WHITE PAPER • JANUARY 2018

ca technologies

Rapidly Deploy Applications in Cross-Domain Environments

CA API Gateway enables new programs to transfer information between security domains through legacy high-assurance guards

Table of Contents

Executive Summary

Challenge

Organizations face difficult challenges when operating computer systems in multiple security domains. Among the most problematic is adding new applications that must communicate across domain boundaries.

The Unified Cross-Domain Management Office has approved only a limited number of high-assurance guards to allow one way information flow from an unclassified to a classified domain. They have approved even fewer that permit information to flow in both directions.

The approved guards have undergone a stringent technical evaluation to earn a certification for a specific communications protocol and security policy. The certification process is expensive, but the time required for certification is more important. No amount of increased funding can reduce the approval cycle. If an organization must add an application with a new protocol, it must restart the guard's multi-year certification process.

Solution

CA Technologies has developed an innovative answer to this problem using CA API Gateway. Since high-assurance guards are limited by protocol and security policy, CA API Gateway transforms information from new applications to the protocol certified for use with the guard. In simple terms, the gateway acts as a universal translator. One gateway is placed with the guard in the low-side domain and a second gateway is placed in the high-side.

The new application communicates with the CA API Gateway using its native protocols. CA API Gateway implements a security policy, transforms the protocols and sends information to the guard in the format the guard was certified to accept. After the guard implements its security policy, the guard transfers the information through the security boundary.

In the second security domain, another CA API Gateway receives the incoming information from the guard and transforms it back to its original format. The new application's counterpart operating in the second domain receives the information as if it had not traversed a cross-domain boundary.

With this solution in mind, CA Technologies gained Common Criteria certification for CA API Gateway on May 30, 2014 and renewed our certification October of 2017. The certification authorizes the transformation of protocols, including XML and TADL, into those approved for use by guards.

Intelligence community members and Department of Defense (DOD) organizations are using CA API Gateway today to transform advanced Web and legacy protocols.

CA API Gateway is a fully certified solution
to rapidly expand cross-domain information flow

SECTION – 1

High-Assurance Guards: Theory and Operation

High-assurance guards enable information to transfer between different security domains such as unclassified, secret and top secret. The military and intelligence communities use the security domains to differentiate protection levels for specific types of information and operations; however, few operations actually occur in only one domain. For example, mission planning for an army unit move, which is done in the secret domain, may require weather information, which is created in the unclassified domain. In another case, deconflicting military aircraft flights from civilian flights may require sending unclassified information from the secret domain to the unclassified domain. To deal with the transfer of information from one security domain to another, the Unified Cross-Domain Management Office has approved high-assurance guards from a limited number of manufacturers. These guards inspect and impose a security policy on information before permitting the transfer from one domain to another.

High-assurance guards are built on a trusted operating system, which provides access control to the elements of the underlying computer including the central processing unit, memory storage, program libraries and input/output devices. The security kernel, within the trusted operating system, validates both the classification of information handled and the authorization of the system requesting that information are appropriate. The trusted operating system appears simultaneously in both the lower security domain and the higher domain networks. It acts as a security wall to make certain only the proper elements of the computer are exposed to either one of the domains.

The software running on the trusted operating system applies a security policy to information attempting to transfer between the two domains. It first decrypts any encrypted information and examines the contents for malware. It then enforces Mandatory Access Control, which confirms the person or system requesting information has the proper privileges to do so. The software examines information contained in the data flow to make certain it is at the appropriate classification level. It inspects security labels, words and phrases then blocks those that violate the security policy. While executing these security processes, the software audits everything that occurs.

A high-assurance guard gains the authority to transfer information between two security domains after successfully completing a certification process. The guiding regulations have changed from the Department of Defense Trusted Computer System Evaluation Criteria (Orange Book) to the National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11). The latter requirements are tested by labs accredited under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme. Only guards that meet NSTISSP-11 requirements gain a Common Criteria certificate.

The Common Criteria evaluation is typically an iterative process where the lab finds a problem, the company repairs it and testing starts again from the beginning. The Common Criteria certification identifies the guard and the approved protocol set. If the owner of the guard needs to process a new protocol or support a new application, the guard must enter the certification process again. As with the initial validation, the re-evaluation process can take up to two years..

SECTION – 2

CA API Gateway: Adding Value to High-Assurance Guards

CA Technologies has developed a unique approach to the problem of rapidly adding new applications to a cross-domain solution. Instead of modifying a Common Criteria certified guard to accept a new or different protocol, CA Technologies uses CA API Gateway to transform the new protocols into the format the guard was certified to process. After the high-assurance guard passes the information through the security boundary, a second CA API Gateway transforms the data stream back to its original form.

SECTION – 3

CA API Gateway: Theory and Operation

Web-based industries faced a problem as they implemented Net-Centric technologies. Service-oriented architecture (SOA) protocols degraded the performance of traditional firewalls. New standards such as Extensible Markup Language (XML) and Web services dramatically slowed network performance. CA Technologies created the CA API Gateway for the civilian market to relieve this network stress and enforce compliance for the emerging traffic types.

CA Technologies optimizes information flow through the gateway with advanced stream processor logic. The gateway comes as either a stand-alone hardware device or as a software engine that runs in a virtual machine. The stand-alone device provides additional hardware-based XML acceleration. In both cases the gateway employs a trusted operating system identical to those used in high-assurance guards.

CA API Gateway enforces security policies on Net-centric technologies and protocols including:

- Simple Object Access Protocol (SOAP)
- Web Services Description Language (WSDL)
- Web Services Security (WS-Security)
- XML Encryption (XML-Enc),
- XML Digital Signature (XMLDSig)
- Security Assertion Markup Language (SAML)
- Web Services (UDDI, SOAP, and WSDL)
- Representational State Transfer (REST)
- Asynchronous JavaScript + XML (AJAX)
- Military protocols including Tactical Digital Information Links (TADIL).

The CA API Gateway security policy enforces protocol compliance with the published standards to prevent buffer-overflow and other types of cyber-attacks. It also evaluates Net-centric messaging and ensures interoperability of service-oriented capabilities.

CA API Gateway implements fine-grained access control including Policy Based Access Control (PBAC) and Attribute Based Access Control (ABAC). Under these models, the gateway performs as a Policy Enforcement Point (PEP) that proxies and inspects every message destined for and/or returned from a gateway-protected service. The policy enforcement decisions are created by the user and can incorporate any combination of user identity, authentication protocol, client device identity, time-of-day, IP address, message count, message content and routing parameters.

CA Technologies gained Common Criteria certification for CA API Gateway on May 30, 2014 and renewed our certification October of 2017. The report certified the gateway successfully enforces security policies including:

- XML Encryption (XML-Enc),
- XML Digital Signature (XMLDSig)
- Security Assertion Markup Language (SAML)
- Web Services (UDDI, SOAP, and WSDL)
- Representational State Transfer (REST)
- Asynchronous JavaScript + XM

As a result of the Common Criteria certification, government organizations have begun using CA API Gateway to augment high-assurance guards and pass Web-centric and legacy application information.

SECTION 4

Conclusion

The capabilities of CA API Gateway complement those provided by certified high-assurance guards. These guards cannot implement a security policy on unsupported services or process unapproved protocols. With CA API Gateway, organizations can impose security policies and transform the protocols used by new applications. Its Common Criteria certification enables agencies to solve their limitations in adopting new programs with a low-risk solution. As a result, organizations have begun deploying CA API Gateway to rapidly implement XML-based services and unique protocols across security domain boundaries.

For more information, please visit **ca.com**

Connect with CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments.
Learn more at **ca.com**.

ca technologies

CS200-332992_0118