642-32021-7_11 (https://doi.org/10.1007/978-3-642-32021-7_11) CrossRef (https://doi.org/10.1007/978-3-642-32021-7_11) Google Scholar (http://scholar.google.com/scholar_lookup?title=Cyber%20Security%3A%20Challenges%20and%20Application%20Areas&author=Gabi%20Dreo.%20Rodosek&author=Mario.%20Golling&pages=179-197&publication_year=2013)

30. Alexander RD, Panguluri S (2017) Cybersecurity terminology and frameworks. In: Clark RM, Hakim S (eds) Cyber-physical security: protecting critical infrastructure at the state and local level. Springer International Publishing, Cham, pp 19–47. ISBN 978-3-319-32824-9. https://doi.org/10.1007/978-3-319-32824-9_2 (https://doi.org/10.1007/978-3-319-32824-9_2) Google Scholar (http://scholar.google.com/scholar_lookup?title=Cybersecurity%20Terminology%20and%20Frameworks&author=Richard%20D..%20Alexander&author=Srinivas.%20Panguluri&pages=19-47&publication_year=2016)

31. Yan, Z, Zhang, P, Vasilakos AV (2014) A survey on trust management for Internet of Things. J Network Comput Appl 42:120–134. ISSN: 1084-8045. https://doi.org/10.1016/j.jnca.2014.01.014 (https://doi.org/10.1016/j.jnca.2014.01.014). URL: http://www.sciencedirect.com/science/article/pii/S1084804514000575 (http://www.sciencedirect.com/science/article/pii/S1084804514000575) CrossRef (https://doi.org/10.1016/j.jnca.2014.01.014) Google Scholar (http://scholar.google.com/scholar_lookup?title=A%20survey%20on%20trust%20management%20for%20Internet%20of%2

0Things&author=Zheng.%20Yan&author=Peng.%20Zhang&author=Athanasios%20V..%20Vasilakos&journal=Journal%20of%20Network%20and%20Computer%20Applications&volume=42&pages=120-134&publication_year=2014)

32. Sicari S et al (2015) Security, privacy and trust in Internet of Things: The road ahead. Comput Networks 76:146–164. ISSN: 1389-1286. https://doi.org/10.1016/j.comnet.2014.11.008 (https://doi.org/10.1016/j.comnet.2014.11.008). URL: http://www.sciencedirect.com/science/article/pii/S1389128614003971 (http://www.sciencedirect.com/science/article/pii/S1389128614003971) CrossRef (https://doi.org/10.1016/j.comnet.2014.11.008) Google Scholar (http://scholar.google.com/scholar_lookup?title=Security%2C%20privacy%20and%20trust%20in%20Internet%20of%20Things%3A%20The%20road%20ahead&author=S..%20Sicari&author=A..%20Rizzardi&author=L.A..%20Grieco&author=A..%20Coen-Porisini&journal=Computer%20Networks&volume=76&pages=146-164&publication_year=2015)

33. Liu J, Xiao Y, Chen CLP (2012) Internet of Things' Authentication and Access Control. Int J Secur Netw 7(4):228–241. ISSN: 1747-8405. https://doi.org/10.1504/IJSN.2012.053461 (https://doi.org/10.1504/IJSN.2012.053461) CrossRef (https://doi.org/10.1504/IJSN.2012.053461) Google Scholar (http://scholar.google.com/scholar_lookup?title=Internet%20of%20things%27%20authentication%20and%20access%20control&author=Jing.%20Liu&author=Yang.%20Xiao&author=C.L.%20Philip.%20Chen&journal=International%20Journal%20of%20Security%20and%20Networks&volume=7&issue=4&pages=228&publication_year=2012)

34. Singh S et al (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Humanized Comput. ISSN: 1868-5145. https://doi.org/10.1007/s12652-017-0494-4 (https://doi.org/10.1007/s12652-017-0494-4)

35. Turan MS, Mouha N, McKay KA, Bassham L (2017) Report on lightweight cryptography. National institute of standards and technologies, department of US and commerce. https://doi.org/10.6028/NIST.IR.8114 (https://doi.org/10.6028/NIST.IR.8114)

36. Perry JS (2017) Anatomy of an IoT malware attack. URL: https://www.ibm.com/developerworks/library/iot-anatomy-iot-malware-attack/ (https://www.ibm.com/developerworks/library/iot-anatomy-iot-malware-attack/) (visited on 01/13/2018)

37. Greenberg A (2017) The reaper IoT botnet has already infected a million networks. URL: https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/ (https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/) (visited on 01/13/2018)

38. CISCO (2017) Annual cyber security report. URL: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf (https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf) (visited on 01/13/2018)

39. Grange W (2017) Hajime worm battles Mirai for control of the Internet of Things. https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things (https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things) (visited on 01/13/2018)

40. Cimpanu C (2017) BrickerBot author claims he bricked two million devices. https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/ (https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/) (visited on 01/13/2018)

41. woolaston V (2017) WannaCry ransomware: what is it and how to protect yourself http://www.wired.co.uk/article/wannacry-ransomware-virus-patch (http://www.wired.co.uk/article/wannacry-ransomware-virus-patch) (visited on 01/13/2018)

42. Hatmaker T (2017) A new ransomware attack called bad rabbit looks related to notPetya. https://techcrunch.com/2017/10/24/badrabbit-notpetya-russia-ukraine-ransomware-malware/ (https://techcrunch.com/2017/10/24/badrabbit-notpetya-russia-ukraine-ransomware-malware/) (visited on 01/13/2018)

43. McAfee Labs (2017) Threat prediction for 2017. https://www.mcafee.com/in/resources/reports/rp-threats-predictions-2017.pdf (https://www.mcafee.com/in/resources/reports/rp-threats-predictions-2017.pdf) (visited on 01/13/2018)

44. Symantec (2016) Internet security threat report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf) (visited on 01/13/2018)

45. Kumar M (2016) Irongate new stuxnet-like malware targets industrial control systems. https://thehackernews.com/2016/06/irongate-stuxnet-malware.html (https://thehackernews.com/2016/06/irongate-stuxnet-malware.html) (visited on 01/13/2018)

46. williams F (2016) Understanding exploit kits: how they work and how to stop them. https://blog.barkly.com/how-exploit-kits-work (https://blog.barkly.com/how-exploit-kits-work) (visited on 01/13/2018)

47. Fotiguard SE Team (2017) Reaper: the next evolution of IoT botnets. https://blog.fortinet.com/2017/11/16/reaper-the-next-evolution-of-iot-botnets (https://blog.fortinet.com/2017/11/16/reaper-the-next-evolution-of-iot-botnets) (visited on 01/13/2018)

48. Dobbins R, Bjarnason S (2016) Mirai IoT Botnet Description and DDoS Attack Mitigation. https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/ (https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/) (visited on 01/13/2018)

49. Ballano M, Wueest C (2015) Insecurity in the internet of things. https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/ (https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/) (visited on 01/13/2018)

50. Zhou Y, Feng D (2005) Side-channel attacks: ten years after its publication and the impacts on cryptographic module security testing. zyb@is.iscas.ac.cn 13083 received 27 Oct 2005. http://eprint.iacr.org/2005/388 (http://eprint.iacr.org/2005/388)

51. Rayome AD (2017) DDoS attacks increased 91 percentage in 2017 thanks to IoT. https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/ (https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/) (visited on 01/13/2018)

52. Stacheldraht (2016) DDOS ATTACK. https://en.wikipedia.org/wiki/Denial-of-service_attack#/media/File:Stachledraht_DDos_Attack.svg (https://en.wikipedia.org/wiki/Denial-of-service_attack#/media/File:Stachledraht_DDos_Attack.svg) (visited on 01/13/2018)

Copyright information

About this chapter

Cite this chapter as:

Patel C., Doshi N. (2019) Security Challenges in IoT Cyber World. In: Hassanien A., Elhoseny M., Ahmed S., Singh A. (eds) Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham

- First Online 05 November 2018
- DOI https://doi.org/10.1007/978-3-030-01560-2_8
- Publisher Name Springer, Cham
- Print ISBN 978-3-030-01559-6
- Online ISBN 978-3-030-01560-2
- eBook Packages Intelligent Technologies and Robotics

Personalised recommendations