CENSUS
IT Security Works

SECURING MILITARY COMMUNICATIONS

CENSUS is an internationally acclaimed IT Security service provider. Through its pioneering IT and OT Security research, CENSUS delivers state-of-the-art services supporting organizations in multiple industries worldwide.

CENSUS can assist both users and suppliers (OEMs, Tier-1 and Tier-2) of military systems to achieve **secure usage**, to **improve security** and eventually to **reduce the applicable risks**.

THE CHALLENGES

Military communications play a vital role in warfare and intelligence gathering operations, with the end goal being the secure transmission and processing of signals. Since new technologies are rapidly emerging, and more devices, vehicles and sensors are connected in the military networks, **cyber warfare** is likely to occur.

In a military operation, the **secure exchange of tactical information** plays a fundamental role in the **success of the mission.** Within this very scope we find a suite of instruments, applications, services and functions synthesised in the acronym **C4I (Command, Control, Communication, Computer and Intelligence)**. Briefly, C4I concerns "Information Superiority"; it is a force multiplier, a key element that provides the means for acquiring an advantageous position and contributes to achieving success, especially in the framework of interagency and international operations. This process of gathering information enables the **acquisition of Shared Situational Awareness,** which is when all the forces are jointly aware of the operative situation.

In this sense, the **digitalisation** of the Armed Forces is the first step towards actualising a net-centric system, which is the integration of technological solutions within a C4I system in order to share the information obtained during the different operational phases at the right time. To digitise also means taking the different **C2 (Command and Control)** systems used by the Armed Forces and, wherever possible, the various assets and platforms utilised by the Navy, the Air Force and the Army, and uniting them in a single network in order to communicate.

APPLICATION SECURITY

Suppliers and consumers of military systems face ample cyber security challenges when manufacturing or integrating such solutions. Firstly, the data is the most crucial parameter to protect across its transit and storage lifetime. Numerous technical limitations and risks of transport channels should be factored in the implementation of secure protocols that can ensure the **confidentiality**, **integrity**, **availability of the transmitted information**, and **interoperability** among the operative forces in an international coalition. This task becomes extremely complicated considering the insecure, by definition, nature of transport channels used in the field, outside air-gapped topologies. Furthermore, secure data transit should be always paired with an equally robust data storage on both sender's and receiver's side. Implementing the latter is an extremely demanding process for field systems with high exposure, such as drones, mobiles devices and sensors. The second essential aspect of a military network is the **authentication and authorization** of the interconnected users and devices. Methods such as biometric authentication and trusted module hardware attestation should be used from peers establishing connections on the military network.

MILITARY GRADE DATA ENCRYPTION

For systems that process or store high-risk or classified data, further in-depth defense strategies should be applied by **hardening the critical modules** and **the storage of cryptographic material**. Therefore, solutions such as tamper-resistant hardware modules should be incorporated to provide a secure baseline for generating, storing, and managing cryptographic material, as well as creating **digital signatures** and **certificates**. For example, the **hardware security module** (HSM) is a physical computing device performing a variety of cryptographic operations such as key management, key exchange, encryption and decryption for digital signature, and other cryptographic functions. These modules traditionally come in the form of a **plug-in card** or an **external device** that attaches directly to a computer or network server.

Due to the critical role of these modules in applications and infrastructures, they are typically certified based on industry accredited standards, such as the Federal Information Processing Standards (FIPS). The requirements specified in the FIPS PUB 140- 2 outline a total of 11 areas of design and implementation of products in applied cryptography. These areas include:

- cryptographic module specification
- roles, services, and authentication
- ports and interfaces
- operational environment
- physical security
- EMI / EMC
- key management
- design assurance

SYSTEM AND DEVICE SECURITY

In some cases, it becomes extremely challenging to implement strong security on **systems** that are **low on resources**, such as battery and power consumption of equipment used by soldiers in the field. For example, in IoT devices, due to limited computing, memory, and storage capabilities, it is common case that traditional security countermeasures and proactive defenses cannot be directly applied. As a result, it is necessary to implement **customized architectures** that do not compromise the main security pillars. **Root of trust designs** can attest that the system has booted into a known and trusted state (or alternatively, uncover the presence of malware with high probability). At the same time, this system should provide adequate resistance against side-channel attacks. **Side-channel analysis** represents a major threat to the security of the cryptographic material and components of embedded devices. Rather than targeting the software directly, these attacks aim to gather information from the program execution of a system, by measuring or exploiting indirect effects of the system or its hardware, e.g., by obtaining power consumption measurements and timing information. Side-channel attacks depend on the relationship between information leaked through a side-channel and the secret data. Consequently, countermeasures consist of two main categories: (i) elimination or reduction of such information release, and (ii) elimination of the relationship between the leaked information and the secret data.

MEETING MISSION OBJECTIVES

To overcome the aforementioned challenges in securing military communications, **CENSUS offers** services such as:

- **Embedded and Mobile Devices Security Assessment**,
- **Application Security Assessment**,
- **Secure Software Development Life Cycle (SDLC)**,
- **Network Security Assessment**, and
- **Penetration Testing**

The first step towards securing these high-value systems is to **identify the critical assets**, and then ensure the security maturity of all the functions around them. For most cases, **air-gapped architectures are no longer feasible** to the same extent due to the increased requirements, and therefore more complicated architectures need to be adopted and implemented. **CENSUS provides a variety of services** that can identify design inefficiencies, gaps in the security architecture and software vulnerabilities in the actual implementation, while providing practical recommendations towards their efficient mitigation.

CENSUS believes that it is critical for **Security by Design** principles to be implemented early in the development lifecycle of the product. For each phase, CENSUS offers a highly customized set of services, whose goal is to develop products that meet high security standards by following models such as **Defense in Depth** and **Zero Trust Security**. Defense in Depth involves multiple-layer security and redundant defensive measures in case a security control fails, or a vulnerability is successfully exploited on a system or network. Moreover, Zero Trust models are developed based on the assumptions that a user or a device cannot be trusted by default and the network faces both external and internal threats, expanding the user verification and granting the least-access privileges. These methodologies allow the **early mitigation of security risks**, **identification**, and **resolution of security vulnerabilities** in a cost-efficient manner.

Due to the increased demand of military information technology systems, it is inevitable that **not all integrated solutions are developed in-house**. Therefore, many commercial, **off-the-shelf**, products are purchased and integrated into the military network. A big concern is that commercial producers are becoming more and more globalized and expose themselves to the risks of complex and intrinsically vulnerable supply chains. Thus, they require vetting of their functions, along with **secure integration and usage**. CENSUS can execute these services and provide **security assurance of the third-party solutions** that are adopted.

CENSUS has **extensive experience** in the military sector with a wide range of projects including:

- Customized and hardened mobile devices for military usage
- Remote control protocols for embedded devices
- Hardware tamper solutions for IoT devices
- Mobile applications for secure communications

KEY TAKEAWAYS

In the past, government and military focused on the cybersecurity of their networks without considering the vulnerabilities of the systems themselves. CENSUS uses the **latest attack techniques** along with the results of its **in-house vulnerability research** to identify common and acknowledged vulnerabilities and distinguish the possibilities of **zero-day attacks**.

CENSUS vulnerability research services ensure that a software product, a system implementation, or a new technology that an organisation is planning to invest in **meets strict security requirements** and does not suffer from vulnerabilities.

Securing critical systems demands a **strategy** and **proactive** approaches to eliminate the risk. It is crucial to understand (i) **the valuable assets**, (ii) **suppliers' security level**, and (iii) **the risk posed by the supply chain**. CENSUS provides detailed deliverables that empower clients to make informed strategic decisions towards new technologies, and to choose the most secure solution that meets their requirements.

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 617-448-5050
E. usa@census-labs.com

EUROPE
128, Leoforos Andrea Syggrou,
11745, Athens, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

UK
4th floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 (0) 1293 763 336
E. uk@census-labs.com