

**CASE STUDY:****EMBEDDED COMPUTER SYSTEMS SECURITY ENGINEERING****CLIENT DESCRIPTION:**

The F/A-22 is the Air Force's newest production, high performance, low observable tactical fighter. It is also the Air Force's first "paperless" fighter. All pilot mission planning functions and all ground maintenance support are performed by networks of embedded fixed and mobile computers that process information of varying sensitivity. Thus, the F/A-22's airborne and ground support communications and computer systems must be certified and trusted to reliably process multiple levels of classified and sensitive information including Special Access Required (SAR) data in a multilevel secure (MLS) mode of operation.

CTA supports this highly critical program with two teams of security engineers:

The first team works directly under contract to the Air Force's F/A-22 program office to provide security certification and accreditation technical support for all airborne and ground support information processing systems and networks in this complex advanced tactical weapon system. In this role, CTA engineers work with Air Force and National Security Agency counterparts to specify information system security policy and to develop information system security certification plans. CTA ensures that policy and plans adhere to evolving national security standards for information processing systems security. CTA also conducts threat and risk analyses to ensure the embedded hardware and software security mechanisms, coupled with physical and procedural security controls, mitigate risks to an acceptable level. CTA engineers work in integrated Government/contractor teams to continually assess risks associated with design decisions, and to ensure the operational impacts of security are acceptable to the users.

The second team provides computer and network security design and implementation support to the Lockheed-Martin Aeronautics Company, the F/A-22's system security engineering prime contractor. This CTA team works closely with F/A-22 weapon system designers to develop security standards for system and software development processes, ensure the adequacy of embedded hardware and software security mechanisms and provide advice on emerging security technology and its applicability within the F/A-22 weapon system. CTA develops and documents computer security designs, concepts of operation, and produces security instructions for computer and network system administrators and users.

**SECURITY ENGINEERING PROJECT DESCRIPTION:**

The F/A-22 program encompasses embedded computer systems on the Air Vehicle itself as well as ground systems that support the aircraft. The scope of CTA's tasking covered the entire weapon system and includes multiple secure networks supporting thousands of F/A-22 developers. These include the Air Vehicle Avionics; the Support Systems, comprised of the Mission Support System (MSS) and the Integrated Maintenance Information System (IMIS); and the System/Software Engineering Environment (S/SEE), which includes multiple secure networks supporting the thousands of F/A-22 developers across the United States and in several other countries.

**WORK ACCOMPLISHED:**

We successfully developed and delivered the System Security Concept of Operations (SSCONOPS), the Descriptive Top Level Specification (DTLS), the Security Vulnerability Analysis (SVA), and the Weapon System Threat/Vulnerability Assessment. CTA was a key member of the F/A-22 weapon system's

Electronic Key Management Working Group, comprised of representatives from the F/A-22 SPO, Air Combat Command operations and maintenance organizations, NSA, and the Air Force Electronic Key Management program office. In this role, CTA worked with Government and contractor teams to define and document the Key Management Plan, the Key Management Theory of Operations, and the Key Management Concept of Operations.

CTA provided technical support and conducted security trade-off studies and analyses for Avionics and ground systems requirements and design-related areas. In this role, CTA assessed emerging security products and technologies against F/A-22 functional and security requirements, operational requirements, and constraints. Recommendations were made to the developers concerning capabilities and limitations of existing or developmental security products and systems. For example, CTA analyzed emerging trusted networking technology against stringent security criteria governing the operational flight program development and production process. Our recommendation to incorporate a specific high-assurance secure network server is now being implemented as part of the development system. CTA's recommended solution securely automates most of the functions and not only supports security requirements, but also supports the strict turnaround times required of Avionics developers and integrators.

CTA also performed security studies and analyses to support development, certification, and accreditation of the F/A-22 as an MLS weapon 'system of systems'. In this role, CTA assessed the needs and developed specifications for automated tools to support security data flow analysis in a complex distributed system characterized by the F/A-22. CTA produced the majority of the Software Development Plan in the areas of trusted software development requirements and provided trusted software development training for Avionics Integrated Product Teams (IPTs).

Under an associated F/A-22 System Security Engineering contract, CTA works directly with the F/A-22 Program Office and the Air Force Information Warfare Center to plan and implement the Weapon System Certification and Accreditation program in accordance with Air Force System Security Instruction (AFSSI) 5024. CTA develops Security Certification and Accreditation Plans (SCAPs), INFOSEC Policies, and is conducting Security Risk Analyses for F/A-22 ground support systems including the MSS and IMIS. These MLS systems are Unix-based client/server networks processing highly sensitive data with direct electronic interfaces to Unclassified systems and networks. They meet or exceed NCSCB2 criteria.

In a recently completed effort, CTA documented the Electronic Cryptographic Key Management Concept of Operations for the entire weapon system. This effort was especially challenging because of the weapon system's high degree of reliance on embedded and integrated cryptography to achieve many of its stringent security requirements. Lockheed chose CTA for this task because of our history of excellent performance and our in-depth knowledge of the weapon system's security architecture.

#### **BENEFITS TO CLIENT:**

The benefits to the customer were numerous, but chief among them was the certified MLS system and network that allows the cost-effective secure and controlled sharing of information of multiple classification levels on a single system or network serving users with varying clearance levels. This accomplishment was best described in a letter of commendation from Lockheed's manager of Software Infrastructure to Dr. Mike O'Neill, Director of CTA's INFOSEC group, in which he states (paraphrased) that: *"The Lockheed Martin.... Multi Level Secure (MLS) approach faced many program security challenges. The thoroughness and care CTA demonstrated in scrutinizing every detail of our MLS architecture enabled Lockheed to address all security vulnerabilities leading to approval of our MLS by the Defense Security Services...to my knowledge this is a 'first'."*

#### **EPILOGUE:**

In October, 2001, the Lockheed Martin JFS Team won the Joint Strike Fighter (JSF) System Development and Demonstration (SDD) program in a fly-off competition over the Boeing team. The JSF is a multi-service, multinational program to develop an all stealth capability as replacements for the Air Force's F-16, the Marine Corp's AV-8B, and the Navy's F/A-18E/F. A substantial portion of the Lockheed Martin JSF's security engineering technical support was subcontracted to CTA. The scope of CTA's tasking covers the entire weapon system, including the Air Vehicle and what is termed the Autonomic Logistics Systems (ALS), composed of the mission planning system, the Automated Logistics Information System (ALIS), and the Training System. The program is expected to extend over the next ten years.

*"We were awarded the JSF contract by Lockheed Martin based on our proven track record of on-time and within budget deliverables for over nine years on the F/A-22 program. Our experience on the F/A-22 will be extremely valuable to Lockheed in developing a secure, effective JSF weapon system that is accreditable under the most stringent military standards. This experience will also be invaluable in assuring the security of other mission critical applications. Water, electricity, gas, communications, commercial aviation and other critical services involve embedded computer controls and are managed by large distributed information networks (e.g., system control and data acquisition systems). The cyber threat to these systems is very real and our experience with embedded military systems provides us with unique experience in protecting these critical services."* Dr. Mike O'Neill, Director, CTA INFOSEC