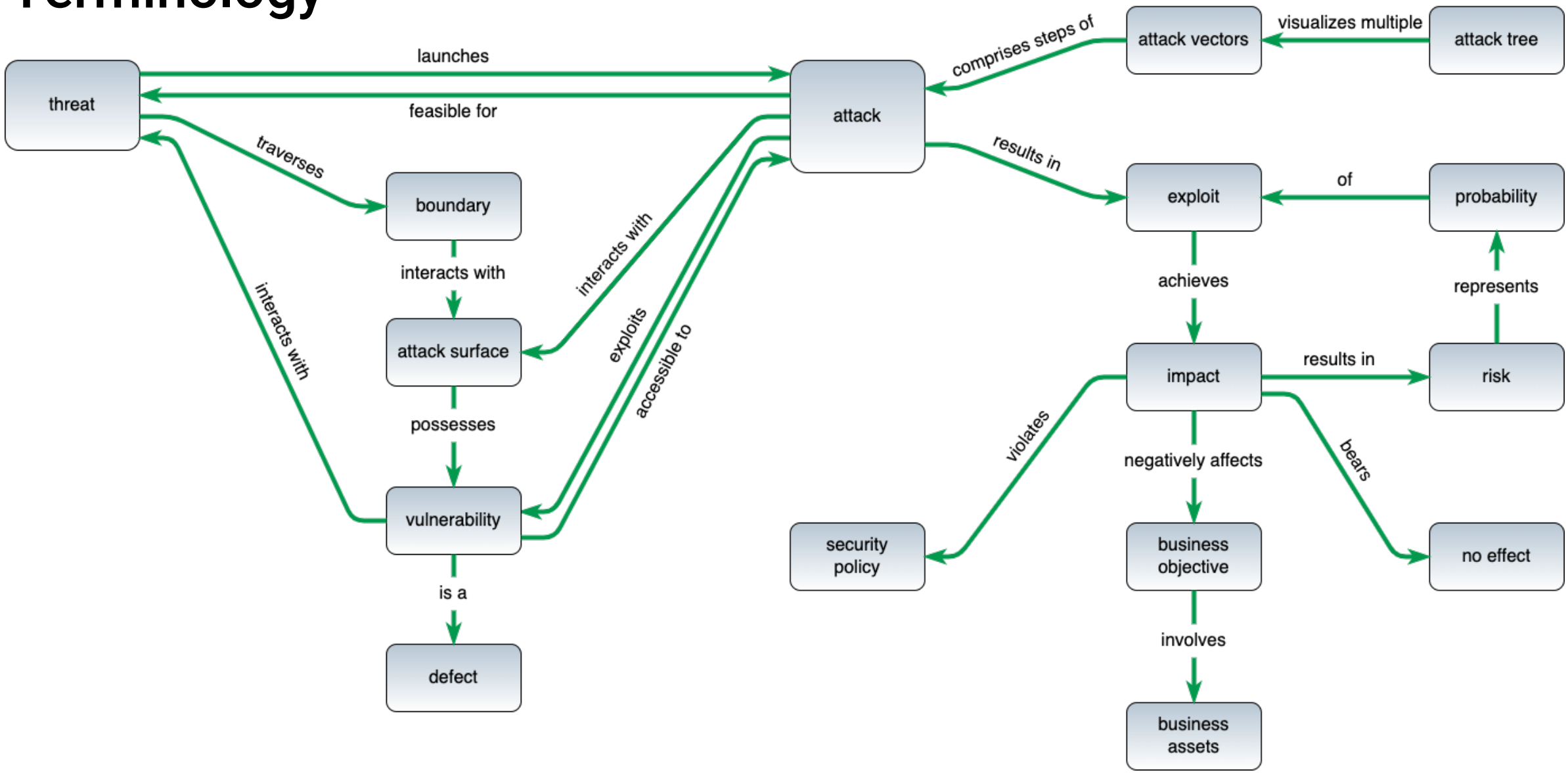
Cybersecurity Requirements Taxonomy-based Threat Modeling

Charles Wilson
Technical Fellow, Cybersecurity Engineering

version 6
2024-04-11

Introduction

Terminology *



* based on threat modeling glossary diagram by Steven and Migues (link in references)

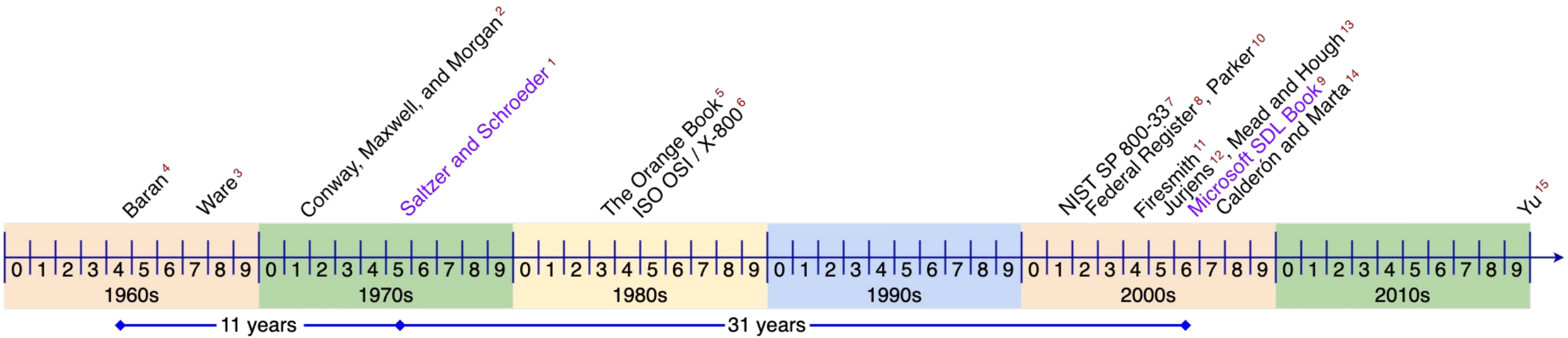
Assets

Asset Classes

Asset	State	Description
Executables	at rest	binary data which may be run on the system
Configuration Data		data used to establish the personality of the system
Databases		data in a structured format typically managed by specialized engines
Unstructured Data		data not handled as a database
Credentials		data intended to establish and manage the identity of an entity
Logs		data used to record system events
PII	in motion	data containing Personally Identifiable Information
Packets		data in transit generally (for example: messages)
Memory	in use	data actively available within executing systems

Cybersecurity Properties

Cybersecurity Properties Timeline *



[1] The Protection of Information in Computer Systems
[2] On the implementation of security measures in information systems
[3] Security and Privacy in Computer Systems
[4] On Distributed Communication: IX. Security, Secrecy, and Tamper-free considerations
[5] Department of Defense Trusted Computer System Evaluation Criteria
[6] Information technology - Open Systems Interconnect - Basic Reference Model - Part 2: Security Architecture
[7] NIST SP 800-33 - Underlying Technical Models for Information Technology Security
[8] 44 U.S.C section 2542. Definitions
[9] The Security Development Lifecycle
[10] Our Excessively Simplistic Information Security Model and How to Fix It
[11] Specifying Reusable Security Requirements
[12] Secure Systems Development with UML
[13] Security Quality Requirements Engineering (SQUARE) Methodology
[14] A Taxonomy of Security Requirements
[15] Distributed Immutable Ephemeral - New Paradigms for the Next Era of Security

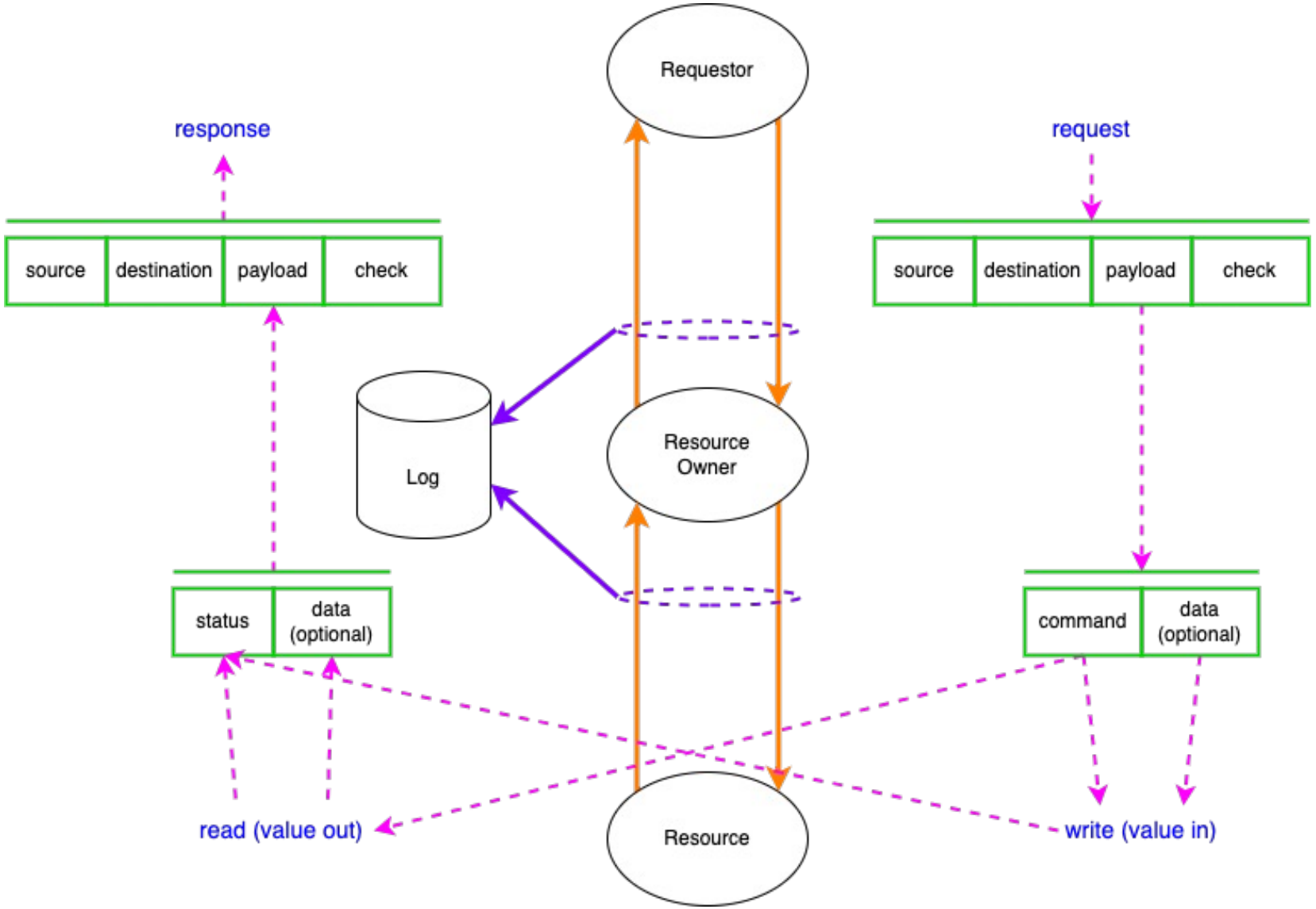
* Understanding the Extended CIA Working Model (AVCDL elaboration document)

Cybersecurity Properties *

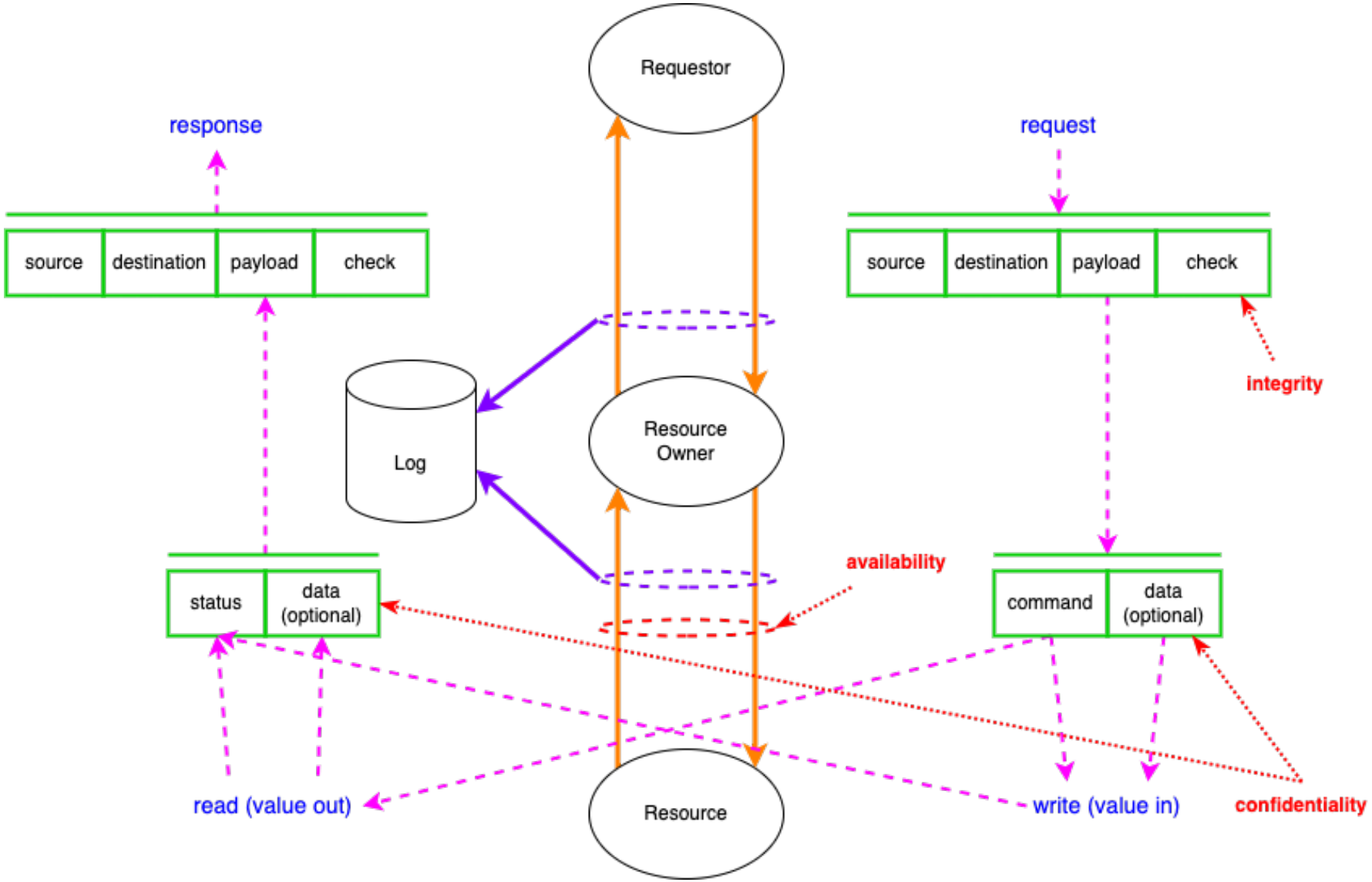
Property	Description
Confidentiality	disclosure of information generally
Integrity	data accuracy and completeness generally
Availability	on-demand access to resources generally
Non-repudiation	denial of action taken or failure to acknowledge request
Authenticity	entity identity
Accountability	system state history (for example: for audit)
Authorization	entity privilege

* NIST SP 800-33, Underlying Technical Models for Information Technology Security (link in references)

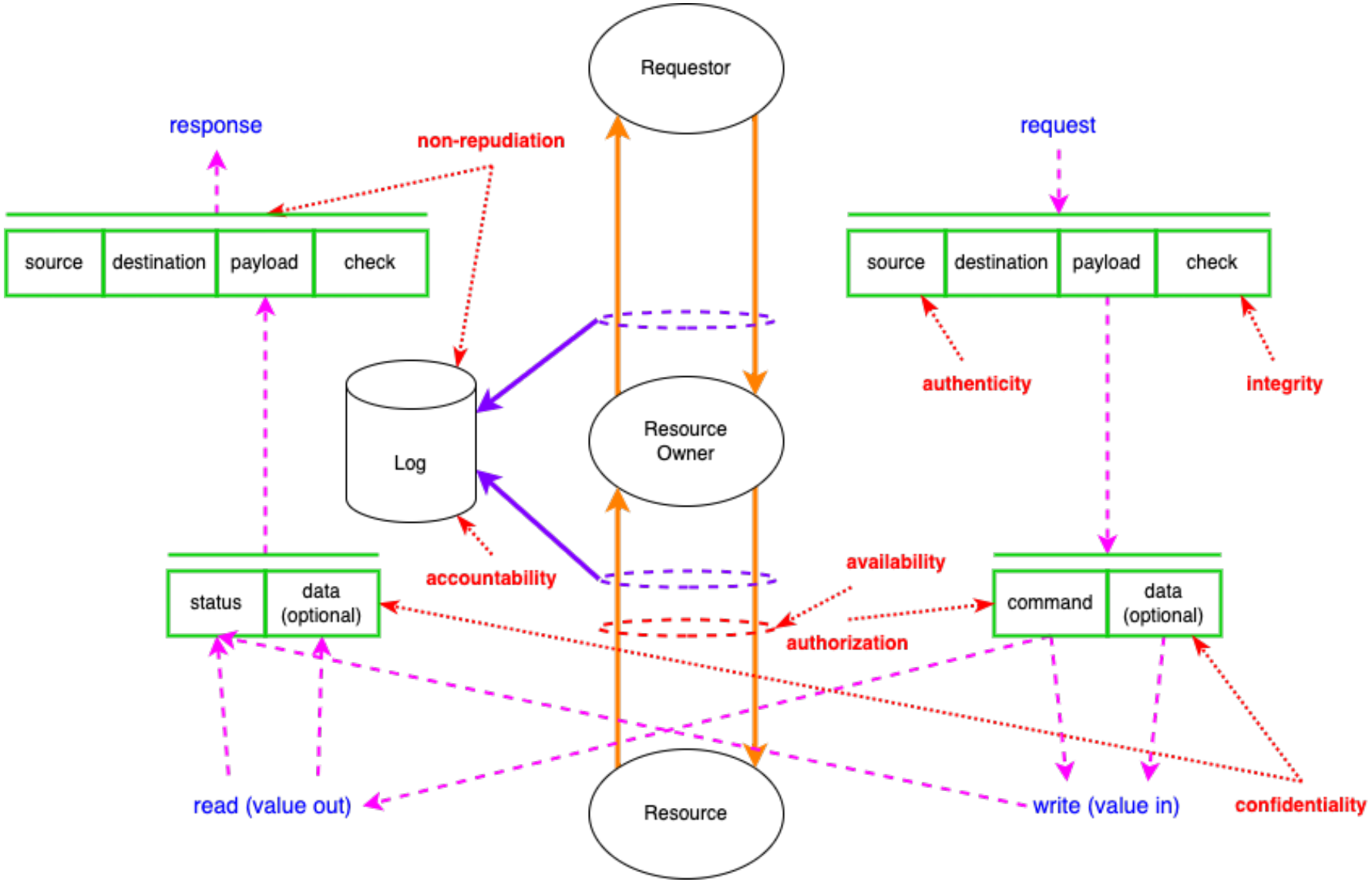
Resource Access Working Model



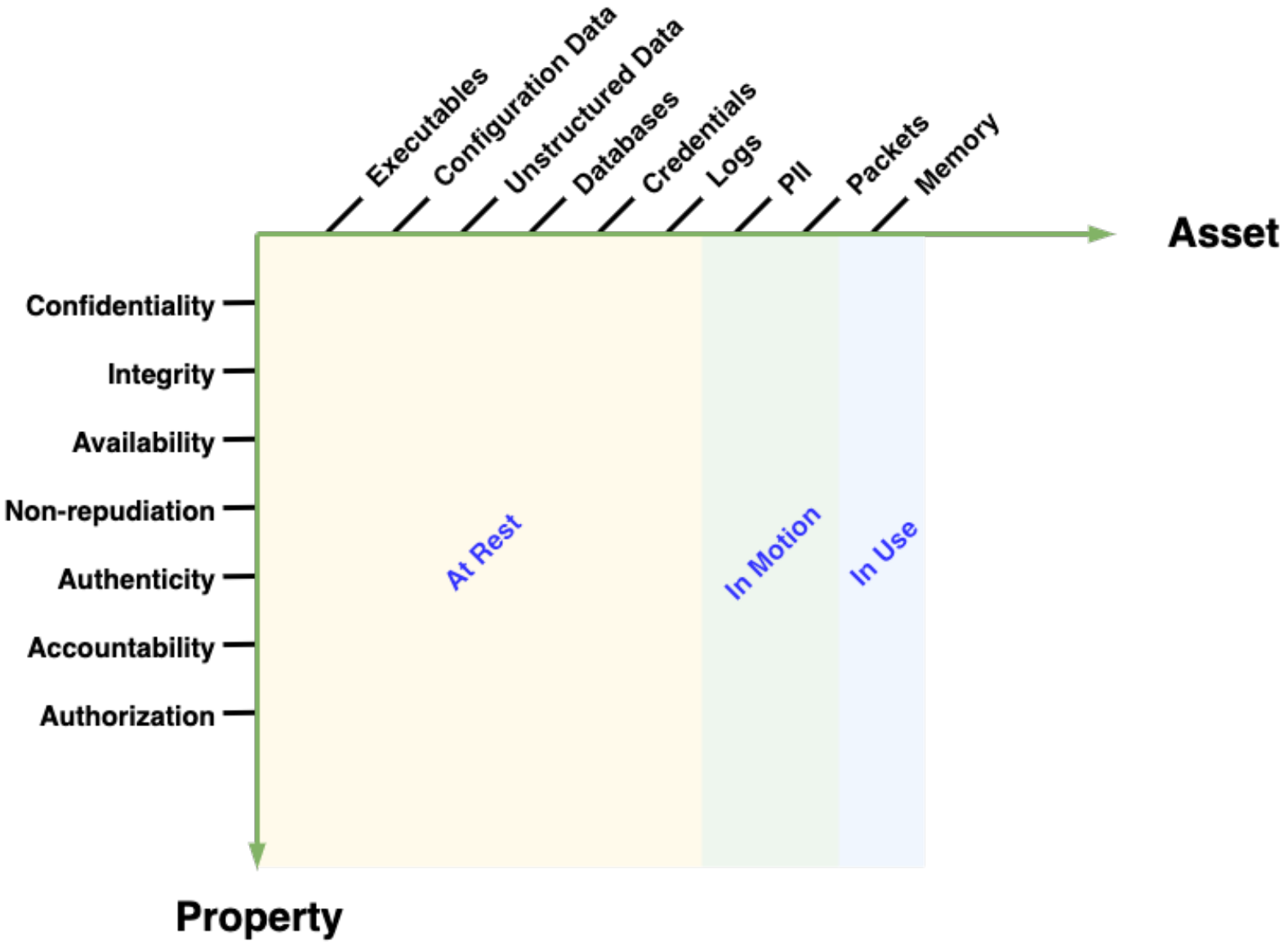
Resource Access Working Model



Resource Access Working Model



Combining Asset and Property

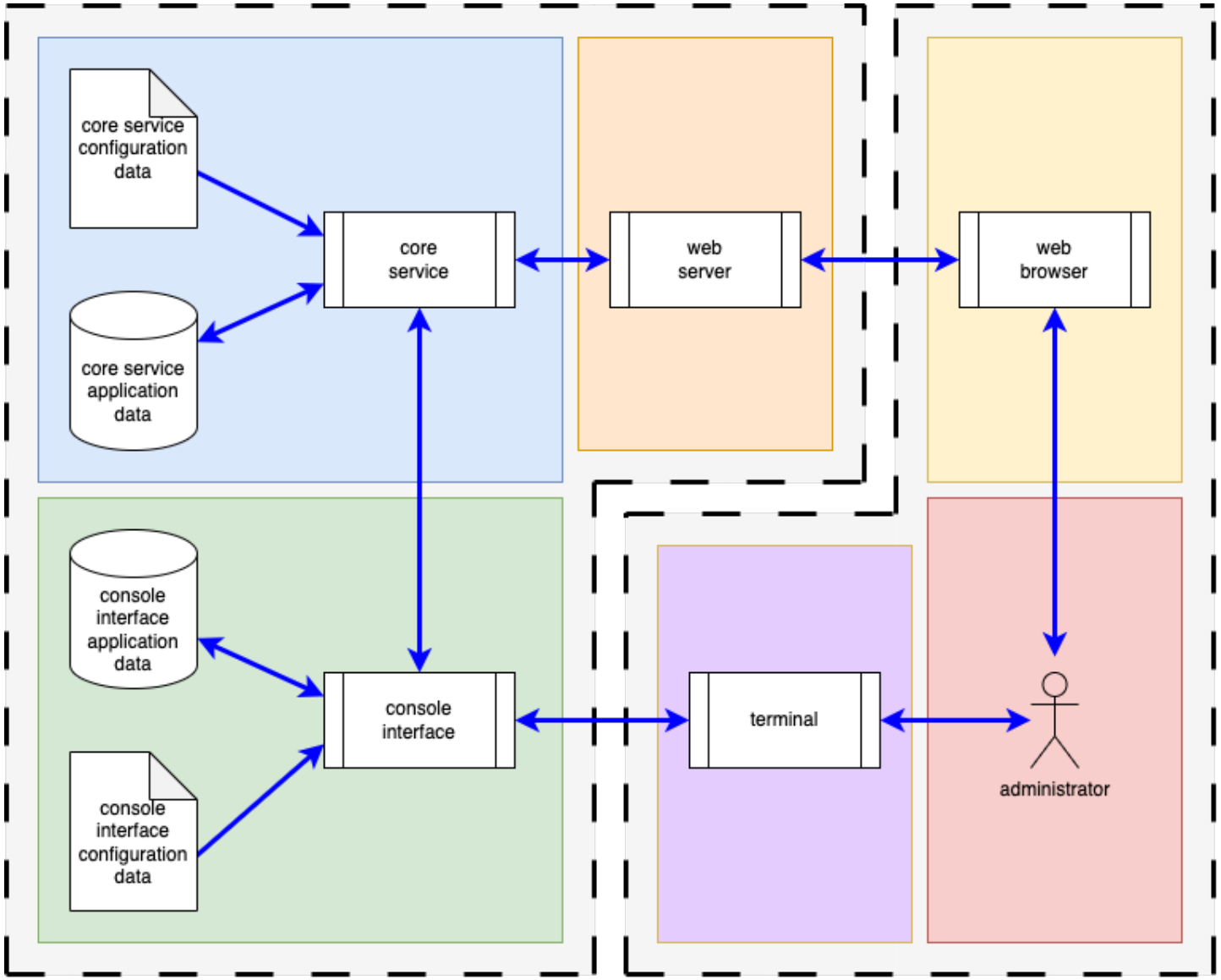


Simple System

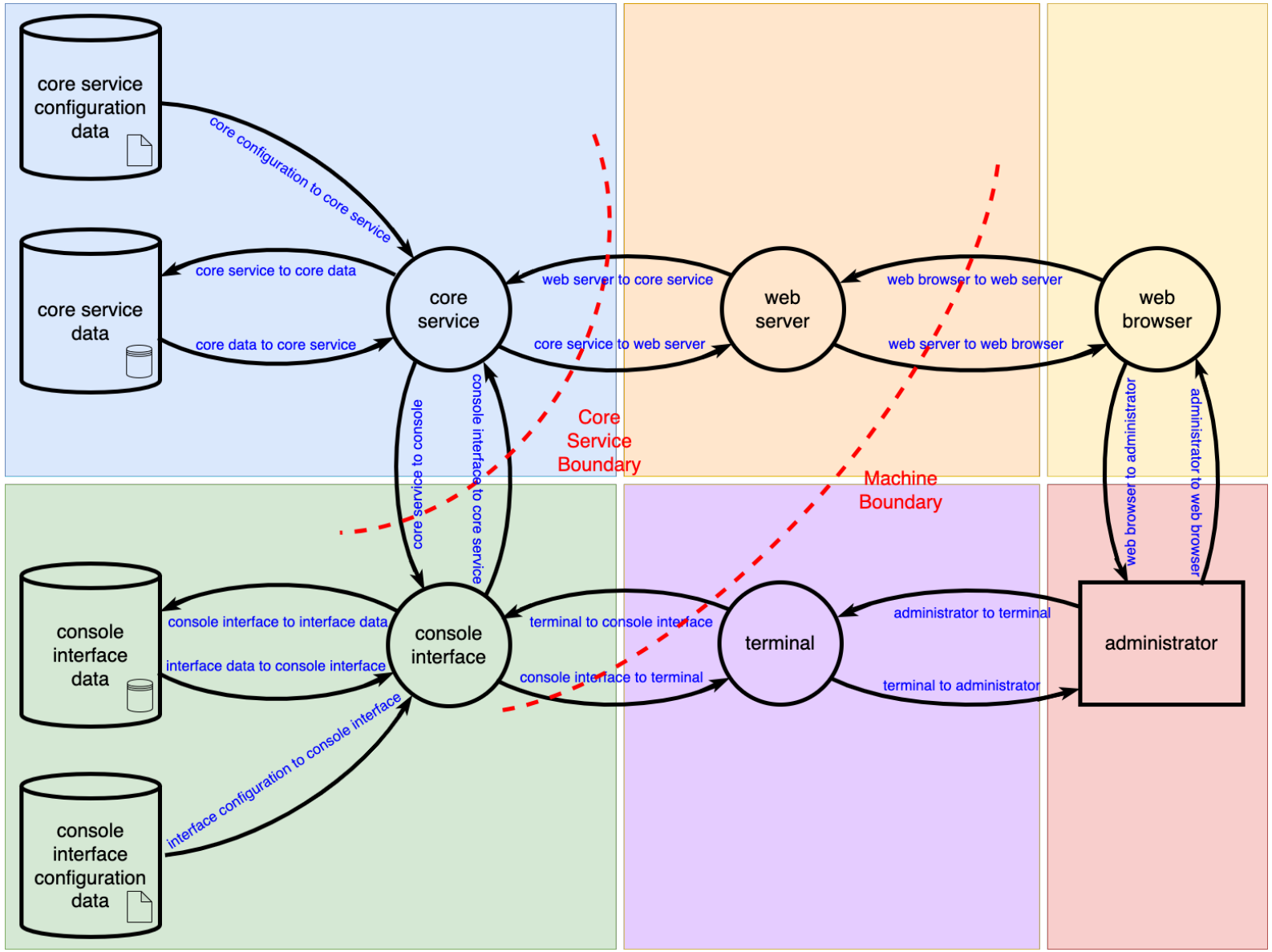
What is a Threat Model?

- representation of a system's data flows, data stores and interactors
- collection of views of a system
- engineering design document

Simple System – Block View

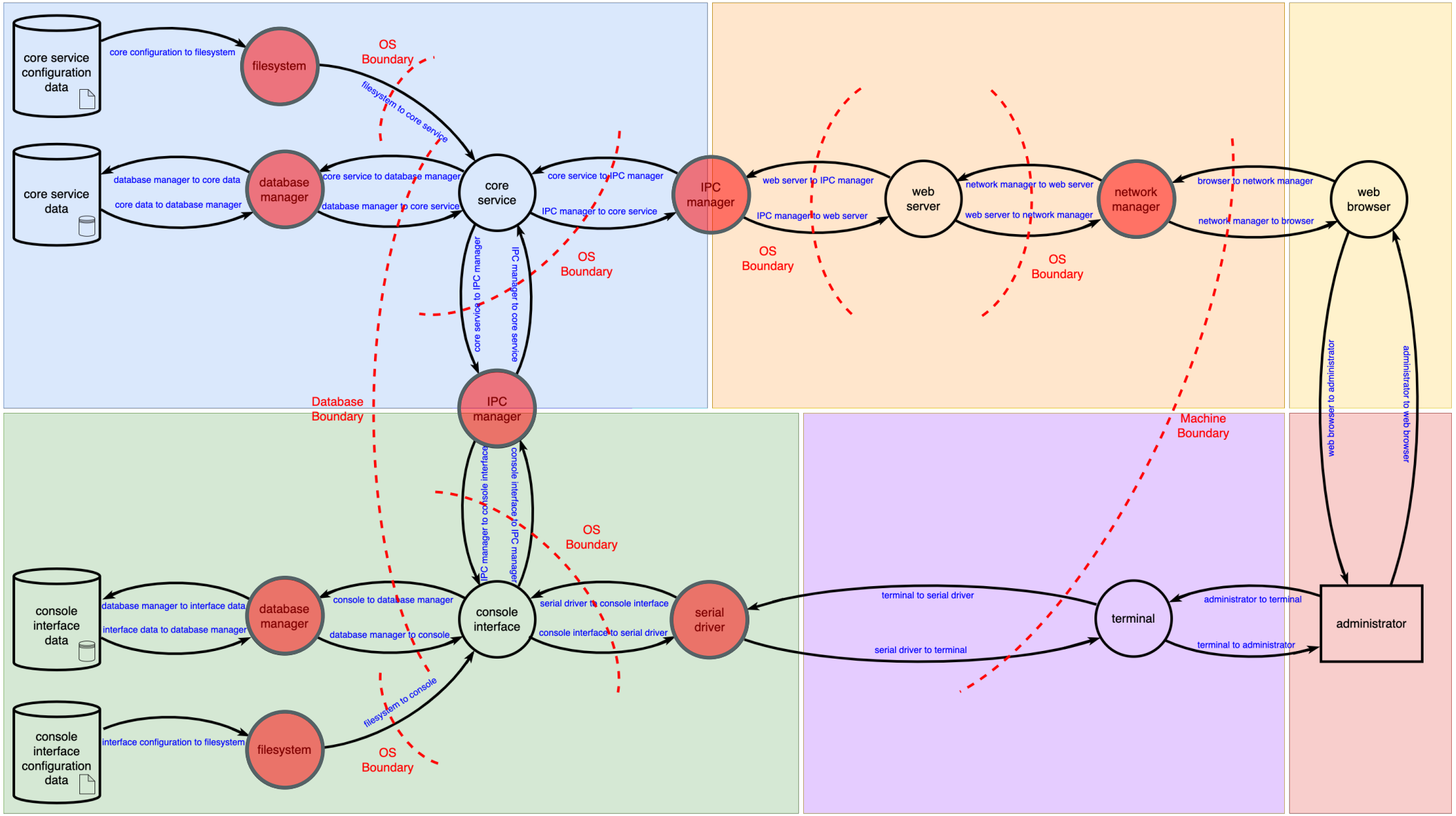


Simple System – DFD

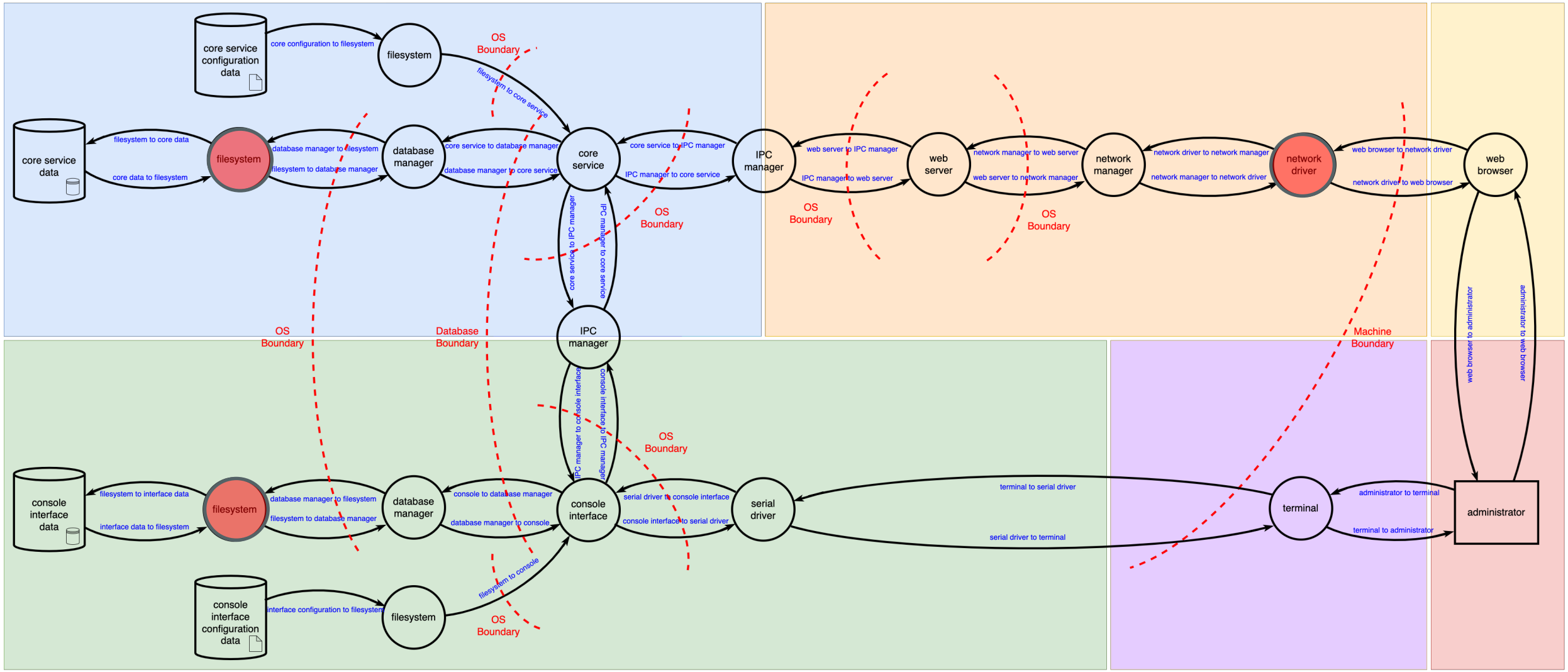


Layers

Simple System – DFD (Level 2)



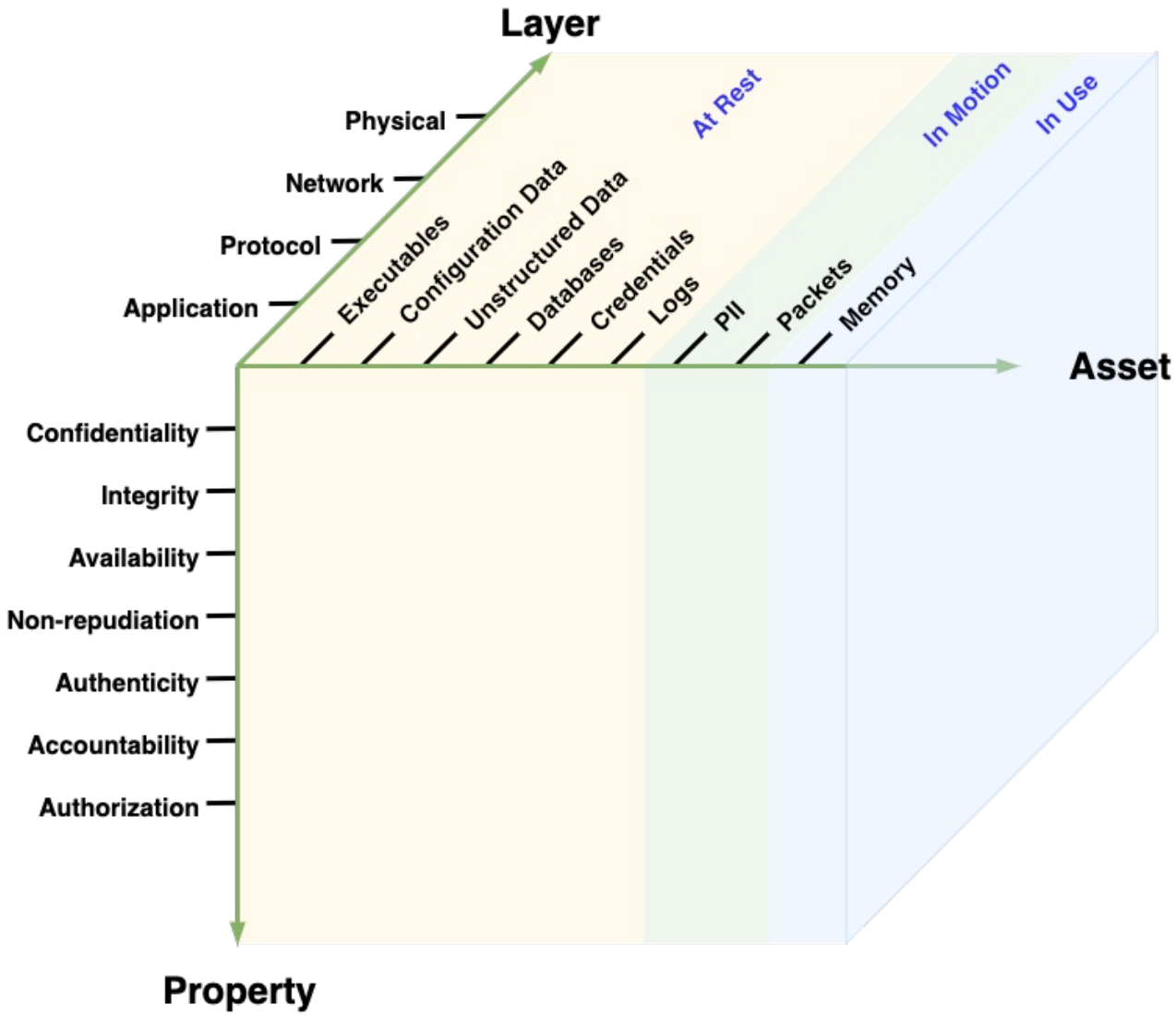
Simple System – DFD (Level 3)



Layers

Layer	Description
Physical	hardware interface
Network	system-mediated transport
Protocol	custom data transport
Application	data handling within executables

Taxonomy Space



Cybersecurity Requirements

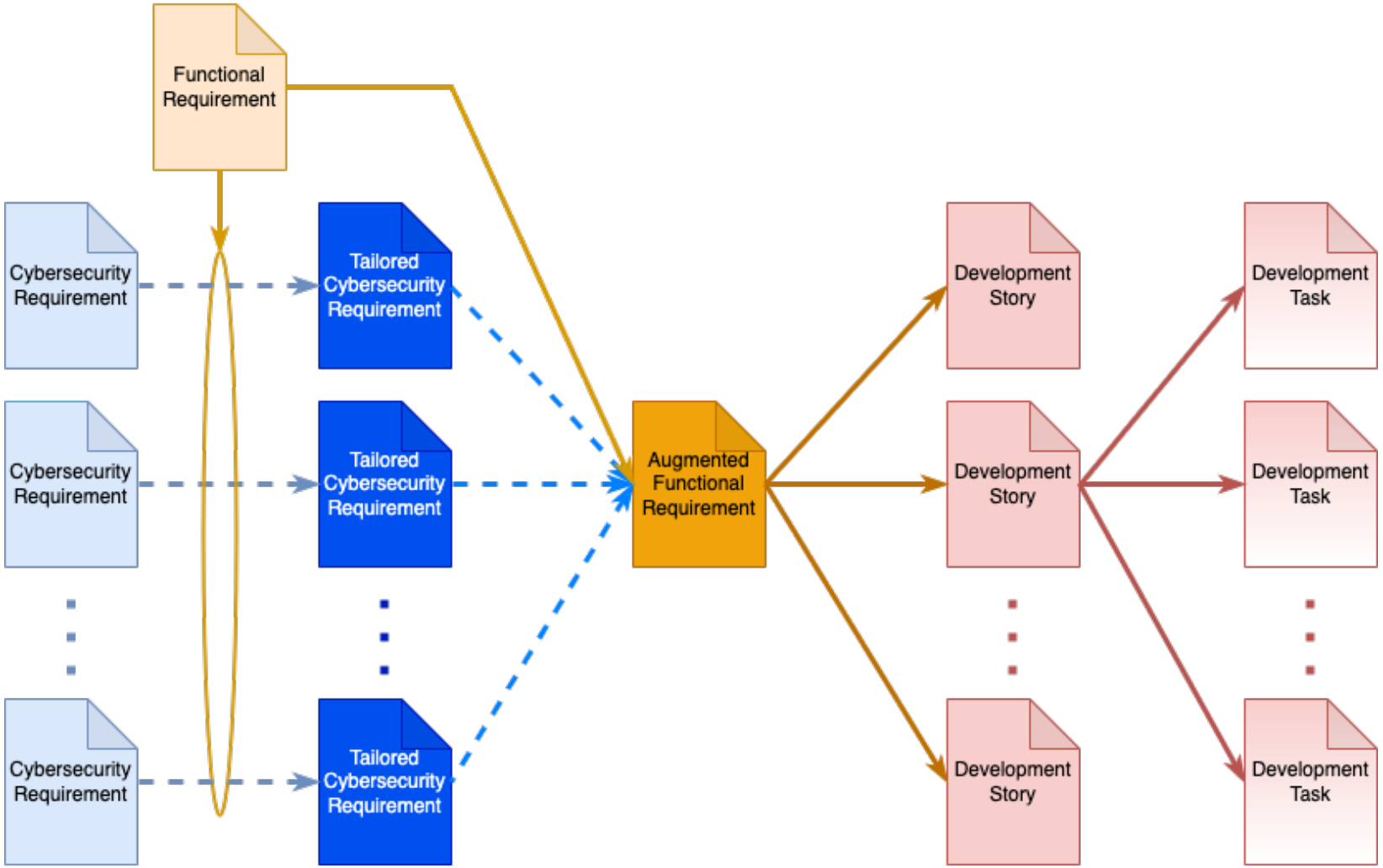
Identifying Requirement Needs – Application Layer

	Executables	Configuration Data	Unstructured Data	Databases	Credentials	Logs	PII	Packets	Memory
Confidentiality	■	■			■	■	■		■
Integrity	■	■	■	■	■	■			■
Availability	■	■	■	■	■	■			
Non-repudiation	■								
Authenticity	■	■		■	■	■			
Accountability	■	■		■	■	■	■		
Authorization	■	■	■	■	■				

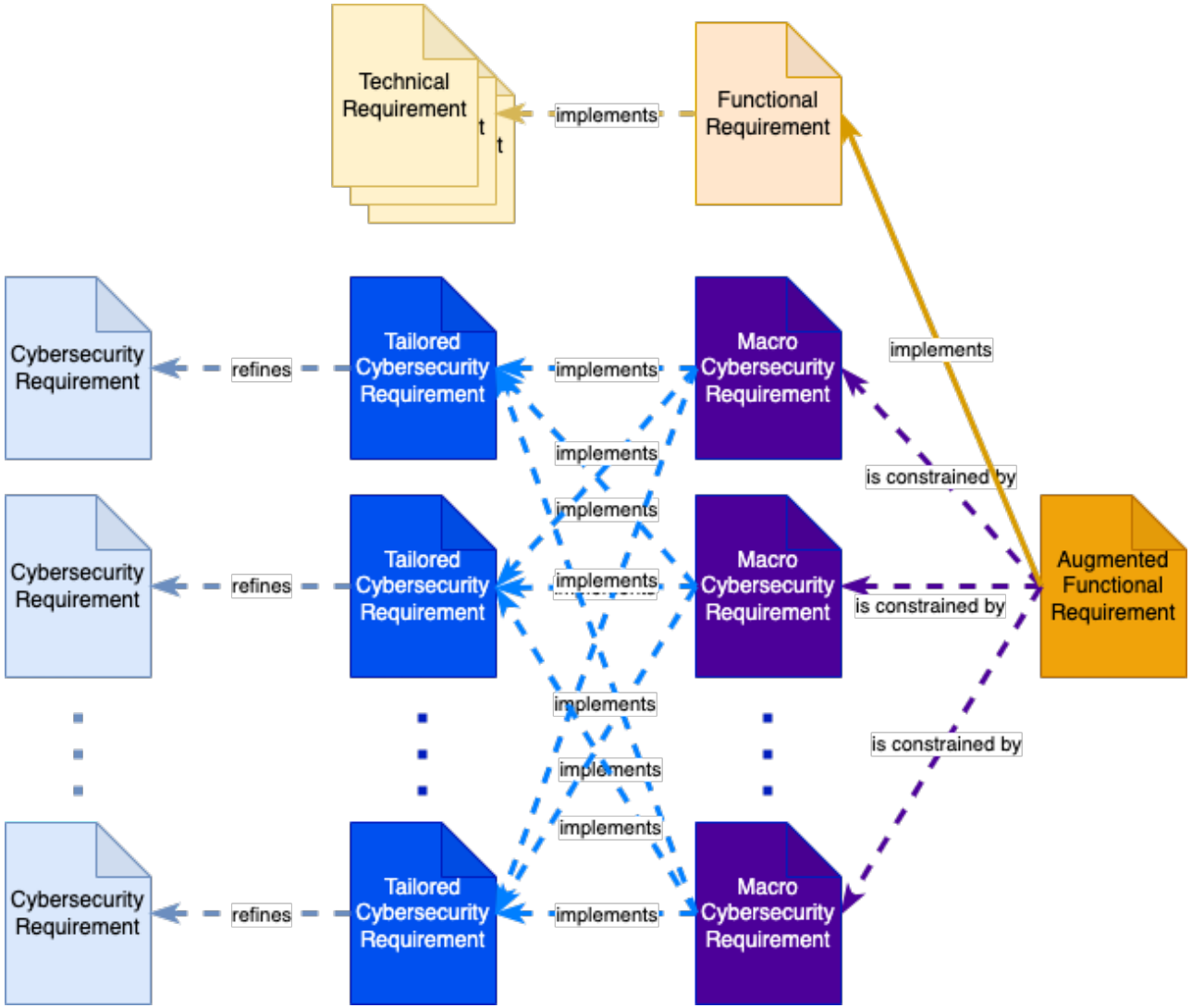
Cybersecurity Global Requirements Catalog

ID	Requirement	Property							Asset										Layer			
		Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity	Accountability	Authorization	Executables	Configuration Data	Databases	Unstructured Data	Credentials	Logs	PII	Packets	Memory	Hardware	Physical	Network	Protocol	Application
CR001	Persistent storage shall be encrypted.		X						X		X	X	X	X								X
CR002	Update payloads shall be decrypted at time of use.		X						X													X
CR003	Update payloads shall be encrypted at build time.		X						X													X
CR004	Update payloads shall be stored encrypted.		X						X													X
CR005	Executable integrity shall be cryptographically verified.		X						X													X
CR006	Executables receiving commands requiring a response shall respond within a quantified period of time.				X				X													X
CR007	Executables sending reply-dependent messages shall have a quantified retry limit.				X				X													X
CR008	Executable authenticity shall be cryptographically verified.					X			X													X
CR009	Executables that are discrete message sources shall have unique identities.					X			X													X
CR010	Cryptographic keys utilized for secure boot shall be protected by a hardware root of trust.					X			X													X
CR011	The update process shall only be initiated by authenticated entities.					X			X													X
CR012	Deviations from standard, normal, or expected conditions shall be detected.						X		X													X
CR013	Deviations that are detected shall be logged.						X		X													X
CR014	Processes receiving data crossing a trust boundary shall be sandboxed.							X	X													X
CR015	Processes shall be granted the smallest set of privileges.							X	X													X
CR016	Only authorized entities shall perform control operations on executables.							X	X													X
CR017	Privileged access shall be permitted only for singular, specific, time-limited operations.							X	X													X
CR018	The system shall contain only secure default privileged accounts if a privileged account is necessary.							X	X													X
CR019	Processes shall have unique owners.							X	X													X
CR020	The system shall enter a safe state when a safety-critical data store is not available.			X						X	X	X										X
CR021	Configuration data confidentiality shall be protected using access controls.	X								X												X
CR022	Configuration data integrity shall be validated prior to use.		X							X												X
CR023	Configuration data shall only be accessed by authenticate entities.					X				X												X
CR024	Configuration data authenticity shall be assured.					X				X												X
CR025	Configuration data modification shall be recorded in the audit logs.						X			X												X
CR026	Configuration data modification shall only be made by authorized entities.							X		X												X

Tailored Cybersecurity Requirements



Macro Cybersecurity Requirement



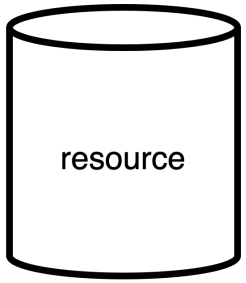
Macro Cybersecurity Requirement Example (SecOC *)

ID	Requirement	Property							Asset										Layer			
		Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity	Accountability	Authorization	Executables	Configuration Data	Databases	Unstructured Data	Credentials	Logs	PII	Packets	Memory	Hardware	Physical	Network	Protocol	Application
CR050	Credentials shall be encrypted when transmitted across trust boundaries.	X											X							X	X	
CR051	PII shall be encrypted when transmitted across trust boundaries.	X													X					X	X	
CR052	Communication crossing trust boundaries that cannot be secured shall be isolated.	X														X				X	X	
CR053	Communication crossing trust boundaries shall ensure data confidentiality.	X														X				X	X	
CR054	Communication crossing trust boundaries shall ensure data integrity.		X													X				X	X	
CR055	Communication crossing trust boundaries shall ensure data availability.			X												X				X	X	
CR056	Communication crossing trust boundaries shall be authenticated.					X										X				X	X	
CR057	Custom protocols that support a retry mechanism shall implement rate limiting.				X											X					X	
CR058	Custom protocols shall use current best practices for authentication and key exchange (NIST SP 800-57, 63B, 131 and 133).					X										X					X	
CR059	Standard network protocols shall be secured using cybersecurity best practices.	X														X				X		

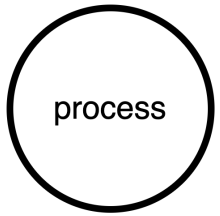
* SecOC Security Profile 1 (link in references)

Applying the Taxonomy

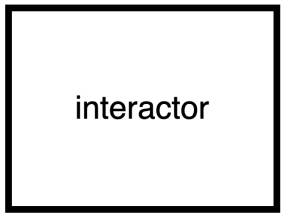
Threat Model Element Attributes



- has unique ID
- is read-only
- is structured
- contains PII
- is encrypted
- is integrity checked
- data type
    - analog
    - executable
    - configuration data
    - data log
    - audit log

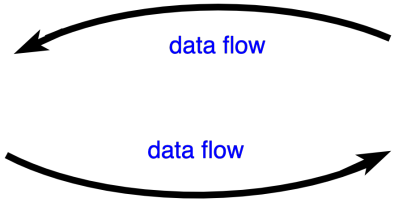


- has unique ID
- type
    - driver
    - service
    - process
- class
    - OS
    - third-party
    - self
- is authenticated
- is authorized



- type (person, analog)

- type
    - machine
    - network
    - interprocess
    - OS
    - resource
    - external interactor



- type (standard, custom)
- requires acknowledgement
- has sequence numbers
- has authenticated source
- has authenticated destination
- is safety critical
- has integrity check
    - none
    - simple (CRC)
    - cryptographic
- uses encryption
    - none
    - symmetric
    - asymmetric

Threat Modeling Tool Rules

Title

TT_4: Data transmitted over custom protocol data flow may be corrupted or modified

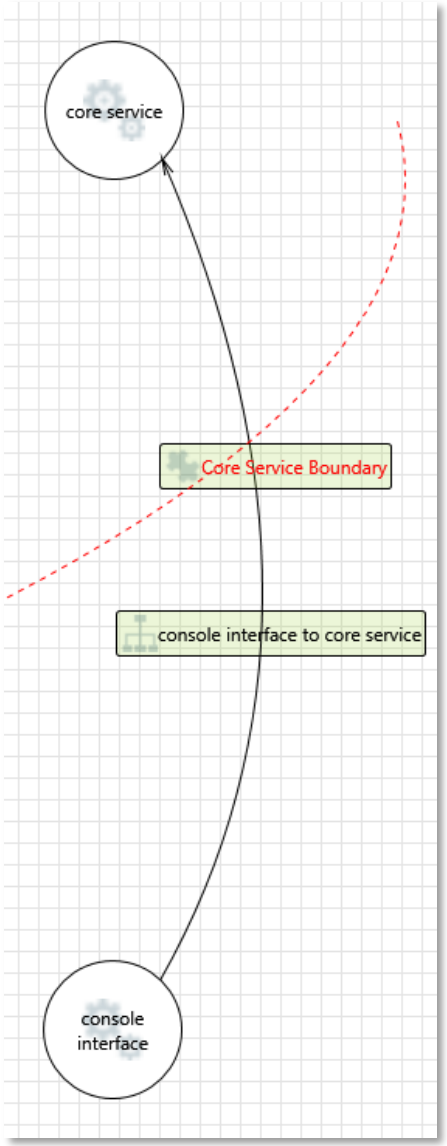
Script with CRT Attributes

```
source is [Generic Process] and target is [Generic Process] and (flow
crosses [Network Boundary] or flow crosses [Machine Boundary] or flow
crosses [Interprocess Boundary]) and (flow.[Custom Protocol] is 'Yes'
and flow.[Integrity Check(Dataflow)] is 'None')
```

Rule description

Data transmitted over custom protocol data flow '{flow.Name}', from source process ‘{source.Name}’ to target process ‘{target.Name}’, may be corrupted or modified accidentally, and it may lead to the loss of integrity on data being transmitted and target process '{target.Name}' may receive incorrect data, because there is no proper integrity check mechanism being used with the custom protocol data flow ‘{flow.Name}’.

Quality of Results



Default MSTMT Results

Category	Title
Spoofing	Spoofing the core service Process
Spoofing	Spoofing the console interface Process
Tampering	Potential Lack of Input Validation for core service
Repudiation	Potential Data Repudiation by core service
Information Disclosure	Data Flow Sniffing
Denial Of Service	Data Flow console interface to core service Is Potentially Interrupted
Denial Of Service	Potential Process Crash or Stop for core service
Elevation Of Privilege	Elevation Using Impersonation
Elevation Of Privilege	Cross Site Request Forgery
Elevation Of Privilege	Elevation by Changing the Execution Flow in core service
Elevation Of Privilege	core service May be Subject to Elevation of Privilege Using Remote Code Execution

Cybersecurity Requirements Taxonomy-based Results

Category	Title
Confidentiality	TT_1: Sensitive information transmitted over data flow may be disclosed to unauthorized access
Integrity	TT_4: Data transmitted over custom protocol data flow may be corrupted or modified
Integrity	TT_6: Data transmitted over custom protocol data flow may be susceptible to loss of message integrity
Authenticity	TT_8: Data flow target process may receive malicious messages from source process.

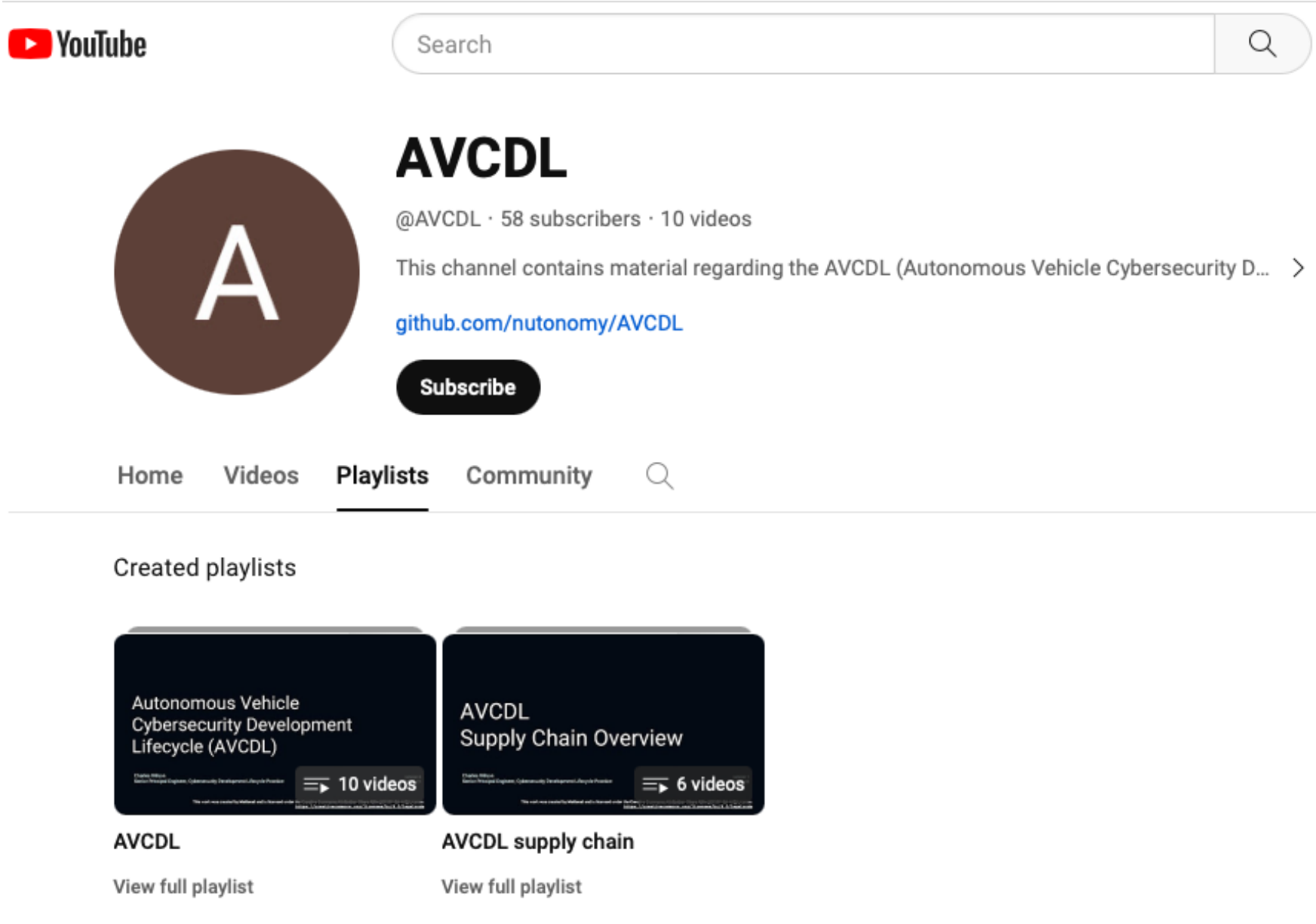
STRIDE vs CRT

	STRIDE	CRT
Focus	Attack	Property
Unique	No	Yes
Unambiguous	No	Yes
Complete	No	Yes
Grounded	No	Yes
Scalable	No	Yes
Actionable	Sometimes	Yes

Where to Go from Here

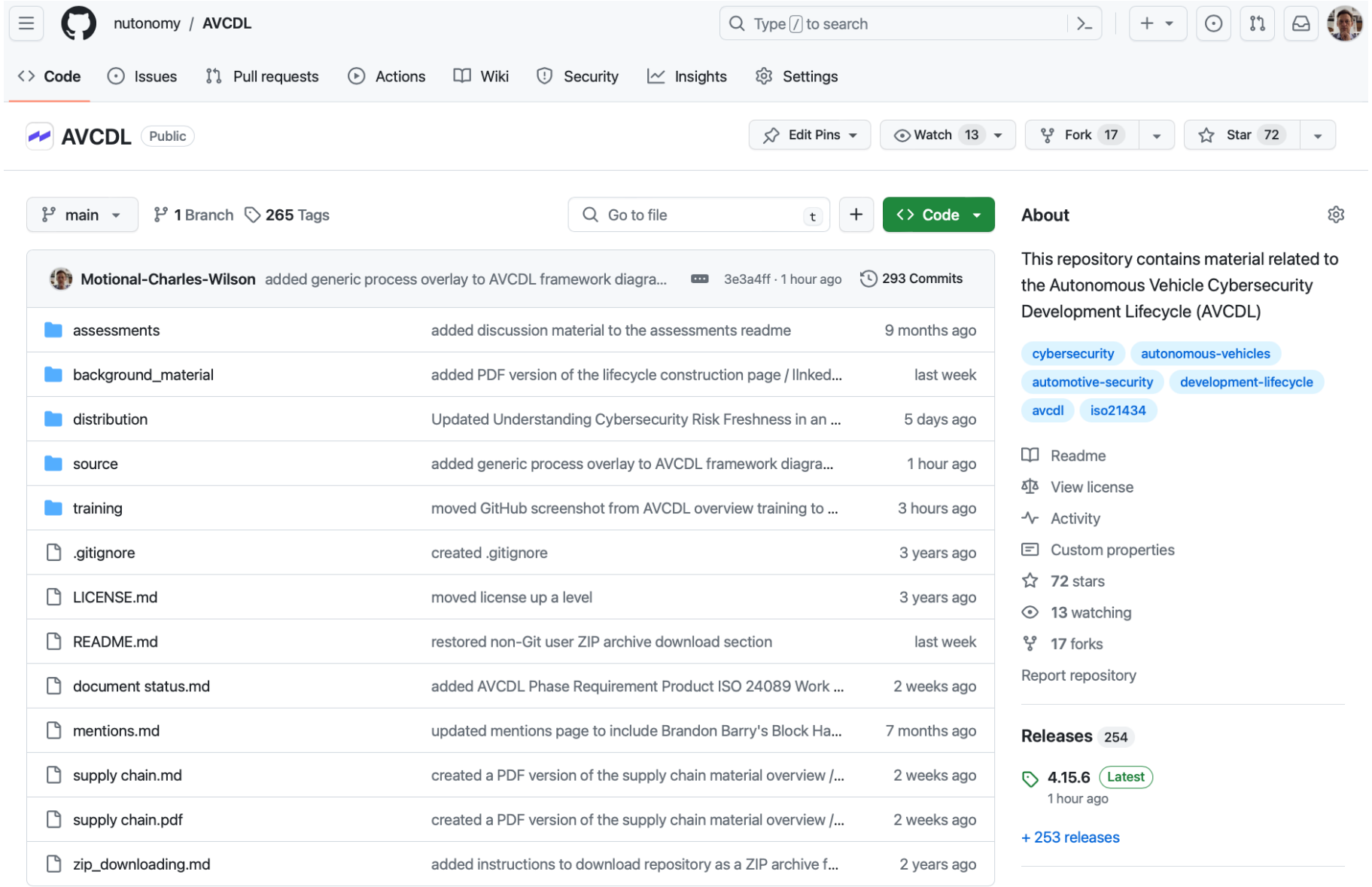
AVCDL on YouTube

https://youtube.com/@AVCDL/playlists



AVCDL on GitHub

https://github.com/nutonomy/AVCDL



References (1 of 2)

AVCDL (primary document)

Security Requirements Taxonomy (AVCDL secondary document)

Product-level Security Requirements (AVCDL secondary document)

Element Cybersecurity Relevancy (AVCDL secondary document)

Design Showing Security Considerations (AVCDL secondary document)

cybersecurity requirements per taxonomy.xlsx (AVCDL workbook)

Global Security Requirements (AVCDL secondary document)

Understanding the Extended CIA Working Model (AVCDL elaboration document)

References (2 of 2)

INCOSE Requirements Working Group
https://www.incose.org/2021-redesign/working-groups-v1/requirements

Specification of Secure Onboard Communication Protocol
https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_SecOcProtocol.pdf

Threat Modeling Vocabulary (capture of 11 May 2011 blog post)
https://web.archive.org/web/20161101093537/https://www.cigital.com/blog/threat-modeling-vocabulary/

Threat Modeling Glossary Diagram (for above blog post capture)
https://www.synopsys.com/blogs/software-security/wp-content/uploads/2015/08/threat-modeling-glossary-diagram.jpg

Using and Customizing Microsoft Threat Modeling Tool 2016
https://roberthurlbut.com/Resources/2017/BCC27/Robert-Hurlbut-BCC27-Using-Customize-MS-Threat-Modeling-Tool-2016.pdf

Questions