Engineering 4 (2018) 1–2

Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Editorial

The New Frontiers of Cybersecurity

Binxing Fang [a,b,c], Kui Ren [d], Yan Jia [e]

[a] China Electronics Corporation, Beijing 100846, China
[b] Guangzhou University, Guangzhou 510006, China
[c] Beijing University of Posts and Telecommunications, Beijing 100876, China
[d] University at Buffalo, State University of New York, Buffalo, NY 14228, USA
[e] National University of Defense Technology, Changsha 410073, China

Binxing Fang

Kui Ren

Yan Jia

Security technology is a special kind of companion technology that is developed for the underlying applications it serves. It is becoming increasingly critical in today's society, as these underlying applications become more and more interconnected, pervasive, and intelligent. In recent years, we have witnessed the proliferation of cutting-edge computing and information technologies in a wide range of emerging areas, such as cloud computing, edge computing, the Internet of Things (IoT), artificial intelligence (AI), Industry 4.0, big data, blockchain technology, and more. While these technologies hold the potential for tremendous impact, they also bring grand and inevitable security challenges. It has been observed that security incidents are growing rapidly both in number and in scale, and most cutting-edge technologies are inherently accompanied by series of security and privacy vulnerabilities. Building secure and privacy-aware environments that can provide high-quality services for the users of these new technologies thus becomes an extremely urgent task. As the frontiers of cybersecurity research extend to unexplored areas, the unique characteristics of these emerging technologies make it difficult to fit them into traditional security paradigms. It is therefore critical to identify the new characteristics, carefully examine the new security requirements of these emerging technologies, and then correctly integrate them into the early stages of development processes.

The need for computation and storage power to catch up with the pace of the skyrocketing data volume required by modern scientific and business applications has led to the development of cloud computing technology. In this context, cloud computing, a paradigm that integrates massive computing resources and offers consumable online services, emerged in favor of resource-limited cloud clients. Despite the remarkable benefits brought by this promising technique, its specific features can lead to non-negligible and unprecedented security concerns that restrict its extensive utilization. A lack of data privacy protection has been acknowledged as one of the main issues of cloud computing, especially for proprietary data or highly sensitive records. What makes the issue intractable is that encryption may result in the loss of data quality, possibly harming the original functionality of the data, such as keyword searching and mathematical computations. Potential research directions to address these security challenges include enriching the functionalities of the operations over encrypted data toward complex applications, providing a stronger security guarantee compared with existing methods, and advancing more practical implementations.

Another important future direction of the Internet is the IoT, in which interconnected physical devices in various forms—often embedded with electronics, software, sensors, actuators, and so forth—jointly perform sophisticated sensing and computing tasks and provide unprecedented services. Incorporating the IoT into our lives will revolutionize the way people interact with the physical world, and will bring enormous benefits to areas such as healthcare, transportation, and manufacturing. However, the rise of the IoT also raises increasing concern regarding the threat of cyberattacks. The ever-expanding variety of interconnected IoT devices provides an enormous attacking surface for adversaries. In addition, the combination of the heterogeneous interfaces, systems, and hardware of IoT devices poses significant challenges to securing these devices. A failure to secure IoT devices may allow attackers to access private information and/or unauthorized control of the devices.

Threats against IoT devices are also possible due to the diversified communication protocols. The wide range of wireless-access technologies currently in use not only increases the complexity of the IoT network but also exposes a large number of vulnerabilities. Exploiting these vulnerabilities might allow an intruder to sniff data generated by an IoT device or compromise the device itself. To tackle this problem, researchers have to provide solutions to protect the networked IoT devices, to empower users to enforce

https://doi.org/10.1016/j.eng.2018.02.007
2095-8099/© 2018 THE AUTHORS. Published by Elsevier LTD on behalf of Chinese Academy of Engineering and Higher Education Press Limited Company.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

security policy across various devices, to enable users to better control and manage sensitive information, and to relieve the frustration of updating devices across the board.

As an enormously powerful tool, AI brings a series of opportunities and challenges to cybersecurity. On the one hand, security techniques that range from phishing detection and surveillance systems to fundamental cryptographic algorithms are becoming increasingly powerful and intelligent with the help of AI. For example, traditional spam-detecting models are being updated by dedicated machine learning models associated with rigorous phishing analysis, which can achieve more than 99% detection accuracy. Using AI instead of human video analysts improves efficiency and accuracy as well as providing enhanced threat perception. Moreover, AI may revolutionize cryptographic techniques in the near future with the emergence of the generative adversarial network (GAN). All of the technical advancements in security brought by AI are due to its self-learning and self-enhancement capabilities. AI is capable of mining and learning various types of data, such as spam e-mails, messages, and videos, and then evolving an autonomous detection/defense system. Continuous self-training will continue to promote the performance of AI-powered systems, including their stability, accuracy, efficiency, and scalability. Therefore, AI holds great potential to transform the future of security.

On the other hand, AI is also pushing the boundaries of the abilities of hackers. Autonomous hacking machines powered by AI can craft sensitive information and find vulnerabilities in computer systems, thus making it much more difficult to fight hackers. Worse yet, AI is able to learn sensitive information, such as personal preferences, from a vast amount of seemingly insensitive data. These facts lead us to believe that hackers weaponized by AI will create more sophisticated and increasingly stealthy automated attacks that will demand effective detection and mitigation techniques.

Considering the interaction between AI and cybersecurity from another perspective, AI itself is facing various kinds of security challenges in adversarial settings. Machine learning models for certain tasks are considered to be valuable intellectual property that usually cost a great deal of effort to obtain. Such models may rely on sensitive training data or may operate in security applications. However, it has been shown that machine learning models can be stolen without prior knowledge of training data or model parameters; the functionality of the models can be duplicated using only publicly accessible query interfaces. Examples of victims include online machine learning services such as BigML and Amazon Machine Learning. Furthermore, even training data can be inferred by exploiting the confidence values that are revealed along with predictions for testing data. For example, an adversary can approximate images used in the training data for face-recognition models. In this way, the identity of participants in the training process could be revealed. Thus, it is a critical and challenging issue to protect machine learning models and training data against adversaries.

Moreover, machine learning models, especially deep neural networks, can be fooled by adversarial examples that are imperceptible to a human. Take image recognition as an example: An image that looks like a bird to human eyes could be recognized as a ship by deep neural networks, as long as the adversary adds specially crafted invisible noise to the image. This kind of vulnerability becomes a key risk in the application of AI in safety–critical scenarios such as self-driving cars and computer-aided diagnostics. Therefore, effectively detecting adversarial examples calls for great research effort in the near future.

Cybersecurity has been a continually trending buzzword over the past ten years or so. The ever-developing security techniques are inherently driven by the success of newborn technologies: the cloud, the IoT, AI, and more. The frontiers of cybersecurity technology keep expanding as continually changing security threats emerge in these underlying applications. New cybersecurity technologies will require an examination of the theoretical and engineering fundamentals of networks, computing systems, and security as a multidisciplinary subject. By investigating the system features and security requirements of underlying applications, we can eventually address challenging security problems and create a truly secure cyberspace. With this special issue, we hope to bring researchers, developers, and practitioners in security, privacy, and computing communities together to continue to shape the future of cybersecurity.

Acknowledgements

This work was partially supported by the National Natural Science Foundation of China (U1636215, 61572492, 61650202, 61772236, and 61372191) and the National Key Research and Development Program (2016YFB0800802, 2016YFB0800803, 2016YFB0800804, 2017YFB0802204, 2016QY03D0601, 2016QY03D0603, and 2016YFB0800303).