Towards Trustworthy Smart Cyber-Physical Systems

M.W. David[1(✉)], C.R. Yerkes[1], M.E. Simmons[1], and W. Franceschini[2]

[1] National Intelligence University, Washington D.C., USA
{michael.david_cntr, christopher.yerkes, mitchell.simmons2}@dodiis.mil
[2] U.S. Army General Staff, Washington, D.C., USA
wilfredo.franceschini.mil@mail.mil

Abstract. This paper looks at issues facing the design and operation of trusted, smart cyber-physical systems (CPS). It does this within the context of current efforts related to developing trusted hardware and software, and identifies issues related to those efforts. The paper also looks at several emerging technologies related to wireless systems, artificial intelligence and security analytics; and assesses how they may be leveraged to advance the goals of current and future efforts to create, operate and maintain trusted smart CPS. The views expressed do not reflect the official policy or position of the National Intelligence University, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

Keywords: Cyber-physical systems · Internet of Things · Trustworthiness · Wireless · Artificial intelligence · Security analytics

1 Introduction

"We can establish trust among a small group of people known to us, but it's harder to achieve trusting relationships on a larger scale" [1]. Vinton Cerf made this comment in a brief commentary back in 2010 when addressing the topic of trust and the Internet. It was true then, and even more relevant now due to continued rapid development and expansion of global supply chains, wireless networks, smart phones and devices, Big Data and data science. A system of trust is imperative to the exchange of all data and communications [2]. As noted by Huang et. al., it is challenging for computer scientists to build metrics-based trust models applicable in large scale; for instance, attempting to codify social sciences' thrust concepts into Pretty Good Privacy (PGP) signature chains [3]. A more recent publication by Huang describes how the Internet of Things (IoT), together with cloud computing, mobile computing, and social computing, will lead to novel Cyber Physical Social Smart Systems (CPS3), such as smart supply chains, smart manufacturing, smart cities, smart product life cycle management.., and so on [4]. However, without strong security foundations, moving beyond traditional protection mechanism—lightweight cryptography, secure protocols, and privacy assurance—, malicious hacks and or glitches in the IoT will outweigh any of its benefits [5].

K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 392–399, 2016.
DOI: 10.1007/978-3-319-50011-9_30

Developers must evaluate current technologies and security protocols and decide if adaptations or entirely new designs will better accomplish the desired security goals. We need to consider IoT cybersecurity problems from a perspective of IoT. In general, although security may not turn out to be a real obstacle in the implementation of IoT, the adoption will have wider and deeper impacts on the general population because it will be immersed into our daily lives. The United States government has undertaken a number of measures and programs in order to deal with its needs for trusted systems. This paper describes some of these activities in order to provide awareness, as well as stimulate dialog and research that will support the goals and objectives of these activities.

2 Trusted Software and Hardware Activities

2.1 The Software and Supply Chain Assurance Forum

Due to repeated cyber based intrusions into critical infrastructure, U.S. Presidential Executive Order (EO) 13636 was issued in 2013, and Section 8(e) required the Department of Defense (DoD) and General Services Administration (GSA) to submit recommendations to the President on improving the cybersecurity and resilience of the nation through the Federal Acquisition System [6]. The EO 13636 vision was to improve cyber security of critical infrastructure through greater government and private sector partnerships. It resulted in a DoD-GSA Report, entitled "*Improving Cybersecurity and Resilience Through Acquisition*", which makes six acquisition reform recommendations and identifies issues relevant to implementation [7]. With EO 13636 and the Report as its backdrop, the Software and Supply Chain Assurance (SSCA) Forum has explored how public and private sector organizations through greater partnering arrangements are addressing various aspects of supply chain risk through their procurement activities and what further improvements might be made in the future.

2.2 Trusted Access Programs

The National Security Agency created its Trusted Access Program Office (TAPO) for the DoD and the U.S. Intelligence Community (IC) to provide guaranteed access to trusted microelectronics technologies for their critical national security based system needs. TAPO's objectives are to provide the DoD and the IC a trusted supplier path for [8]:

- Guaranteed access to trusted foundry suppliers for mission applications.
- Ability to fabricate classified designs up to the secret level.
- Access for low volume customers to leading edge technology.
- Quick turnaround times for prototyping and production.
- Technology support through industry partnership.

The DoD created its own Trusted Defense Systems Strategy based on DoD Instruction 5200.44 in November 2012, which was updated in August 2016, to provide additional focus on cybersecurity. DoDI 5200.44 establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be

impaired due to vulnerabilities in system design or sabotage, or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements. This is also extended to include all spare or replacement parts and software upgrades to those mission critical functions or critical components over their full life cycles. Basically, the intent is to achieve Trusted Systems and Networks (TSN) [9].

In a related activity, the goal of Defense Advanced Research Project Agency's (DARPA) Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program is to eliminate counterfeit integrated circuits from the electronics supply chain by making counterfeiting unprofitable from a complexity and time perspective. SHIELD seeks to combine NSA-level encryption, sensors, near-field power and communications into a microscopic-scale chip capable of being inserted into the packaging of an integrated circuit. This 100 × 100 μm "dielet" will act as a hardware root of trust, detecting any attempt to access or reverse engineer the dielet. Authentication of the integrated circuit will be achieved by an external probe that provides power to the dielet to establish a secure link between the dielet and a server, and the designed fragility of the dielet also makes it inherently more tamper resistant from physical removal or alternation [10].

3 Artificial Intelligence and Security Analytics

Security and trust have been a unique challenge in the design and adoption of information systems since the early days of their development. Unintentional and intentional vulnerabilities can be imbedded deep within the design of our hardware and software. This design challenge has been exacerbated and become increasingly more complex as our technology has moved from standalone hardware into the age of distributed and tightly networked information systems. With advances in and infusion of artificial intelligence (AI) technology as it applies to autonomous vehicles, weapon systems, and intelligent personal assistants, as well as a host of other systems, the issue of trust will undoubtedly persist [11, 12].

Trust in AI systems can be sectioned into three broad categories: (1) Integrity of Data, (2) Integrity of AI Algorithms and Hardware at an operational level, and (3) Integrity of Hardware and Software Design. Both Data Integrity and Integrity of Design are broadly covered under the Trusted Software and Hardware Activities section of this paper. Much of the trust work in this area depends on development of trusted hardware manufacturing, software development and supply chains.

The unique aspects of trust in AI systems, for instance, the integrity of algorithms and hardware, has garnered much recent attention. Several prominent technology developers and scientists, including Elon Musk, Bill Gates and Stephen Hawking, have expressed concern that AI could pose an existential threat to mankind, in an open letter on *Research Priorities for Robust and Beneficial Artificial Intelligence* [13]. One hundred and fifty AI scientists and technologists call for research on the societal impacts of advanced AI. This concern has also reached the highest levels of government with the White House Office of Science and Technology Policy releasing a June 2016 *Request for Information on Preparing for the Future of Artificial Intelligence*

[14]. One of the primary concerns is that AI systems of the future are expected to learn and develop with little or no human intervention in an autonomous fashion mimicking the behavior of living organisms. Automated machine decision processes could potentially be developed that lack the ethical conceptual frameworks of human decision processes.

Entirely new models of trust and security will be required to address this concern as technology develops. Frameworks of machine-to-machine trust will need to be conceptualized, designed and implemented. Situations never before encountered, the bane of the designer, will inevitably be part of the process. As AI algorithms play an ever increasing role in our lives we will need to understand how trust, security and advanced automation interplay.

As noted in the introduction, we also need to consider the IoT, and the enormous amounts of data and security problems it creates, from an IoT perspective. That being said, it may be somewhat difficult to describe the perspective of IoT. One view suggested by the Potomac Institute for Policy Studies (PIPS) is a redefined "data, information, knowledge, and wisdom" (or DIKW) framework. PIPS has proposed a framework or thought process to apply to IoT issues. The construct is intended to assist analysts in understanding intelligence, regardless of source, in terms of distinct levels of complex thinking to measures individuals' unique physical or behavioral characteristics in order to recognize or authenticate their identity [15].

As already mentioned, the wide adoption of the IoT and other cyber-physical systems will have significant impacts, and inevitably, unexpected consequences. With respect to Big Data, CPS devices are expected to generate an unprecedented flood of "real world information," possibly pushing current Big Data architectures to new limits [16]. Advances in machine learning and AI will likely alleviate scalability challenges, but the aggregation and correlation of CPS Big Data involving real-world entities and people will raise privacy and security concerns.

4 Emerging Technologies

Since the scope of this paper is limited, the intention is to only touch on two items in this section, and both are related to wireless systems.

The first is related to research on wireless product design and fabrications at Finland's Aalto University's Radio Science and Engineering. They have reportedly developed a method that allows 50 year old analog technology antennas to shift into the digital world. Antennas are typically tuned only to a few frequencies but using multiple smaller antennas can, with the help of advanced digital electronics, operate digitally with any frequency thus making them reconfigurable to changing environments such as intentional jamming or background interference. The removal of a larger antenna in exchange for smaller ones makes phone design much less complex. This could possibly allow for larger phone screens, lengthen battery life, and facilitate increased data transfer speeds from 100 to 1,000 times faster. Furthermore, this new antenna concept permits the creation of more compact antennas with better radiation efficiency and thus greater range of use from the base systems. Due to the correlation of greater radiation efficiency to greater distances, this means a lower cost physical network to operate and

maintain [17]. A paper entitled "Concept for Frequency Reconfigurable Antenna Based on Distributed Transceivers" describing the principles of the method has been published in IEEE's *Antennas and Wireless Propagation Letters* [18].

The Defense Advanced Research Projects Agency (DARPA), which serves as a key research arm of the Department of Defense, is focused on wireless systems to exploit the power of the IoT to help the U.S. dominate battlefields. DARPA is funding the development of sensors and artificial intelligence systems that could help break into, extract and analyze information from, enemy devices and communication systems. The components and systems will arm the U.S. with more data to analyze enemy moves and strategy.

DARPA has some interesting projects, as stated by a collaborating company representative supporting a DARPA program. "They are talking about going into any situation and extracting information at any time, [with] artificial intelligence systems that can attack and hack any network," said Jim McGregor, principal analyst at Tirias Research [19]. The DARPA program mentioned plans to fund the development of sensors and electromagnetic systems that could access point-to-point wired and wireless communications, even ones that are not linked to the internet.

In another initiative, DARPA announced the intent to develop components that can operate in a dynamic and contested electromagnetic spectrum by leveraging machine learning for spectral reasoning. The same announcement acknowledges that "extensive heterogeneous sensor arrays" will be part of future conflicts, therefore, DoD needs tactical sensors with "novel sensing modalities", higher performance, and lower costs."

It should be noted that not all DARPA research comes to fruition or reaches operational capability. However, the goal of being able to identify and select relevant data at the front end of the collection cycle, would certainly contribute to being able to predict or respond to an emerging situation.

In addition to leveraging technology to enhance warfare, DARPA is interested in developing the knowhow for detecting and recovering from cyber-attacks on US critical infrastructure. The Rapid Attack Detection, Isolation and Characterization System (RADICS) program will research early detection of cyber threats against the power grid and how to reduce the time required to restore service [20]. Understandably, technological breakthroughs in industrial control systems (ICS) cybersecurity—e.g. threat detection and/or machine-to-machine data analytics—are expected to propagate to CPS and the IoT.

5 Dealing with the Issues and Recommendations for Future Research

Academia and industry are working hard to develop tools and technologies to deal with some of the issues raised above.

For example, in the area of Artificial Intelligence and security analytics, IBM Research and the University of Maryland Baltimore County (UMBC) have launched a project to collaborate on the advancement of cognitive cybersecurity. Traditional security systems can ingest the massive amount of security data but the ability to process it for exploitation is lacking. By exploring the intersection of cybersecurity and

cognitive technology, the IBM-UMBC team hopes to better exploit this large amount of security data and evolve how security professionals and technologies collaborate to help overcome cyber threats. The project involves the creation of the Accelerated Cognitive Cybersecurity Laboratory (ACCL) which is opening in the Fall of 2016. The lab will work to advance the application of cognitive computing to cybersecurity through data analytics and machine learning. It will also explore the optimization of computer power for very large data throughput [21].

In relation to the trusted hardware and software issue, several interesting proposals have been made by academic and industrial researchers. For example, Columbia University has proposed a new Trojan detection tool called FANCI (Functional Analysis for Nearly-unused Circuit Identification). It is part of a proposal designed to discover backdoors in hardware designs prior to the fabrication using functional analysis. If backdoors can be detected statically, then the design can be fixed or rejected before it is sent to the market [22].

Interestingly, researchers in China are also looking into the area of trust verification and the hardware Trojan issue. They have proposed a tool called FASTrust (Feature Analysis for Third-Party IP Trust Verification). It is designed to address shortcomings in existing hardware trust verification techniques, which suffer from high computational complexity, low extensibility and inability to detect implicitly-triggered hardware Trojans (HT). Reportedly, it is different from existing HT detection methods, and lab results show that FASTrust is able to detect all HTs from TrustHub benchmarks and DeTrust benchmarks [23].

Researchers in India are also working on trusted systems and Trojan detection schemes. In one case, the focus is on Advanced Encryption Standard (AES) related hardware. They note that an adversary may insert hardware Trojans to destroy a system at some future time or leak the confidential information or secret keys it is supposed to protect [24].

The above items offer some solutions for specific issues, but in the IoT we are dealing not only with systems-of-systems, but multiple smart cyber-physical systems. All the way from DARPA's "dielet" to Smart Cities, all of these devices produce huge volumes of data, and we must leverage artificial intelligence and machine learning to take advantage of it. As noted by Dr. J.A. Stankovic, new research problems arise due to the large scale of interconnectedness between devices, and the increased volume of connections to the physical world. To deal with this, more cooperation is needed between the research communities in order to advance the underlying technologies in the right direction, and create, operate and maintain trusted smart CPS [25].

References

1. Cerf, V.G.: Trust and the internet. IEEE Internet Comput. **14**(5), 95–96 (2010)
2. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., et al.: Keys under doormats: mandating insecurity by requiring government access to all data and communications. J. Cybersecurity **1**(1), 69–79 (2015)

3. Huang, J., Nicol, D.: A formal-semantics-based calculus of trust. IEEE Internet Comput. **14** (5), 38–46 (2010)
4. Huang, J., Seck, M.D., Gheorghe, A.: Towards trustworthy smart cyber-physical-social systems in the era of internet of things. In: 2016 11th System of Systems Engineering Conference (SoSE), pp. 1–6. IEEE (2016). https://fs.wp.odu.edu/j2huang/wp-content/uploads/sites/…/SoSE2016-CPS3Trust.pdf. (Accessed 5 Sep 2016)
5. Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Comput. **44**(9), 51–58 (2011). http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6017172. (Accessed 18 Sep 2016)
6. Exec. Order No. 13636, 3 C.F.R (February 2013). https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (Accessed 5 Sep 2016)
7. Department of Defense and General Services Administration (GSA). Improving Cybersecurity and Resilience Through Acquisition. Report, pp. 1–23 (2013). http://www.gsa.gov/portal/mediaId/185367/fileName/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.action. (Accessed 5 Sep 2016)
8. National Security Agency (NSA). https://www.nsa.gov/business/programs/tapo.shtml
9. Department of Defense Instruction 5200.44. www.dtic.mil/whs/directives/corres/pdf/520044p.pdf. (Accessed 17 Sep 2016)
10. Defense Advanced Research Projects Agency (DARPA) SHILED Program. http://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense
11. Karger, P.A., Schell, R.R.: Multics security evaluation: vulnerability analysis. In: Proceedings of the 18th Annual Computer Security Applications Conference, pp. 127–146. IEEE (2002)
12. Thompson, K.: Reflections on trusting trust. Commun. ACM **27**(8), 761–763 (1984). http://dl.acm.org/citation.cfm?id=358210
13. Russell, S., Dewey, D., Tegmark, M.: Research priorities for robust and beneficial artificial intelligence. AI Mag. 105–114 (2015)
14. Office of Science and Technology, The White House. https://www.whitehouse.gov/webform/rfi-preparing-future-artificial-intelligence
15. Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/studies/DIKWIntelligence2AugFINAL.pdf. (Accessed 5 Sep 2016)
16. Jara, A.J., Genoud, D., Bocchi, Y.: Big data for cyber physical systems: an analysis of challenges, solutions and opportunities. In: 2014 Eighth International Conference on Innovative Mobile and Internet Service in Ubiquitous Computing Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 376–380. IEEE (2014)
17. Aalto University Press Release: new digital antenna could revolutionize the future of mobile phones. http://www.aalto.fi/en/current/news/2016-08-31-002/
18. Hannula, J.-M., Holopainen, J., Viikari, V.: Concept for frequency reconfigurable antenna based on distributed transceivers. IEEE Antennas Wirel. Propag. Lett., 24 August 2016 (2016). http://dx.doi.org/10.1109/LAWP.2016.2602006. (Accessed 18 Sep 2016)
19. Narayan, S.: DARPA See IoT and AI as ways to dominate new wars. http://www.techgig.com/tech-news/editors-pick/DARPA-sees-IoT-and-AI-as-weapons-to-dominate-wars-63910
20. Defense Advanced Research Projects Agency (DARPA): Rapid Attack Detection, Isolation and Characterization Systems (RADICS). Advertisement. FedBizOpps.gov., 11 December 2015. https://www.fbo.gov/index?s=opportunity&mode=form&id=cecbcd2b6ae554c874b4b3a326887949&tab=core&_cview=1
21. Rao, J.R.: IBM and UMBC Collaborate to Advance Cognitive Cybersecurity. In: News Release, May 10, 2016. IBM News Room (2016). http://www-03.ibm.com/press/us/en/pressrelease/49684.wss. (Accessed 17 Sep 2016)

22. Waksman, A., Suozzo, M., Sethumadhavan, S.: FANCI: identification of stealthy malicious logic using boolean functional analysis. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pp. 697–708. ACM (2013). http://www.cs.columbia.edu/~simha/preprint_ccs13.pdf
23. Yao, S., Chen, X., Zhang, J., Liu, Q., Wang, J., Xu, Q., Wang, Y., Yang, H.: FASTrust: feature analysis for third-party IP trust verification. In: 2015 IEEE International Test Conference (ITC), pp. 1–10. IEEE (2015)
24. Kumar, K.S., Chanamala, R., Sahoo, S.R., Mahapatra, K.K.: An improved AES hardware Trojan benchmark to validate Trojan detection schemes in an ASIC design flow. In: 2015 19th International Symposium on VLSI Design and Test (VDAT), pp. 1–6. IEEE (2015)
25. Stankovic, J.A.: Research directions for the internet of things. IEEE Internet of Things J. **1** (1), 3–9 (2014)