International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 2.635| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 5, September-October 2017 ||

The Applicability of Various Cybersecurity Services to Prevent Attacks on Smart Homes

Pankit Arora[1*], Sachin Bharadwaj[2]

Data Analyst, Innovaccer Analytics Pvt. Ltd., India[1]

Assistant Manager (GRC), EXL Service Pvt Ltd. India[2]

ABSTRACT: With connected home ecosystems in the future, the threats of cybercrime and cybersecurity are greater than ever. The bulk of research efforts are focused on the defence mechanisms of national and cooperative infrastructures, oblivious to the fact that one of the weakest links in these systems comes from the devices utilised in connected smart homes of today and tomorrow. A research that looks at the implications and challenges of cyber security for smart devices in smart homes includes the report as one of its components. In order to provide users with access to a variety of features and capabilities, we provide some pertinent background information as well as the factors that are driving the rise and necessity for seamless smart device connectivity. The paper highlights the fact that while these devices provide more features and functionality, they also introduce new risks. Subsequently, current cyber security issues related to smart devices within connected homes discussed and analyzed.

KEYWORDS: Cybercrime, cyber physical systems, connected home, mobile malware, smart device security; Data Analytics; Big Data; Apache Spark; Anomaly based algorithm; Classification algorithms.

I. INTRODUCTION

It is difficult to ignore the issue of cyber security in reference to the growing presence and usage of smart devices within home and workplace around the world. They are conveniently smarter, lighter, portable and with excellent storage and connectivity capabilities. This not only apply to mobile and tablets but to the whole concept of white goods within the domain of Internet of Things (IoT) [1-9]. Although this provides many benefits to home users, it also gives rise to new security threats. We therefore need to ensure that relevant policies and tools are developed to protect the vulnerable. The concept of connected home is not only about allowing devices to be connected; it is also about "content anywhere" and information sharing. Although this provides many advantages to the home user, but the resulting security and privacy issues not been addressed. This has been on the rather for some time in the form of Personal Networks.

In a personal context, concepts such as the Home Network and the Personal Area Network (PAN) focus on facilitating the interconnection of Personal Computers as well as other smart devices. Recent development means that other types of networks such as a Vehicular Area Network (VAN) are becoming common. The key defining characteristic of all of these networks is that the network topology relates to a geographic locality (by means of a ―local area‖ or ―proximity). This connotes that the network only includes devices and systems that are present in a specific area, while at the same time the devices can be connected and reconnected seamlessly [10-21]. Use of smart devices within smart environments generates an ever-increasing amount of data,

often without the consent of the consumer, or without the user being fully aware of the implications of sharing their personal data or using and sharing these devices. Hence, in some instances, a user centric-approach in designing such networks to facilitate users' involvement and control is needed. Researchers define the concept of a Personal Network (PN). They envisioned the personal network as a dynamic extension of the PAN to encompass the user's home network as well as other networks such as a VAN. A recent example of the implementation of a PN is the EU FP7 research project, webinos. This project has developed and demonstrated architecture for creating and using personal networks that span across the PAN (mobile), home and vehicle environments as well as cloud-based functionality. The webinos project also presents a model for communicating between different personal networks.

We have seen the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilities to users. Nevertheless, we also know the vulnerabilities that exist inside of it. However, these vulnerabilities normally considered for the larger infrastructures and little attention to the cyber security threats that can be resulted from the usage and power of smart devices because of IoT. The smart spaces are interconnected, with powerful smart devices (smartphones, tables, etc.) [22-29]. We also have the backbone, the power grid that powers our nations. Those two are coming together. Moreover, the smart meter on your home or business is now

allowing that connectivity as well as home services or the interconnected powerful smart devices. The example of the smart grid also provides means of controlling and monitoring smart grid infrastructures via the use of portable smart device. The vulnerability of the connected home and development within the energy industry's new wireless smart grid will inevitably lead to lights out for everyone while the multitude of interconnected smart devices in IoT will become a hotplate for cyber-attack or robot network (botnet) and security nightmare for smart space users and possibly national infrastructures as a whole.

Latest research reported that on average one modern person own three internet-connected smart devices such as smartphone and tablet. According to market analysts, consumers spend over USD2 trillion a year on devices, services and content from three perspectives: the devices consumers use; the content, applications and services they support; and the behaviour and demographics that drive their purchasing decisions and buying patterns [30-39]. We also have seen the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilitiesto users. While these devices provide more features and functionality, they also introduce new risks. Therefore, because of the ubiquity of smart devices, and their evolution as computing platforms, as well as the powerful processor used in smart devices has made them suitable objects for inclusion in a cyber bot. Smart devices are now widely used by billions of users due to their enhanced computing ability, practicality and efficient Internet access, thanks to the advanced of solid-state technologies. Moreover, smart devices typically contain a large amount of sensitive personal and corporate data and used in online payments and other sensitive transactions.

The wide spread use of open-source smart device platforms such as Android and third-party applications made available to the public also provides more opportunities and attractions for malware creators. Therefore,for now and the near future smart devices will become one of the most lucrative targets for cybercriminals. Another more worrying impact of such hacking capability is enabling hackers use the vast resources of the home network to turn it to a botnet in order to launch a cyber-attack on nationalinfrastructures. There are some Android based apps that when downloaded from a third party are capable of accessing the root functionality of devices and turning them into botnet components without the users' explicit consent. People could easily and unwittingly download malware to their smart devices or fall prey to "man in the middle" attacks where data thieves pose as a legitimate body, intercept and harvest sensitive information, and then forward it to the legitimate recipient.

In 2011,over 50 Android apps were pulled from theAndroid Market because they contained malware—they werecopies of apps from legitimate publishers that were modified to include two root exploits and a rogue app downloader. The main focus of this paper in twofold: firstly to provide and highlight the possible threats and vulnerability of smart devices, secondly to analyze the challenges involved in detecting mobile malware in smart devices as well as other threats within connected home ecosystem futures. The rest of the paper is organized as follows. In section 2 we provide detailed analysis of the security threats on smart devices and their links with cyber security. We identified mobile malware as well as others threats as the main issues and we discussed it in more details in Section 3. The paper is concluded in section 4.

II. SECURITY THREATS ON SMART DEVICES

The weakest link in any IT security chain is the user. Thehuman factor is the most challenging aspect of mobile device security. Home users generally assume that everything will work just as it should, relying on a devices' default settings without referring to complex technical manuals. Therefore, service and content providers, and hardware vendors need tobe aware of their responsibilities in maintaining networksecurity and content management on the devices theyprovide. Service providers might also have the opportunity toprovide add-on security services to complement theweaknesses of the devices.

The issue of cyber security is much closer to home environment. Hence, the problem of cyber security extends beyond computers, it also a threat to portable devices. Many electronic devices used at home are practically a computer from mobile phones, video consoles and car navigation systems. While these devices provide more features and functionality, they also introduce new risks. Attackers may be able to exploit of these technological progressions to target devices previously considered as secure.

The information stored and managed within such devices and home networks forms part of individuals Critical Information Infrastructure (CII) as identified by the POST note on cyber security in the UK. For example, an attacker may be able to contaminate your smart device with a virus, steal your mobile phone or wireless service, or access the data on your tablet. Not only do these activities have implications for your personal information, but they could also have serious consequences if you also kept corporate information on your smart device.

According to Juniper Networks report, 76 percent ofmobile users are relying on their mobile devices to access their

most sensitive personal information, such as online banking or personal medical information. This trend is even more noticeable with those who also use their personal mobile devices for business purposes. Nearly nine in ten (89 percent) business users, report they use their mobile device to access sensitive work-related information.

Another more worrying impact is the ability of cybercriminals using the vast resources of the network to turn it to a botnet and lunch a cyber-attack on national critical infrastructures. Juniper Networks Mobile Threat Centre (MTC) reported that in 2011 there were unparalleled increase of mobile malware attacks with a 155 percent increase from the previous year across all platforms.

While it may sound overwhelming, devices such as TVs, digital picture frames, smart meters and e-readers are quite vulnerable and competent of causing problems on your network. The next few years will provide various types of malware developers to explore unlikely methods of achieving their evil goals. Smartphones are not invulnerable and Macs can get malware, such as CVE-2012-0507vulnerability.

Android-based devices suffered from more cybercriminal attacks due to their increase in usage and exposition to cyber threats. Well-established hacker groups such as the Anonymous target this exploited; it will pose a bigger threat to smart environments that protect highly sensitive data, targeting individuals for various political and financial reasons. Mobile phishing is also particularly popular among cybercriminals because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and multimedia messaging services (MMS). In the 2012 first quarterly report from Trend Micro, it has been pointed out that the large diffusion of mobile devices and the outflow of awareness on the principal cyber threats have resulted in an increase in the interest of cybercrime in the mobile sector.

III. THREAT ASSESSMENTS

In this section, we provide a summary of some of the securitythreats associated to future connected home because of rapid increase in the availability and use of smart interconnected devices. The assumption is that the enterprise is where the big security challenges are, but home is where the hearts of consumers are.

The home is becoming the battleground for developing new devices and push point for consumer electronics. The numberof devices available at our disposal at home domain is increasing on daily basis. This creates a huge hole in the connectivity and security of such devices. So also is the need of these devices to interact with each other seamlessly to provide us with service that we have not dreamed of before. In addition, it is of paramount importance to provide home users with simple interface to configure and change security requirements within the system.

Security threats and attacks to connected home infrastructures will likely come in two ways: either by or to the sensors/devices connected to the network or to the serversthat gather, store, and analyze information from the sensors. Both kinds of vulnerability need consideration. From the device or sensors connected to dummy devices, they are the weakest link in the system.

Device connected to the Internet can take many forms, ranging from simple devices that measure things like temperature to video cameras that monitor the physical security of anything from homes, city streets to remote oil pipelines. As shown on Figure 1, most of the data breaches in 2013 are targeting web applications, this follows with cyber espionage. These attacks are much easier on smart devices or unprotected home networks.

A recent report identified that nearly half of web applications cyber-attacks target retailers, in this case most online shopping is via personal home networks and of smart devices. One of the challenges is that simple devices or sensor devices are very inexpensive to be affordable on a mass scale, it will be vital to embed security in the device networks before they are installed, rather than trying to retrofit them later.

In past few decades, some work has been done to defend computer servers and networks from malicious attacks, but the emergence of the Internet of Things (IoT) and smart homes is forcing cyber-security experts to rethink how such assets could be protected. One of the key strategies for protection control systems was to isolate them from other networks. Now that control systems are, connected to the Internet, that approach will not work well anymore.

Hence, there is a crucial need for multi-tier user-centered security system–blending safeguards for individual devices, servers, networks and applications with more powerful access controls, content management and network monitoring.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 2.635| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 5, September-October 2017 ||

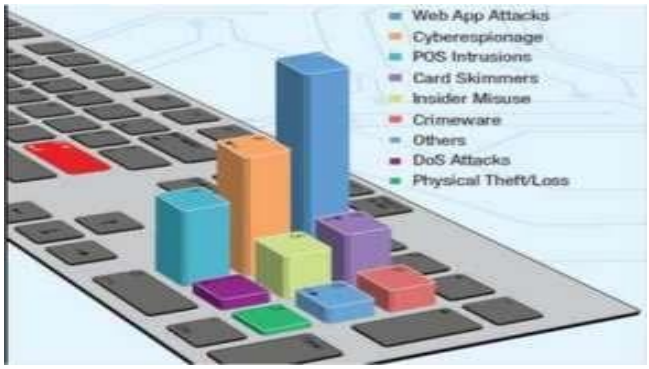


Figure 1. Data Breaches

The IoT and smart home developments have created excitingnew possibilities, but it can only deliver on its promises if itis reliable and trustworthy. Now is the time to start addressing these concerns. Half of mobile applicationtransmits personal details or device information, as a results threats associated to rogue applications and social engineering expected to keep on rising.

Lost or Stolen Devices

The security risks to the enterprise associated with lost or stolen employee devices is nothing new, but the growing mobile workforce leaves these tools open to loss or theft. Out of the 187 million compromised identities found by Symantec in 2011, about 10% (18.5 million) were as a result of a lost device

Open Wi-Fi and Public Network

Studies show that consumers (and hence, employees) are lax about mobile phone security. A recent report from Juniper Networks states that Wi-Fiattacks are on the rise, as open connections give hackers easyaccess to social networks and email.

Malware and Viruses

With emerging technologies comes new and evolved malware. Malware of itself can be of two main forms. Firstly, agents based developed and operated by government agencies, law enforcement agencies or corporate that needsto intercept and monitor a specific user, network, or service.

Secondly, developed and managed by an organized criminal network or criminals who want to capitalize on the widespread distribution of malware for financial gains or other malicious intends. Smartphone security threats are increasing, according to a new Symantec report. According the Symantec report, the story of one gang earned $1 million/year using this technique. The criminals donot need a huge number of phones to do it.

Corporate Policy

Unclear corporate policies to address new technologies while supporting employee benefits that come with the increasing consumerization of IT may not seem like a security threat. Many enterprises are overwhelmingly supportive of employee choices when it comes to the variety of devices andapplications available to them to boost productivity. Yet the same companies have been slow to adopt corporate policies that address the specific threats that these emerging technologies bring into the workplace. Employees were seen as the most likely source of an attack, this follows by consumers accounting for 57% and 10% respectively.

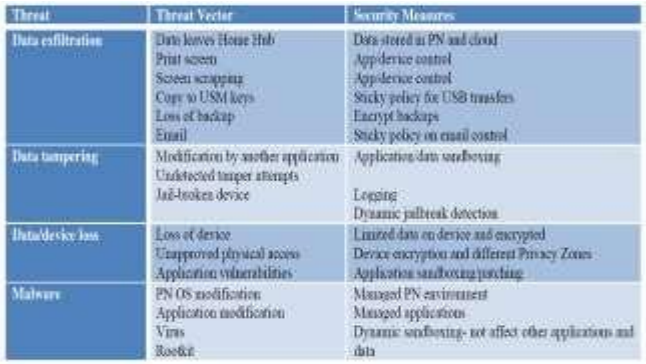
Theft/Abuse of Services

The connected home ecosystem both provides and consumes internal services as well as consuming external services. By definition, these services provide some value to the user orthe other elements of the network. An attacker could obtain the benefit provided by these services. An example of theft ofan external service would be smartphone malware that uses the device‘s mobile broadband connection, for which the usermay be billed. Since computation considered as internal service, an example of theft of this service would be anattacker using a target device to perform computational operations such as mining crypto-currency.

Unauthorized Cyber-Physical Control

A relatively recent possible objective of the attacker is unauthorized control of cyber-physical systems. In the context of the connected home futures ecosystems, the term cyber-physical refers to any computational system, which forms part of the network but also has the capability to control external physical infrastructure. This will mostly likely also

have the Remote accessibility characteristic.



Threat	Threat Vector	Security Measures
Data exfiltration	Data leaves Home Hub Print screen Screen scrapping Copy to USM keys Loss of backup Email	Data stored in PN and cloud App/device control App/device control Sticky policy for USB transfers Encrypt backups Sticky policy on email control
Data tampering	Modification by another application Undetected tamper attempts Jail-broken device	Application data sandboxing Logging Dynamic jailbreak detection
Data/device loss	Loss of device Unapproved physical access Application vulnerabilities	Limited data on device and encrypted Device encryption and different Privacy Zones Application sandboxing/patching
Malware	PN OS modification Application modification Virus Rootkit	Managed PN environment Managed applications Dynamic sandboxing- not affect other applications and data

Figure 2. Threats and counter measures

For example, cyber-physical systems include various types of (future) smart meters, smart home appliances such as smart refrigerators, lighting controllers or heating, ventilation and air-conditioning (HVAC) systems, which can control aspects of the physical environment.

Cyber-physical systems focus on enabling a user to control his or her physical environment and usually provide this functionality through the personal network. Therefore, unauthorized control of cyber-physical infrastructure would be a possible objective for an attack on the personal network. However, as the number of smart cyber-physical systems increases, this attack objective is likely to become a relevant concern in the connected home ecosystem futures. Therefore, the brief summary of some of threats presented above provides a useful starting point for efforts to enhance the security of current and future personal networks.

IV. CONCLUSIONS

The paper discussed the issue of connected home ecosystem futures in reference to various threats that makes such systems vulnerable and a lucrative target for cybercriminals. In the near future, cyber security experts will see an increasing threat to the home infrastructures as the key targetand challenge for them to address as cybercriminals will findsuch systems easy to use and infiltrate. This is also true to mobile smart device users who can expect to see a striking increase in malware and notable advancements in malware-related attacks, particularly on the Android platform as the user base grow exponentially.

Today‘s users utilize their mobile smart devices for everything from accessing emails to sensitive transactions such as online banking and payments. As users become more dependent on their mobile devices as digital wallets, this creates a very lucrative target for cybercriminals, and a huge challenge for security experts. Mobile smart device users canexpect to see a significant malware increase on finance related applications, such as mobile banking.

This work is part of ongoing research to design and implement a security model for smart devices in smart home connected ecosystem futures, where in our previous publications we have proposed frameworks and provide some implementations of how to handle some of the identified threats discussed in this paper. The focus of our future work is to provide a test bed that will allows cyber security experts experiments on way of addressing this increasing threats and how to align this with the developmenton tackling cyber security in national infrastructures.

REFERENCES

1. A. Serageldin, H. Alturkostani, and A. Krings, “On the reliability of DSRC safety applications: a case of jamming,” in International Conference on Connected Vehicles and Expo, 2013, pp. 501–506.
2. B.K. Chaurasia, R.S. Tomar, S. Verma, G.S. Tomar, Suitability of manet routing protocols for vehicular ad hoc networks, in: 2012 International Conference on Communication Systems and Network Technologies, IEEE, 2012, pp.334–338.
3. C. Laurendeau and M. Barbeau, “Threats to security in DSRC/WAVE,” in Proc. 5th International Conference on Ad-Hoc Networks & Wireless, LNCS 4104, 2006, pp. 266–279.
4. E. Hamida, H. Noura, and W. Znaidi, “Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures,” Connected Vehicles, V2V Communications, and VANET, vol. 4, no. 3, pp. 380–423, 2015.

5. F.K. Karnadi, Z.H. Mo, K.-c. Lan, Rapid generation of realistic mobility models for vanet, in: 2007 IEEE Wireless Communications and Networking Confer-ence, IEEE, 2007, pp.2506–2511.
6. H. Hasbullah, I. Soomro, and J. Ab Manan, "Denial of service (DOS) attack and its possible solutions in VANET," International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol. 4, no. 5, pp. 813–817, 2010.
7. H.-M. Zimmermann, I. Gruber, C. Roman, A Voronoi-based mobility model for urban environments, in: 11th European Wireless Conference 2005-Next Generation Wireless and Mobile Communications and Services, VDE, 2005, pp.1–5.
8. J. Härri, F. Filali, C. Bonnet, M. Fiore, Vanetmobisim: generating realistic mo-bility patterns for vanets, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, ACM, 2006, pp.96–97.
9. J. Harri, M. Fiore, Vanetmobisim–vehicular ad hoc network mobility exten-sion to the canumobisim framework, Institut Eurécom Department of Mobile Commu 6904 (2006) 1–19.
10. J. Zhao, G. Zucchelli, and M. Roggero, "Design of FMCW radars for active safety applications," http://embedded-computing.com/articles/design-fmcw-radars-active-safety-applications/, 2015.
11. L. Bononi, M. Di Felice, M. Bertini, E. Croci, Parallel and distributed simulation of wireless vehicular ad hoc networks, in: Proceedings of the 9th ACM In-ternational Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, ACM, 2006, pp.28–35.
12. M. Brooker, "Mutual interference of millimeter-wave radar systems," IEEE Transactions on Electromagnetic Compatibility, vol. 49, pp. 170–181, 2007.
13. M. Piorkowski, M. Raya, A.L. Lugo, P. Papadimitratos, M. Grossglauser, J.-P. Hubaux, TRANS: realistic joint traffic and network simulator for vanets, Mob. Comput. Commun. Rev. 12 (2008) 31–33.
14. N. Li and Y. Zhang, "A survey of radar ECM and ECCM," IEEE Trans. Aerospace and Electronic Systems, vol. 31, no. 3, pp. 1110–1120, 1995.
15. N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, V. Sadekar, Broadcast storm mitigation techniques in vehicular ad hoc networks, IEEE Wirel. Commun. 14 (2007) 84–94.
16. Q. Chen, T. Roth, T. Yuan, J. Breu, F. Kuhnt, M. Zollner, M. Bogdanovic, C.Weiss, J. Hillenbrand, and A. Gern, "DSRC and radar object matching for cooperative driver assistance systems," in IEEE Intelligent Vehicles Symposium, 2015, pp. 1348–1354.
17. Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in Proceedings of the 1st ACM International Workshop on Vehicular ad hoc Networks, 2004, pp. 19–28.
18. R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4983&context=etd, 2014.
19. R. Fernandes, P.M. d'Orey, M. Ferreira, Divert for realistic simulation of hetero-geneous vehicular networks, in: The 7th IEEE International Conference on Mo-bile Ad-Hoc and Sensor Systems (IEEE MASS 2010), IEEE, 2010, pp.721–726.
20. R. Mangharam, D.S. Weller, D.D. Stancil, R. Rajkumar, J.S. Parikh, Groovesim: a topography-accurate simulator for geographic routing in vehicular networks, in: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, ACM, 2005, pp.59–68.
21. S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, "Autonomous navigation robot", International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
22. S.-Y. Wang, C.-L. Chou, Nctuns Simulator for Wireless Vehicular Ad Hoc Net-work Research, Ad Hoc Networks: New Research, Nova Science Publishers, 2009.
23. T. Fujiki, M. Kirimura, T. Umedu, T. Higashino, Efficient acquisition of local traffic information using inter-vehicle communication with queries, in: 2007 IEEE Intelligent Transportation Systems Conference, IEEE, 2007, pp.241–246.
24. T. Jeyaprakash, R. Mukesh, A survey of mobility models of vehicular adhoc networks and simulators, Int. J. Electron. Inf. Eng. 2 (2015) 94–101.
25. T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: challenges and a solution framework," IEEE Internet of Things Journal, vol. 1, pp. 10–21, 2014.
26. V. Richard, Millimeter wave radar applications to weapons systems, USA Ballistic Research Laboratories, 1976.
27. V.D. Khairnar, S. Pradhan, Comparative study of simulation for vehicular ad-hoc network, preprint, arXiv:1304 .5181, 2013.
28. W. Zhang, H, Zeng, Y, Li, and X. Wang, "Polarimetric radar performance test of signal processing for anti-active jamming," in IET International Radar Conference, 2009, pp. 1–4.
29. X. Qiao, T. Jin, X. Qi, M. Zhang, S. Yuan, and Q. Zhang, "Anti-millimeter wave polarization agile active jamming," in Proceedings of the International Conference on Microwave and Millimeter Wave Technology, 2007, pp. 1–4.
30. Y.P. Fallah, C. Huang, R. Sengupta, H. Krishnan, Congestion control based on channel occupancy in vehicular broadcast networks, in: 2010 IEEE 72nd Ve-hicular Technology Conference-Fall, IEEE, 2010, pp.1–5.