A DARPA Approach to Trusted Microelectronics

Disaggregate the circuit

Functional Disaggregation
Functional disaggregation countermeasures increase protection against malicious insertion and loss-of-information threats by disaggregating critical micro-electronics into functional, independently manufactured component parts. By dividing the manufacture of well-defined circuit components across foundries, DoD can employ state-of-the-art commercial suppliers while disguising the true function, performance, and military relevance of sensitive devices. Final assembly of these devices would occur at a trusted facility. This approach delivers improved security while allowing DoD to dynamically alter smaller portions of an IC without redoing the entire IC design. This partial redesign capability has the major benefit of enabling more rapid security upgrades and more seamless shifting between vendors than is typically the case.

Application
Functional disaggregation countermeasures may be most appropriate for the protection of electronics that contain or produce sensitive algorithms and data, such as radar signal processors, weapons control computers, and electronic attack and protection systems. Functional disaggregation countermeasures can implement protections against threats during fabrication and assembly by:

- Preventing loss-of-information threats by withholding both the complete design information and the final function of DoD electronics from manufacturers
- Preventing malicious insertion threats by disguising the military relevance of component parts
- Preventing loss-of-access threats by enabling DoD to employ commoditized IP blocks and to switch between them using modular interfaces
- Detecting and responding to malicious insertion or quality problems during system operation by using trusted components to monitor and control untrusted components

Current approach and emerging gaps
To avoid loss-of-information and malicious insertion threats, DoD currently relies on the accreditation of trusted vendor facilities and personnel, the majority of which are domestically-owned and -operated firms. Globalization and consolidation within the semiconductor industry may render exclusive reliance on this option unsustainable, especially for leading-edge microelectronics.

Proposed technology: DARPA’s DAHI program
The Diverse Accessible Heterogeneous Integration (DAHI) program enables the subcomponent-level integration of multiple semiconductor materials (e.g. silicon, indium phosphide, etc.) and feature sizes. This capability should allow DoD to disaggregate IC designs into component pieces that do not reveal the entire IC functionality, helping prevent malicious insertion and loss-of-information threats. By concealing the function and military relevance of device components and manufacturing them at different locations, the DAHI approach should protect critical IP and complicate attempts to target DoD’s supply chain. The program demonstrated subcomponent integration in 2014.

Proposed technology: DARPA’s CHIPS program
A primary goal of the Common Heterogeneous Integration and IP Reuse Strategies (CHIPS) program is to enable the use of common, standardized IP blocks in the design of custom DoD ASICs. Disaggregating ASIC designs into standardized, pre-verified, commercially available IP “chiplets” should amortize the
costs of IP validation and verification across all DoD ASICs. Pre-verified IP should also reduce the risk posed by the malicious insertion of problematic IP in the design phase.

Proposed technology: DARPA’s SPADE program
DARPA’s Secure Processing Architecture by Design (SPADE) program proposes that DoD leverage leading-edge, unaltered commercial technologies by securely packaging them with less advanced, trusted microelectronics. Using this approach, DoD could simultaneously leverage the superior capabilities offered by commercial sector technologies while using a trusted silicon component to encrypt and provide trust for critical data and algorithms. The trusted component and packaging material could also monitor the integrity of the electronics and respond to potential compromises, including malicious insertions and quality and reliability issues.
Fine disaggregation

Fine disaggregation countermeasures further disaggregate sensitive DoD microelectronics in order to protect against malicious insertion and loss-of-information threats. Countermeasures of this type can require manufacturers to independently produce non-functional layers of a component device, which would later be assembled in a trusted facility. The IARPA Trusted Integrated Chips (TIC) program is part of this effort.

Application

Fine disaggregation countermeasures may be most appropriate for the protection of sensitive electronics—such as cryptokeys—that contain CPI or that could be reverse engineered. These countermeasures can protect against threats during fabrication and assembly by:

- Preventing loss-of-information threats by withholding the true function of DoD electronics from manufacturers
- Preventing fraudulent product threats by denying access to discarded or lost equipment that adversaries could use to design counterfeits or clones
- Responding to loss-of-information threats such as hardware theft or the loss of hardware in the field

Current approach and emerging gaps

DoD currently protects against loss-of-information and malicious insertion threats during fabrication by accrediting trusted vendor facilities and personnel, as previously described. At the other end of the electronics lifecycle, it is extremely difficult for DoD to ensure the recovery and disposal of all of its microelectronic devices. Unauthorized recovery of these devices, which are pervasive on the battlefield, can compromise sensitive information and risk DoD’s technological advantage. Improper disposal of electronics is also a concern, as recycled components from electronic waste are a major input to electronics counterfeiting. The destruction of transient electronics at the end of their usable lifetimes could help to curtail this risk.

Proposed technology: IARPA’s TIC program

Unlike the DAHI program, which has developed the means for assembling functional components sourced from various facilities, IARPA’s Trusted Integrated Chips (TIC) program proposes to divide chip fabrication processes across facilities. TIC’s layered approach splits front-end-of-line and back-end-of-line transistor manufacturing across locations, ensuring that the chip itself would remain non-functional until it is completed in an approved location. Circuit designers could also implement obscuration techniques for additional protection. TIC can help DoD prevent loss-of-information threats that would occur from revealing sensitive design IP to suppliers. By concealing this IP, TIC could also allow DoD to leverage a broader range of commercial suppliers during the early stages of chip manufacturing.