

CTA INFORMATION SECURITY CASE STUDY:

SECURING FINANCIAL MANAGEMENT NETWORKS

CLIENT DESCRIPTION:

The Defense Finance and Accounting Service (DFAS) has management responsibility for the finance and accounting functions of United States Department of Defense organizations. In the course of fulfilling its mission, DFAS has embarked on a program of modernization to improve finance and accounting services for its customers and reduce costs by standardizing and improving procedures and systems, streamlining operations, and eliminating redundancies. Under the direction, authority and operational control of its Director, DFAS is responsible for the performance of the following major functions:

- Providing accounting and reporting services for all levels of DoD management for appropriated, non-appropriated, revolving, and trust funds; paying military members and collecting and disbursing DoD funds, including contract, vendor, security assistance, transportation and travel payments.
- Providing guidance and technical assistance to DoD financial networks around the world.
- Designing, developing, testing, implementing, operating, and maintaining financial systems.

CTA has a long-standing association with DFAS, starting in 1995 as one of its first security contractors. We have completed security risk management services for many DFAS applications and its Enterprise Local Area Network (ELAN). ELAN supports the government's mission of providing critical information communication services during times of peace and conflict. The ELAN provides storage, processing, and communications services to authorized users and the general public.

CTA SECURITY ENGINEERING PROJECT DESCRIPTION:

CTA was tasked to provide a full range of network security assessment and engineering services to help the government determine if the ELAN had sufficient security to meet its mission and if the ELAN complied with the rigorous DoD security Certification and Accreditation requirements.

In our support of this task, we were charged to :

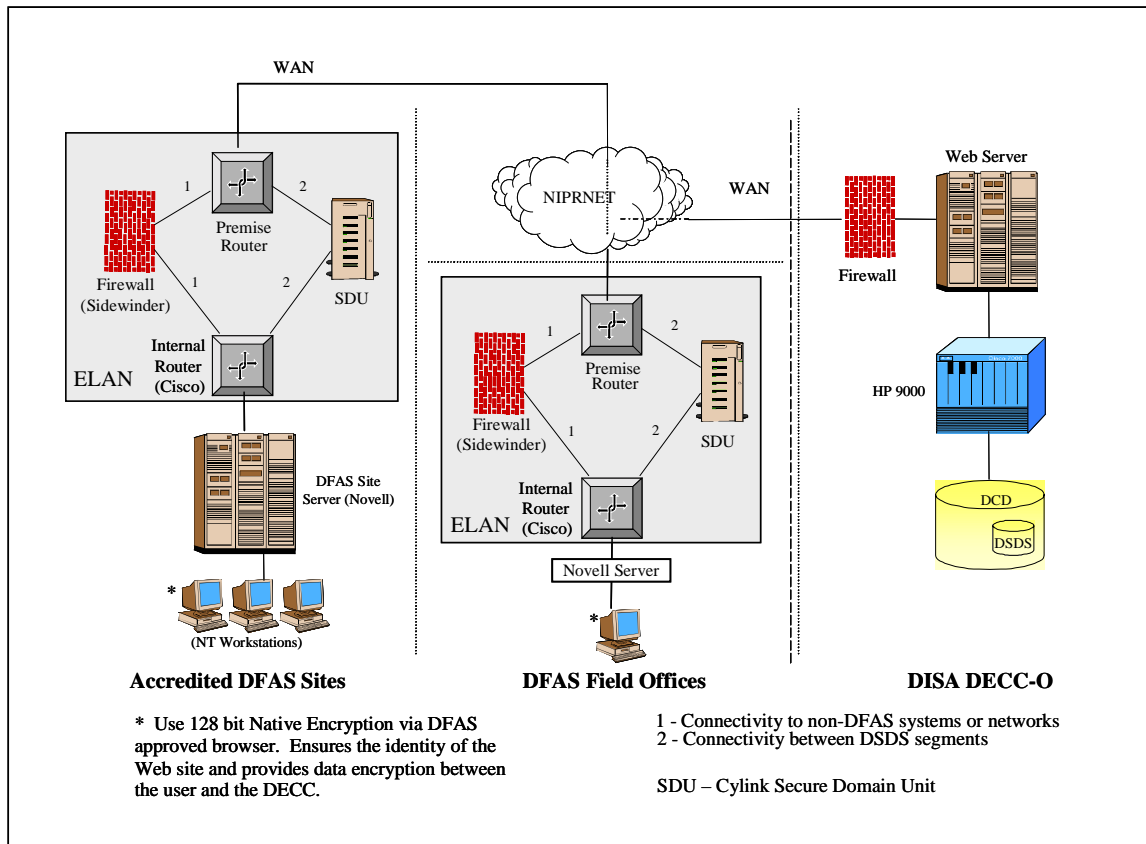
- Identify security weaknesses in management, operational, and technical controls;
- Report and provide an objective, independent risk analysis of each weakness against projected threat profiles;
- Validate that the weakness was a vulnerability that required remediation and assisted in developing risk mitigation strategies;
- Post remediation, validated that the risk was indeed eliminated or mitigated.

SYSTEM ARCHITECTURE:

The Enterprise Local Area Network (ELAN) is an agency-wide collection of geographically dispersed but interconnected segments¹. ELAN Segments are located at Headquarters, and over twenty-three Operating Locations (OPLOCs). ELAN Segments are interconnected by means of the Sensitive but Unclassified Internet Protocol Router Network (NIPRNET). The NIPRNET is an untrusted IP/TCP network operated by the Defense Information Systems Agency (DISA). The ELAN provides several user services including office automation, E-mail, and connectivity between DFAS users and Defense Megacenters (DMC). The ELAN is a heterogenous network of over 15,000 nodes that include Microsoft Windows workstations, NetWare 4.11 servers, NT servers, and HP-UX servers as well as Cisco 7000 series

¹ Segment - A section of a network that is bounded by bridges, routers, or switches.

routers, Cisco switches, Cabletron, and Bay Networks hubs and switches. With over 400 NetWare 4.11 servers the ELAN is one of the largest NetWare networks in the world. The figure below provides a high level view of the security implemented.



PROJECT APPROACH:

We started the process by collecting data and identifying the components and the boundaries of the ELAN network. (No matter what the size of the assessment, we need to bound the network and find out what is important to the client.) Data collection generally includes an intense information exchange with the client's IT staff.

We used the technical assessments to discover component vulnerabilities and assess component technical security. The technical security assessment included internal and external scans to identify components running unauthorized services; internal and external scans and probes of TCP and UDP ports; tests to identify SNMP weaknesses; and penetration tests to identify security vulnerabilities in network components and servers such as routers, UNIX hosts, NetWare hosts, WWW servers, FTP servers, and hubs and switches. We also conducted tests of ELAN's network intrusion detection capability and checks and tests to determine how the government's security policy was applied and security policy weaknesses in network components and servers.

We performed 10 on-site security assessments to identify vulnerabilities in the network's support structure. The environment that surrounds the network also has protective mechanisms. Physical, procedural, and administrative security mechanisms like back-up power, door locks, badge systems, policies, operational procedures, location, trusted users, etc., are all examples of security mechanisms present in the network's environment. Although the component and environment offer security mechanisms to protect information, the protection is not absolute — both can have weaknesses.

Unauthorized individuals use the weaknesses to gain access to critical or sensitive information stored, processed, or transmitted by the network. An authorized user may exploit a weakness to misuse the network. The security mechanisms that protect the network can fail, be improperly configured, or not be implemented at all. The site security assessments included assessment of network management controls such as network risk management and security policy. We assessed network operational controls such as Security Training and Awareness, vulnerability and incident reporting, network support and operations, contingency and disaster planning, and physical and environmental controls.

Data analysis and reporting were the final task. We pulled together information from the site assessment and technical assessment as well as threat information. We analyzed information and determined the risks to the network. We provided recommendations on how to mitigate the risks. We prepared an accreditation support package that presented a full assessment of the ELAN's security posture.

BENEFITS TO CLIENT:

The customer has benefitted from this project in a number of very significant ways:

- The customer has a heightened understanding of threats and risks to their network (the threat that in a future--or present--crisis, a criminal cartel, terrorist group, or hostile nation could seek to inflict economic damage by attacking its critical networks);
- The customer has gained an appreciation of some serious vulnerabilities that could be exploited by such outsiders and malicious insiders;
- The customer has established a risk management approach to protect his critical assets while maintaining the level of service and operational efficiencies afforded by the network with the use of countermeasures CTA identified for them; and
- The customer now has the ability to more effectively monitor their network for penetration attempts by insiders and outsiders and, most importantly, react as necessary to security incidents assuring critical services are not disrupted.