

Infrastructure **Secure Access Control**



Establishing Identity and Managing Information Access

Individual privilege

Technology evaluation

Standards-based

Strong authentication

Trusted labeling

Human/machine readable

Overview

The changing nature of information network access has meant a need for evolution in Secure Access Control. Information networks started with computers sitting on employee's desks, then the computers were networked and passwords were implemented. Along came remote access, so hardware was added at the network entry points to control connectivity. Eventually the network was connected to the internet, and who was really behind the IP address became a difficult question to answer.

One of the keys to determining individual privileges for information and services access is establishing the identity of the individual requesting access. In addition to the identity, there is also a need to determine what information the individual is cleared to access. This is a complicated problem in the military and intelligence communities because access privileges are based on an individual's security clearance, as well as the multiple roles and group (community of interest) memberships this individual may require. Complicating the problem even further is the need for information access across organizational boundaries requiring electronic identification by other than just the home organization.

Secure Access Control

To begin to achieve the desired level of access control, two technologies must be integrated into the information network: first, strong authentication; second, trusted data marking and labeling. Implementing one without the other will not achieve the secure access control needed in today's dynamic information environment.

Approach

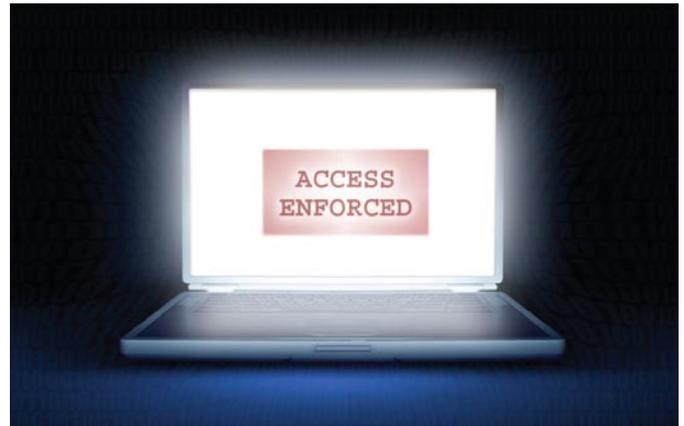
The General Dynamics approach to Secure Access Control is to leverage our experience in Information Assurance to develop systems that not only protect the information but also enable access for everyone needing it — but only those needing it. Our experience has shown that there is no silver bullet and each customer system requires some tailoring to fit within the technical and operational constraints of the organization. We also understand that creating custom solutions for every problem is expensive, time-consuming and counter-productive in a standards-driven world.

To reduce the time and expense to customize and implement solutions for customers, General Dynamics has created a High Assurance lab to integrate and evaluate technology available from vendors around the country. General Dynamics is also active in working with the government in developing standards-based information assurance architectures for implementation on the Global Information Grid. The combination of technology evaluation, participation in working groups and our legacy of delivering integrated systems results in solutions that meet customer requirements for access and information assurance.

Strong Authentication

The most secure access control processes start with multi-factor authentication. The paradigm of what you have, what you know and who you are is nearly impossible to covertly defeat when implemented correctly. However, it is not always necessary given other access control mechanisms, operational environments or security risks. Designing systems that are flexible enough to scale with security risks is a specialty at General Dynamics. We apply technology based on customer business practices and operational procedures, quantify the risks associated with the security implementation options and integrate the final solution.

Our lab is actively investigating standards used to cross var-



ious DoD and government agencies and their relationships to strong access control. We are also combining this with our background in public key infrastructure and cryptography to provide systems that can be scaled and accredited for military and intelligence applications.

Managing and monitoring access is also an integral part of our solutions. We have developed approaches and tools for network management that include multi-domain network management from a single network operations center. These tools are focused on keeping the network and its managed elements and services available, as well as reducing the effort required to maintain the system.

Trusted Labeling

Strong authentication does no good without the underlying technology of trusted labeling. Validating the individual's identity and privileges would be useless if information is not stored by a system which can maintain machine actionable and human readable labels. The labels are used by the system to both provide and prevent user access to data. Because the labels are key to protecting the underlying information, their integrity and authenticity must be protected. The labels also must be irrevocably tied to the data they represent. This insures that the labels and data are tied together as they pass through the information system.

At General Dynamics we are defining and integrating data labeling into operational systems based on defined standards being developed for use across the military and intelligence agencies.

GENERAL DYNAMICS C4 Systems

8220 East Roosevelt Street, M/D R7229 • Scottsdale, Arizona 85257 • Website: www.gdc4s.com/sac
Phone: 480-441-5448 • Toll-free: 866-400-0195 • Email: IASystems@gdc4s.com