Detecting Foreign Nation Cyberattacks with Classified Threat Sensors

Dr. Stephen Weis, Dr. Aloni Cohen, Dr. Amina Asim
Aspen Tech Policy Hub

The US intelligence community holds unique information about foreign nation cyberattackers, which is not available to private companies trying to defend themselves. We propose adopting **secure enclave** technology to apply classified intelligence in non-classified settings, while maintaining intelligence secrecy. We suggest the development of a **classified threat sensor** that US companies can run in enclaves without leaking classified intelligence or private security data.

The Information Sharing Challenge

Foreign nation-state cyberattacks against US-based companies create a national security risk and result in the loss of competitive intellectual property. The US intelligence community holds classified information that could help detect nation state attacks. However, that intelligence cannot be shared without risking sources and methods. Private security data held by industry, which might not be accessible due to regulatory or public perception issues, could in turn aid intelligence agencies in identifying broader attack campaigns.

Today, the time to declassify information and share it through existing channels may reduce intelligence's relevance by the time a company can act on it. Recent developments in **secure enclave** technology may empower companies and governments to rapidly act on classified intelligence, without requiring declassification.

Secure Enclaves & Classified Threat Sensors

Secure enclaves are an off-the-shelf technology that provides a **safe space to run audited software and process secret data on someone else's computer**. We propose using secure enclaves to operate **classified threat sensors** that run on a private company's servers. These threat sensors would be able to scan a company's local security data for signs of cyberattack or classified vulnerabilities without revealing the indicators for which the sensor was searching.

Classified threat sensors solve the information sharing challenge without declassifying intelligence or exposing private data to governments. They may be built from off-the-shelf technology using existing open source tools. These sensors could speed detection and attribution of cyberattacks by foreign powers. Sensors can also act as an early-warning system to discover broader campaigns, without exposing private company data to the government.

Rollout Plan

We suggest a phased trial between the National Security Agency (NSA), Department of Homeland Security (DHS), and private industry partners. Secure enclave data sharing technology is already funded through the DHS's IMPACT program's FIDES project. This technology can be migrated to an open source project, then run in parallel trial deployments for both industry-to-industry and government-to-government sharing between the NSA and DHS. After proven in trials, a government-to-industry sharing program could be deployed between DHS and industry partners.