Detecting Foreign Nation Cyberattacks with Classified Threat Sensors

Operational Plan

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

We offer a five-stage operational plan to build and deploy **classified threat sensors** running in a secure enclave, which can safely process classified intelligence. This plan would be implemented and funded through a partnership of government, industry, and academic teams. It could be largely built from existing open source libraries and the output would be made publicly available as open source software.

Cost and Time Estimates

Each stage of the plan delivers some useful deliverable which may benefit industry at large. We believe that the minimum proof of concept could be ready in a **month with 2 full time developers,** since it can be built from existing open source tools. Our rough estimate of the entire plan is **1 year of work ranging between 2-8 developers, project managers, or lawyers**. Much of that velocity depends on obtaining approval within organizations, agreeing on data format standards, and cross-organizational collaboration.

Potential Partners

Microsoft is a strong candidate partner since their Azure Confidential Computing[1] product supports Intel Software Guard Extensions (SGX)[2] technology. Microsoft also has ample security logs from themselves and customers, are a target of nation state attacks, and have a history of government work.

Another potential partner, Galois Inc. is a private research company that is building SGX enclave software for the Department of Homeland Security's Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program[3] under the Framework for Information Disclosure with Ethical Security (FIDES) project [4]. Galois has a long history of working with the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA).

On the government side, the NSA is considered the primary agency holding classified intelligence and context that help private industry defenders. The NSA currently distributes declassified intelligence through DHS. Thus, both agencies could be involved in different deployment phases of the project.

---

[1] Microsoft Azure Confidential Computing, https://azure.microsoft.com/en-us/solutions/confidential-compute/
[2] Intel Software Guard Extensions, https://software.intel.com/en-us/sgx
[3] Department of Homeland Security, https://www.dhs.gov/science-and-technology/cybersecurity-impact
[4] Galois Inc, "Framework for Information Disclosure with Ethical Security", https://galois.com/project/fides/

Detailed Plan

1. **Open Source Proof of Concept**: Demonstrate a proof of concept Intel SGX enclave and attestation server which successfully do the following:
    1. The **enclave** will generate an ephemeral, self-signed TLS certificate. Multiple Software Development Kits (SDKs) exist, for example, Intel's Linux SGX SDK[5], Microsoft Openenclave[6], or Baidu's Rust SGX SDK[7].
    2. A **remote service** will be able to successfully attest the enclave.[8]
    3. The **remote service** will be able to establish a TLS connection to the **enclave** itself, using the enclave certificate to authenticate the connection.[9]
    4. The **enclave** will be able to establish a connection to a **local database**.[10]
    5. Over an encrypted channel, the **remote service** will be able to provision a payload consisting of two parts:
        1. **Threat intelligence**: Classified, private, or proprietary intelligence
        2. Optionally, a **detection engine** which will be able to input **threat intel** and the **local database**, and output a **detection report.**
    6. The **enclave** will be able to send the **detection report** over an encrypted channel back to the **remote service**.

    Resources: 2 people, 1 month
2. **Industry-to-Industry Proof of Concept Deployment:** Two industry partners will mutually run enclaves and remote services, then demonstrate the ability to search for the presence of private intelligence in their respective databases. For example, partners could search for respectively known bad actor IP addresses in network logs. *Resources: 2-4 people, 2 months.*
3. **Government-to-Government Proof of Concept Deployment:** A source **intelligence agency** will run a remote service and a second, **defense agency** will run an enclave. They will demonstrate the ability to search for classified threat intelligence on a lower classification government network. *Resources: 4-8 people, 3 months*
4. **Government-to-industry unclassified deployment:** A source intelligence agency will run a remote service and an industry partner will run an enclave. They will demonstrate the ability to search for unclassified threat intelligence on unclassified, private networks. *Resources: 4-6 people, 3 months.*
5. **Government-to-industry classified deployment:** A source intelligence agency will run a remote service and an industry partner will run an enclave. They will demonstrate the ability to search for classified threat intelligence on unclassified, private networks. *Resources: 6-8 people, 3 months.*

---

[5] Intel SGX Software Development Kit, https://github.com/intel/linux-sgx
[6] Microsoft Openenclave, https://github.com/openenclave/
[7] Baidu SGX Rust SDK, https://github.com/baidu/rust-sgx-sdk
[8] Example remote service: https://github.com/intel/sgx-ra-sample
[9] Example TLS termination: https://github.com/lsds/TaLoS
[10] Example enclave database design: https://www.microsoft.com/en-us/research/uploads/prod/2018/02/enclavedb.pdf