United States Army Cyber Command

Technology Areas of Interest

As of JUN 2024

INTRODUCTION

TECHNOLOGY AREAS OF INTEREST

To enhance collaboration with our Industry partners, we have identified several technology topics that reflect the areas of interest for the Army Cyber Command. These topics are:

I. Category: Software Vulnerabilities

Defects exist in virtually every part of the digital ecosystem ranging from computer programs, network protocols, web-based services. The challenges in this space include discovering exploitable vulnerabilities before adversaries do, decreasing the time to patching, implementing defensive measures, and detecting and identifying defects with attribution to adversaries. Included as part of this category are two particular focus areas that present both enhanced risk: Supervisory Control and Data Acquisition (SCADA)/Industrial Control System (ICS) networks protecting critical infrastructure and the burgeoning Internet of Things (IoT) device networks.

1.1 TOPIC AREA: Identifying Malware - Rapid and accurate discovery of anomalous activity on a network and other indicators of malware. What are the best ways to analyze relevant log events, metadata or Packet Capture (PCAP) files, such as employing automated extraction of essential elements of information and automated summarization of PCAP files to allow for more efficient and faster triage.

1.2 TOPIC AREA: Leverage Malware – What are innovative ways to quickly and effectively reverse engineer malware to discover novel Tactics, Techniques, and Procedures (TTPs). What are ways to identify and observe vulnerabilities malicious cyber actors will/are exploiting for initial access?

1.3 TOPIC AREA: Polymorphic Malware/Countering Adversarial Signature Diversity – What are the best methods for detecting polymorphic malware in real-time, at the perimeter of a network or when malware has penetrated a perimeter in security. What are some innovative new ideas to enhance immediate malware recognition?

1.4 TOPIC AREA: Global Malware Tracking – What are the best ways to detect malware across architectures and detect integrated libraries employed and observe malware ecosystems attributable to a specific actor?

1.5 TOPIC AREA: Operational Technology Defense – What are the best methods for reducing the risks associated with OT Architectures? What are the best methods for identifying devices on networks and recognizing vulnerabilities arising from the presence of these devices?

1.6 TOPIC AREA: Wireless Network Visibility – What are the best way's to quickly visualize and map wireless networks and services to understand threats?

1.7 TOPIC AREA: Anticipatory market research – What are the best ways to monitor IT (software and hardware) trends in specific markets?

1.8 TOPIC AREA: Common Vulnerabilities and Exposures (CVE) Reproduction and Analysis Automation – What are the best ways to implement an automated process that derives software defects from published CVEs through continuous monitoring of repositories that contain CVE related proofs of concepts? What are the best methods for utilizing AI and machine learning to produce proofs of concept codebases that enable analysts to fully understand the risk and threat to platforms.

II. **Category: Network Security, Monitoring, and Visualization**

How to successfully and continuously secure Department of Defense (DoD) infrastructure while simultaneously defeating malicious cyber actor activity. What are the best methods for detecting intruders, track their movements, estimate risk throughout the network, apply defensive countermeasures, and assess damage and information exposure. What are the best methods for monitoring and visualizing the network terrain through manual and automated means. Topic Areas in this space involve visualizing network topologies and connections and communities, with solutions involving large-scale graph theory/graph analytics and network visualization at their core.

2.1 TOPIC AREA: **Automated Network Mapping and Asset Discovery** – What are the best ways to see and account for devices on networks. Which automated tools best produce physical, logical, and functional network maps of networks? What are the best ways to leverage Artificial Intelligence in this topic area?

2.2 TOPIC AREA: **Deep Network Knowledge and Awareness** – Which tools best describe complex networks (including devices, software/firmware versions, and patch level) but also overlay command and control logic, data flow, protocols, and physical locations in near real-time? What are the best ways to understand threats to Cyber Physical Systems?

2.3 TOPIC AREA: Network Traffic Redirection/Obfuscation – What are the best ways to understand methods that obfuscate or redirect selected network traffic in novel ways. How can we leverage Artificial Intelligence on this topic?

2.4 TOPIC AREA: Radio Frequency (RF) analysis – What are the best ways to analyze and understand RF emissions generated during cyberspace and electromagnetic warfare operations? What are the best ways to implement RF systems in ways that enable maximum integration? How can we leverage Artificial Intelligence on this topic to gain advantage?

2.5 TOPIC AREA: Self Healing Systems – What are the best ways to build, configure, integrate and manage self-healing computer networks and systems that fail safely when exceptional conditions occur?

2.6 TOPIC AREA: Secure data Search and exchange – What are the best ways to leverage technologies such as homomorphic or multi-party encryption for query/analysis/data dissemination and protection of critical data?

III. Category: Data Modeling and Predictive Analytics

What are the best ways to leverage modeling and analytics to capture past physical, virtual, or behavioral-based observations and derive decision support information? What are the best methods for using mathematical or statistical modeling, time series analysis, or some other mechanism contributes to predict or automate detection and response?

2.7 TOPIC AREA: **Normal and Abnormal Operating Conditions** – What are the best ways to detect anomalous behavior in cyberspace environments, without numerous false positives? What are the best methods to accurately measure and characterize the baseline state of a network and determine what constitutes a deviation from normal activity.

2.8 TOPIC AREA: Automated Software Defect Discovery – What are the best ways to implement or augment automated solutions for repetitive, data-intensive tasks. What are the best tools or methods for developing solutions to detect indicators of possible threats, alert analysts of their presence, and, when appropriate, apply appropriate mitigations or countermeasures to compensate for low human response time? How can automated and AI driven solutions link these challenges together?

2.9 TOPIC AREA: Prescriptive and Predictive Network Modeling – What are methods and tools to identify and characterize adversary behaviors and potential attack vectors to enable offensive and defensive operations. Are there ways to leverage computer modeling, graph structures, game theory, and machine learning to generate recommendations or evaluations of behaviors and adversary attacks to reduce the time of agency response? How can we best determine the most effective responses?

2.10 TOPIC AREA: Synthetic Users – What are the best ways to implement a mechanism for simulating network operating conditions for various purposes, including the education and training of cyber forces on tactics, techniques, and procedures (TTPs) and the rehearsal of cyber missions? Which methods or tools best enables the development of a system that creates synthetic activities and anonymizes real-world network and hosts data for configurable, adjustable, deterministic, or stochastic re-use in a simulated environment?

IV. Category: Persona and Identity

Identity issues may intersect with aspects of network community detection, topic or influencer identification focusing on individuals and their characteristics.

2.11 TOPIC AREA: Misrepresentation – What are the best ways to detect adversary use of masquerading techniques to avoid identification and detection? How are the results different for various network devices and services? What methods are used to create and maintain multiple online identities, or personas for conducting online research, or engaging in online activities under a different identity?

2.12 TOPIC AREA: Multi-Factor Authentication Vulnerabilities – What are the various multi-factor methods used by typical software applications including but not limited to cloud-based programs and software as a service? What are the most effective multi-Factor Authentication defeat and credential stuffing mitigations?

V. Category: Infrastructure and Transport

This category focuses on global mission management, risk management, global situational awareness, and command-and-control operations. This category is mainly focused on hardware platforms, movement and tracking of data, and security and risk surrounding these operations.

5.1 TOPIC AREA: Infrastructure/Platforms – What are the best tools or platforms used to provide a range of cyber effects? What are the best tools or methodologies that can be deployed on existing platforms? What specific tools, frameworks, and techniques are most capable in this demanding field?

5.2 TOPIC AREA: Network and Device Knowledge Storage System – What's the best way to implement systems that process and store massive amounts of data. What are the best approaches to help store, share and quickly retrieve relevant information. What are the best methods to manage multiple information data points, many different software tools, running various versions of software, operating on many different hardware devices, utilizing a variety of protocols? What is the best way to detect new vulnerabilities at scale?

5.3 TOPIC AREA: Automated Mission Risk Management – What are the best ways to automate risk management tasks? What are the best ways to determine how critical should risk components be tracked and visualized, and how can they be effectively communicated? Which methods are best to calculate and highlight 2nd and 3rd order of magnitude effects?

5.4 TOPIC AREA: Long Range RF Propagation – What are the best methods for securely, reliably use RF to communicate over long distances? How can we best receive RF signals or a representation covering a large area and return signals to a central processing station? What are the best tools and methods to execute and manage these types of activities?

VI. Category: Cloud

6.1 TOPIC AREA: Cloud Forensics – What are the best ways to perform Cloud Forensics in the cloud environments without downloading images for prosecution using on-prem forensics tools? What is the best way to train a workforce to conduct Cloud Forensics operations?

6.2 TOPIC AREA: Cloud Pentesting – What are the best ways to perform Cloud Penetration Testing and Threat Emulation? What are the best tools and methods to execute and manage this task?

6.3 TOPIC AREA: Cloud Analytics – What are the best ways to leverage automation and Artificial Intelligence to drive Cloud based Security analytics that reduce complexity for the workforce while optimizing detection effectiveness?

6.4 TOPIC AREA: Cloud Environment Provisioning – What are the best ways to implement cloud environments for operations, training and research?

VII. Category: Other

7.1 TOPIC AREA: Software Supply Chain - Given the Complexity of highly integrated systems, what are the best mechanisms to gain visibility of and assure the software supply chain?

7.2 TOPIC AREA: Graph Analytics – What are the best methods and tools for leveraging Graph analytic Engines or Graphing methodologies applied to monitoring IT infrastructures? How can these types of analytics be used to gain previously unseen insights or execute functions in a predictive way?

7.3 TOPIC AREA: Provably Secure Systems – What are the best ways to implement and leverage formal methods or other techniques to build systems that are provably secure and can operate in the most extreme security environments?