Detecting Foreign Nation Cyberattacks with Classified Threat Sensors

Grant Proposal

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

We request grant funding for a research project with a computer security program at an American university. This funding will be for the research and development of open source **classified threat sensor** software running in a secure enclave. The funds will cover 2 graduate or undergraduate students, ¼ principal investigator time, and equipment.

Deliverable

The deliverable is open source software that can run in an Intel SGX enclave. This enclave will be able to attest itself to a remote attestation service, be provisioned key material, receive an encrypted payload of threat intelligence, then search for matches over a local database.

Milestones and Timeline

The entire project should be completed and published on an open source repository within **6 months** based on part-time student development. Full-time developer time would be approximately 3 months.

1. Equipment Procurement, Open Source Project & Development Environment Setup (2 weeks)
2. "Hello World" enclave running (1 week)
3. TLS termination in a running enclave (1 month)
4. Attestation service running and a successful attestation of an enclave (3 weeks)
5. Local SQL database connectivity into enclave (1 month)
6. Key provisioning and encrypted payload format design and specification (2 weeks)
7. Key provisioning and payload parsing engine running in enclave (1 month)
8. End-to-end integration using simulated threat data (2 weeks)
9. Documentation and Open Source Project Management (2 weeks)

Budget

A grant of **$150,000** will cover development, facilities, and administrative costs to fund two graduate or undergraduate students for one semester.

2 Semesters Student Funding	$50,000
¼ Principal Investigator Funding	$40,000
Intel SGX-compatible development systems	$7,000
Conference Travel	$3,000
University Indirect Costs	$50,000
Total	**$150,000**