Innovation Crossover Preliminary Research Report
IT/Cyber – Cybersecurity

Context/Scope

This paper represents research conducted by OVO Innovation for the NSWC Crane Innovation Crossover event October 12-13, 2016. This research is intended to provide more insight into key challenges that were identified within the four technology clusters (Advanced Manufacturing, Cyber/IT, Life Sciences and DoD Technologies) first documented in the Battelle report. OVO consultants interviewed subject matter experts (SMEs) from the private sector, academia and the government identified by NSWC Crane to gather insights into key challenges in each cluster. This report is meant to inform the participants of the Innovation Crossover event and identify new research and new technologies that might address the key challenges.

This research was collected during August and September, 2016. The reports were submitted by OVO to NSWC Crane in late September 2016.

Introductory Narrative

The Innovation Crossover event, scheduled for 12-13 October 2016 in Bloomington is the culmination of months of planning and hard work. Some of this preparatory work involved the initial Battelle study which identified key technology clusters (Advanced Manufacturing, Life Sciences, Cyber/IT and DoD Technologies) in southern Indiana. From these clusters NSWC Crane and its contractor OVO Innovation conducted further, more detailed research, to examine detailed challenges and opportunities in each technology cluster. The reports attached document the research OVO conducted with subject matter experts identified by NSWC Crane in academia, industry and in the government. The reports are meant to document specific challenges within each technology cluster that could become areas of joint research and cooperation across the three constituents in southern Indiana. The reports are provided to you to help you prepare for your participation in the upcoming Innovation Crossover event and to frame both the challenges and active research underway to address these challenges.

Problem Statement

Cybersecurity Challenge

Crane Problem Definition

- Context: Making cyberinfrastructure relevant and useful. We face an increasing diversity in cyberinfrastructure (research IT) hardware systems and delivery mechanisms (supercomputers, clouds, containers, etc.) This increase in diversity comes at the same time as ever increasing needs for utility of cyberinfrastructure systems across many diverse areas of research, development, and commerce. There is a real challenge in meeting critical needs for US security and global leadership in an environment of such great change. Be sure to examine vulnerabilities between hardware, software and wireless communications as part of this challenge.

Problem Context

- Cybersecurity is a huge and rapidly expanding field with many areas of research underway
- The Subject Matter Experts (SMEs) specified by NSWC Crane identified two major cybersecurity themes that need focus:
  - Addressing cybersecurity/vulnerability at a systems level
  - Keeping data private

Problem Context

Addressing Vulnerability at a Systems Level

- Systems have vulnerabilities that exist in different levels—hardware, software, communication, and physical
- Most vulnerability analyses are focused on a specific level. For example
  - Hardware might focus on trusted electronics
  - Software might focus on injection, buffer overflow or operating systems
  - Communication might focus on probing or spoofing
- We need an integrated effort to get everyone thinking outside their particular domain. Security, reliability, and accountability are ultimately what we are looking for, and those transcend individual components of the system

Problem Context

Addressing Vulnerability at a Systems Level

- Drone example
  - We can analyze the software that controls the drone to identify buffer overflow, injection, etc., and patch the software to prevent attackers from utilizing these vulnerabilities.
  - More advanced attackers will understand the control model for the drone, identify the most brittle parameter and tweak that slightly, which looks harmless but long term will cause physical damage. The software isn't changed, so the vulnerability is not detected; however the system is compromised and the drone fails
- Stuxnet used a very minor adjustment of centrifuge speed that looked like a normal variation but eventually damaged the rotors
- The Internet of Things (IoT) is making the system level vulnerability increasing important, since there are physical things that can cause significant damage. IoT include software, hardware, and, in many cases, control of physical systems

Problem Context

Addressing Vulnerability at a Systems Level

- Individual components are becoming too complex to completely test
  - Software has made great strides but complexity is limiting our abilities. Given an unknown binary (no source) code, we can construct vulnerability. Within the last 10 years, DARPA, ONR and others have shown great progress. However, as systems scale, move to the cloud, and become increasing complex, we are unable to keep up with complete testing, which leaves us open to vulnerability.
  - Hardware is becoming hugely complex with billions of transistors—our ability to do complete coverage testing leaves us vulnerable. One approach to this has been to attempt to validate trusted electronics (which is a challenge being addressed at the Crossover Event)
  - Wireless communications are sniffable and data can be sent independently of the system. For example, at a recent cybersecurity conference, UK researchers showed how to capture communication signals from a key fob and duplicate them to break into any number of cars.

Problem Context

Addressing Vulnerability at a Systems Level

- Testing technology has been unable to keep up with the increasing scaling and complexity of systems
  - This means that we have to settle for “reasonable coverage” in order to deliver systems in a timely, and therefore cost effective, manner. This leaves systems open to attackers
  - Accuracy suffers as well. State of the art testers yield many more warnings for both hardware and software, resulting in many false positives which are expensive to track down or result in vulnerabilities when true positives are ignored
- Testing at the hardware, software, communications, and physical levels ignores vulnerabilities in the interfaces between components.
  - This could lead to breaches taking advantage of tweaking multiple components in an undetectable way so that their interactions cause failure.

Problem Context

Addressing Vulnerability at a Systems Level

- Addressing vulnerabilities at individual levels lags attacks. A big challenge is that everyone is trying to patch a house that is on fire and falling down. Instead of reacting, we need to be better at delivering systems that are secure at delivery.
- The speed at which new devices (e.g., mobile is exploding) are introduced limits our ability to keep up with vulnerabilities
  - Software innovation is so fast compared to hardware (which is rate limited because it is physical) that it is impossible to keep up with vulnerabilities.
    - We don't know whether the person coding has any knowledge of security
    - There are many ways to develop software
    - There are, in general, no financial incentives for many coders to address vulnerabilities

Problem Context

Addressing Vulnerability at a Systems Level

- Standards can't keep up with development. They take time and money, and by the time they are implemented, systems have advanced to the next state.
- Scalability, completeness, and accuracy all suffer from increased complexity. We need to address these at the system level.

Problem Context

Keeping Data Private

- The amount of data gathered, stored, and transmitted has exploded
  - Sensor technologies are everywhere. Some, like cameras, capture large amounts of data.
  - Multimedia data for entertainment routinely streams across the internet
  - Massive amounts of personal data (e.g., medical, financial) are generated everyday
- A big challenge identified by the interviewed SMEs is keeping data private.
- This is related to vulnerability challenge in that breaches of systems expose data; it is also a separate challenge, since data is routinely transferred between systems

Problem Context

Keeping Data Private

- Visual processing poses challenges in addition to keeping stored data private
  - We have powerful processing algorithms that can identify people, infer people's emotional state, etc., which are very useful when use appropriately
  - In order to identify things we want to protect, we have to gather lots of data which can cause privacy issues. For example, in gathering and storing visual data to identify possible terrorists or criminals, we also gather and store data on bystanders. This data could be used later and violate the privacy of those subjects.
  - This can make the very thing you seek to protect more apparent
- Large data sets limit the real time processing of data, resulting in more data being stored, which increases vulnerability
- Fears of privacy violations reduce data sharing, which decreases our ability to utilize the data. For example, medical data might not be shared, which means that a patient might not receive the best care.

Problem Context

Keeping Data Private

- How do we respect personal privacy while protecting people from bad things happening or while sharing data that can help good things happen?
- If we could share data securely, we can enable better collaboration, which means we can solve problems like keeping people safe, curing diseases, etc.
- Knowing how data flows and keeping it private can help alleviate vulnerability issues as well—if a system is vulnerable but the data is not, we have limited the ability of an attacker to affect us

Addressing Vulnerability at a Systems Level

- Current technology addresses system components, not the entire system
  - Most organizations practice good hygiene—the have good administrators, apply the right patches for software issues, minimize software installations, require two factor identification, etc. These are "ticket to ride" items—they deal with what we currently know and they deal with the software component
  - Trusted systems for electronics (hardware) are becoming more and more difficult as more and diverse suppliers enter the supply chain (see Trusted Electronics challenge)
  - The computers are only a portion of what we need to address. Knowing the data flows, where data is, and what the data is doing would help us monitor at the system level
- Very little technology exists to address the interfaces between system components

Technologies

Addressing Vulnerability at a Systems Level

- Testing technology has not scaled as fast as software and hardware advances
  - Software vulnerability is very well established. Given an unknown binary (no source) code, we can construct vulnerability—you can supply an input and make things evident automatically. Within the last 10 years, DARPA, IARPA, ONR have shown great progress.
  - However, the computational power can't keep up with advancing software. Coverage is shrinking and there are less and less financial incentives for the trade off between coverage and time, unless the organization directly depends on the vulnerability (financial institutions, for example, depend directly on protection so they expend resources, whereas medical data affects the patient more than the healthcare provider, so there are fewer resources expended)
  - Similarly, as hardware becomes more and more complex, testing technology has not kept pace

Addressing Vulnerability at a Systems Level

- The Internet of Things is currently in the wild west state
  - More and more physical devices are being connected via intranets and the Internet
  - Many different technologies are used for IoT devices, even where the functionalities are the same (e.g. microcontrollers, Bluetooth, and Wi-Fi components). Few component manufacturers implement security—it is generally up to the software running on the component
  - There are a multitude of protocols for sharing data across IoT devices and systems, each with its own vulnerabilities
  - Until recently, security was not a primary concern for IoT products, which leaves many products in the field vulnerable
  - There is no current standard for IoT devices for hardware, software, communications or physical configurations

Technologies

Addressing Vulnerability at a Systems Level

- Machine Learning technologies show promise for helping solve this challenge
  - Machine learning could be applied at the systems level to understand how to look for patterns that indicate vulnerabilities
  - Machine learning has the capability to recognize for more complex patterns than humans, which might allow for more complete testing and different ways of looking at the problem
  - Machine learning has the potential to evolve faster than current human-based testing

Technologies

Keeping Data Private

- Technology to perform faster embedded processing could address this challenge
  - If data was processed at the capture point, only the results would need to be transferred, rather than all the data, resulting in protecting ancillary data that could be compromised.
    - For example, researchers at the University of Kentucky have developed a stereo camera that estimates the depth of the scene, sets thresholds, and only captures data within a specific depth of the scene. This prevents people outside the range of interest from being part of the data set. Applications include police body cameras and security cameras.
    - Currently the processing is too complex to be completely embedded. Data still has to be distributed over the network, which is less secure and results in data being in multiple places (another security risk)

Keeping Data Private

- Technology to perform processing on encrypted data can help with this challenge
  - For example, if a phone conversation can be analyzed in an encrypted, private way, then we can more successfully fight terrorism. Only specific algorithms would be run on small portions of encrypted data—that would allow courts to issue warrants to run algorithms on encrypted data to listen in to the conversations. That way processes can identify suspicious conversations, but they are protected until the court decides they are necessary and then only part of the conversation (the identified part) can be listened to for security reasons.
  - For example, medical data could be encrypted so that only authorized algorithms that run on the data could yield results for medical personnel. This would allow data to be shared in a more secure manner.

Relevance

- Keeping our systems secure reduces terrorism and increases national defense
- Decreasing system vulnerability increases safety—preventing hacking commercial jets and cars on the road, and keeping power grids safe, for example
- Personal Privacy. Solving this challenge allows us to protect people from bad things happening while sharing data that promotes good things to happen.
  - Medical records could be shared to help cure diseases and enhance patient care at lower costs
  - Financial data could remain secure
  - Phone conversations could stay private while bonafide law enforcement/preventing terrorism efforts are conducted
  - Etc. etc.—every aspect of data sharing becomes protected

Relevance

- Better collaboration in every domain means we solve problems faster and better
- In short, addressing the vulnerability at the systems level and protecting data saves lives, lowers costs, increases effectiveness and efficiencies, advances what humans can do together and impacts everyone around the world

Scope

- For the purpose of this challenge, the technical scope was computing systems and networks
  - Technical infrastructure
    - Hardware
    - Software
    - Communications
    - Physical devices
  - Data
    - Generated
    - Stored
    - Transmitted across networks

Work/Research Underway

- Academic organizations identified by interviewed SMEs
  - University of Louisville
    - Hongxiang Li works on security from physical communication perspective: e.g., tradeoff between security reliability and capacity reliability
    - Huacheng Zeng works on wireless and security and on the network layer
    - Adrian Lauf works on the application layer and is also an expert in embedded systems
    - Jeff Hieb works on hardware interface security and has patented, built and commercialized successful working SCADA system for utility companies
    - Nihat Altiparmak works on operating systems
    - Roman Yampolskiy specializes in biometric based security
  - University of Kentucky
  - Indiana University
  - Purdue University
  - Carnegie Mellon University
  - University of Pennsylvania
  - Pennsylvania State University
  - (Cybersecurity is a huge issue and is being researched at many other universities and companies)

Work/Research Underway

- Funding Organizations identified by interviewed SMEs
  - Defense Advanced Research Projects Agency (DARPA)
  - Intelligence Advanced Research Projects Activity (IARPA)
  - Office of Naval Research
  - National Science Foundation
  - Department of Homeland Security
  - Department of Defense
  - Department of Energy

Summary

- Cybersecurity is a huge research area of interest across many government, commercial, and academic institutions
- The Subject Matter Experts specified by NSWC Crane identified challenges in two major areas
  - Addressing cybersecurity/vulnerability at a systems level
    - Systems have vulnerabilities that exist in different levels—hardware, software, communications, and physical
    - Most vulnerability analyses are focused on a specific level. We need an integrated effort to focus more at the system level
    - Individual components are becoming too complex to completely test
    - Testing technology has been unable to keep up with the increasing scaling and complexity of systems
    - Testing at the hardware, software, communications, and physical levels ignores vulnerabilities in the interfaces between components
    - Addressing vulnerabilities at individual levels lags attacks
    - The speed at which new devices are introduced limits our ability to keep up with vulnerabilities
    - Scalability, completeness, and accuracy all suffer from increased complexity. We need to address these at the system level.

Summary

- The Subject Matter Experts specified by NSWC Crane identified challenges in two major areas (cont.)
  - Keeping Data Private
    - This is related to the vulnerability challenge in that breaches of systems expose data; it is also a separate challenge, since data is routinely transferred between systems
    - The amount of data gathered, stored, and transmitted has exploded
    - Visual processing poses challenges in addition to keeping stored data private
    - Large data sets limit the real time processing of data, resulting in more data being stored, which increases vulnerability
    - Fears of privacy violations reduce data sharing, which decreases our ability to utilize the data
    - If we could share data securely, we can enable better collaboration
    - Knowing how data flows and keeping it private can help alleviate vulnerability issues as well

Summary

- Addressing these challenges has the potential to
  - Significantly enhance US defense
  - Protect privacy while utilizing data in a protected manner
  - Significantly advance effectiveness for medical, educational, commercial, pubic utilities, and countless other domains
  - Advance the fight on terrorism
  - Advance the human race
- These challenges and the their potential solutions for keeping networks and data safe are widely recognized and funded by government agencies. Universities around the world, including those near NSWC Crane, are working on these challenges.

Sources

Subject Matter Experts consulted / interviewed

- Dr. Samson Cheung, University of Kentucky
- Dr. Olfa Nasraoui, University of Louisville
- Mr. Von Welch, Indiana University
- Dr. Dongyan Xu, Purdue University