



COA¹ Service

Trust Management - Control Stratification

Introduction

Information must be classified using an appropriate Classification Scheme as defined in the Jericho Forum's Information Classification² position paper. The classification of information will define associated information protection requirements in terms of restricting the circulation of information based on identity, legality, and temporal components. Confidentiality, Integrity, Availability and Authenticity (CIA&A) must also be considered for information created within organisations. Thus, information must be categorized to reflect the level of business impact that would occur if any of these requirements were not correctly enforced, as defined in the Jericho Forum's Impact Sensitivity Categorization³ position paper.

Information Classification and Impact Sensitivity Categorization drive control requirements to ensure the protection of information in de-perimeterised environments. As well as controlling the creation, handling, transfer and deletion of information as defined using Impact Sensitivity Categorization, it is also essential to establish a level of trust in the identity of entities that access and handle information, and even the controls that provide this protection. Control Stratification enables trust in an identity to different levels based on the level of authentication given by an entity.

The Problem

In a de-perimeterised environment, Information Classification should define the domain in which information is allowed to be circulated, for example, internal organisation or inter-organisational collaboration groups. Impact Sensitivity Categorization of information should mandate controls to be enforced that protect the information protection requirements in terms of Confidentiality, Integrity, Availability and Authenticity, during the information lifecycle within the specified domains. For example, if information classified as amber is sent outside of the specified shared domain, the controls should prevent the information from moving. Likewise, if the endpoint location of shared information is within the domain but the location is not backed up or mirrored, the information should be prevented from moving if there is a high impact requirement for availability.

A third consideration in the Jericho Forum Trust Management model is Control Stratification. This extends the considerations of Information Classification and Impact Sensitivity Categorization to include the identity assurance of an entity accessing or handling the information as part of operational process. For example, information with specific classification and impact sensitivity categorization labels must only be accessed by entities given clearance to access such information classified with that label and to perform actions

¹ The Collaboration Oriented Architectures (COA) paper and associated COA Framework paper are available at <http://www.opengroup.org/jericho/publications.htm>

² Information Classification paper – available at <http://www.opengroup.org/jericho/publications.htm>

³ Impact Sensitivity Categorization paper – available at <http://www.opengroup.org/jericho/publications.htm>

that maintain the required levels of CIA&A assurance. The higher the impact sensitivity, the more important it is that the entity requesting access can prove to be who they say they are (authentication), and the higher the requirement for the authentication result to be trusted. For low level information, a simple user name and password may suffice. For high level information, two-factor authentication with the addition of a secure token may be necessary. For the highest level impact sensitivity, biometrics may be required.

Why Should I Care?

The entities responsible for accessing and handling information are responsible for its protection and survival throughout its lifetime. If it has been decided that information is sensitive enough to classify then it must be ensured that the classification is recognised when allowing access to entities who intend to handle, store, transfer and delete information within an organisation and externally, in collaborative, de-p environments.

The identity of entities responsible for information must be trusted to a level based on the level of business impact they can threaten while in this position of responsibility. Categorising trust in identity can allow you to distinguish between trusted and distrusted entities for any given piece of information by mapping the assured trust level provided by the entity to the level of business impact defined by Information Classification and Impact Sensitivity Categorization.

Recommended Solution

The requirement here is to develop a common language (taxonomy) and set of trust levels in the identity of entities accessing and handling information. A set of standardised Identity Trust Levels should be defined, using the standard CIA&A frame and adding identity. We define 6-level trust taxonomy for authenticity as follows:

C5: ASSURED (biometric)

C4: AFFIRMED (positive physical or logical authentication)

C3: PROVEN (authenticated by trusted third party)

C2: CONFIRMED (confirmed by strong attributes)

C1: ASSERTED (self-asserted)

C0: UNKNOWN (no authenticity assertions made - anonymous)

Background and Rationale

It is essential when considering the CIA&A requirements of information that the identity of an entity attempting to access and handle the information can be assured to specified, standardised levels to ensure its identity can be trusted to fulfil the defined CIA&A requirements of that particular piece of information. Identity does not only refer to people, it can include devices, systems, network and environments.

For example, the fire alarm system within a building handles critical information when the signal is sent to sound the alarm in the event of fire. Thus, the information transferred to the fire alarm has a catastrophic impact sensitivity value in terms of availability. The entities accessing and handling information in this case are the cable that carries the signal to the fire alarm, and the endpoint that sends the signal. Identity assurance through Control Stratification must mandate the assurances required from the entities. The information is classified as critical; therefore the identity of entities accessing and handling the information must be at least “Affirmed” to be able to handle this level of information. The identity of the cable must be trusted to carry the signal. To guarantee this this, it must be physically affirmed

to be tamper-evident, availability monitored and fireproof. The endpoint that sends the signal must be affirmed as being backed up, mirrored and tamper-evident so that it can be trusted to maintain connection to the fire alarm at all times, especially in the event of emergency when buildings may be damaged or on fire.

If identity assurances cannot be given to this extent, the information must not be accessed or handled using these entities as it means placing the information in an insecure environment in terms of CIA&A. Not all entities need identify themselves to this extent, only those accessing and handling information classified at the highest levels.

Challenges to Industry

Consideration of the identity of entities accessing and handling information to this level is essential to maintaining trust in the environment in which information lives out its lifecycle. Even more so in environments that are de-perimeterised and in which organisations do not always maintain control over the actions and configuration of entities that access and handle their information.

It is important to consider the implications of the assurances offered (or not offered) by entities outside of an organisation's immediate control.