GRANT PROPOSAL

Detecting Foreign Nation Cyberattacks with Classified Threat Sensors

STEVE WEIS, ALONI COHEN AND AMINA ASIM

EXECUTIVE SUMMARY

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

DELIVERABLE

This project will result in open-source software that can run in an Intel SGX enclave. This enclave will be able to attest itself to a remote attestation service, load secret keys, receive an encrypted payload of threat intelligence, and 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 six months, based on part-time development by students.

Equipment procurement, open-source project and development environment setup | 2 weeks
"Hello World" enclave running | 1 week
TLS termination in a running enclave | 1 month
Attestation service running and a successful attestation of an enclave | 3 weeks
Local SQL database connectivity into enclave | 1 month
Key provisioning and encrypted payload format design and specification | 2 weeks

Key provisioning and payload parsing engine running in enclave | 1 month
End-to-end integration using simulated threat data | 2 weeks
Documentation and open-source project management | 2 weeks

The entire project should be completed and published on an open-source repository within six months, based on part-time development by students.

Equipment procurement, open-source project and development environment setup | 2 weeks
"Hello World" enclave running | 1 week
TLS termination in a running enclave | 1 month
Attestation service running and a successful attestation of an enclave | 3 weeks
Local SQL database connectivity into enclave | 1 month
Key provisioning and encrypted payload format design and specification | 2 weeks
Key provisioning and payload parsing engine running in enclave | 1 month
End-to-end integration using simulated threat data | 2 weeks
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.

Student Funding, 2 Semesters	*$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***