

At a Glance

What is it?

- The Anti-Tamper (AT) Protection program develops innovative techniques and technologies to deter the reverse engineering and exploitation of our military's critical technology. This investment in the protection of critical systems will help to impede technology transfer and alteration of system capability and prevent the development of countermeasures to U.S. systems.

How does it work?

- Systems monitor critical technology and information. Upon detection of a tamper event, significant penalties are inflicted to deter or delay an adversary from obtaining critical information or reverse engineering the critical technology elements. Features may also be incorporated to make tampering and reverse engineering significantly more difficult to perform.

What will it accomplish?

- This program will provide the fleet and forces with a robust, long-lived, layered set of technologies with the ability to operate in unattended and unpowered environments. Technical approaches will provide a very high probability of tamper detection and low probability of false alarm. In addition, they are undetectable in the host system and will not alert the adversary once the tamper event has been detected.

Point of Contact

Betsy DeLong
betsy.delong@navy.mil

The Anti-Tamper Protection program is developing innovative techniques and technologies to protect critical technology (CT) and critical program information (CPI) contained in U.S. military systems from tampering and reverse engineering.

The U.S. Navy spends billions of dollars to achieve a technological advantage on the battlefield. If that critical technology is not protected, that advantage will be lost. The AT program is developing measures to protect against the tampering and reverse engineering of Navy and Marine Corps systems. These advances can deter or delay information compromise due to combat losses, foreign military sales, joint U.S./foreign production or espionage.

The AT program consists of three thrusts: tamper event monitoring, hardware/software destruction and obfuscation of anti-tamper measures.

Current projects are developing trigger mechanisms that monitor CT and CPI to accurately sense, detect and classify tamper events. Efforts apply an appropriate penalty without any indications to the adversary that the CT and CPI are being monitored. Project teams are also delivering hardware and software destruction technologies that can be applied in varying layers to effectively destroy CT and CPI without any indications to the adversary of the specific destruct mechanisms being employed. Lastly, these efforts will ensure that the AT protection measures are obscured in various ways so that adversaries may not reverse engineer the protection measures, rendering them ineffective.

Technical approaches that are being pursued include wafer level hardware and firmware to protect CT and CPI, low- or no-power sensors to detect tampering and reverse engineering, and low- or no-power destruction mechanisms. Performers are also developing and combining multiple advanced electronic packaging techniques at the board and component level to provide no power protection against tampering and reverse engineering.

Research Challenges and Opportunities

- New approaches for completely and irreversibly erasing data stored in non-volatile memory that do not use energetics or produce damage beyond the active portion of the memory device.
- High-density 3D electronics packaging capable of integrating into a single package the multiple COTS and custom devices necessary for a complete secure processing system.
- Techniques for implementing reliable physical unclonable functions (PUFs) in FPGAs and then using these PUFs to provide FPGA authentication and to generate volatile keys for encryption/decryption.

