RIoT: A Rapid Exploit Delivery Mechanism against IoT Devices Using Vehicular Botnets

Mevlut Turker Garip, Peter Reiher, Mario Gerla
Department of Computer Science, University of California Los Angeles
{mtgarip, reiher, gerla}@cs.ucla.edu

***Abstract*—Vehicular ad hoc networks (VANETs) are designed to provide traffic safety by enabling vehicles to broadcast information—such as speed, location and heading—through inter-vehicular communications to proactively avoid collisions. However, one powerful threat against VANETs is vehicular botnets. In our earlier work, we demonstrated several powerful vehicular botnet attacks that can have damaging impacts on the security and privacy of VANETs. In this paper, we present RIoT—the first attack in the literature against Internet of Things (IoT) devices using vehicles—and demonstrate that vehicular botnets are threats not only to VANETs, but also to other important systems and networks. We show via simulation that RIoT can compromise up to 87 percent of the IoT devices in an area of interest within a short amount of time, by taking advantage of the mobility and collective communication range of vehicular bots.**

***Index Terms*—Vehicular Ad Hoc Networks, Vehicular Botnets, Internet of Things, IoT Security, Wardriving, Exploit Delivery**

I. Introduction

Many traffic accidents are caused by unsafe driver actions due to insufficient traffic information [38]. In vehicular ad hoc networks (VANETs), vehicles exchange traffic information via Basic Safety Messages (BSMs) [40], which contain current speeds, locations, directions, etc. Vehicles use this information to prevent collisions by automated and prompt reactions to abrupt traffic events. However, the advantages of VANETs could be counterbalanced by the dangers posed by one of the most powerful adversaries against them—vehicular botnets. A vehicular botnet is a network of compromised vehicles under the control of a remote attacker—botmaster. The owners of these vehicles are not aware that their cars are compromised while, secretly and under the directions given by the botmaster, they cooperate as a distributed resource of greater total power that can achieve much more powerful attacks compared to a single attacker. We already described how these vehicular bots can cooperate by exchanging secret messages concealed in the VANET control channel [14], and demonstrated some of the attacks that they can perform on VANETs [12] [15] in our earlier work. In this paper, we show that vehicular botnets can also be used by attackers as an effective tool to perform powerful attacks against other important systems and networks, particularly Internet of Things (IoT) devices.

The concept of IoT is expected to significantly improve many aspects of our lives, from Industry 4.0 and health applications to efficient workspaces and smart homes. Therefore, its popularity is growing more and more each day, along with its market share, supported by emerging applications and business models. The IoT market is expected to reach $1.2 trillion in 2022 [7] with 42.62 billion IoT devices worldwide [36]. The security of IoT devices is often neglected by their manufacturers due to financial concerns and the insufficient hardware capabilities of these devices, such as limited battery capacity and computing power. Attackers are likely to come up with more and more exploits to compromise IoT devices as they become an increasingly integral part of our lives [25]; therefore, the security of these devices will soon be too important to overlook. However, due to their hardware limitations, the most feasible way to protect IoT devices would be outsourcing the task of preventing possible attacks to the firewalls installed on the gateway access points, through which these devices connect to the outside world [22]. Such security measures, on the other hand, could protect IoT devices only from the attacks performed over the Internet, leaving their wireless ad hoc communication vulnerable. Therefore, an attacker could either directly use the peer-to-peer wireless connections to IoT devices if they support Simple Service Discovery Protocol/Universal Plug and Play Protocol (SSDP/UPNP) [3], or spoof the wireless access points through which they connect to the Internet [18], or force them to revert to a known insecure communication mechanism [37]—in order to deliver exploit payloads to them. Yet, given the number of IoT devices expected to exist, it would be infeasible for a single attacker to compromise them one by one this way.

In this paper, we present RIoT—a rapid exploit delivery mechanism that can compromise a significant percentage of the IoT devices in an area of interest within a short amount of time, by taking advantage of the mobility and collective communication range of vehicular bots. It is the first attack in the literature against IoT devices using vehicles. RIoT takes the simple concept of wardriving [8] [34] to a much more powerful level—using multiple cooperating vehicles for compromising IoT devices, rather than a single vehicle scanning for only wireless access points. This paper does not present new exploits against IoT devices. Its novelty comes from the mechanism that can quickly deliver the payloads of existing exploits to the IoT devices in an area of interest, as well as from the extensive experimentation with realistic traffic patterns and placement of these devices. RIoT's exploit database used by vehicular bots consists of several IoT vulnerabilities identified by earlier research. Identifying all possible vulnerabilities of every type of IoT device is out of the scope of this paper and not necessary for demonstrating

the effectiveness of our exploit delivery mechanism. However, RIoT's exploit database can be easily extended with new and possibly more effective exploits due to its adaptive design. While RIoT could also be used for constructive purposes such as penetration-testing a smart city, it is much more likely to be used for malicious intent. Therefore, it is crucial to defend against attacks like RIoT, and our work is an important step toward this goal.

In Section II, we identify the categories and percentages of the IoT devices and their vulnerabilities that are used for the evaluation of our attack. In Section III, we present the details of the simulation map and how the IoT devices are realistically placed on it, along with the description of RIoT. In Section IV, we discuss the effectiveness metric for the evaluation of our attack, and show its success via extensive and realistic experimentation. In Section V, we suggest possible solutions to protect IoT devices against attacks like RIoT. In Section VI, we conclude with the contributions of our work to future research on IoT security.

II. IoT Device Categories

In order to accurately evaluate the effectiveness of our attack, it is important to determine the number and types of IoT devices to be used in the simulation, as realistically as possible. Therefore, we first identified the most popular IoT device categories that are expected to be on the market: industrial, consumer, medical, security, and retail [19]. We then determined the types of existing devices that are expected to be IoT-capable, under all these categories. Afterwards, we used the market sales data in the US in order to estimate the total number of IoT devices under each category, as well as the percentages of the categories. The types of these devices are as follows: under the industrial category, there are temperature sensors [9] [26] [33] and robotic machinery [16]; the consumer category consists of smart televisions [29], smart speakers [31] and smart refrigerators [27]; the medical category includes wearable devices [17] and health monitoring sensors [2] [28]; the security category contains smart security cameras [39] and smart locks [24]; and finally, the retail category comprises retail sensors [32] and barcode scanners [1]. Obviously the popularity of particular classes of devices might change over time, but that factor does not substantially alter our results, and could be easily tested for by including newly popular device types in the simulation.

	Expected Number of IoT Devices	Percentage (%)
Industrial	122,337,619	36.88
Consumer	99,450,000	29.98
Medical	52,918,610	15.95
Security	32,000,000	9.50
Retail	25,500,000	7.69

Figure 1. Percentages of individual IoT device categories and their expected number of devices

Figure 1 shows the expected number of devices under each IoT device category and the corresponding percentages. For realistic experimentation, at the beginning of each simulation, the IoT devices under each category are inserted into the simulation according to the percentage of the category. Existing vulnerabilities of the individual device types under each category comprise RIoT's exploit database: [23] for industrial, [5] and [21] for consumer, [4] and [20] for medical, and [30] for security. There are also vulnerabilities in the exploit database—such as [10], [11] and [37]—that might affect every IoT device regardless of their types or categories. In order to test the effectiveness of our exploit delivery mechanism regardless of the effectiveness of individual exploits, during the simulation, we consider an IoT device as compromised if it simply gets inside a vehicular bot's communication range. The reason for excluding the effectiveness of the exploits in the exploit database from experiment results is that the database content is expected to change as the IoT standards, device types and their specifications change. Also for the same reason, assessing the effectiveness of individual exploits is out of the scope of this paper and is irrelevant with regards to showing the effectiveness of our exploit delivery mechanism.

III. RIoT

A. Simulation Map and IoT Device Placement

Besides the realistic number and types of IoT devices used in the evaluation of RIoT, deploying an accurate city scenario and a realistic placement of these devices in it also play an important role in providing realistic experimentation. Therefore, we use a 24-hour Luxembourg scenario designed based on the real traffic patterns and volumes of the city. This scenario simulates the real traffic patterns throughout the day, as well as interactions with the road infrastructure, such as actuated traffic lights, with very high accuracy. Therefore, it enables us to evaluate RIoT with realistic mobility patterns on a scale as large as an entire city. The details of the Luxembourg scenario are described in [6].

Figure 2. Luxembourg map that is used for the evaluation of RIoT

Figure 2 shows the Luxembourg map used in the simulation. For the best evaluation of RIoT, using only realistic traffic

patterns and volumes—which determine the mobility and number of vehicular bots in each individual area on the map—is not enough. We also need realistic locations for the IoT devices based on their categories. In order to address this, we designed a novel placement mechanism that identifies all the locations on a given map associated with each IoT device category. It first determines the keywords for each category using Google Maps data (e.g., industrial keywords are factory, manufacture, plant, etc.). After identifying these keywords, our mechanism uses the Google Maps API to query for all the locations associated with each keyword. Finally, it builds a *location set* for each category that consists of the coordinates of all the locations related to the keywords for that category. For the evaluation of RIoT, we apply this placement mechanism to the Luxembourg map; however, our mechanism can be used for the placement of IoT devices on any map.

B. RIoT Attack

In order to better describe the dynamics of our exploit delivery mechanism, Figure 3 shows the RIoT architecture with an example scenario of the interactions among the botmaster, vehicular bots, and IoT devices.

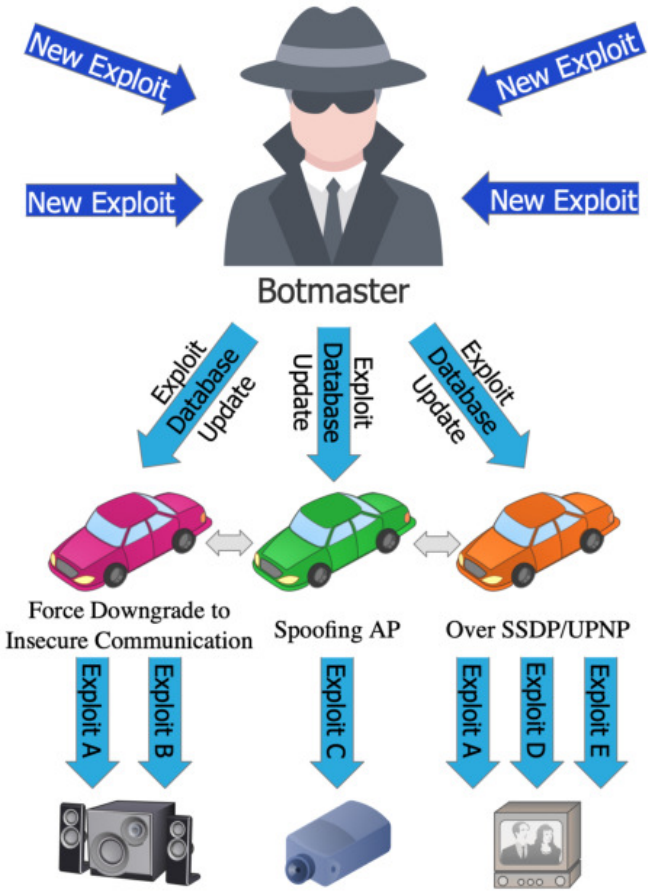

Figure 3. Diagram of RIoT architecture and an example scenario of interactions

In the beginning of the attack, the vehicular bots sync their exploit database with the botmaster. The botmaster is expected to have the most up-to-date exploit database and is responsible for adding new types of IoT devices and their vulnerabilities to its database as they become available, along with new vulnerabilities for the existing devices in the database. Once the vehicular bots obtain the most up-to-date exploit database from the botmaster, they start searching for any IoT device in their communication range as they move along their routes. The vehicular bots do not alter their original routes in any way for the purpose of finding more IoT devices, since it would otherwise be suspicious to the legitimate owners of these vehicles. For each IoT device detected in their communication range, the vehicular bots identify its type, query their exploit database for all applicable exploit payloads and determine the most suitable wireless ad hoc connection method(s) to deliver them. The arrows at the bottom of Figure 3 depict this process. Depending on the type of the detected IoT device, the vehicular bots might decide to either use SSDP/UPNP, spoof the wireless access point that the device uses, force the device to revert to a known insecure communication mechanism, or use any combination of these methods to deliver the exploit payloads to the device. This way, the vehicular bots can bypass any firewalls that might be installed on the gateway access point, through which the IoT device connects to the Internet. Similarly, there might also be multiple applicable exploit payloads for the device in the exploit database, as well as an exploit payload applicable for multiple types of IoT devices. For example, in Figure 3, the payload of Exploit A is delivered to both the smart speaker and smart television since it is applicable for both. Due to the limited amount of time for which the vehicular bots can hold the IoT device in their communication range, they deliver all applicable exploit payloads to it at once to maximize the probability of compromising it. Using the vehicular botnet communication, the vehicular bots share the areas that they covered so far with each other so that they can stay inactive in already covered areas in order to minimize the chance of getting detected.

RIoT is a highly effective mechanism for compromising the IoT devices in areas as large as a city—an infeasible task for any single attacker. The mobility and collective communication range of vehicular bots, as well as the variation in their routes, enable the compromise of a significant percentage of the IoT devices in a whole city in a very short amount of time. Also, since it is natural for vehicular bots to pass by IoT devices along their paths, compromising them in the background would raise less suspicion compared to a single attacker moving around to compromise them.

IV. Evaluation

We used Veins [35] (which combines the SUMO and OMNeT simulators) to evaluate RIoT. SUMO is responsible for simulating realistic vehicular traffic while OMNeT simulates the IEEE 802.11p standard [40].

In order to fairly and accurately compare the effectiveness results for different values of the attack parameters, we define the effectiveness metric as the percentage of IoT devices that the vehicular bots were able to compromise within a specified

amount of time. The reason for setting a time limit is that the parameter values mostly affect the attack speed; due to the effectiveness of RIoT, given a sufficient amount of time, similar percentages of IoT devices get compromised regardless of these values. Therefore, we chose this time limit to be the first 6 hours of the simulation—after which the effectiveness of RIoT does not improve significantly with the optimal parameter values, and at which the effectiveness with different parameter values are still differentiable (see Figure 6). The effectiveness metric is calculated for each IoT device category separately in order to capture the differences in effectiveness between them. These differences are caused by the spatial characteristics of the devices under these categories.

We evaluated RIoT using rigorous and long experiments. We ran 60 simulations in total, each of which simulated the 24-hour Luxembourg scenario. For these experiments, we used two attack parameters that could alter the attack's effectiveness: vehicular bot percentage and communication range. Each graph in this section is produced by varying each relevant attack parameter while keeping the other one constant at its standard value—which is 20% for the vehicular bot percentage and 300 meters for the communication range (as defined by IEEE 802.11p [40]). After each simulation, using the effectiveness metric described above, we calculated the effectiveness for all the IoT device categories. For each simulation, we introduced significant randomness in several components of RIoT so that conditions that could give high effectiveness were not constantly favored. The first source of randomness is built into the Luxembourg scenario; each vehicle's rerouting choice is randomized in order to load-balance traffic flows. Also, we determine which vehicle is going to be a vehicular bot randomly for each simulation. Finally, we place the IoT devices on the map by selecting random locations from the *location set* for each IoT device category—created by our placement mechanism—according to the percentages of each category (see Figure 1). Due to these random factors in each simulation, we ran 10 simulations for each pair of attack parameter values. The final effectiveness for each value on the x-axis of each graph are then calculated by averaging all the effectiveness values from these 10 simulations.

The effectiveness of RIoT is correlated with the size of the area on the map that is collectively covered by the vehicular bots. Figure 4 shows the effectiveness for all IoT device categories with each percentage of vehicular bots over the total number of cars created during the simulation. The reason that the same category has similar effectiveness for different vehicular bot percentages is explained later in Figure 6. The most important factor that influences how the different values of the attack parameters affect the effectiveness of RIoT is the spatial characteristics of the IoT devices based on their categories. These characteristics are the geographical locations and types of the places where the devices under each category are expected to exist. For example, industrial IoT devices are mostly located in remote areas where the traffic is sparse, and industrial buildings such as factories are generally located in large campuses away from roads. Therefore, RIoT has the

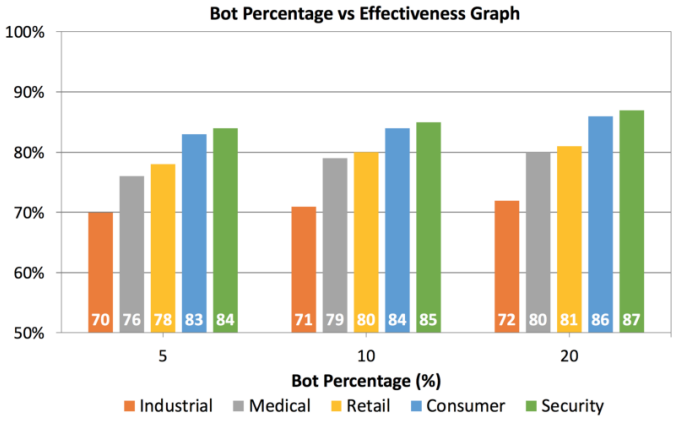

Figure 4. Effectiveness for each IoT device category with different percentages of vehicular bots

lowest effectiveness for this category since not many vehicular bots come in the vicinity regardless of the vehicular bot percentage due to the traffic sparsity, and if they do, their communication range is not sufficient to reach the devices in the large industrial campuses. Medical IoT devices are located in relatively less remote areas but still in large campuses such as hospitals. Retail IoT devices are in more urban areas and in smaller but still somewhat large campuses close to roads, such as shopping malls. Consumer IoT devices are in urban areas and located in buildings close to roads rather than campuses, whereas security IoT devices are found in any type of location.

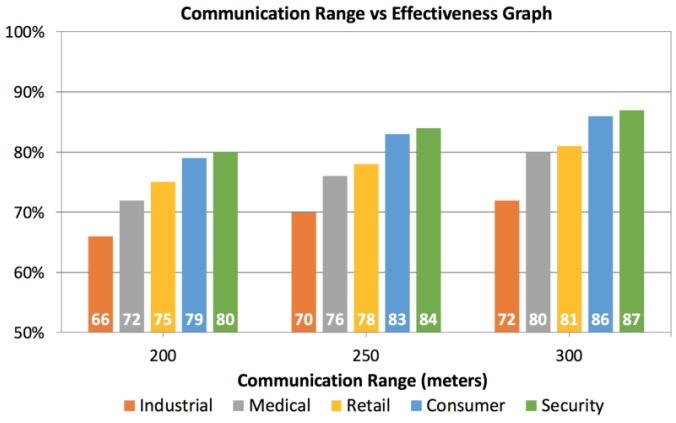

Figure 5. Effectiveness for each IoT device category with different wireless communication ranges

The effectiveness of RIoT is more sensitive to the communication range than the vehicular bot percentage. Figure 5 shows the effectiveness for all IoT device categories with each communication range. Since there is a correlation between the effectiveness and the size of the area covered by the vehicular bots, as stated earlier, the change trends in them are similar. For example, the covered area shrinks linearly with the number of vehicular bots, as opposed to exponentially with the communication range due to being proportional to the communication range squared. As a result, the effectiveness of

RIoT decreases exponentially with the communication range in Figure 5, whereas we observe a logarithmic decrease in the effectiveness with the vehicular bot percentage in Figure 4. In addition to the covered area size, there is also another reason why the communication range has a bigger effect on the effectiveness than the vehicular bot percentage. Although a smaller number of vehicular bots could be compensated for given an adequate amount of time, an insufficient communication range might have a more permanent impact on the effectiveness, as later discussed in Figure 6. With a limited communication range, some IoT devices might never be reachable regardless of the amount of time given or how high the number of vehicular bots is. Effectiveness, especially for the industrial and medical IoT devices, is even more affected by the decreases in the communication range, since they would have to be compromised over their long distances to roads.

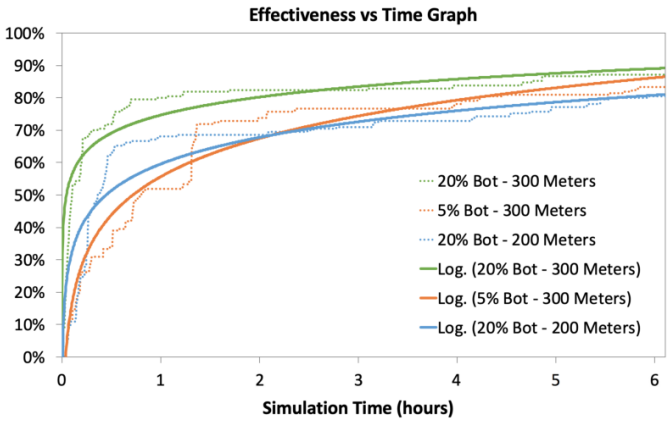

Figure 6. Attack speed of RIoT with different attack parameter values

Figure 6 shows the effectiveness of RIoT over time with different attack parameter values, and depicts how a low vehicular bot percentage impacts the attack speed, compared to a short communication range and vice versa. The attack speed is the slope of the effectiveness-time line. In Figure 6, values of the effectiveness over time are represented with a dotted line. They all follow a logarithmic trend line, which is represented with a solid line, as the attack speed decreases over time. It can be clearly seen in the graph that the vehicular bot percentage is the main factor in determining the initial attack speed, with the communication range still having a noticeable—though limited—impact. In both experiments with 20% vehicular bots, regardless of the communication range, the initial attack speed is much faster than in the experiment with 5% vehicular bots. However, between the experiments with 20% vehicular bots, the effectiveness grows faster initially in the experiment with a longer communication range, which demonstrates that the communication range still has some impact on the initial attack speed even though not as much as the vehicular bot percentage. Despite the initial attack speeds, the effectiveness-time lines almost flatten eventually, and we observe that the values of the attack parameters have a different impact on the effectiveness of RIoT than they do on the initial attack speed. In this case, the communication range has a more significant impact than the vehicular bot percentage on the effectiveness in the long term. The effectiveness-time lines with the same communication range converge to similar values regardless of the vehicular bot percentage, which explains the similar accuracies for each IoT device category in Figure 4. This is also why we set the time limit for the effectiveness metric to the first 6 hours of the simulation; as shown in Figure 6, the effectiveness-time line with the optimal attack parameter values is almost completely flat after the first 6 hours, and each effectiveness-time line is still differentiable from the others. The communication range, on the other hand, has a more severe and permanent impact on the effectiveness. The effectiveness-time line with 20% vehicular bots and 200-meter communication range—despite a faster initial attack speed—falls and stays below the line with 5% vehicular bots and 300-meter communication range. Afterwards, it follows a logarithmic trend line, at lower accuracies, almost parallel to the line with 20% vehicular bots and 300-meter communication range.

V. Possible Countermeasures

Vehicular bots compromise IoT devices by delivering exploit payloads to them directly over a wireless ad hoc connection. Therefore, a honeynet approach could be used for detecting the vehicular bots. When a vehicular bot attempts to compromise an IoT device that is a honeynet node, it could notify all the other devices over the Internet so that they ignore any message from this vehicle.

Since IoT devices that communicate among themselves over a wireless ad hoc connection are generally very close to each other—mostly even in the same building—they could use a localization mechanism, similar to the one described in [13], to cooperatively pinpoint locations of senders, and ignore everything sent by nodes more than a threshold away.

If IoT devices have the sufficient computing resources, they could exchange a session key using a direct connection over the Internet with each other, and encrypt everything sent over their wireless ad hoc connections with this key. Then, anything that is not encrypted with this key—which would be challenging for vehicular bots to intercept—would be ignored, preventing possible deliveries of exploit payloads.

VI. Conclusion

In this paper, we presented RIoT—a rapid exploit delivery mechanism that can compromise a significant percentage of the IoT devices in an area of interest as large as a city within a very short amount of time. In order to achieve this, RIoT takes advantage of the mobility and collective communication range of vehicular bots, as well as the diversity in their routes. It is the first attack in the literature against IoT devices using vehicles. For testing RIoT in conditions as realistic as possible, we first determined the percentage of each IoT device category and its expected number of devices. We then described a realistic 24-hour Luxembourg scenario that we used for the

evaluation of RIoT, along with our novel mechanism that places the IoT devices in this scenario at realistic locations. We showed via realistic and thorough experimentation that RIoT can compromise up to 87 percent of the IoT devices in the whole city of Luxembourg within just the first 6 hours of the simulation. This paper showed that, if not defended against, vehicular botnets can threaten not just VANETs but also other important systems and networks—such as IoT devices. We proposed possible solutions to protect these devices against attacks like RIoT.

VII. Acknowledgement

We would like to thank Amir Saad for his great work contributing to the identification of the IoT device categories and vulnerabilities used in this paper, and to the implementation of the IoT device placement mechanism.

References

[1] ABI Research. Enterprise wearable scanner and reader technologies: Devices, use cases, and supplier ecosystem analysis. https://www.abiresearch.com/market-research/product/1025688-enterprise-wearable-scanner-and-reader-tec/, 2016.

[2] American Hospital Association. Fast facts on u.s. hospitals. https://www.aha.org/statistics/fast-facts-us-hospitals, 2019.

[3] M. B. Barcena and C. Wueest. Insecurity in the internet of things. Technical report, Security Response, Symantec, 2015.

[4] K. W. Ching and M. M. Singh. Wearable technology devices security and privacy vulnerability analysis. *Int. J. Netw. Secur. Appl*, 8(3):19–30, 2016.

[5] C. Cimpanu. About 90% of smart tvs vulnerable to remote hacking via rogue tv signals. https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/, 2017.

[6] L. Codeca, R. Frank, and T. Engel. Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research. In *IEEE VNC*, 2015.

[7] L. Columbus. 2018 roundup of internet of things forecasts and market estimates. https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/, 2018.

[8] T. Dasilva, K. Eustice, and P. Reiher. Johnny appleseed: Wardriving to reduce interference in chaotic wireless deployments. In *ACM MSWiM*, 2008.

[9] M. Fitzgerald. An internet for manufacturing. https://www.technologyreview.com/s/509331/an-internet-for-manufacturing/, 2013.

[10] L. Franceschi-Bicchierai. Nasty bug left thousands of internet of things devices open to hackers. https://motherboard.vice.com/en_us/article/gybm4b/internet-of-things-camera-axis-bug, 2017.

[11] Y. Fratantonio, A. Bianchi, W. Robertson, E. Kirda, C. Kruegel, and G. Vigna. Triggerscope: Towards detecting logic bombs in android applications. In *IEEE Symposium on Security and Privacy*, 2016.

[12] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla. Congestion attacks to autonomous cars using vehicular botnets. In *NDSS*, 2015.

[13] M. T. Garip, P. H. Kim, P. Reiher, and M. Gerla. Interloc: An interference-aware rssi-based localization and sybil attack detection mechanism for vehicular ad hoc networks. In *IEEE CCNC*, 2017.

[14] M. T. Garip, P. Reiher, and M. Gerla. Ghost: Concealing vehicular botnet communication in the vanet control channel. In *IEEE IWCMC*, 2016.

[15] M. T. Garip, P. Reiher, and M. Gerla. Botveillance: A vehicular botnet surveillance attack against pseudonymous systems in vanets. In *IFIP WMNC*, 2018.

[16] A. Glaser and R. Molla. The number of robots sold in the u.s. will jump nearly 300 percent in nine years. https://www.recode.net/2017/4/3/15123006/robots-sold-america-growth-300-percent-jobs-automation, 2017.

[17] V. Gruessner. Market for wearable devices expected to double by 2018. https://mhealthintelligence.com/news/market-for-wearable-devices-expected-to-double-by-2018, 2015.

[18] M. Hill. It pros: Iot devices most vulnerable to wi-fi attacks. https://www.infosecurity-magazine.com/news/iot-devices-most-vulnerable-wifi/, 2018.

[19] Intel Corporation. A guide to the internet of things infographic. https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html, 2019.

[20] A. James and M. B. Simon. Medical device hijack cyber attacks evolve. https://www.rsaconference.com/writable/presentations/file_upload/hta-r02-medjack.3-new-research-on-attacks-on-hospital-medical-devices.pdf, 2017.

[21] J. Leyden. Samsung smart fridge leaves gmail logins open to attack. https://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/, 2015.

[22] H. Lin and N. Bergmann. Iot privacy and security challenges for smart home environments. *Information*, 7(3):44, 2016.

[23] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, and S. Zanero. Rogue robots: Testing the limits of an industrial robot's security. Technical report, Technical report, Trend Micro, Politecnico di Milano, 2017.

[24] C. Martin. Smart door lock sales heading to $357 million. https://www.mediapost.com/publications/article/305118/smart-door-lock-sales-heading-to-357-million.html, 2017.

[25] P. Martini. Hackers graduate to financial gain as motivation for iot attacks. https://www.itproportal.com/features/hackers-graduate-to-financial-gain-as-motivation-for-iot-attacks/, 2018.

[26] National Association of Manufacturers. United states manufacturing facts. https://www.nam.org/Data-and-Reports/State-Manufacturing-Data/2014-State-Manufacturing-Data/Manufacturing-Facts–United-States/, 2015.

[27] Navigant Research. Executive summary smart appliances. https://www.navigantresearch.com/wp-content/uploads/2012/09/SAPP-12-Executive-Summary.pdf, 2012.

[28] L. H. Newman. Medical devices are the next security nightmare. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/, 2017.

[29] N. Nguyen. If you have a smart tv, take a closer look at your privacy settings. https://www.cnbc.com/2017/03/09/if-you-have-a-smart-tv-take-a-closer-look-at-your-privacy-settings.html, 2017.

[30] D. Palmer. 175,000 iot cameras can be remotely hacked thanks to flaw, says security researcher. https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/, 2017.

[31] S. Perez. 47.3 million u.s. adults have access to a smart speaker, report says. https://techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says/, 2018.

[32] E. Pioryshkina. What every retail cmo should know about beacons and proximity marketing. https://www.iflexion.com/blog/every-retail-cmo-know-beacons-proximity-marketing/, 2017.

[33] Plant Automation Technology. Types of sensors used in industrial automation. https://www.plantautomation-technology.com/articles/types-of-sensors-used-in-industrial-automation, 2019.

[34] H. Said, M. Guimaraes, N. Al Mutawa, and I. Al Awadhi. Forensics and war-driving on unsecured wireless network. In *IEEE International Conference for Internet Technology and Secured Transactions*, 2011.

[35] C. Sommer. Veins: Vehicles in network simulation. http://veins.car2x.org, 2015.

[36] Statista. Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2016.

[37] A. Tierney. Z-shave. exploiting z-wave downgrade attacks. https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/, 2018.

[38] U.S. Department of Transportation. National motor vehicle crash causation survey. *DOT HS 811 059*, 2008.

[39] J. Vlahos. Surveillance society: New high-tech cameras are watching you. https://www.popularmechanics.com/military/a2398/4236865/, 2009.

[40] Wireless LAN Working Group. Wireless access in vehicular environments. *IEEE Standards*, July 2010.