Innovation Crossover Preliminary Research Report
DoD Technologies – Trusted Electronics

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

DoD Technologies – Trusted Electronics

- We are interested in discovering methods to validate existing electronics components and systems to confirm that they are of the quality and capability that is reported, to ensure these components and systems can do what they were specified to do and have not been altered, tampered with, modified or hacked, without destroying the component or system.
- Full spectrum of Trusted electronics capabilities ranging from anti-tamper technologies, counterfeit detection, component engineering, radiation-hardened microelectronics, radiation-hardened component design, independent validation and verification of microelectronic component performance, RF microelectronics, Printed Circuit Board technologies, and failure and material analysis

Problem Context

- Problem or Challenge:
  - IBM sold the on-shore trusted foundry to investors in the UAE
  - Vast majority of semiconductor manufacturing is overseas, in countries not necessarily our allies
  - Many components are COTS (commercial off the shelf)
  - We must know if the components are reliable, designed and manufactured according to specification, with no additions, malicious capability, are not compromised or tampered with
  - These electronic chips and components must perform as expected over the life of the system
- How do we validate the components perform as designed and have no inserted malicious content, inexpensively, quickly and thoroughly, without destroying the component?

Problem Context

- Supply Channels / Vendors:
  - Most semiconductor manufacturing and packaging is done off shore, in countries that aren't necessarily friendly to the US and its interests
  - The supply chain is distributed and complex, often hard to know where components come from or if they are legitimate parts
  - Too expensive to build and operate a trusted foundry in the US
- Given the distribution and location of manufacturers and packagers of these components, and the distribution and lack of transparency in the supply chain, how can we be sure components are legitimate, haven't been tampered with or compromised in some way?

Technologies

- Today, a single chip can have billions of transistors. These components are:
  - Difficult to design
  - Difficult to build
  - Difficult to test
- Since much of the manufacturing happens overseas and the distribution chain is complex, we have to:
  - Create designs that are difficult to change or steal
  - Improve visibility and tracking in the supply chain
  - Improve our ability to identify issues with electronic components using testing and validation

Technologies

Testing and validation technologies in use today:

Technical

- Acoustic Microscopy Imaging
- Cross sectioning
- Component Decapsulation and Die Verification
- X-Ray Spectroscopy
- Heated Solvent
- Microscopy Inspection
- Principle Component Analysis

Source: http://smtcorp.com/counterfeit-detection

Other

- Visual Inspection
- Brute force electrical testing

Sophistication and Detection

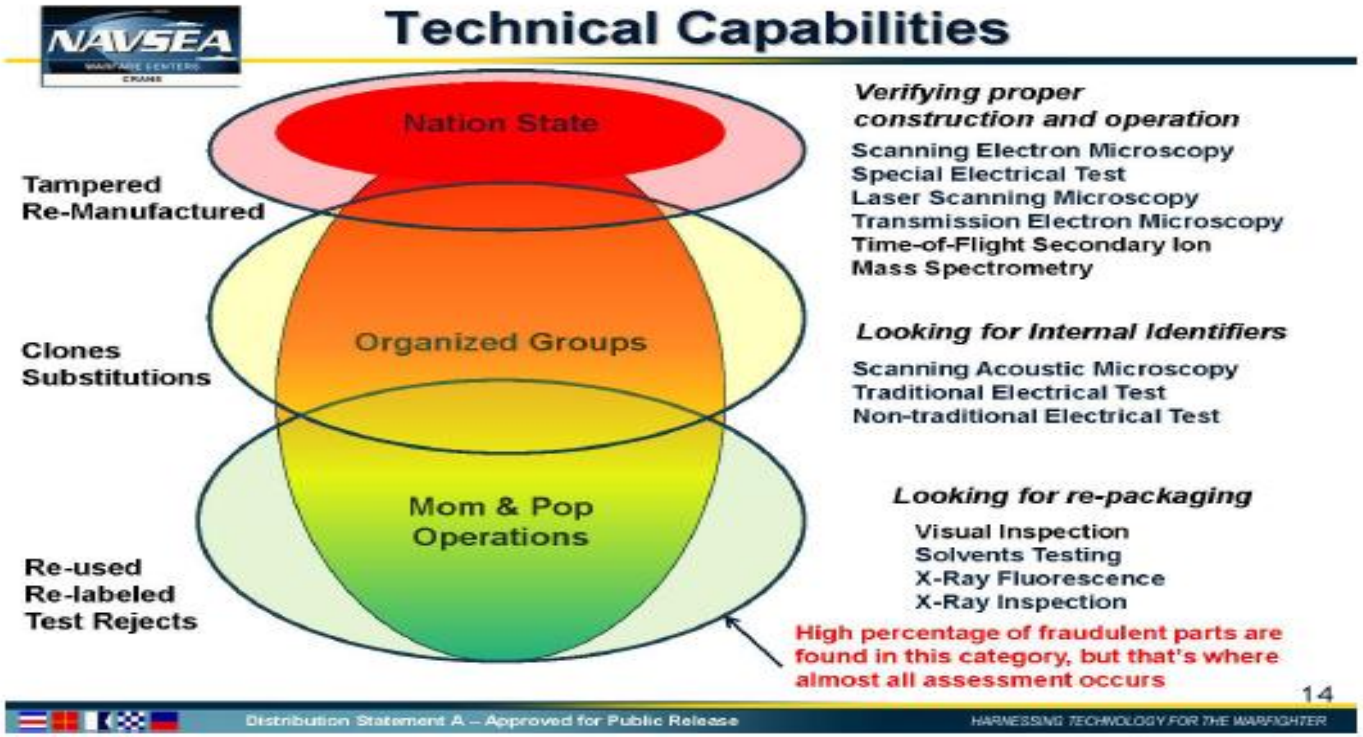

FIGURE 2-2 Technological capabilities and approaches to detecting counterfeits. SOURCE: Brett Hamilton, Chief Engineer Trusted Microelectronics, JFAC Hardware Assurance Lead, Global Deterrence and Defense Department/Flight Systems Division, Naval Surface Warfare Center, presentation to the workshop on March 16, 2016.

From: Trust Study: Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components, P. 26

Problem Relevance

- The challenge of trusted electronics is a pervasive, even “existential” problem given the importance of these electronic components to almost any electronic system in the military or civilian sphere.
- The problem impacts the trust and reliance we can have in any electronic system:
  - Will it perform as expected?
  - Over the lifetime expected?
  - Will it fail at a critical moment? Can an enemy cause it to fail catastrophically?
  - Does it contain malicious code or intent?
  - Does it send important data to an enemy or competitor?

Problem Relevance

- The challenge of trusted electronics is a pervasive, even “existential” problem given the importance of these electronic components to almost any electronic system in the military or civilian sphere. Every major system is reliant to some degree on electronic systems and components.
- For the military, for example, a compromised or counterfeit electronic component could catastrophically fail during a missile launch, causing the missile to crash.
- In the civilian world, a compromised or counterfeit electronic device could cause electrical grid issues, water distribution system issues, communication issues and much more.

Scope

- For the purposes of this research, we've defined the scope of the problem as semiconductor chips or electronic components, and the trustworthiness and reliability of these components.
- We did not include electronic systems (systems made up of multiple components)

Scope

- Included in this scope:
  - Counterfeits
  - Compromised systems
  - Malicious code / transistor insertion
  - Intentional planned failure
  - Clones
  - Components built to send signals or data
  - Component obsolescence
  - Components that had been tampered with

Depiction of risk

FIGURE 1-1 Microelectronics in Department of Defense systems. NOTE: Acronyms are defined in the front matter. SOURCE: Brian Cohen, Institute for Defense Analyses, presentation to the workshop on March 18, 2016.

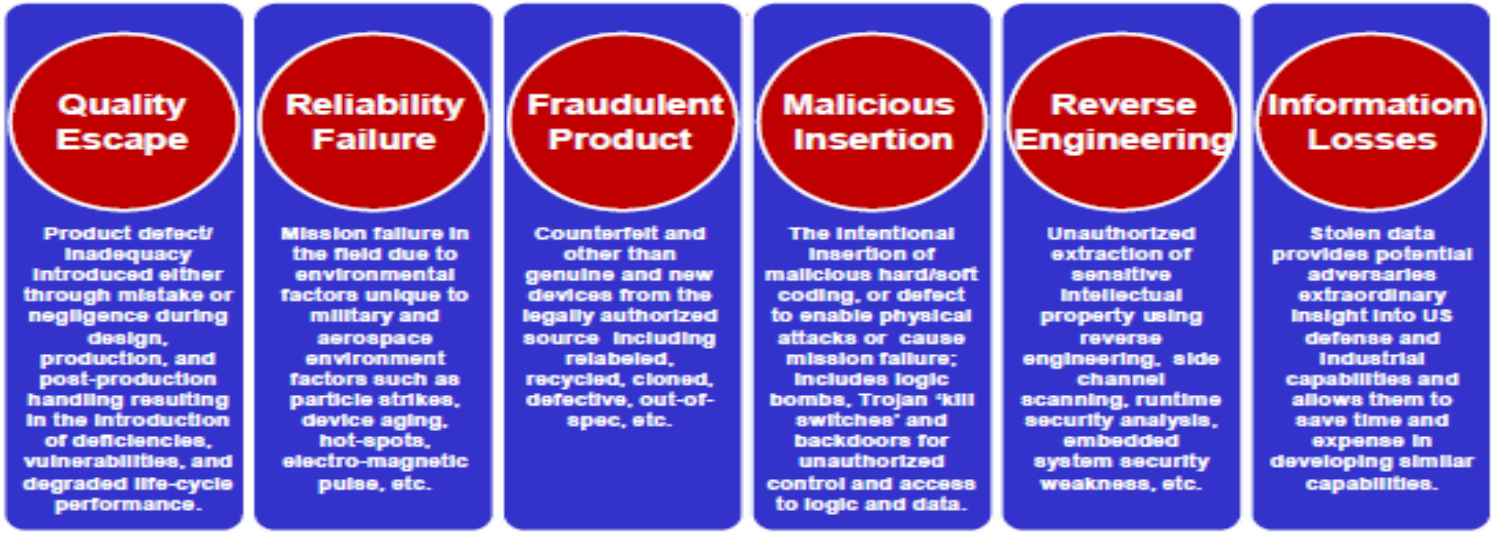

FIGURE 1-2 Spectrum of supply chain risks. SOURCE: Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineering and Principal Deputy Assistant Secretary of Defense for Systems Engineering, presentation to the workshop on March 16, 2016. Distribution Statement A – Approved for public release by DOPSR; SR#15S-1541 applies. Distribution is unlimited.

From: Trust Study: Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components, P. 18

Scope

- Included in this scope:
  - Key participants: Semiconductor manufacturers, packagers and distributors
  - Component classifications: Commercial, Off the Shelf (COTS) devices as well as specially designed, unique devices
  - Rationale: Our scope includes those who provide counterfeits for both *economic benefit* and those who do it with *malicious intent*

New Research

- There are a number of groups doing research into the testing and validation of electronic components. These include government agencies and university research.
- Much of the research underway is focused on a specific issue: cloning, tampering, compromised systems
- There are many different approaches for detecting issues, mostly based on the different forms of compromise or alteration of the device

Research

- Tampering
  - NSWC Crane is focused on tampering, as is the AFRL (classified work)
  - JFAC is conducting work into discovering or identifying tampered electronics
  - Several universities have conducted research into tampering
    - Dr. Shamus McNamara from the University of Louisville has worked with NSWC Crane on this issue

Research

- Cloning
  - Matt Kay and Brent Hamilton at NSWC Crane have done research into clones

Research

- Compromised electronics
  - NSWC Crane is focused on compromised electronics, as is the AFRL (classified work)
  - JFAC is conducting work into discovering or identifying tampered electronics
  - Indiana University and Purdue are both conducting research into compromised electronics

Research

- Counterfeit electronics
  - NSWC Crane has ongoing research led by Brett Hamilton on counterfeit electronic components.
  - Rolls-Royce is exploring research into identifying counterfeit parts in its engines

Research

New research indicates that the following approaches have promise in addressing this challenge:

- Fuzzing: a brute force method to test as many potential inputs to the device as possible
- Scanning Magnetic microscopy
- Computer vision (Research by Dr. David Crandall at Indiana University)
- The use of power trace technologies
- Computational Microscopy (Rob Templeman from NSWC Crane and Indiana University)
- Work on PRISM 2.0 (Matt Kay from NSWC Crane and Dr. Peter Bermel from Purdue)
- Some work with Rose-Hulman on photonics. Research is advanced but the relationship needs to be strengthened
- Power Spectrum Analysis using square waves (Sandia National Labs)

Organizations

- Associations / Organizations
  - DARPA IRIS (Integrity and Reliability of Integrated Circuits) program
  - Joint Federated Assurance Center (JFAC) – identifies, promotes and facilitates access to hardware and software assurance across the DoD
  - DMEA – Defense Microelectronics Activity the manager of the Trusted Access Program Office (TAPO)

Summary

- Trusted Electronics is an important, “existential” problem given our reliance on electronics and the increasingly distributed nature of manufacturing, packaging and distribution
- Military and civilian systems can fail catastrophically if compromised, counterfeit or other tampered electronics are used, or our competitors or enemies can receive information from malicious embedded circuits
- The challenge is complex because of the nature of the manufacturing and supply chains, as well as the diversity of the components (analog devices to ASICs to FPGAs and other processors)

Summary

- In the past, it was possible to use statistical sampling, visual inspection and brute force testing to identify counterfeits, clones and compromised electronics but as form factors shrink and the complexity of the components grow, this is no longer the case.
- As our ability to identify and detect compromised electronics decreases, our dependence on these devices grows just as quickly
- The complexity of the problem is exacerbated by the fact that research is divided up into incremental components often walled off from other researchers to maintain secrecy. Researchers work on specific attributes or characteristics but few see the bigger picture

Summary

- Beyond complexity and compartmentalization, the research is further hampered by the different technologies and approaches to solve the problem, and the mere definition (counterfeit, compromised, tampered, cloned, etc) as well as the range of components (simple COTS to ASICs, FPGAs and processors)
- Further complexity is introduced by the lack of transparency in the supply chain

Summary

- General consensus is that there is no easy solution to identifying and validating semiconductor chips or electronic components. The task is daunting but the risks are “existential”.
- We must improve the trusted relationships with manufacturers, packagers and distributors
- More importantly, we must develop testing approaches and standards that will allow us to quickly identify compromised components in little time, with little cost and without damaging the device.

Sources

Subject Matter Experts consulted / interviewed

- Greg Reece, NSWC Crane
- Kyle Werner, NSWC Crane
- Rob Walker, NSWC Crane
- Matt Kay, NSWC Crane
- Darren Crum, NSWC Crane
- Dr. Shamus McNamara, University of Louisville
- Dr. Dan DeLaurentis, Purdue
- Dr. Razi Nalim, IUPUI
- Bill Harrison, AFRL

Sources

- Trust Study: Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components https://www.nap.edu/catalog/23561/optimizing-the-air-force-acquisition-strategy-of-secure-and-reliable-electronic-components