Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

Introduction to Cross Domain Solutions

APRIL 2019

Introduction

This document introduces technical and non-technical audiences to the concept of Cross Domain Solutions (CDS), a type of security capability that is used to connect discrete systems within separate 'security domains' in an assured manner.

Security domains explained

A security domain is a system (or collection of systems) operating under a consistent security policy that defines the security classification, releasability and special handling caveats for information stored and processed within the domain.

For example, an organisation's OFFICIAL and SECRET networks are separate security domains; as are the SECRET networks of two different organisations; as are the SECRET AUSTEO and SECRET REL networks of a single organisation.

Cross Domain Solutions explained

CDS are systems comprising security-enforcing functions tailored to mitigate the specific security risks of accessing or transferring information between security domains. A CDS may be an integrated appliance or, more commonly, be composed of discrete technologies or sub-systems, with each sub-system consisting of hardware and/or software components.

Secure CDS implementations ensure that the security policy of each security domain involved is upheld in a robust and highly assured manner, across all physical and logical layers of the connection between domains. To achieve this, the use of certified High Assurance products and evaluated components is strongly encouraged where appropriate.

Example use cases for a CDS include ingesting publicly available data from an OFFICIAL network into a SECRET classified analysis system; consolidating the presentation of differently-classified desktop systems into a single client; or aggregating input from multiple differently-classified environments into a central audit system.

CDS security threats and risks

Understanding the security risks specific to each cross domain use case is essential, as to be secure a CDS must address an organisation's specific business requirements and risk environment. Any approved or accredited solution is likely to require modification to be suitable for use in another organisation or risk environment.

When CDS security controls are inadequately enforced, connections between different security domains may allow an adversary to:

- gain unauthorised access to steal, copy or interfere with sensitive information
- establish covert channels into or out of sensitive systems
- compromise the integrity of trusted systems or data (such as audit logs)
- bypass security-enforcing functions
- interrupt the availability of critical systems or services, or
- propagate to access sensitive systems by pivoting through less-protected networks.

CDS security design principles

A CDS prevents the flow of information between different security domains by default. A CDS will only permit selected information to pass security enforcement points where appropriate, based on conformance of all data to a security policy. Security-enforcing functions may be implemented by discrete hardware or software components, and a CDS architecture must ensure that these security-enforcing components are unable to be bypassed. Examples of security-enforcing components include data diodes, protocol adaptors and content filters.

CDS are typically designed to mitigate threats to the more sensitive or trusted security domain (the ‘high side’ of the connection) originating from the less sensitive or trusted security domain (the ‘low side’). However, it is important to consider that certain threats may be introduced by the more sensitive or trusted security domains.

To uphold the effectiveness of a CDS, each security domain connected by a CDS must also implement appropriate security controls to protect its core systems and boundary connections.

CDS security risk management

Organisations should perform an analysis of the potential security, financial and sustainment risks before considering a CDS in their environment. While in order to gain assurance in the effectiveness of security-enforcing functions performed by a CDS, systematic risk-based analysis and thorough technical assessments are strongly recommended.

Some organisations house delegated CDS advisory bodies to provide tailored security advice and assistance. CDS projects should engage with their organisation’s security teams and any CDS advisory bodies early and often to ensure that security risks are comprehensively understood and managed. In addition, the Australian Signals Directorate’s Australian Cyber Security Centre (ACSC) provides advice and assistance to those seeking further guidance on the threats to security-relevant components of a CDS or the strength of security-relevant components.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations’ systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

The ***Guide to the Secure Configuration of Cross Domain Solutions*** (GSCC) publication offers detailed guidance on CDS security controls from a technical perspective. This document is available on request from the ACSC.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).