OPERATIONAL PLAN

Detecting Foreign Nation Cyberattacks with Classified Threat Sensors

STEVE WEIS, ALONI COHEN AND AMINA ASIM

EXECUTIVE SUMMARY

We offer a five-stage operational plan to build and deploy **classified threat sensors** that can safely process classified intelligence while running in a secure enclave. This plan would be implemented and funded through a partnership of government, industry, and academic teams. The system 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 will deliver useful outcomes that may benefit industry at large. We believe that the minimum proof of concept could be prepared in three months with two full-time developers, as it can be built from existing open-source tools. Our rough estimate for the entire plan is one year of work, with between 2-8 developers, project managers, or support staff. We estimate this would cost $950k in total. Much of the timing will depend on obtaining approval within organizations, agreeing on data format standards, and cross-organizational collaboration.

POTENTIAL PARTNERS

Microsoft is a strong candidate to become a partner in this initiative, as its Azure Confidential Computing[1] product supports Intel Software Guard Extensions (SGX)[2] technology. Microsoft also has ample security logs from internal sources and customers; it is frequently a target of nation-state attacks and has a history of government work.

1 *"Azure Confidential Computing," Microsoft Azure, https://azure.microsoft.com/en-us/solutions/confidential-compute/, accessed November 2019.*
2 *"Intel Software Guard Extensions: Develop and Deliver More Secure Solutions," Intel Software Developer Zone, https://software.intel.com/en-us/sgx/, accessed November 2019.*

Another potential partner, Galois Inc., is a private research company that is building SGX enclave software for the Department of Homeland Security's 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.

DETAILED PLAN

Open-Source Proof of Concept: Demonstrate a proof-of-concept Intel SGX enclave and attestation server that successfully do the following:
Resources: 2 people, 3 months, $100k

1. The **enclave** will generate an ephemeral, self-signed TLS certificate. Multiple software development kits (SDKs) exist: for example, Intel's Linux SGX SDK , Microsoft Openenclave , and Baidu's Rust SGX SDK.
2. A **remote service** will be able to successfully attest the enclave.
3. The **remote service** will be able to establish a TLS connection to the **enclave** itself, using the enclave certificate to authenticate the connection.
4. The **enclave** will be able to establish a connection to a **local database**.
5. Over an encrypted channel, the **remote service** will be able to provision a payload consisting of two parts: 1. **Threat intelligence data**: Classified, private, or proprietary intelligence 2. A **detection engine** 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**.

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 known bad actor IP addresses in network logs.
Resources: 2-4 people, 2 months, $100k

3 *"Information Marketplace for Policy and Analysis of Cyber-risk & Trust," Department of Homeland Security, Science and Technology, https://www.dhs.gov/science-and-technology/cybersecurity-impact, accessed November 2019.*

4 *Jonathan Daugherty and David Archer, "Framework for Information Disclosure with Ethical Security (FIDES)," Galois, https://galois.com/project/fides/, accessed November 2019.*

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, 2 months, $200k

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, $250k

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, $300k