AF254-0801: AI/ML-Generated Decoy Networks

ADDITIONAL INFORMATION

N/A

TECHNOLOGY AREAS:

Information Systems

MODERNIZATION PRIORITIES:

Integrated Sensing and Cyber

KEYWORDS:

Honey pot; honey net; decoy networks; artificial intelligence; machine learning; AI/ML

OBJECTIVE:

Provide a software application that generates decoy networks that are 1) efficient to employ (maximum automation, minimum manual inputs) and 2) realistic enough to deceive a sophisticated state-sponsored hacker. It is expected that recent advancements in machine learning and artificial intelligence will support this objective.

ITAR:

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 3.5 of the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

DESCRIPTION:

Defensive Cyber Operations (DCO) across the Air Force and DoD face a daily onslaught of state-sponsored expert hackers. Due to the quantity and sophistication of these adversaries, it is insufficient to rely solely on firewalls, anomaly/intrusion detection software, and human monitors. An additional method of defense is to create decoy networks, often referred to as “honey pots” or “honey nets” (in the case of multiple connected decoy networks). These decoys are intended to lure adversaries into wasting time and exposing their tactics, techniques, and procedures (TTPs) in a simulated environment where they can do no harm. While promising, past attempts to create decoy networks have been overly burdensome to create and largely ineffective against expert hackers because they are too easy to identify as fake. Air Force CyberWorx, 16th Air Force, and Air Combat Command are highly interested in novel approaches to create more realistic “digital twin” decoy networks that are dynamic. These networks need to accurately simulate users, infrastructure, data, and data flows. It is believed that emerging work in artificial intelligence, machine learning, expert systems, virtualization, and block chain technologies could dramatically improve realism and assist in counter measures. Proposed solutions could be trained on live networks to mirror characteristics and behaviors then apply algorithms to create the decoy and dynamically change like real networks would and adapt to threat behavior. Additional training of the algorithms could be provided by expert “white hat” cyber operators to improve fidelity. The system should detect, distract, and track the adversary and report activity to authorized defensive cyber operators. Decoy modifications or actions against the threat in real time should be selectable as automated, semi-automated, and/or manual.

PHASE I:

Provide a feasibility study that evaluates potential AI/ML or other similar methodologies and recommend an approach to implement these methodologies in a user-friendly software application that allows defensive cyber operators to generate and manage realistic, dynamic decoy networks and track hacker activity in real-time without the hacker knowing they are being watched or manipulated.

PHASE II:

Provide a prototype software application that allows defensive cyber operators to generate and manage realistic, dynamic decoy networks and track hacker activity in real-time without the hacker knowing they are being watched or manipulated. Demonstrate the prototype in a realistic development "sand box" environment (TRL 6 maturity).

PHASE III DUAL USE APPLICATIONS:

Advance from a TRL 6 lab tested prototype to a TRL 9 product in an operational environment. This will require a Risk Management Framework and Authority to Operate approval with assistance from Air Force CyberWorx and the 67th Cyberspace Wing. Once proven effective, this technology is expected to have applications throughout DoD, USG, and commercial markets.

REFERENCES:

1. Sun, Kim. "Design and Implementation of Decoy Enhanced Dynamic Virtualized Networks." Final Technical Report. Grant #N00014-15-1-2396. 12/12/2016
2. Dougherty, Jeffrey T. "Evasion of Honeypot Detection Mechanisms Through Improved Interactivity of ICS-SCADA Systems." Technical Report. Naval Post Graduate School. Sept 2020
3. Chong, Wai H. and Koh, Chong K. "Learning Cyberattack Patterns with Active Honeypots." Technical Report. Naval Post Graduate School. 8/1/2018.

TOPIC POINT OF CONTACT (TPOC):

TPOC-1: Matthew Hays
PHONE: 7193333399
EMAIL: matthew.hays@afacademy.af.edu

TPOC-2: Duncan Stewart
PHONE: 7193333399
EMAIL: duncan.stewart@afacademy.af.edu