Cybertrust in the IoT Age

Jeffrey Voas, US National Institute of Standards and Technology (jeff.voas@nist.gov)
Rick Kuhn, US National Institute of Standards and Technology (kuhn@nist.gov)
Constantinos Kolias, George Mason University (kkolias@gmu.edu)
Angelos Stavrou, George Mason University (astavrou@gmu.edu)
Georgios Kambourakis, University of the Aegean (gkamb@aegean.gr.)

Today, computing and communications are embedded in products as mundane as lightbulbs and kitchen faucets. These capabilities are said to be the result of the Internet of Things (IoT).

IoT generates new opportunities but creates new challenges with respect to trustworthiness [1]. Computing, architecture, and verification changes are inevitable to meet these challenges, particularly if predictions of 20 billion to 50 billion new IoT devices being created within the next three years come true. What will be required to provide trust in IoT? And what new opportunities will IoT bring to the computing profession and to consumers? To better understand this, let's look at a few key concerns.

First, there are numerous definitions of IoT; however, there is no robust, universally accepted, and actionable definition. That is a problem – too many different opinions that cloud the waters by making an understanding of cybertrust and IoT harder because it creates competing cybertrust perspectives. Worse, does "IoT" include any noun that you can stick 'smart' onto the front of, like "smart toy" or "smart house" or "smart city?"

Scalability and heterogeneity are cybertrust concerns. Scalability creates complexity, and complexity does not lend itself to easily verifiable trust. And heterogeneity causes problems with getting 'things' to connect and interoperate with other 'things,' particularly when they are from different and often competing vendors. Heterogeneity is an ideal economic goal because it fosters competition, but in IoT, it creates technical problems, similar to years past when there were numerous flavors of Unix and Postscript that did not interoperate well. Heterogeneity also enables security vulnerabilities related to the chain of custody.

Ownership and the control of 'things' is a cybertrust issue. Third-party black-box components (hardware or software) make trust and assurance difficult to assess by users and consumers. When a 'thing' is a black-box, your hands are tied. And liability claims are hard to enforce since there is usually not an option to opt-out of the "I agree to all terms" button.

IoT cybertrust and IoT security is not a singular problem – it is as multifaceted as are specializations in modern medicine. IoT security standards have been hard to create. IoT security measurement is also hard to develop; currently used security metrics are crude and not well designed from a metrology standpoint. In the short term, guidelines and recommendations may be the best we can offer for IoT security standards and measures.

Certification of a 'thing,' system, or service is a cybertrust challenge [2]. Why? Certification of cybertrust is nearly impossible unless the threat space and operational environment is known and

bounded. To bound requires a definition of IoT, and we already addressed that issue. Further, the cost to certify a ‘thing’ relative to the value of that ‘thing’ must be considered. And then who does the certification? What criteria do they use? And at what cost?

Other certification issues that must be considered are the impact on time-to-market and the cost to vet or certify? Further, what is the lifespan of a ‘thing’ or service? And in terms of composing ‘things,’ what if all ‘things’ are not certified? And if all ‘things’ are certified, that still does not mean they will interoperate correctly in a fixed environment? Certifying ‘things’ as standalone entities does not solve the fundamental problem of trusting a system that resides in a specific environment. These are concerns for IoT cybertrust.

IoT cybertrust cannot ignore reliability. Who is to blame when a ‘thing’ fails? What is the probability that a ‘thing’ will fail? In other words, what is the risk associated with using a specific ‘thing’? Also, which “ility” is more important to address for cybertrust: reliability, security, privacy, performance, resilience, etc.? Were faulty or subpar architectures employed? Were the ‘things’ that were employed defective, and were the best ‘things’ available at that time used? Was the IoT system over-engineered and too much money spent? And it is foolish to discount the importance of the expected operational usage profile. Do you know the environment and context your IoT system will exist in? And is your system designed with respect to the expected operational usage profile? The point here is that IoT cybertrust cannot ignore reliability.

IoT testing is also a cybertrust concern. This is partially due to scalability and heterogeneity, but more importantly, it is the massive number of combinations of potentials inputs and the fact that many IoT systems control actuators and have binary or very small output spaces [3].

Data is the lifeblood of IoT systems. Where data originates from has an impact on cybertrust. Leased data originates from vendors at the time of their choosing and with the integrity of their choosing. The possibility of data tampering cannot be dismissed. Data integrity is pivotal. Knowing how secure data is from accidental problems or malicious tampering, delay, or theft is a cybertrust concern. Further, what about faulty interfaces, faulty communication protocols, unreliable clouds or clouds that leak data, and unreliable wireless service providers? These too are IoT cybertrust concerns.

And finally, artificial intelligence (AI) is associated with “smart.” With access to the computing power offered by clouds and the refinement of machine learning and other AI techniques, AI is a mainstay in automation, robotics, and the Industrial Internet of Things (IIoT). But how do you trust the AI algorithms and implementations? Must you be a quant to do so?

This special issue is devoted to such questions, through five research papers:

Roman, Lopez, and Gritzalis introduce some of the changes in information security accompanying the adoption of IoT, in "Evolution and Trends in the Security of the Internet of Things." In many areas, the challenges of IoT security have been met by adapting existing approaches, but for some problems, advances have been limited. These include forensics and human factors aspects of security and usability. Additionally, it is not clear how to do security engineering for IoT, due to the significant differences between these systems and traditional

client-server environments. While research has lagged in some of these areas, some interesting new developments may dramatically change the way security can be engineered for IoT systems. These include physical unclonable functions, hardware elements that work like one-way functions, with fingerprints that are easy to evaluate but hard to predict. The authors survey these and other developments, charting where progress is being made and where significant hurdles remain for protecting IoT systems.

In "IoT as a Land of Opportunity for DDoS Hackers," Natalija Vlajic and Daiwei Zhou investigate the changes to DDoS risks being brought about by IoT equipment and search engines specifically focused on these small devices. By gathering all the information that a hacker would need for a DDoS attack using webcams, the authors show the ease with which an actual attack could be organized and carried out. They suggest that the attack potential of these devices may differ in both degree and in kind compared with conventional attacks on servers. In particular, the existence of search engines that make it possible to identify large numbers of potentially vulnerable IoT devices, through highly specific search parameters, makes it possible for attackers to skip the reconnaissance step in gathering devices for a botnet. At the same time, IoT devices studied in the paper generally had little or no adherence to industry standards for anti-DDoS protection, as outlined in IETF RFC 4987. Recommending this RFC and other specific provisions, the authors outline a series of criteria for both vendors and users of IoT devices to reduce the DDoS threat.

Detecting attacks in IoT systems is particularly challenging because of the rapidly changing size and configuration of subnets. Weizhi Meng provides a case study showing how this problem can be addressed, in "Intrusion Detection in the Era of IoT: Building Trust Via Traffic Filtering and Sampling." The case study illustrates the application of packet filtering and sampling in a hierarchical IoT network, using both Bayesian and blacklist-based filtering, and two different sampling methods. The article identifies conditions under which intrusion detection techniques can be reasonably effective, and factors that reduce this effectiveness. Challenges remain in applying filtering and sampling, and the author summarizes aspects of attack models and limitations of Bayesian approaches in the IoT environment, demonstrating the need for different detection methods and finding the right balance among multiple techniques.

One approach to securing privacy is the use of attribute-based credentials. De Feuntes, Gonzalez-Manzano, Solanas, and Veseli describe this method in "Attribute-Based Credentials for Privacy-Aware Smart Health Services in IoT-based Smart Cities." The authors provide illustrative scenarios in which smart city technologies can improve the life of citizens, while simultaneously protecting their privacy. They advocate the use of attribute-based credentials, where users obtain some credentials or assured attributes from an issuer. With these, users can then create tokens proving possession of the credentials without revealing any other information, using zero-knowledge proofs possibly with blind signatures. Commercially available systems are analyzed in the context of realistic health scenarios, recommending one technology as the most effective for the hypothetical applications.

Beyond technical issues, IoT also presents new complications for law and regulations, as a result of some of the same factors that bring technical challenges. Singh, Millard, Reed, and Crowcroft

highlight some of the many legal issues of IoT in "Accountability in the Internet of Things: Systems, Legals, and Ways Forward." In particular, IoT components may be owned and operated by different organizations, separated by management and geography. Additionally, the dynamic nature of IoT systems means that relationships among responsible parties are ever changing, and individual devices may be used simultaneously by multiple parties for different purposes. Yet accountability is critical to the success of the IoT industry, as it is in any IT field. This article gives insights into accountability aspects including governance and responsibility; privacy and surveillance; and safety and security issues, providing a valuable background that is essential but often not well understood by technologists.

The papers in this special issue were selected to explore the state of cybertrust and IoT. We hope that readers will find these articles an interesting and informative introduction to the challenges of developing trust in IoT-based systems.

References

[1] I. Bojanova and J. Voas, “Trusting the Internet of Things”, Guest Editor Intro, *IEEE IT Pro*, October 2017
[2] J. Voas and P. Laplante, “IoT’s Certification Quagmire”, *IEEE Computer*, April 2018
[3] J. Voas, R. Kuhn, and P. Laplante, “Testing IoT-based Systems”, 12th IEEE International Symposium on Service-Oriented System Engineering, March 26-29, 2018, Bamberg, Germany