A DARPA Approach to Trusted Microelectronics

Obscure the design & manage the supply chain

Obscuration and marking countermeasures either conceal the IP expressed in an electronic component or enable the authentication of genuine devices. These countermeasures can circumvent loss-of-information and fraudulent product threats. In the commercial sector, for instance, vendors have leveraged reprogrammable memory and electronically activated fuses to delay imprinting sensitive functions on a device until after the device has been manufactured. Once a manufactured device is personalized, tracking countermeasures such as low-cost electronic component markers can allow DoD to determine the device’s previous location and to detect tampering. Obscuration and marking countermeasures use or expand upon current industry practices; DARPA intends for their impact upon commercial processes to be minimal.

Application

Obscuration countermeasures may be most appropriate for protecting those portions of an IC that express critical IP. Marking countermeasures may be appropriate for the authentication of most electronic parts and of commercial items, such as computer and automotive products. These countermeasures can implement protections against threats during fabrication and assembly by:

- Preventing malicious agents from exploiting DoD design IP to create fraudulent products
- Preventing malicious agents from discerning the full design intent of a manufactured device
- Detecting attempts to tamper with, copy, or exploit the IP of genuine microelectronics
- Detecting the insertion of counterfeit or fraudulent parts into the supply chain

Current approach and emerging gaps

To avoid loss-of-information threats, DoD currently certifies the reliability of the trusted vendor facilities and personnel, traditionally at Five Eye-owned and -operated firms. Globalization and consolidation trends within the semiconductor industry may make exclusive reliance on this option unsustainable, especially for leading-edge microelectronics. Meanwhile, many of the available techniques for detecting counterfeits or authenticating genuine microelectronic components either incur high costs or are not well suited to countering advanced threats. Most of these techniques are specific to a manufacturer, can be circumvented, or require off-site forensic analysis for authentication.

Proposed technology: DARPA’s CRAFT program

The Circuit Realization at Faster Timescales (CRAFT) program aims to address the high design and fabrication costs associated with advanced technology nodes. These costs limit the number of custom ICs that can be designed and built for low-volume customers like DoD. By increasing design modularity and reuse, CRAFT could sharply reduce the amount of effort required to design high-performance ASICs. CRAFT could also alleviate the challenge resulting from loss of access to a particular foundry by minimizing the effort required to move IC designs across facilities.

CRAFT also includes research into electronically activated fuses (either eFuses or anti-fuses), which can obscure an IC’s function and prevent adversaries from exploiting the CPI expressed by stolen design data or manufactured devices. Given these countermeasures, the circuit’s design intent would only become apparent after personalization, which uses fuses to change the IC’s internal connections post-manufacture. For military purposes, personalization would occur at a trusted facility. Although obscuration and
personalization techniques increase design complexity and test times, they are well established and inexpensive.

**Proposed technology: DARPA’s SHIELD program**
The DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program aims to provide a unique and encrypted identification for electronic components. SHIELD can help DoD prevent, detect, and respond to fraudulent product threats. SHIELD would incorporate an unpowered, microscopic IC into the packaging of an electronic device. These fragile and hard-to-replicate “dielets,” at a projected unit cost of less than $0.01, would deter fraudulent product threats by increasing the cost and difficulty of counterfeiting. SHIELD would also enable DoD to authenticate genuine devices and to better identify and respond to likely counterfeit attempts. For instance, the dielet would record thermal events associated with unauthorized component recycling. To identify and respond to potential threats, DoD would correlate recorded tampering events with an online database containing each dielet’s status and location. The database would update during each SHIELD-enabled inspection.