Understanding the Extended CIA Model

Revision

Version 7
4/22/24 2:38 PM

Author

Charles Wilson

Abstract

This document provides an overview of the extended CIA model called out in the **UN R155** background material.

Motivation

This document is motivated by the need to ensure a proper understanding of the basis of the cybersecurity properties used within the AVCDL's cybersecurity requirements taxonomy.

Audience

The audience of this document are those cybersecurity SMEs tasked with creating base or tailored cybersecurity requirements, and those performing threat modeling activities.

Note: This document is not subject to certification body review.

License

Overview

One of the core elements of the **AVCDL** [1] is a taxonomy for cybersecurity requirements [2]. This taxonomy is used to identify areas where cybersecurity controls should be applied, and informs what those controls should be. These controls are documented in a global cybersecurity requirements catalog [3] which is then tailored to each element of the system. These requirements have distinct impact on all later activities within the cybersecurity development lifecycle. Two of the dimensions of the taxonomy (layer and asset) are motivated within the taxonomy document itself. The cybersecurity properties set comes from the **UN R155** background [4] material and lacks proper motivation.

Formal Definitions

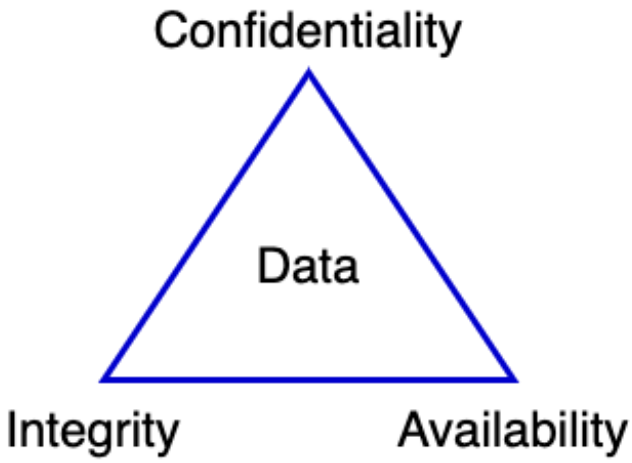
The formal definitions for the extended CIA model's properties are as follows:

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	The property that data has not been altered or destroyed in an unauthorized manner.
Availability	The property of being accessible and useable upon demand by an authorized entity.
Authorization	The granting of rights, which includes the granting of access based on access rights.
Authentication	The corroboration that a peer entity in an association is the one claimed.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Accountability	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

The remainder of this document will detail the development of the CIA and extended CIA models.

CIA Model

The **CIA model** is a long-accepted set of cybersecurity properties. These properties (confidentiality, integrity, and availability) are used to establish various guarantees regarding the data they are applied to. The following diagram is a typical visualization of these properties.



Foundation

Like many long-accepted concepts, the specific origins of this model are difficult to establish. Some sources [5] attribute the CIA's origin to a paper by Saltzer and Schroeder [6] from 1975. This paper does not speak specifically to the CIA as a model. Earlier works by Conway, Maxwell, and Morgan [7] (1971); Ware [8] (1967); Baran [9] (1964); all discuss to data confidentiality and integrity (typically without using those terms). Even **The Orange Book** [10] (1983) makes no direct mention, which is especially odd given its relative modernity. Nor is the CIA model referenced in **NIST SP 800-33** [11] (2001) which specifically covers the technical models for security. The oldest sources found in the creation of this document referencing the CIA model are Microsoft's SDL book [12] (2006) which mentions the CIA as a taxonomy in comparison to STRIDE; and the definitions of the three properties in the US Federal Register [13] (2002).

Fundamentally Necessary Properties

From all identified historic sources, it is clear that the properties of confidentiality and integrity are expressly desired. The property of availability is implicit in early sources. Together these form a minimal necessary set of cybersecurity properties as applied to data.

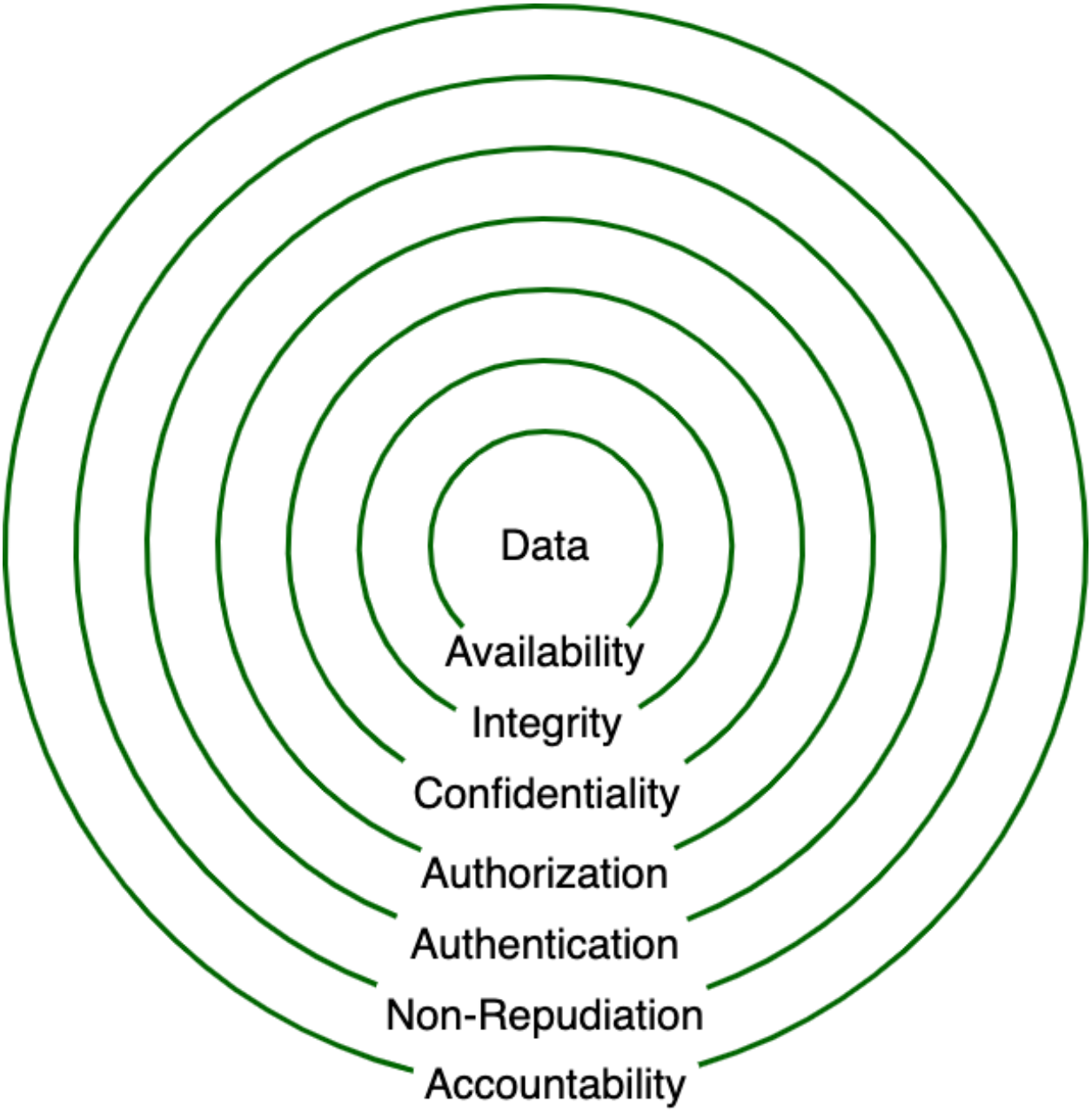
Necessary But Not Sufficient

Since it came into common use, people have been asserting that the CIA model was deficient. Some of those assertions have come with proposals for alternative models. Some proposals include Parker [14] (2002); Jurjens [18] (2005); Firesmith [19] (2004); Calderón and Marta [21] (2007); Mead and Hough [20] (2005); and Yu [17] (2019). The reason for the concern is that the CIA model didn't sufficiently provide underpinnings for the cybersecurity requirements (mitigations) that were found necessary to ensure cybersecurity sufficiency.

Extended CIA Model

The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) bases their cybersecurity threat mitigations on what they term the extended CIA model. The model's elements are enumerated in the abovementioned WP.29 background material. Its use is also evidenced in a worksheet [16] showing the approach used to relate the extended CIA to mitigations.

The following is diagram visualizes how the additional cybersecurity properties extend the CIA model.



In the above diagram, the base CIA model is shown protecting the data. Surrounding this are four additional cybersecurity properties:

- Authorization
- Authentication
- Non-repudiation
- Accountability

These are presented as concentric circles surrounding the base model. The reason for this is that the four additional cybersecurity properties relate to controls applied to data movement and not to the data itself.

Note: Not all systems require application of all these properties (base or extended).

Note: In deeply embedded systems, authentication implies authorization, as there exists only a single level of privilege.

ISO/IEC-7498-2, **Information technology – Open Systems Interconnection - Basic Reference Model — Part 2: Security Architecture** [22] provides the basis for the extended CIA.

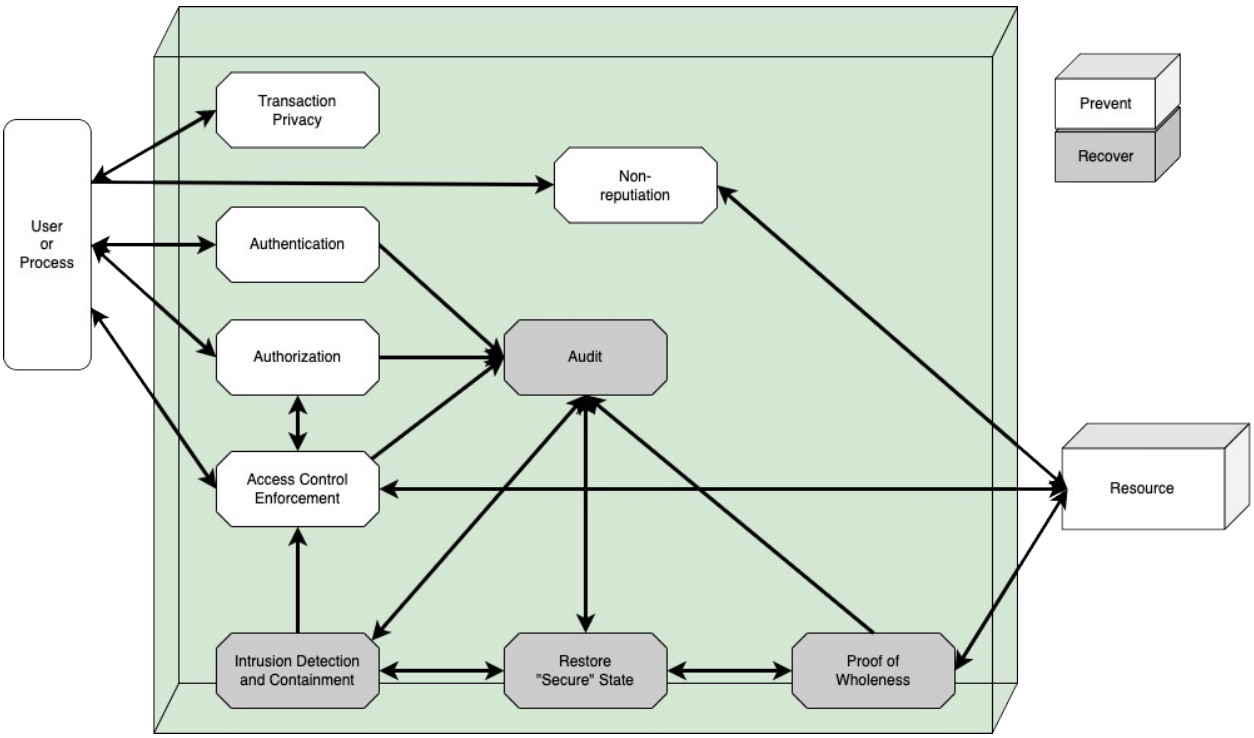
Note: ISO/IEC-7498-2 is also released as ITU TR X-800, **Security Architecture for Open Systems Interconnection for CCITT Applications** [23]**.**

Within these documents, a set of five security services are discussed. These are:

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation

They also discuss the optional need for audit capability. Finally, availability is discussed as necessary in order to consider protection against denial of service.

NIST SP 800-33, **Underlying Technical Models for Information Technology Security**, expands upon the OSI material. The following diagram shows their security services model.



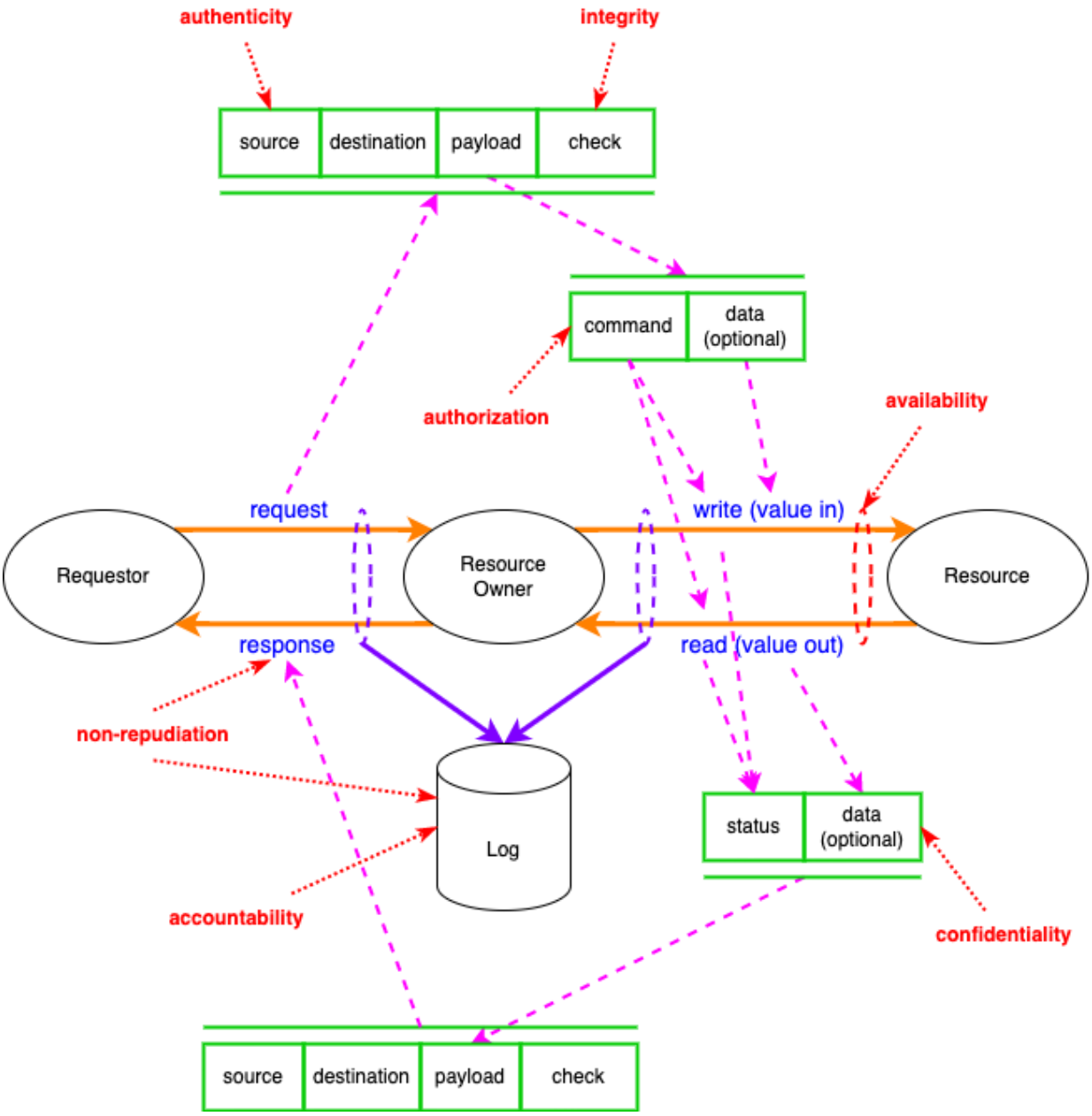
Here we can see the four additional cybersecurity properties used in the extended CIA model. Access control has become authentication, which better aligns with the other property names.

Minimally Sufficient Properties

The combination of the three base properties (confidentiality, integrity, and availability) and the extended properties (authorization, authentication, non-repudiation, and audit) allows us to establish requirements upon both the data and the mechanism of access. This minimal set of cybersecurity properties is sufficient to allow us to cover all mitigation types in an unambiguous manner.

Extended CIA Model Visualized

The following diagram (taken from the **Security Requirements Taxonomy** secondary document). It shows how the extended CIA relates to the archetypical data flow sequence.



References

1. **AVCDL** (primary document)
2. **Security Requirements Taxonomy** (**AVCDL** secondary document)
3. **Global Security Requirements** (**AVCDL** secondary document)
4. **ECE/TRANS/WP.29/GRVA/2019/2 Proposal for a Recommendation on Cyber Security**
   https://unece.org/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf
5. **A Vulnerable System: The History of Information Security in the Computer Age**
   https://www.amazon.com/dp/1501758942
6. **The Protection of Information in Computer Systems**
   http://cs.uccs.edu/~cs691/designPrinciples/ProtectionOfInformationInComputerSystems1975.pdf
7. **On the implementation of security measures in information systems**
   https://ecommons.cornell.edu/bitstream/handle/1813/5964/71-120.pdf
8. **Security and Privacy in Computer Systems**
   https://www.rand.org/content/dam/rand/pubs/papers/2005/P3544.pdf
9. **On Distributed Communication: IX. Security, Secrecy, and Tamper-free considerations**
   https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3765.pdf
10. **Department of Defense Trusted Computer System Evaluation Criteria**
    https://upload.wikimedia.org/wikipedia/commons/4/4f/Trusted_Computer_System_Evaluation_Criteria_CSC-STD-001-83.pdf
11. **NIST SP 800-33** - **Underlying Technical Models for Information Technology Security**
    https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-33.pdf
12. **The Security Development Lifecycle**
    https://www.amazon.com/dp/0735622140
13. **44 U.S.C. section 3542. Definitions**
    https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf
14. **Our Excessively Simplistic Information Security Model and How to Fix It**
    https://www.bluetoad.com/publication/?m=1336&i=41813&p=12&ver=html5
15. **Organizational effects and management of information security**
    https://www.diva-portal.org/smash/get/diva2:1148330/FULLTEXT01.pdf
16. **(OICA-CLEPA) Table on CS threats - ext CIA approach + mitigations**
    https://wiki.unece.org/download/attachments/44269826/TFCS-06-10%20%28OICA-CLEPA%29%20Table%20on%20CS%20threats%20-%20ext%20CIA%20approach%20%2B%20mitigations.xlsx?api=v2
17. **Distributed Immutable Ephemeral - New Paradigms for the Next Era of Security**
    https://www.slideshare.net/sounilyu/distributed-immutable-ephemeral-new-paradigms-for-the-next-era-of-security
18. **Secure Systems Development with UML**
    https://www.amazon.com/dp/3540007016
19. **Specifying Reusable Security Requirements**
    https://www.jot.fm/issues/issue_2004_01/column6.pdf

20. **Security Quality Requirements Engineering (SQUARE) Methodology**
https://resources.sei.cmu.edu/asset_files/technicalreport/2005_005_001_14594.pdf
21. **A Taxonomy of Software Security Requirements**
https://repositorio.unal.edu.co/handle/unal/24281
22. **ISO/IEC-7498-2, Information technology – Open Systems Interconnection - Basic Reference Model — Part 2: Security Architecture**
https://www.iso.org/standard/14256.html
23. **ITU TR X-800, Security Architecture for Open Systems Interconnection for CCITT Applications**
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-E&type=items