A DARPA Approach to Trusted Microelectronics

Manage end of life

Transience
Transience countermeasures would allow for the triggered destruction of sensitive electronics and protect against loss-of-information and fraudulent products threats. DARPA’s Vanishing Programmable Resources (VAPR) program, for instance, uses transient substrates to construct electronics. These substrates can be designed to rapidly disintegrate in response to specific radio frequency signals or to attempts at reverse engineering.

Application
Transience countermeasures may be most appropriate for the protection of sensitive electronics that contain CPI or that could be reverse engineered. These countermeasures can protect against threats by:

- 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
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.1 The destruction of transient electronics at the end of their usable lifetimes could help to curtail this risk.

Example technology: DARPA’s VAPR program
Performers on DARPA’s Vanishing Programmable Resources (VAPR) program have developed a robust glass substrate capable of shattering into dust-like particles on command, rendering the overlaid electronics nonfunctional and unrecoverable. The technology, which DoD can broadly apply to inexpensive COTS electronics, could help prevent or respond to loss-of-information threats due to lost or abandoned DoD technologies. Civilian applications include the protection of personal data and other critical information stored in memory. VAPR leverages COTS precursor materials and existing manufacturing techniques to facilitate technology transition and to ensure broad application in DoD and civilian markets.

---