On Security Challenges of Future Technologies

Thomas Lange and Houssain Kettani
The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, USA
Email: thomas.lange@trojans.dsu.edu; houssain.kettani@dsu.edu

Abstract —Considering emerging technologies and applications is an important step in assessing future security needs. For example, Advances in Internet of Things (IoT) and Autonomous Systems have presented new cyber security challenges. The severity of such cyber threats is magnified as societies are becoming more and more dependent on such emerging technologies. The purpose of this paper is to identify these emerging technologies and the associated threat landscape based on current knowledge and ongoing research. This can help protect societies from cyber threats associated with such technologies.

Index Terms—Autonomous systems, emerging technologies, internet of things (IoT), vulnerabilities, cyber security, cyber threat

I. Introduction

Throughout human history, it has been those societies and individuals who have been the quickest to adapt to technological shifts that have survived and excelled, and those that have refused to adapt their ways to the tides of progress who have fallen by the wayside. Indeed, entire dynasties and civilizations have crumbled due to such lack of innovation. The incredible speed at which technology is now being developed has only made it more difficult to retain a technological edge. What is more, societies are growing increasingly dependent upon technology. While fifty years ago it would have been uncommon for even a wealthier household to own a computer, now it is completely normal. According to U.S. Census Bureau data, in 1984 only 8% of those households counted owned a computer, while in 2016 that number increased to 89% [1]. Cell phones, which were once the size of bricks and owned by only a relatively small number of people are now commonly used everywhere even among children. Technology is integrated into medicine, business, civil administration and about every other aspect of urban life. For this reason, it is not only important, but imperative that governments and organizations predict the growth of technology to prepare for it.

An entire field dedicated to predicting the characteristics of future technologies exists, which is called technology forecasting. It is the practice of identifying and monitoring technological developments and predicting the direction these developments will take in the future [2]. The reasons for such forecasting can vary greatly, and the concerns of which are not delegated only to governmental organizations and nation states. Companies may want to be the first to apply some new technology to better fulfilling some consumer need. One particular story regarding the failure of one such company to do so is Kodak. It once was the premier camera company which invented the digital camera, but then it failed to accurately predict and prepare for the dominance of digital photography, leading to other camera companies taking the lead and Kodak subsequently going bankrupt [3]. What examples like this show is the power of preparing for and adapting to future technologies. While the various methods of performing technology forecasting are far beyond the scope of this paper, the results of such forecasts are of the utmost importance for policy makers and industry leaders, and therefore very relevant to the topic of this paper. The importance of such preparation becomes exponentially more important on a national scale, where failure to prepare for technological innovations can cause widespread devastation.

From a cyber security perspective, preparing for the technologies of the future is not only important, but it is also an imperative. Many of the technologies that societies have grown to depend on were developed with little to no thought for security. As Microsoft security expert Glen Schoonover recounts, older versions of Windows were shipped out with barely any built-in security before Microsoft's Trustworthy Computing Initiative was started in 2002, as were many other operating systems [4]. Thus, it is no surprise that many older operating systems are completely vulnerable and easily exploitable by even novice hackers. Many internet protocols have also gone through countless updates attempting to remedy the security concerns that might well have been prevented if developers had correctly theorized how their technologies would be used or abused in the future. As only one example, Border Gateway Protocol, a protocol which routes much of the Internet was designed using a trust model, which has made it vulnerable to cyber security threats [5]. Of course, it would have been very difficult to correctly predict how much of society would come to lean on the technologies it uses today or how hackers would learn to abuse such technologies; in some cases, it may have been impossible. Nonetheless, had even generalized predictions been made during the conception of the Internet and of software solutions, it is possible that the current state of software security could be much more secure than it is today.

Manuscript received March 8, 2019; revised September 25, 2019.
Corresponding author email: houssain.kettani@dsu.edu.
doi:10.12720/jcm.14.11.1002-1008

In 2018, the European Network, and Information Security Agency (ENISA) compiled a report which expounded on many of the upcoming technologies and the security concerns subsequently raised [6]. Some of the emerging technologies discussed, and topics presented in this ENISA report which are also addressed in this paper are, in order and in separate sections: The Internet of Things (IoT) in Section II, the interplay between society and technology in Section III, next generation IT infrastructure in Section IV, virtual and augmented reality in Section V, autonomous systems in Section VI, the Internet of Bio-Nano Things (IoBNT) in Section VII, Artificial Intelligence (AI) and robots in Section VIII. Considering the large scope of these topics, and the depths of research that has already gone into them, giving a proper in-depth investigation into each of these would require numerous papers for each single topic. Nonetheless, it is possible and desirable to provide a compilation of these topics and their security implications. This paper will then investigate these technologies, as well as the threats or potential threats facing these technologies, and finally the mitigations and counter-initiatives to these threats. Finally, concluding remarks are included in Section IX. Through reports and papers similar to this and the previously referenced ENISA report, it is hopeful that greater awareness and understanding may be redirected to these concerns.

II. The Internet of Things

The Internet of Things (IoT) is a massive and convoluted topic, the breadth of which would take many pages of research to fully understand. According to [7], IoT is defined as an interconnected network of uniquely identifiable, programmable devices with capabilities with the ability to change state and collect information. This definition provides a reasonable starting point for any discussion on the broader IoT, although the exact definition may change depending on the context. To understand the security implications of IoT, it is immensely helpful to understand how it came to be. The term was first coined by Kevin Ashton in 1999 [8]. However, the practice of manufacturing IoT-like devices had been increasing ever since the inception of the Internet. This practice continued to grow and still grows as companies and organizations add sensors and interfaces onto everyday objects [9]. Furthermore, the number of such IoT devices being developed is growing at an unprecedented rate. Gartner analysis estimates that the number of deployed IoT devices will reach 25 billion by 2021 from eleven billion in 2018, increasing at a rate of almost a third per year [10].

While it would be difficult to deny the good brought about by these devices, whether that is in recording patient bio-medical data at a hospital, helping farmers feed their animals, or simply allowing an absent parent to lock the doors to their home while away, the unfortunate reality is that many of these devices are terribly insecure. According to a study conducted by Hewlett Packard, 70% of commonly used IoT devices contain security vulnerabilities [11]. This same study places much of the blame on manufacturers sacrificing security to quickly output devices to meet the rapidly expanding demand for IoT technology. Likewise, it is not difficult to find examples of these vulnerabilities being exploited. For instance, the Mirai Botnet attack is likely one of the most well-known example. Other examples include the Jeep hacking in 2015, where security researchers remotely compromised a Jeep Cherokee, taking complete control over the vehicle [12]. Another example is the FDA announcement that certain cardiac devices used at St. Jude's Medical were vulnerable to exploitation, potentially killing the user [13]! Many other potential threats from IoT exploitation exist, including loss of data, theft or worse.

Due to the dramatic nature of these exploitations, it is no surprise that many researchers have offered recommendations on this issue. Expecting manufacturers to begin securely programming IoT protocols is probably not based on any likely reality. Especially due to the speed these devices are being manufactured and the diversity in function from one device to another. Therefore, many researchers have suggested mitigations involving the network layer. For example, [14] proposed an SDN-based framework to enforce network access controls while [15] suggested an intrusion detection technique working at the network layer. Other solutions exist, and likely an optimal solution will involve multiple layers of these mitigations. Nonetheless, due to the meteoric rise to prominence of IoT security, it will likely be many years before an optimal solution is developed.

III. Interplay between Society and Technology

This is a rather broad topic and it deals more with how society and technology interact. For the purpose of this paper, it will be narrowed down to the issues presented by social media. The latter is an aspect of modern life which has risen to prominence extremely quickly. According to Pew Research Center [16], just 5% of adults used a form of social media in 2005, which increased tenfold to 50% in 2011 and was at 69% in early 2018. While many experts would disagree on whether this is a beneficial or negative trend, such social media adoption has had serious security implications.

The security issues brought about by social media are in large part due to data privacy issues. On a website like Facebook or Twitter, a user is usually requested to submit to data collection in the terms and conditions. Oftentimes, users do not read these license agreements, and are thus surprised when a data breach occurs and much of their data is lost. One study conducted by researchers found that out of every thousand online retail software shoppers, only about one or two will access End User License Agreement (EULA) and usually those that do only read a small portion [17]. While in most of cases, users would

probably agree with the terms contained in the EULA, in some cases this is not true. For example, in the case of the 2018 Cambridge Analytica scandal, users unwittingly agreed to have their personal data collected to build psychological profiles used to establish mappings of the current political landscape [18]. In other cases, however, users simply post personal and sensitive information freely to the websites, which represent an entirely different threat.

As in other cases, there are of course suggestions and initiatives in place to help increase the security of users on social media. In some cases, governments have begun to enforce new privacy laws on social media, such as the European Union (EU) has done in 2018 [19]. However, it is also possible that these privacy concerns will be mitigated through user education and awareness. According to another Pew study [20], social media users are taking more effort to manage the information exposed on their accounts than in the past. Indeed, according to one survey [21], users are beginning to take more breaks from social media and more often deleting their accounts. Thus, a fair case could be made that the solution to privacy concerns in social media can be best solved by the users themselves through a combination of awareness and education.

IV. Next Generation IT Infrastructure

It is also worthwhile to discuss next generation IT infrastructure. Because as was the case with the previous section, it is a very broad subject, this paper will examine one such infrastructure, hardware virtualization and how that pertains to security. Virtualization technology is what allows a computer to run multiple virtual machines independent of the host hardware. The benefits of such a network are many-fold. As one Lippis Consulting white paper pointed out [22], this allows single IT assets to be expanded to numerous users and managing multiple resources as a single server. These resources can then be subdivided into virtual networks with their own access controls, which can be a major boon to organizational security.

Unfortunately, the convenience afforded by virtualization can also come with some potential security problems. For example, if attackers can compromise the VM hypervisor, they can potentially gain high levels of privilege on the virtual machines under that hypervisor, as well as access sensitive data contained in them [23]. Many other similar vulnerabilities that can stem from virtualization were listed out in a report by the InfoSec Institute [24]. For instance, a compromised guest VM with file sharing can infect the host machine. According to this InfoSec report, some of the more common virtualization attacks include VM jumping, host traffic interception, and Denial of Service (DoS) attacks.

Despite these potential vulnerabilities, with strong security settings, proper configuration and frequent monitoring for suspicious activity, virtualization can still be a very secure and convenient option for many organizations. Security steps that should be implemented include securing the individual elements of the virtual environment, protecting administrative access to the virtualization solution and securing the hypervisor properly [25]. Thus, with extra effort, a virtual network may be made secure.

V. Virtual and Augmented Reality

Another interesting technology which may eventually lead to broad security implications is virtual and augmented reality. Security and virtual reality are not yet related in any significant way, although this may change as time goes on. Rather, the relevance to this paper has more to do with the privacy risks that may be present. Virtual and augmented reality are both similar concepts. While Virtual Reality (VR) completely immerses a user in a computer-generated virtual environment, Augmented Reality (AR) simply adds virtual components and graphics to an otherwise real environment [26]. There are certainly many positives to this technology. Many experts have championed using VR for training employees in various fields [27]. For example, it has been used to train medical students in a safe and educational environment [28]. Numerous other examples also exist, from firearm training to customer service education [29]. In addition to this, many games and other forms of entertainment have been developed to take advantage of this technology. The prime example of this being Pokémon Go [30], a mobile application game which became extremely popular and brought about new interest into AR.

Unfortunately, as with many other new technologies, there are privacy concerns in VR and AR. Many of these virtual reality devices collect significant amounts of user data. For example, the privacy policy of Oculus Rift [31], a popular VR headset company, explicitly states that data such as name, email address, phone, purchase history and communications are collected [31]. While this is concerning, it is in no way peculiar to Oculus Rift. Most of the major VR headset companies collect similar data on their users [32]. For example, Pokémon Go, the previously mentioned popular mobile phone application, allowed users to login using their Google accounts, potentially exposing their user accounts to malicious hackers [33]. Similar to IoT, it is likely that these VR devices and applications are not designed with security in mind, but rather they are sped through production to meet demand. Similar as in other cases, mitigations for these privacy concerns may lie with the consumer. Users should be careful to understand and do research on devices that could be collecting personal information on them. Likewise, companies producing these types of devices should make it clear to the user what kind of data is being collected and why. In some cases, governments have even stepped in and established laws enforcing unambiguous user agreements, as is the case of EU regulation 2016/679 [34]. The issue is a complicated one,

but one that may be mitigated with proper educational awareness.

VI. Autonomous Systems

Next, it is worthwhile to discuss autonomous systems with autonomous vehicles being the primary example. The development of self-driving vehicles began as a sponsored project by the Defense Advanced Research Projects Agency (DARPA) which is an agency of the United States Department of Defense (DoD) responsible for the development of emerging technologies for use by the military. Due to the technological challenges presented by this problem, DARPA outsourced this problem to the world by eventually hosting a race in 2004 for autonomous vehicles across a desert between California and Nevada which was open to everyone, the winner of which would receive a million-dollar prize [35]. Since that time, many developers have begun working to design safe and error-free self-driving vehicles. For example, two leaders in this field are Google, with its Waymo project (https://waymo.com/) and Tesla's Autopilot (https://www.tesla.com/autopilot). Due to the still new and sometimes buggy software in self-driving cars, many states have yet to legalize and regulate them yet. As of 2017, 33 states have established legislations related to self-driving vehicles [36]. Nonetheless, there are many benefits to be seen from the concept of self-driving vehicles. For instance, people with physical or mental disabilities preventing them from driving may find new independence in such vehicles. Likewise, the labor required to operate taxis, busses or farm equipment can be redirected to other matters.

Unfortunately, there are also negative security costs associated with autotomizing vehicles. Similar to the previously mentioned Jeep hacking, many autonomous vehicles are vulnerable to hackers. Taking advantage of an autonomous vehicle's protocols, hackers could potentially crash the vehicle, disable it and attack the rider, or simply use the GPS to track the rider's coordinates [37]. Unfortunately, simply disabling an autonomous vehicle's communications with the outside world would not work either, as vehicles need to be able to communicate with other vehicles and transportation systems to effectively and safely navigate different terrains [38]. Given these threats, many experts have weighed in on the matter. Integrating intrusion detection systems into autonomous vehicles is one possible solution to the risks presented here. These intrusion detection systems have been shown to be very effective and can be used to alert the rider if their vehicle is being compromised so that they can take the appropriate actions or pull-over if needed [39] and [40]. Other mitigations which have been proposed involve adding anti-malware programs to such autonomous vehicles and isolating the victim vehicle if it becomes compromised to avoid feeding other vehicles false information [41]. With these efforts among others, it is hopeful that autonomous vehicles will become as secure as any other vehicle in the future.

VII. The Internet of Bio-Nano Things

It is then worthwhile to discuss a very important subsection of IoT, that is, the Internet of Bio-Nano Things (IoBNT) which is a very new concept. It is the idea of producing synthetic biological and technological sensors to collect and signal information [42]. The science and technology that enables this is out of scope of this paper, however, the security protecting these devices is certainly worth an examination. Given that these devices can be implanted into the human body, a vulnerability in the security of these devices can literally become a life or death situation. In one paper about security vulnerabilities in IoBNT [43], researchers show how malicious IoBNT devices can be used in biological terrorism or to hamper benign IoBNT devices. Protecting against these types of biological threats in IoBNT, as in the case of regular IoT devices, should lie in preparing secure protocols at the network layer. The potential of IoBNT to save many lives by providing monitoring and research capabilities where previously none was possible should be noted. For these reasons, security research in this field is an imperative, as failure to do so could well lead to many deaths.

VIII. Artificial Intelligence and Robots

While this concept often evokes images of robots conquering the earth, in the imagination of the public, due in large part to science fiction books and movies, the current reality is that Artificial Intelligence (AI) has brought many benefits to society at large, while at the same time also presenting risks and vulnerabilities that need to be dealt with. For example, police can use facial recognition software with embedded AI in order to capture dangerous criminals [44]. Companies like Amazon, Google and Apple have embedded voice recognition AI in their "smart" devices, such as Alexa, which can help physically disabled people perform tasks which might otherwise be difficult [45]. The ENISA report lists out some of the security challenges related to AI and Robotics [6]. While all the reasons listed are valid, probably one of the most relevant concern is that of data privacy. For AI to function accurately, one of the most important requirements is access to large amounts of data [46] and [47]. Due to this, it comes as no surprise that these devices collect large amounts of personal data relating to users in many cases. Likely the solutions to privacy issues in AI devices may lie with consumers to hold producers responsible for data collected, and to know which data that is. In some areas, such as the EU, regulation has been enacted to force developers to be more transparent with which data is used and why, which may also help alleviate these problems [48].

IX. Conclusion

In conclusion, there is a plethora of new technologies currently being developed at an unprecedented rate. Many of these technologies have been very well received and have had enormously positive impact upon their respective beneficiaries. Unfortunately, as with all wonderful and valuable technological developments, malicious actors are capable of taking advantage of weaknesses in these new technologies. This issue is only worsened by the presence of potentially severe security concerns in each of these technologies, as discussed previously in this paper. The subsequent threats which present themselves in respect to these vulnerabilities are numerous and can include anything from loss of privacy to even death in the case of a medical device exploit or a vehicle hacking. With these threats in mind, it is clearly imperative that sufficient effort be expended by researchers and developers to prevent threats like these from reaching fruition. With that said, much literature and research has been written over these topics, such as the ones cited in this paper. Research can also help to inform lawmakers and other legislators on these issues, as successfully countering the threats presented by these technologies will require no small amount of cooperation between industry leaders and lawmakers, who need to create informed legislation and guidelines to deal with these newer technologies. Likewise, even with effort by lawmakers and industry, individual consumers still need to be aware of the risks they accept each time they use a technology. Especially in regard to the many privacy concerns which arise in these concepts, an aware and informed consumer may better protect themselves from becoming the victim of a severe data breach. Nonetheless, only through high cooperation and planning can truly successful solutions be reached, and through them a more secure future can be obtained.

References

[1] C. Ryan. (2018). Computer and Internet use in the United States: 2016. *American Community Survey Reports, 39*. [Online]. Available: https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf

[2] W. L. Shiau, L. C. Huang, and Y. L. Cheng, "Pok émon go: A study on fit in virtual-reality integration," in *Proc. Pacific Asia Conference on Information Systems (PACIS)*, Langkawi Island, Malaysia, 2017, p. 141.

[3] C. Mui. (January 18, 2012). How Kodak failed. *Forbes*. [Online]. Available: https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/

[4] G. Schoonover, "Enhancing customer security: Built-in versus bolt-on," *The DoD Software Tech News, Secure Software Engineering*, vol. 8, no. 2, pp. 11-14, 2005.

[5] M. J. Ham, "BGP route attestation: Design and observation using IPV6," Masters theses & Doctoral Dissertations, Dakota State University, USA, 2017.

[6] European Union Agency for Network and Information Security (ENISA). (2018). Looking into the crystal ball: A report on emerging technologies and security challenges. Heraklion: ENISA

[7] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," in *Proc. IEEE Internet Initiative*, Piscataway, NJ: IEEE, May 27, 2015, pp. 72-73.

[8] K. Ashton, "That 'Internet of Things' thing: In the real world, things matter more than ideas," *RFID Journal*, 2009.

[9] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *Proc. International Conference on Science Engineering and Management Research (ICSEMR)*, Chennai, India, 2014.

[10] P. Middleton. (December 27, 2017). Forecast analysis: Internet of Things – endpoints, worldwide, 2017 update. *Gartner*. [Online]. Available: https://www.gartner.com/doc/3178626/forecast-analysis-internet-things-

[11] Hewlett-Packard (HP). (2014, July 19). HP study reveals 70 percent of Internet of Things devices vulnerable to attack. *HP News Advisory*. Palo Alto, CA: HP. [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[12] A. Greenberg, "Hackers remotely kill a Jeep on the highway – with me in it," *Wired*, July 21, 2015.

[13] U.S. Food & Drug Administration (FDA). (January 9, 2017). Safety communications – Cybersecurity vulnerabilities identified in St. Jude medical's implantable cardiac devices and Merlin@johm Transmitter. *Safety Communication*. Silver Spring, MD: FDA. [Online]. Available: https://www.fda.gov/medicaldevices/safety/

[14] M. Al-Shaboti, I. Welch, A. Chen, and M. A. Hahmood, "Towards secure smart home IoT: Manufacturer and user network access control framework," in *Proc. 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, Poland, 2018, pp. 892-899.

[15] J. Habibi, D. Midi, and A. Mudgerikar, "Heimdall: Mitigating the internet of insecure things," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 968-978, 2017.

[16] Pew Research Center. (2018, February 5). Social media fact sheet. Washington, DC: Pew Research Center. [Online]. Available: http://www.pewinternet.org/fact-sheet/social-media/

[17] Y. Bakos, F. Marotta-Wurgler, and D. Trossen, "Does anyone read the fine print? Consumer attention to standard-form contracts," *The Journal of Legal Studies*, vol. 43, no. 1, pp. 1-35, 2014.

[18] R. Meyer. (March 20, 2018). The Cambridge Analytica scandal, in three quick paragraphs: What it means for Facebook, for President Trump's world, and for every American *the Atlantic*. [Online]. Available: https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046

[19] The Economist. (October 6, 2018). GrrDPR; The EU's new privacy law is starting to bite Facebook: The social network is likely to face more limits on how it uses data.

The Economist. [Online]. Available: https://www.economist.com/business/2018/10/06/the-eus-new-privacy-law-is-starting-to-bite-facebook

[20] M. Madden, "Privacy management on social media sites: Most users choose restricted privacy settings while profile "pruning" and unfriending people is on the rise," in *Pew Research Center's Internet & American Life Project*, Washington, DC: Pew Research Center, February 24, 2012

[21] A. Perrin, "Americans are changing their relationship with Facebook," in *Fact Tank: News in Numbers*, Washington, DC: Pew Research Center, September 5, 2018.

[22] N. J. Lippis III, "Network virtualization: The new building blocks of network design," *Lippis Consulting White Paper*, 2007.

[23] S. J. Vaughan-Nichols, "Virtualization sparks security concerns," *IEEE Computer Magazine*, vol. 41, no. 8, pp. 13-15, 2008.

[24] T. Komperda, "Virtualization security," *InfoSec Institute*, December 17, 2012.

[25] R. Anand, S. Sarswathi, and R. Regen, "Security issues in virtualization environment," in *Proc. International Conference on Radar, Communication and Computing (ICRCC'12)*, Tiruvannamalai, India, 2012, pp. 254-256.

[26] J. Tokareva, "The difference between virtual reality, augmented reality and mixed reality," *Quora*., January 5, 2018

[27] M. Li, L. Li, R. Jiao, and H. Xiao, "Virtual reality and artificial intelligence support future training development," in *Proc. Chinese Automation Congress (CAC)*, Jinan, China, 2017, pp. 416-419.

[28] A. S. Mathur, "Low cost virtual reality for medical training," in *Proc. IEEE Virtual Reality (VR)*, Arles, France, 2015, pp. 345-346.

[29] C. Fink, "VR training next generation of workers," *Forbes*, October 30, 2017

[30] X. G. Wang and Y. J. Tang, "A case study of technology innovation approach: The construction of technology forecasting system," in *Proc. International Conference on Information Management, Innovation Management and Industrial Engineering*, Sanya, China, 2012, pp. 150-153.

[31] Oculus. (September 4, 2018). Oculus privacy policy. *Oculus Legal Documents*. [Online]. Available: https://www.oculus.com/legal/privacy-policy/

[32] C. Hunt, "VR and your privacy: How are these companies treating your data? Know where you data's going," *Windows Central*, April 20, 2018

[33] A. Griffin, "Pokémon GO privacy concerns raised after App gives itself permission to read players' Gmail messages," *Independent*, July 11, 2016.

[34] The European Parliament & The Council of the European Union, "Regulations: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General data protection regulation)," *Official Journal of the European Union, L 119/1*., May 4, 2016.

[35] A. Davies, "The WIRED guide to self-driving cars," *WIRED*, February 1, 2018.

[36] National Conference of State Legislatures (NCSL). (October 18, 2018). *Autonomous vehicles: Self-driving vehicles enacted legislation.* Washington, DC: NCSL. [Online]. Available:http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[37] A. Weimerskirch and D. Dominic, "Assessing risk: Identifying and analyzing cybersecurity threats to automated vehicles," Mcity. Ann Arbor, MI: University of Michigan, January 4, 2018.

[38] K. M. A. Alheeti, A. Gruebler, K. McDonald-Maier, and A. Fernando, "Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model," in *Proc. International Conference on Consumer Electronics (ICCE'16),* Las Vegas, NV, 2016, pp. 502-503.

[39] K. M. A. Alheeti, R. Al-Zaidi, J. Woods, and K. McDonald-Maier, "An intrusion detection scheme for driverless vehicles-based gyroscope sensor profiling," in *Proc. International Conference on Consumer Electronics (ICCE'17),* Las Vegas, NV, 2017, pp. 448-449.

[40] J. Straub, J. McMillian, B. Yaniero, M. Schumacher, A. Almosalami, K. Boatey, and J. Hartman, "Cybersecurity considerations for an interconnected self-driving car system of systems," in *Proc. 12th System of Systems Engineering Conference (SoSE)*, Waikoloa, Hawaii, 2017, pp. 1-6.

[41] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defenses," in *Proc. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, China, 2016, pp. 164-170.

[42] I. Akyidiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of bio-nano things," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 32-40, 2015.

[43] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in Bio-Nano Things communication networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 665-676, 2015.

[44] J. Kite-Powell, "Making facial recognition smarter with Artificial Intelligence," *Forbes*, September 30, 2018.

[45] A. Jesus, "AI for speech recognition – Current companies, technology, and where it is headed," *Tech Emergence*, September 19, 2018.

[46] R. Bean, "How big data is empowering AI and machine learning at scale," *MIT Sloan Management Review*, May 8, 2017.

[47] B. Marr, "Why AI would be nothing without big data," *Forbes*, June 9, 2017.

[48] D. Meyer, "AI has a big privacy problem and Europe's new data protection law is about to expose it," *Fortune*, May 25, 2018.

Thomas Lange was born in Altus, Oklahoma, USA, in 1996. He received the B.S. degree in Cyber Operations from Dakota State University in 2018 and is currently pursuing a M.S. degree in Applied Computer Science from the same university. His research interests include software security, malware analysis and machine learning.

Houssain Kettani was born in Khobar, Saudi Arabia, in 1978. He received the B.S. degree in Electrical and Electronic Engineering from Eastern Mediterranean University, Cyprus in 1998, and M.S. and Ph.D. degrees both in Electrical Engineering from the University of Wisconsin at Madison in 2000 and 2002, respectively. Dr. Kettani served as faculty member at the University of South Alabama (2002-2003), Jackson State University (2003-2007), Polytechnic University of Puerto Rico (2007-2012), Fort Hays State University (2012-2016), Florida Polytechnic University (2016-2018) and Dakota State University since 2018. Dr. Kettani has served as Staff Research Assistant at Los Alamos National Laboratory in summer of 2000, Visiting Research Professor at Oak Ridge National Laboratory in summers of 2005 to 2011, Visiting Research Professor at the Arctic Region Supercomputing Center at the University of Alaska in summer of 2008 and Visiting Professor at the Joint Institute for Computational Sciences at the University of Tennessee at Knoxville in summer of 2010. Dr. Kettani's research interests include computational science and engineering, high performance computing algorithms, information retrieval, network traffic characterization, number theory, robust control and optimization, and Muslim population studies. He presented his research in over seventy refereed conference and journal publications and his work received over five hundred citations by researchers all over the world. He chaired over hundred international conferences throughout the world and successfully secured external funding in millions of dollars for research and education from US federal agencies such as NSF, DOE, DOD, and NRC.