Accepted Manuscript

Topic Insights

Cybersecurity Research—Essential to a Successful Digital Future

Jackie Craig

PII: S2095-8099(18)30124-3
DOI: https://doi.org/10.1016/j.eng.2018.02.006
Reference: ENG 39

To appear in: *Engineering*

Please cite this article as: J. Craig, Cybersecurity Research—Essential to a Successful Digital Future, *Engineering* (2018), doi: https://doi.org/10.1016/j.eng.2018.02.006

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Engineering 4 (2018)

Topic Insights

Cybersecurity Research—Essential to a Successful Digital Future

Jackie Craig
Fellow of the Australian Academy of Technological Sciences and Engineering

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-systems 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 this 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,

[†] 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.

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/).

Download English Version:

https://daneshyari.com/en/article/6893335

Download Persian Version:

https://daneshyari.com/article/6893335

Daneshyari.com