CIGENT

Advanced Protection for Sensitive UxV Data

Safeguarding UxV Missions from Unauthorized Access and Data Threats

ADVANCED PROTECTION FOR UXV DATA:

Safeguarding UxV Missions from Unauthorized Access and Data Threats

Problem Statement

UxVs store and collect sensitive and classified data including applications, algorithms, mission, and target data stored for and captured during the mission.

UxV mission parameters guarantee many will be recovered by adversaries.

Unauthorized access to UxV data will have significant consequences.
Failure to prevent unauthorized data access will result in:

- **Adversary accessing UxV algorithms**
  a. Gain insight into ATR (Automated Target Recognition) criteria. Utilize to modify configurations undermining UxV efficacy.
  b. Compromise the efficacy of swarms with automated reactions. Utilize algorithms to understand and develop countermeasures.
  c. Degrade the effectiveness of PNT (Position, Navigation, and Timing) algorithms used to map the terrain in GPS denied environments.
- **Adversary accessing mission information** including location, tactics, targets, and capability data.

UxV data is not being adequately protected with manufacturers lacking expertise in data protection, widespread use of an insecure mobile device platform, and lack of defined data protection policies.

Mission requirements increase the complexity of protecting UxV data as they will be operating in extreme environments, require seamless experience for operators, and support autonomous operations.

Protection of UxV data must cover the full lifecycle of data including mobile workstations analyzing field telemetry and developing new algorithms, external media used to transfer data to UxV management systems and the UxV devices. Adversaries will seek the weakest data security in the full data lifecycle to compromise UxV missions.

Cigent Capability Summary

To address the outlined risks while ensuring operational availability of UxV, Cigent provides a layered approach, including secure storage, firmware-rooted capabilities, and data access control software.

Protect Data at Rest	Fundamental to data security is the prevention of unauthorized access to DAR. UxV data is secured with three layers of encryption including both hardware and software encryption. The solution meets NIST, FIPS, and CSfC DAR compliance requirements.
Ensuring critical data is protected from data attacks	Advanced data recovery, malware, and denial of service attacks can result in data extraction, modification, access prevention, and erasure of critical data. Cigent protection includes zero-trust access controls and isolated storage partitions ensuring constant, secure availability of critical data only by trusted users and applications.
Seamless Operations	Protection is delivered without impacting operations or the user experience. This is accomplished through integration with existing user workflows and automated authentication enabled by existing system components and user credentials. Automated authentication is critical as UxVs often operate with limited or no human interactions.
Insider Threat Mitigation	There are two elements in reducing risk of insider threat: controlling access and monitoring activity. The separate partitions previously described provide for the segmentation of data and controlling access to required personnel. Firmware secured data access logs collect all data access, providing an uncompromised record of activity. Data logs can be exported for analysis to detect malfeasance and for event forensics.
Data Destruction	UxV operations make data destruction an essential element of each mission. Device sanitization must be executed remotely or automated, based on parameters including mission complete, rapid descent, UxV out of range, etc. Cigent implements erasure in seconds via cryptowipe, full block-level erasure, and firmware-based verification ensuring UxV can safely be left in the field without needing to deploy recovery teams.
Maintenance and Updates	UxV will regularly be updated with mission requirements, algorithms, and new applications. To ensure data remains protected throughout the update and data lifecycle process, an ecosystem of secure storage for rugged laptops, tablets, and external media along with file encryption is further implemented.

Cigent Operational Capabilities

UxVs play a critical role in collecting, processing, and storing sensitive system files, mission data, and reconnaissance information. This requires a layered security approach that ensures data integrity and system resilience without disrupting operations. UxVs are often deployed in high-risk missions involving stealth and reconnaissance, which leave them vulnerable to data extraction, tampering, malware insertion, and insider threats.

Portfolio

Cigent solutions include multiple secure storage form factors required across UxV form factors and meet extreme temperature environments.

These include:

Category	Product	Descriptions
Media	SSD BGA	Integrated directly on the UxV board
	M.2 SSD BGA	Plugs into the M.2 slot on the UxV
	Micro SD	Plugs into the MicroSD slot on the UxV
External Media	Enterprise Management Application / Server	Supports external media management and control

Data at Rest Protection

Fundamental to data integrity is protecting data while in use and not in use. Data at rest (DAR) protection is provided with multiple security layers, using a defense-in-depth strategy to protect data from all adversarial attack vectors during all operational scenarios.

Cigent's integrated solution addresses these threats with a combination of hardware, firmware, and software protection.

This solution is agnostic to the control system's software or operating system, providing seamless, robust security.

CIGENT

1. *Hardware Full Drive Encryption.* Encryption is AES-256 and FIPS compliant in accordance with the TCG (Trusted Computing Group) Opal 2.0 or similar guidelines. Storage may also adhere to the FIPS 140-2 Level 2 requirements, including using epoxy on the drives.

2. *Locked Ranges.* Ranges are defined segments of data storage that are monitored and protected independently. To protect data from attempts to wipe, clone, or view data at the hex level storage ranges are locked at the firmware layer, rendering the ranges/data unreadable by cloning tools and hex readers.

3. *ADR Protection.* To protect data from advanced data recovery methodologies such as chip off or utilization of an electron microscope:
   - All storage utilizes hardware encryption. If an adversary removes the data from the drive with advanced techniques, the data remains in an encrypted state. Without the decryption key, adversaries will be unable to decrypt the data.
   - The key will not be stored in its entirety anywhere on the drive and the pieces of it that are stored on the drive will be encrypted. Between these two measures, the key will not be able to be accessed or recreated.

4. *Secured Firmware*. In addition to the encryption capabilities, the storage firmware has been modified to resist advanced threat vectors. SSD firmware has been modified to meet compliance with FIPS 140-2, NIAP Common Criteria FDE_EE standards, and CSfC DAR Capabilities Package 5.0 requirements. Including:

Multiple security layers ensure protection against all adversarial attack vectors during all operational scenarios.

   - Standalone approved cryptographic algorithm certification, power-on self-tests of all cryptographic algorithms, a module entering error states when any cryptographic function fails, NIST approved methods for cryptographic key generation and using approved techniques for the generation of random bits, and minimum entropy of hardware random bit generator evaluated according to SP 800-90B, and tamper-evidence protection.

Pre-boot Authentication

Pre-boot authentication (PBA) provides a secure user authentication platform on the device that is fully protected at rest. Properly configured PBA prevents adversaries from circumventing encryption by manipulating the boot process.

1. Prior to proper pre-boot authentication, the entire drive, minus a small Shadow MBR (Master Boot Record) partition, will be locked in a locked range.
2. Upon power-up, an O/S designated for the purpose of authentication will boot from the shadow partition and pre-boot authentication (PBA) software will load.
   a. The PBA software has been validated to meet FIPS CAVP, NIAP Common Criteria FDE_AA, and CSfC DAR Capabilities Package 5.0 requirements.

3. Upon boot, authentication will take place in a manual manner if an end user can be involved in the boot process. If infeasible, an autonomous manner, so as not to impede the boot process and facility operations, while still meeting best practices and compliance requirements as much as possible in this environment, will be used.
4. Multifactor Authentication is supported with factors including Trusted Platform Module (TPM) 2.0 detection/processing, Hardware Security Module (HSM) - FIPS where possible, a security key (i.e. YubiKey), and/ or detection of a specific network device. MFA for File Access. When a file is attempted to be accessed, the file filter driver will be engaged and determine whether to require MFA. This prevents malicious actors from extracting files from systems.

Protection while Device is In-use / Malware Prevention

Methodology and technology designed and tested for UxV will not impede operations while mitigating risk of unauthorized data exfiltration and minimizing malware compromise and eliminating risk of spread. Cigent utilizes separate ranges that can segregate system files, mission data, and reconnaissance information, limiting access and mitigating risk of malware introduction.

Locked Ranges	Devices can be configured where data, software, and configuration files can be stored separately providing the ability to create “read only” secure enclaves where software and configuration files will be sequestered. Devices will still be able to “write” collecting and processing data as their role requires. These partitions will also enable access controls defined by user requirements.
File Filter Driver	Once the O/S loads a file filter driver will be initiated. The file filter driver will provide a layer of runtime protection ensuring only appropriate (allow list) apps and processes can access and save files, preventing malicious access, data extraction, and compromise (such as modification, deletion, overwriting, etc.)
App Whitelisting	The appropriate file or application for accessing a file can be allow list preventing the MFA prompt. This ensures proper execution of the system functionality, while simultaneously preventing malicious access and data extraction.
OS Partition	The O/S partition will further be mounted in read-only mode. This will ensure malware is not loaded on this partition and a reboot process will reload the system into a known good state.

Both system and firmware logs can be captured and uploaded to the enterprise management software for reporting, analysis, and suspected insider threat alerts. These can also be exported to a SIEM for ongoing analysis.

Data Access Controls

Access is controlled with 2FA/MFA. In the event an adversary attempts to access files in an unauthorized manner, a prompt will be displayed, requiring the user to authenticate. If they are unable to authenticate, they will not be able to access the file. An adversary attempting to access a file will not disrupt the allowed list apps or processes from accessing the file. All access log attempts will be stored on the system in a secure location in a special log file designated for this purpose.

Recovery Capabilities

To effectively recover from a malware attack, systems must be able to quickly return to a known, secure state. Standard base configurations are secured in "read-only" partitions with restricted access. If control system components are compromised by malware or unauthorized changes, these base configuration files can be accessed to "reboot" the system. This approach acts as a failsafe, protecting UxV operations from being subverted during an attack.

Insider Threat Protection

Mitigation of risks associated with malicious insiders includes preventive protection and protected log files of data activity.

1. *File Level Encryption*. Preventive protection is delivered through file-level encryption that encrypts data collected and stored on UxV devices. File-level encryption sustains encryption protection if data is removed from the device. The approach prevents an insider from exfiltrating data in clear text.
2. *Secure Data Logs*. Document immutable records for all data activity. These tamper-proof records can be examined for potential malicious activities and used in forensic investigations.

Data Sanitization

Data on ICS that are repurposed or at end-of-life needs to be sanitized. Sanitization solution will include the ability to both erase and verify data has been erased. The solution may provide an alternative to physical device destruction and can be used in emergency situations.

1. *Crypto and block erasure*. Crypto erase deletes encryption keys thereby rendering data permanently inaccessible. Block erase utilizes an electrical charge to erase data.
2. *Verified Data Erasure*. Firmware immediately verifies that all data has been erased with block-by-block analysis. Block erasure can be re-run until all data successfully sanitized.
3. *Santization Execution.* Sanitization command can be initiated manually either locally or remotely or utilizing automated requirements. For example, if connectivity is severed or an UxV falls below a pre-determined altitude sanitization can be set to execute.

Maintenance & Updates

An effective data protection solution requires a methodology for updates and management. Cigent capabilities include maintenance PCs, servers and external media to support secure and efficient maintenance and updates. This is to mitigate risk of the insertion of malware on UxV devices, the malicious utilization of these devices to exfiltrate data, or the protection of data if a computer device is lost or stolen.

Conclusion

UxV will collect, process, and warehouse sensitive information. Mission requirements make UxV susceptible to being lost, creating the potential for unauthorized data access. Adversaries who gain access to data could gain insight to mission-map information, compromise ongoing UxV operations, and reverse engineer valuable system codes and algorithms. UxV operational requirements including operator capabilities, automation requirements, and extreme environments complicate data protection on UxV.

About Cigent

Cigent provides unparalleled technology, ecosystem, and expertise to ensure your sensitive data is protected no matter what your mission. The Cigent solution was developed for and with US Federal agencies by leading experts in data recovery and sanitization. Partnering with leading UxV manufacturers, Cigent has developed technology and processes to support the unique nature of UxV operations.

The United States-based organization includes cleared personnel (TS/SCI) with extensive operational experience. Cigent can provide off-the-shelf capabilities or support custom projects with United States-staffed firmware and software development teams.

See how Cigent keeps you **AlwaysPROTECTED**.

www.cigent.com
info@cigent.com
844.256.1825