PROBLEM TITLE
Protecting Networks Using Highly Sensitive Information

CHALLENGE
Cybersecurity analysts at government agencies need an efficient way to use highly sensitive information for network defense (such as the detection and identification of malicious cyber network activity) while protecting that information from compromise in order to prevent their adversaries from knowing how to change their behavior to avoid detection.

BACKGROUND
Many network defense mechanisms depend on information about the tradecraft the malicious cyber actors employ. By detecting the use of actor tradecraft, defensive systems can alert defenders, block activity, or activate other mitigations. However, some information and indicators about actor tradecraft are highly sensitive and must be protected from exposure (e.g., IP addresses, DNS names, file signatures, and network traffic patterns). This creates a dilemma: how can defensive organizations rapidly use their unique information on adversarial cyber tradecraft and capabilities while preventing those same adversaries from obtaining or deducing that information and potentially exposing the sources and methods behind the information? Once exposed, access to that unique information may be lost. Currently, cybersecurity analysts might utilize cryptographic methods (e.g., homomorphic encryption), system hardening, and/or isolated computation (e.g., AWS Nitro Enclaves) to resolve this dilemma, but these solutions are often very expensive, computationally intensive, time-consuming, and/or difficult to deploy across different environments.

Of note, commercial cybersecurity companies have delicate sources and face concerns similar to those of government agencies when disseminating information drawn from those sources. The diversity of modern IT environments further complicates this dilemma. Many enterprises, in both public and private sectors, spread their enterprise and mission infrastructure across public clouds, private clouds, and traditional on-premise IT facilities. Defensive mechanisms must be deployable across all of these environments to provide comprehensive protection.

CONSTRAINTS
- While adversary tradecraft information is classified, there are analogous data sets (such as commercial threat feeds) that students can experiment with.

PROBLEM SPONSOR
Neal Ziring, Cybersecurity Directorate Technical Director, National Security Agency (nlzirin@uwe.nsa.gov, neal.l.ziring.civ@mail.mil)

Joman Chu, Research Leader, Laboratory for Advanced Cybersecurity Research, National Security Agency (jcchu@uwe.nsa.gov)

PROBLEM SPONSOR LOCATION
Fort Meade, Maryland

SENIOR LEADER
John Lockwood, Strategic Mission Manager, Cybersecurity Directorate, National Security Agency (jalockw@nsa.gov)

Do not exceed one page