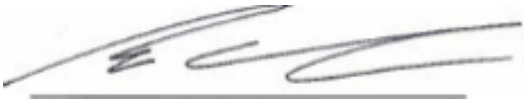
AIR FORCE CYBERWORX REPORT 18-001
CyberNext Event
Software Guard Extensions



Michael Chiaramonte, Lt Col, USAF
Director, AF CyberWorx

Velynda Prakhantree
Innovation Strategist, AF CyberWorx

PROJECT CONDUCTED
11 January 18, Scott AFB

Produced with input from numerous units including, ACC A2/A2Y, ACC 25 AF/A2Y, AFLCMC/EN/HNC/HNCE, AFSPC/A/2/3/6M, AMC A6, DAU, HAF NASIC, HAF/A3/A4/A4C, HAF-A2, PEO BES, SAF/CIO, SAF/FM, SAF/FMFS, SAF-CIO A6, SAF-FM CIO and our valuable partners in industry including, Intel, Jeppesen, and Fortanix.

Air Force CyberWorx™
2354 Fairchild Dr.
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

Introduction to AF CyberWorx

CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking & CyberNext at AF CyberWorx

Design thinking is a common sense, human-centric problem solving method embraced by innovation leaders in industry, but often overlooked in the government sector. The CyberWorx design thinking process is a transdisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede creativity, collaboration, and knowledge sharing vital to innovation. CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The transdisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

Air Force CyberWorx offers facilitated design thinking sessions that bring stakeholders, industry and academic experts together to develop solutions to hard problems. These sessions are tailored to best meet AF needs with differing lengths based on time sensitivity and CyberWorx capacity. One method, which maximizes solution agility and the educational benefit to warfighters and industry partners, is to offer a design sprint where the week-long design project answers a challenge being worked for AF stakeholders. The goal of such a design sprint is to develop low fidelity prototypes that clearly convey the desired Airman experience and the technical and policy developments needed to bring that experience to fruition. These projects help refine the requirement by seeking the right problem to solve and finding meaningful, forward-looking solutions by exploring a wide range of possible answers to the design problem.

The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

In addition to facilitating design sprints, CyberWorx hosts events in which an established industry technology is brought before the Air Force to generate potential use cases for application of the technology within the Air Force environment. Participants in this type of event vary based on the technology being showcased. This particular event highlighted Intel's Software Guard Extensions (SGX) technology, which provides security at the hardware level rather than strictly through software. SGX protects applications and data as they are exposed to malicious attacks by hiding the data in secure enclaves.

Background & Participants

CyberWorx' Center of Innovation has a long-standing relationship with Intel in conducting research with US Air Force Academy Cadets. The CyberNext SGX event provided an opportunity for Intel to demonstrate its technology with partner, Jeppesen and its Electronic Flight Bag (EFB). The event took place at Scott AFB and included Air Force representatives from ACC A2/A2Y, ACC 25 AF/A2Y,

AFLCMC/EN/HNC/HNCE, AFSPC/A/2/3/6M, AMC A6, DAU, HAF NASIC, HAF/A3/A4/A4C, HAF-A2, PEO BES, SAF/CIO, SAF/FM, SAF/FMFS, SAF-CIO A6, and SAF-FM CIO.

Use Case Scenarios

The event began with Intel demonstrating SGX proof of concept with the EFB in regards to memory security, lost device security, and exploit security. Once the technology was demonstrated, participants were divided into groups, each with military and industry representatives and were prompted to ideate potential use case scenarios centered on the human experience with SGX or like technology. In other words, how might we use this type of technology to best improve AF/DoD ops? How might we use it to accelerate these types of technology into the DoD enterprise?

With dozens of potential solutions, groups were then asked to choose their top two or three and share-out to the whole group. The group voted on the ideas in three categories: Impact, Easy Win, and Innovative. The top five solutions were studied more closely and became solid recommendations from the event.

Recommendations

The use cases with the most votes were expanded upon into strategy boards to include a brief future vision, potential barriers to that vision, and a suggested way ahead.

1. Remote Data Destruct

Use Case	Future Vision
A **System Administrator** needs a way to ensure data on lost devices is secure from unauthorized access because data contains PII and PHI and some devices may not have full disk encryption.	Airman Joe is not fired for losing his devices containing classified and PII data. Whether the device is a smartphone, laptop, or UAV, the sensitive data is remotely accessed and destroyed by the tactical team.
Barriers to Vision	**Way Ahead**
How do I trust the out-of-station server? How do I secure that? Development: No one has done this before.	Develop a prototype/MVP for E3 servers and very specific UC Open a challenge: Who can do this? Perhaps a development challenge to win a prize.

2. Multi-Level Single-System C2

Use Case	Future Vision
C2 elements need a better way to process multiple levels of data on fewer systems in a secure manner so that they can collaborate	C2 elements can securely process multiple levels of data on a single system and transmit & receive securely from connected systems.

more effectively with fewer systems and data leaks.	
Barriers to Vision	**Way Ahead**
NSA Certification – who owns it? Policy Funding	1. NSA Certification of SGX (or similar). 2. Ownership/sponsor/funding 3. Develop requirements & architecture

3. PII Protection Parameters

Use Case	**Future Vision**
A **System Administrator** needs a way to ensure data on lost devices is secure from unauthorized access because data contains PII and PHI and some devices may not have full disk encryption.	Information system owners can easily and adequately protect PII using defined parameters.
Barriers to Vision	**Way Ahead**
Establishing mission supportive parameters (i.e., how long until data is "shredded"?) Auditing/notifications: Make sure access and use parameters are consistently applied	1. Develop use case matrix 2. Develop time & sensitivity matrix based on use case 3. Submit matrix for approval from stakeholder communities 4. Prototype, Test & Modify based on feedback 5. Implement (and continue to modify)

4. Airmen's Any Device

Use Case	**Future Vision**
A **Tele-Worker** needs to complete work with appropriate access to work data so that they would have a secure work space in any location. Benefits: Increase morale and maximize workers' time. Potential decrease workplace public health issues (spreading illness) and workplace violence.	Extend to **all Airmen** (not just Tele-Workers). All Airmen will have the ability to complete their work anytime, anywhere, on any device.
Barriers to Vision	**Way Ahead**
1. Connectivity 2. SGX not yet in mobile space	1. Enable functionality on capable devices 2. Update personnel policies

3. Ownership and control 4. Cross-chip communication 5. Personnel policy 6. RMF	3. RFI to industry

5. Single Joint Access Point

Use Case	Future Vision
A **Multi-National Partner** needs a way to securely control who can see what information so "Mission Partner Networking" without having to have numerous single-use networks (i.e., NOFORN vs. 5-EYES vs. MNFI)	A NATO Joint Forces member walks into work and logs into a computer where everyone has access to the same network and data but views readable information based on need-to-know.
Barriers to Vision	**Way Ahead**
Policy/Law	Design/develop architecture Common credential Find a contract vehicle

Next Steps

Upon consultation with Intel, CyberWorx has further narrowed the solutions and proposes easy, medium and high level of difficulty options. These applications are relevant for the Department of Defense as well as other government agencies, such as Department of Homeland Security.

The opportunity that offers the quickest win is combining solutions #1 and #3 for improved PII protection and exclusion. Prototyping can begin immediately using SGX to secure PII. Protected PII comes in two flavors – first, if a user loses a device, the PII can be remotely destroyed or hidden in secure enclaves. The second, secures PII that has not been used for a specific period of time. That is, a user automatically loses the keys to the PII at a date specified by the organization. It still exists but cannot be accessed. AF CyberWorx can assist in development of this tool through E3 or E5 second-run server prototypes provided by Intel.

The solution with the intermediate level of difficulty is #4. Prototyping for this challenging solution involves co-locating data using the Electronic Flight Bag. Co-locating data on a single device in separate enclaves allows users to securely access the data from any location with Wi-Fi. The biggest hurdle in developing an applicable prototype is that third party vendor adoption of SGX. For example, SGX is not used within Microsoft Office yet which DoD uses heavily. This will be addressed over time as SGX and like technologies garner more market exposure.

Finally, the proposal with the greatest level of difficulty is solution #5, developing digital redaction into secure enclaves. This would likely require policy and legislative changes or waivers. The US has a long-lasting relationship with the current security policy and creating a means to redact specific words, sentences, or paragraphs would take significant development to integrate within existing systems.

In deciding what step to take next, it is important to weigh risk against the solutions' potential benefit. The greatest benefit may also come with the greatest risk of failure, time consumed, or money spent. Often, the reluctance to make a decision leads to ambivalence, which inevitably results in failure through lost opportunity. CyberWorx believes all three solutions have merit and offer the opportunity for further development and investigation. In order for our Air Force to remain agile and on the leading edge of technological solutions, CyberWorx stands ready to support prototyping and moving forward with SGX and similar technologies.