Engineering 4 (2018) 9–10

Contents lists available at ScienceDirect

Engineering

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

Topic Insights

Cybersecurity Research—Essential to a Successful Digital Future

Jackie Craig

Fellow of the Australian Academy of Technological Sciences and Engineering, Australia

1. Introduction

The ability of technology to profoundly affect our lives is exemplified by the digital transformation that is occurring in many aspects of our lives and being played out in the virtual world of cyberspace.[†] Cyberspace provides unparalleled connectivity and global reach, and is central to societal and economic well-being. Our dependence on cyberspace is increasing. At the same time, the vulnerability of cyberspace to harmful events is also increasing, and cyber threats are becoming more agile, potent, persistent, and difficult to detect and counter. As a consequence, cybersecurity is a top priority for all digital nations, and many now have national cybersecurity strategies (examples can be seen in Refs. [1,2]).

2. Cyber dependence

Cyberspace is a dynamic, evolving environment that provides us with capabilities that are not possible through other means. Governments, organizations, and individuals now rely on cyberspace to communicate, collaborate, and provide or use services, and concepts such as e-commerce, e-learning, e-research, and e-health are now part of the norm.

Devices with embedded controllers are on the increase and we are at the dawn of the Internet of Things, with an estimated 20 billion devices expected to be connected by 2020 [3]. The concept of smart cities, which carries the vision of remotely monitoring and managing critical infrastructure, public buildings, transport, businesses, and homes, is gathering pace. Already, there are smart energy meters in homes, home security systems linked to mobile phones, the promise of driverless cars, and the appearance of smart city plans (examples can be seen in Ref. [4]).

3. Vulnerability, threats, and cybersecurity research

As cyberspace grows and evolves, it becomes increasingly vulnerable due to a number of factors [5]. The increase in the number of networks, devices, and users is giving rise to an ever-expanding attack surface. Increasing interconnectedness and interdependency significantly increase risk, where a failure in one part of a system can cause cascading and far-reaching effects. Increasing complexity and outsourcing make complete visibility or securing of a system difficult to achieve. Other significant risk factors include legacy systems, poor cyber hygiene, insufficient control over the cyber technology supply chain, and an insufficient pool of trained cybersecurity professionals.

The cyber threat is persistent and continuously evolving. In the future, the threat landscape will be augmented by a greater number of hardware threats (i.e., hardware Trojans), a shift from code-based attacks to attacks on data integrity and business processes, and the emergence of systemic effects.

It is being demonstrated on a regular basis that the threat-countermeasure cycle favors the attacker. Research is essential to providing insight, tools, and methods to strengthen cybersecurity approaches and capabilities—not only to improve our current situation, but also to secure a digital future that is safe and resilient. Cybersecurity research can be broadly categorized into three areas: systems, information, and people.

4. Systems

Conceptual frameworks are useful for capturing and addressing the key elements of cybersecurity in what are complex, interconnected, interdependent, and adaptive systems. One such framework is discussed by Xiao-Niu Yang et al. in this special issue.

Regardless of the framework being used, it must be founded on the premise that it is not possible to guarantee a completely secure system; the focus must be on ensuring mission resilience in the face of harmful cyber events. This requires a whole-system approach based upon a common understanding of mission goals, shared comprehensive situational awareness, and coordinated response.

Comprehensive situational awareness is formed from data on the architecture, vulnerabilities, potential threats, cybersecurity policies, activity, and status of the system. This is a big-data problem, and research is necessary to provide the tools and techniques for the automated ingestion, processing, fusion, analysis, and display of these data in order to meet the real-time requirements of cybersecurity.

Similarly, research will be necessary for coordinated action because it provides capabilities such as decision-aid tools, tools to support effective collaboration, and artificial intelligence (AI) to generate course-of-action suggestions.

Overall, we can expect research into AI and autonomy to increase, as these will emerge throughout system architectures

[†] For the purposes of this paper, *cyberspace* is defined as being an interconnected global domain consisting of the Internet, communication networks, computer systems, and cyber-physical (embedded-controller) systems.

https://doi.org/10.1016/j.eng.2018.02.006

to supplement human capabilities in interpreting and responding to the advanced, persistent cyber threat.

5. Information

Information is the foundational resource of the digital world; as such, the availability, privacy, and integrity of information must be kept secure. Privacy has recently become a notable topic, as there have been several high-profile examples of data breaches in which the personal information of individuals has been publically released. Individuals regularly share personal information online, particularly photographs. They also regularly share information (whether intentionally or unintentionally) with online providers, who use this information in recommender systems to personalize their service. Analysis of shared information can be used to develop knowledge of an individual's preferences, social networks, lifestyle choices, and patterns of life. The importance of securing shared information therefore extends well beyond the intrinsic value of that information.

Research into privacy-preserving techniques for photo sharing ranges from manipulation of the image to techniques that help the user control distribution. It includes methods such as end-to-end encryption of part of the image, tagged photo-management schemes, and social relation impression-management techniques to recommend sharing policies (Fenghua Li et al., this special issue).

Similarly, a number of methods are being researched for privacy preservation in recommender systems. These vary based on the techniques used within the recommender systems, and are reviewed in this special issue by Cong Wang et al.

In our concern regarding privacy, we cannot ignore data integrity. Information underpins all of our decision-making and actions, and poor data integrity can have very serious consequences for system stability and business continuity. All data are subject to integrity requirements. This includes network data, traffic flows, protocols, and user data. Integrity testing includes simple processes such as checking for missing values and determining whether values sit within certain bounds. Checking the integrity of sophisticated data such as real images is complex and relies on multidisciplinary techniques to check for authenticity. This field is reviewed in this special issue by Xiang Lin et al.

6. People

People are a key element of good cybersecurity. Regardless of cybersecurity measures, humans are often the source of cybersecurity failures, be it through malicious actions or poor cybersecurity practices. Understanding human characteristics such as cognitive function, motivation, behavior, and influence is vital for maintaining and improving cybersecurity [6]. For example, an understanding of cognitive function can help shape the visualization of important cybersecurity messages. Similarly, knowledge of motivation and behaviors can provide guidance into the likelihood of cybersecurity policies being successfully implemented.

Social influence analysis provides insight into how individuals and groups can be influenced by others, and is an active area of research. There are a range of models that describe and predict social influence (Kan Li et al., this special issue). Such models can provide information on who best to influence to gain an outcome, who is most likely to be influenced, and in what way. In the area of cybersecurity, this information is a very useful tool. For example, understanding influence can help to improve the resilience of individuals to phishing—a very common and successful attack method that is increasing in sophistication.

Recognition of the importance of research into the human aspects of cybersecurity is growing. This research will shape future system design, cyber policy, and online behaviors, and will advance human factors as an integral part of cybersecurity architecture.

7. Summary

Science and technology have provided us with a digital world that we are becoming increasingly dependent upon. As cyberspace grows and changes, so does its vulnerability to attack from an ever-evolving and persistent cyber threat. Research into cybersecurity cannot be underestimated, as it is this research that will provide the solutions to make the digital world a vibrant and safe place to be.

References

[1] Her Majesty's Government. National cyber security strategy 2016–2021. London: Her Majesty's Government; 2016.
[2] Cybersecuritystrategy.pmc.gov.au [Internet]. Canberra: Department of the Prime Minister and Cabinet, Australian Government; [cited 2018 Jan 15]. Available from: https://cybersecuritystrategy.pmc.gov.au.
[3] Nordrum A. Popular Internet of Things forecast of 50 billion devices by 2020 is outdated [Internet]. New York: IEEE Spectrum; c2018 [updated 2016 Aug 18; cited 2018 Jan 15]. Available from: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
[4] Buntz B. The world's 5 smartest cities [Internet]. New York: Informa USA, Inc.; c2018 [updated 2016 May 18; cited 2018 Jan 15]. Available from: http://www.ioti.com/smart-cities/world-s-5-smartest-cities.
[5] Science and Technology for Safeguarding Australia. Future cyber security landscape: A perspective on the future. Canberra: Defence Science and Technology Group; 2014.
[6] Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8.