USCC-J9-TO-2019-03-12

# U.S. Cyber Command
# Technical Challenge Problems
# Guidance

U.S. Cyber Command has developed a set of Technical Challenge Problems to enhance potential solution providers' ability to fill key mission gaps. These unclassified Technical Challenge Problems are informed by operators who work the highest priority missions.

These Technical Challenge Problems are not requirements for which we anticipate solutions exist today. Rather, they are significant challenges which will require developers to use existing capabilities in novel ways, add new features, innovate, or drive new research.

It is the intent of U.S. CYBERCOM J9 to help draw the attention of solution providers and focus them on our most pressing needs. J9 will use these Technical Challenge Problems to enrich our engagement with capability providers in Industry, Academia, and the Labs. If a challenge problem is of interest to an outside organization, at a minimum, U.S. CYBERCOM will want to know who is working it and be kept appraised of their progress towards achieving all or portions of the challenge.

J9 Technical Outreach will continue to be the engagement lead for pushing out challenges to different communities and tracking participation in challenges. As solutions begin to materialize, it may be beneficial for the Command to give more detailed guidance to the developers. The J9 Applied Research Division will take the lead on providing technical advice or reaching out for deeper operator advice, as needed.

Successfully completing a challenge problem will not directly result in funding, but doing so will increase the chances that appropriate acquisition and/or transition processes will be employed.

POC: Mr. Berl "Mike" Thomas, J9 Deputy Director for Technology, March 2019

***U.S. CYBER COMMAND***
***UNCLASSIFIED TECHNICAL CHALLENGE PROBLEMS***
***12 March 2019***

**VULNERABIILTY**

1. *CHALLENGE PROBLEM*: MAGETOWER

Description: Engage Industry, Academia, and others by integrating USCYBERCOM's Private Intermediary Agreement, DreamPort, into the ongoing Project VOLTRON efforts happening in USCC J9 in coordination with Cyber National Mission Forces (CNMF) and DoD Defense Innovation Unit Experimental (DIUx). Currently, J9 Applied Research Division (ARD) and CNMF are working with the performers on the VOLTRON contract with DIUx. Project VOLTRON is a collection of tools to perform automated vulnerability discovery in binaries of interest, and it is a follow-on to the DARPA Cyber Grand Challenge program that ended in 2016. ARD and CNMF are working with the contract performer (For All Secure) to further the development and usability of state-of-the-art automated binary fuzzing engines for the purpose of vulnerability discovery. Non-traditional solutions providers are encouraged to engage in the MAGETOWER research via the DreamPort unclassified technical innovation facility located in Columbia, MD.

2. *CHALLENGE PROBLEM*: Reduce patch timelines to plug vulnerabilities before we become a victim of an attack.

It takes time to assess, test, and deploy patches that fix newly identified vulnerabilities. This is as much a resource management issue as it is a technical issue. We lack a rapid patch methodology based on newly released Common Vulnerability Exposures (CVEs). First we must be able to recognize we have a system that is vulnerable to the new CVE, then we would need to patch it. It can take significant time to employ new patches as we need to assess the impact of the patch to critical systems. This timeline must be shortened to be positioned for success.

We need to be able to patch faster than our adversaries can exploit us. This requires information to be streamlined. We need to quickly match newly released CVE vulnerabilities that are employed on our networks. Perhaps a "seeker" system could look for and identify where in the network new CVE's are relevant. Once identified, we would need tools that will quickly assess the impact of applying the CVE patch to our complex critical systems. We need to then be positioned to rapidly deploy patches across the federated networks. We need to be able to go from CVE release notification to patch at speed. What capabilities can enable us to meet these aggressive goals? Are there resource management tools that we could employ to help reduce the timeline as well?

3. *CHALLENGE PROBLEM*: Exploitability.

USCYBERCOM needs novel analytical methods that can analyze software and its function to identify vulnerabilities. Then for each vulnerability, determine how the vulnerability is exploitable and prove it. Our concern is directed towards certain software verses any software.

4. *CHALLENGE PROBLEM*: SCADA Vulnerabilities.

USCYBERCOM is concerned with vulnerabilities that some SCADA capability may possess. This challenge will focus on proving how a SCADA capability of concern can be exploited.

5. *CHALLENGE PROBLEM*: API Research.

USCYBERCOM would like to leverage open source research to actuate publicly available Internet-accessible APIs.

**MALWARE**

6. *CHALLENGE PROBLEM*: Environment for easy in/out malware analysis and reverse engineering.

Today USCC has a safe and secure albeit cumbersome process to access malware for analysis. We also need a faster approach. Could we create an off-line environment for antivirus signature testing for developed tools? What is the supporting agile infrastructure that will allow for virtual build up and teardown in an automated process to rapidly test and analyze malware safely?

7. *CHALLENGE PROBLEM*: USCC wants to explore the state of the art techniques for malware rapid triage, reverse engineering, correlation (e.g., grouping into families), and obfuscation.

8. *CHALLENGE PROBLEM*: Countering Polymorphic Malware.

   Adversaries are increasingly avoiding anti-virus detection tools by rapidly morphing their signatures. Small changes by adversaries create an asymmetric advantage by significantly increasing the work factor to defeat existing malware.

   USCC needs new techniques that would enable defenders to recognize polymorphic malware in real-time at the perimeter. What are some innovative new ideas to enhance immediate malware recognition? How could they be implemented to defend our networks and reduce the impact of their polymorphic nature? What applications are available to counter fuzzing and signature diversity in an automated fashion where traditional hashes or heuristics fail to detect malware?

9. *CHALLENGE PROBLEM*: Open Source Malware Research. Conduct open source research into latest malware trends and techniques.

10. *CHALLENGE PROBLEM*: Publish Defensive Data.

How can USCC leverage classified threat data in unclassified sensors? Could USCC anonymously publicize the detection of adversary malware, to include uploading malicious binaries and possibly network traffic to open source communities?

**ANALYTICS**

11. *CHALLENGE PROBLEM*: Know our networks. Can passive analytics alone map a multi-tiered, distributed network with a heterogeneous equipment implementation?

Currently we lack up to date complete documentation or a repeatable method to report fully on the networks we must defend. There are many tools on the market today that can help map networks. Are they able to completely describe our complex networks? What are their limitations and what are the implications for our knowledge gaps?

We need tools that will not only describe complex networks to include devices, software/firmware versions and patch level but also overlay command and control logic, data flow, protocols, and physical locations in near real-time. We need to be able to observe the aggregate network in order to select appropriate points that would enable us to catch adversaries in our midst. Can active implants or system agents help to bridge the knowledge gap, if so, how?

12. *CHALLENGE PROBLEM*: Predictive Modeling

U. S. CYBERCOM has limited resources to defend our networks. Today this is a very resource intensive effort largely reliant on experts to guide future efforts.

Are there ways to augment our efforts with machines? Can we generate attack graphs to model our defense? Can machine learning generate ideal attack paths informing defense of potential weakness or network design support?

13. *CHALLENGE PROBLEM*: Effective automation and analytics

USCC is eager to have analytics to reduce the burden on our operators. But often we jump without stepping through a thoughtful process. We can't create meaningful analytics without data accessibility and analysis. We too often accept data without a proper class guide limiting the ultimate effectiveness of the desired analytic.

We must define and employ a rigorous analytic process development methodology. We need to create a data submission/handling process. We need to then review class guide and context before accepting data. We need to build tools around desires of the experienced operator, build out "what-if" case studies to merge previously un-compared or disparate datasets for new insights. We need to ask ourselves what about this job may be automated to enable future discovery or analytic pursuit. How can I onboard a new operator and build upon previous operational experience or knowledge?

14. *CHALLENGE PROBLEM:* Normal and Abnormal Operating Conditions

As USCC digs deeper into the data available, we learn new information. We often don't know if this insight is anomalous or normal behavior. We must enable personnel to act quickly in the face of abnormal conditions, but we flood them with information typically out of context often out of order of operation relative to timeline.

We need to accurately and efficiently determine, measure and characterize the baseline state of a network and systematically specify what constitutes deviation from 'normal' activity. We need to recommend actions to situations that defenders can quickly understand and take.

15. *CHALLENGE PROBLEM*: Defensive Machine Learning/Autonomy

USCC is interested in building and training Machine Learning models to characterize and detect unknown malware infections on computer networks.

16. *CHALLENGE PROBLEM*: Analytic Development Efforts.

USCC desires to collaborate with other government agencies, industry, and academia to build data sets and analytics to compare analytic platforms, data sets, models, and techniques.

17. *CHALLENGE PROBLEM*: Artificial Intelligence for Exploit and Capabilities Discovery

Today's mission environment can be analyst intensive. It takes staff resources to strengthen network conditions.

How can we augment our cyber workforce with artificial intelligence? Where can we add automation, and machine learning to augment our cyber forces? After events like the DARPA Cyber Grand Challenge, how can we leverage AI for vulnerability discovery in real systems and then integrate stronger defenses into our systems, via industry or Cyber Mission Force developers?

**IMPLANT**

18. *CHALLENGE PROBLEM*: Network traffic Redirection/Obfuscation

We need ways to redirect selected network traffic so that an adversary cannot detect or determine that the selected network traffic route has been altered.

19. *CHALLENGE PROBLEM*: IOT Redirector Development/Defense.

Conduct open source research and reverse engineering of commonly used IOT devices

20. *CHALLENGE PROBLEM*: Code Persistence.

We need solutions to keep code or functionality persistent within network devices when various things are done to de-activate the code/functionality (i.e. the system is re-booted). Certain devices would be of greater interest than other devices.

21. *CHALLENGE PROBLEM*: Diversity/Survivability

Common software, common libraries, and even shared infrastructure reduces costs and increases interoperability. It also enables the vulnerability of one to be shared by all. We need new approaches to avoid the devastating impact a highly used but vulnerable capability. How can we reduce the risk?

Moving Target Defense Strategy has become an accepted method to thwart attackers from exploiting singular vulnerabilities across a similar software base. What are some capabilities we can employ now to increase our defenses? How can we reduce the risk? What can we do to manage risk better across missions? This need applies to development and operations. What new approaches can illuminate and reduce our aggregate risk? How do we develop more robust counter forensic and analysis resistant capabilities?

22. *CHALLENGE PROBLEM*: Testing / Experimentation – How can we test and experiment with special hardware OR special services?

Currently USCC develops and test in secure environments which preclude operating certain devices. This in turn limits our understanding of the challenges and opportunities for potential proposed solutions. We need flexible and accessible operational test environments while still protecting our equities.

What new operational testing environments should we consider to enable us to emulate hardware or network services to evaluate the risk of implementing new technologies outside our secure environments? How can we rapidly host virtually or emulated architecture and/or code on alternate hardware to reduce the risk of compromise to the system/network?

**SITUATIONAL AWARENESS**

23. *CHALLENGE PROBLEM*: Global Situational Awareness of Malware

Today it is difficult to track adversaries' maneuver of malware on our own infrastructures. When we lack this insight, it limits our ability to understand the specific goals and objectives of the malware, let alone the user's intentions.

We need to be able to "see" malware in our network. We need file and log level details distilled to meaningful data for comparison to a global viewpoint. We need an automated link and link types discovery application that can form associations useful in attribution. We need to see the software versions employed and observe malware ecosystems through evolution and in the context of it being a managed environment ultimately attributable to an actor.

24. *CHALLENGE PROBLEM*: Visualization

Today we view the cyber domain in limited segments with charts and graphs that fail to enable defenders and leaders to quickly act on rapidly changing situations. We struggle to intuitively understand the domain picture at all levels. Visio diagrams and manual reconstruction are time and human intensive. How do we holistically represent, integrate, and manipulate network traffic data and metadata into useful configurable graphic visualizations?

**CAPABILITY DEVELOPMENT**

25. *CHALLENGE PROBLEM*: Rapidly prototype solutions

How can we enable cyber personnel to rapidly prototype solutions on a "cyber playground"? How do we test and experiment with unique hardware OR online-only services?

Today we have several independent cyber ranges where new ideas can be implemented and assessed. These cyber ranges can be used for classified or unclassified experiments. In addition, U.S. CYBERCOM just launched the DREAMPORT initiative to enable collective collaboration between industry, academia and military entities in DREAMPORT unclassified spaces to explore and resolve problems. These are all valuable steps to enable rapid prototyping.

What we need is the ability to work collaboratively in a shared secure virtual environment so that we can effectively leverage the best and brightest minds not just the local or occasionally local minds and tools. How do we leverage a wider community to develop foundational and other capabilities at lower classifications? Can it be done? Do we need specialized tools? What are the challenges?

**PERSONA**

26. *CHALLENGE PROBLEM*: Recognizing Adversarial use of False Persona Registration and Operation.

Today our adversaries are creating and using on-line personas. Today's tools to recognize them are limited. They all too often evade fraud detection.

As adversary on-line persona based operations increase, we must recognize and stop them. In fact, we need to defeat them earlier in the persona development cycle. Are their signatures or patterns we can associate with false persona development and operations? How are they successfully registering false accounts? Do they register with false information? Are the false personas variations of real people or are they completely made up entities? Do these false adversarial personas pay with anonymous crypto currencies? How are these adversarial false personas similar or different from criminal behavior in establishing these personas?

27. *CHALLENGE PROBLEM*: Misrepresentation.

We are concerned with the use of masquerading techniques and would like to determine if there are masquerading techniques that avoid identification and detection. Also, it is important to know if this result would be different for various network devices.

28. *CHALLENGE PROBLEM*: Synthetic Users

Design and build a system to create synthetic user and network activity on a network to be used in a customizable and re-playable manner for high-fidelity mission capability and TTP testing. Current systems used throughout the Command and the greater DoD lack the detail needed to simulate real world networks at the fidelity needed to support capability testing and to perform mission rehearsal. The system should be able to collect and anonymize real world network and host data to enable it for re-use in a simulated environment in a configurable manner. This effort would be a lash up of existing

USCC J9, JHU/APL, and MIT/LL personnel who are working on this effort currently; potential to incorporate an OUSD (R&E) study into this and possibly others.

**HUNT**

29. *CHALLENGE PROBLEM*: Hunt "Exercise".

Experimentation to identify the best practices, TTPs, and data needed to conduct DCO Hunt.

**MISSION MANAGEMENT**

30. *CHALLENGE PROBLEM*: Automated Mission Risk Management

We have limited ability to assess the risk associated with most missions. At best we have a fragmented understanding of our posture and our risk often based on outdated or incomplete data. We need to understand the risks to mission execution and we need to be able to effectively convey those to our partners and those we support.

Leaders can take calculated risks, if they are known. What are the key risk components, how should they be tracked, visualized and how can they be effectively communicated? How do we calculate and include 2nd and 3rd order of magnitude effects of risk alternatives and preposition for adversary contingencies to mitigate risk exposure?

31. *CHALLENGE PROBLEM*: Data and Information Sharing

Moving large amounts of data over unclassified links is critical to enable defenders and leaders to visualize their area of responsibility in the domain. Not only do they need to see their responsible areas but need to share insights and gain insights from the larger context.

We need dynamic, mission configurable, anonymized data collection and transport. Is there a service element technology development effort that can expedite massive storage on the scale of petabyte to Exabyte storage and transfer?

32. *CHALLENGE PROBLEM*: Auto Installer.

We need the ability to remotely change, upgrade, or install software within a network enabled device through automated means when a human operator is incapable, doesn't have time, or doesn't have the knowledge to make the necessary changes while the system is operational.

**ATTACK**

33. *CHALLENGE PROBLEM*: Innovative computing resources.

We have a number of hard problems that require tremendous computing power. We don't have enough compute power to perform all the tasks at hand.

Are their innovative ways we could harness the DoDIN computing power for Brute Force attack actions or parallel processing of complex problems sets without adversely impacting mission needs. Can we leverage commercial cloud compute resources effectively as an alternative for surges of compute and

data analytic needs?

**SECURITY**

34. *CHALLENGE PROBLEM*: Strengthen the Cyber terrain to be defended.

U.S. CYBERCOM and our military partners have extensive, complex, and continuously evolving cyber terrain to defend. Further these networks have varying degrees of security baked into their architectures and built into their implementations. The strength of their security is further compounded by the need to maintain legacy systems while constantly patching networks to fix newly discovered vulnerabilities. The defense of our networks are resource intensive. In addition, the size and skills of our attackers are improving and the scale of their attacks are also increasing.

What changes should we consider to our approaches for our networks and their defense? Are there novel approaches to shore up what we have as well as game changing ideas? For example, should we consider moving away from traditional networks to zero trust approaches like software defined perimeters?

35. *CHALLENGE PROBLEM*: Best Practices for Secure, resilient processors, protocols, operating systems, APIs, compilers for U.S. CYBERCOM Key Terrain.

Our networks must be protected. Key Terrain must be even more protected. We must use a multi-layer approach. As we design and develop our infrastructure and tools, we need to ensure we are baking in security at every step. We must plan to use the latest security best practices.

We need to be aware of best practices, tools, techniques that we can employ early so we can plan for them to be incorporated. What recommendations should we pursue implementing?

36. *CHALLENGE PROBLEM*: Specialized Solutions to Enhance the Defense of Key Terrain.

Currently our network defense posture is focused on defending the network at the perimeter. As it becomes increasingly clear that adversaries are gaining ground inside networks, it is unwise to assume the networks we defend are as robust as we intend.

We must increase the defensive layers and depth of our most valued assets in a layered approach. USCC must be the gold standard for network design and operations. We must not lose our most critical information, implement full data at rest encryption, access control and authentication methods. While we cannot protect the entire network at the same level, we must protect our key terrain. What combination of specialized hardware and software can and should be used.

37. *CHALLENGE PROBLEM*: User Activity Monitoring.

Description: Design, implement, or enhance User Activity Monitoring (UAM) solutions for detecting live and recent insider threat attacks or unauthorized activities. Identify UAM solutions that employ advanced real-time analysis of multiple data sources, which includes predictive monitoring (configuration-less) features and not just policy-based (Allow/Deny) monitoring features.

**BLOCKCHAIN**

38. *CHALLENGE PROBLEM*: Can block-chain help attribute adversaries?

Where does block-chain create challenges and opportunities in our ability to attribute or identify actors in cyberspace?

Today we recognize some actors in cyberspace but not all. The work is painstaking especially with advanced adversaries using advanced tradecraft to obfuscate entities and actions. How do we discriminate nation state adversary activity?

Are there techniques we can employ that can link entities through employing or analyzing block-chain and/or block-chain based cryptocurrencies? Applying these techniques to entities we do not create adds extra complexity but could potentially provide game changing insights. What are the real opportunities and challenges? How can we merge target identifier information with data in order to attribute identity information?

39. *CHALLENGE PROBLEM*: Defensive Cryptocurrency.

Conduct open source research and experimentation to develop prototypes to counter adversary use of cryptocurrency and cryptocurrency mining.