WIND RIVER TECHNOLOGY FORUM 2023

Security In Wind River Linux

风河Linux的信息安全实践

蔡志鸿，CISSP/技术应用经理

2023.10.17

WNDRVR

Agenda

1
Automotive Security Overview

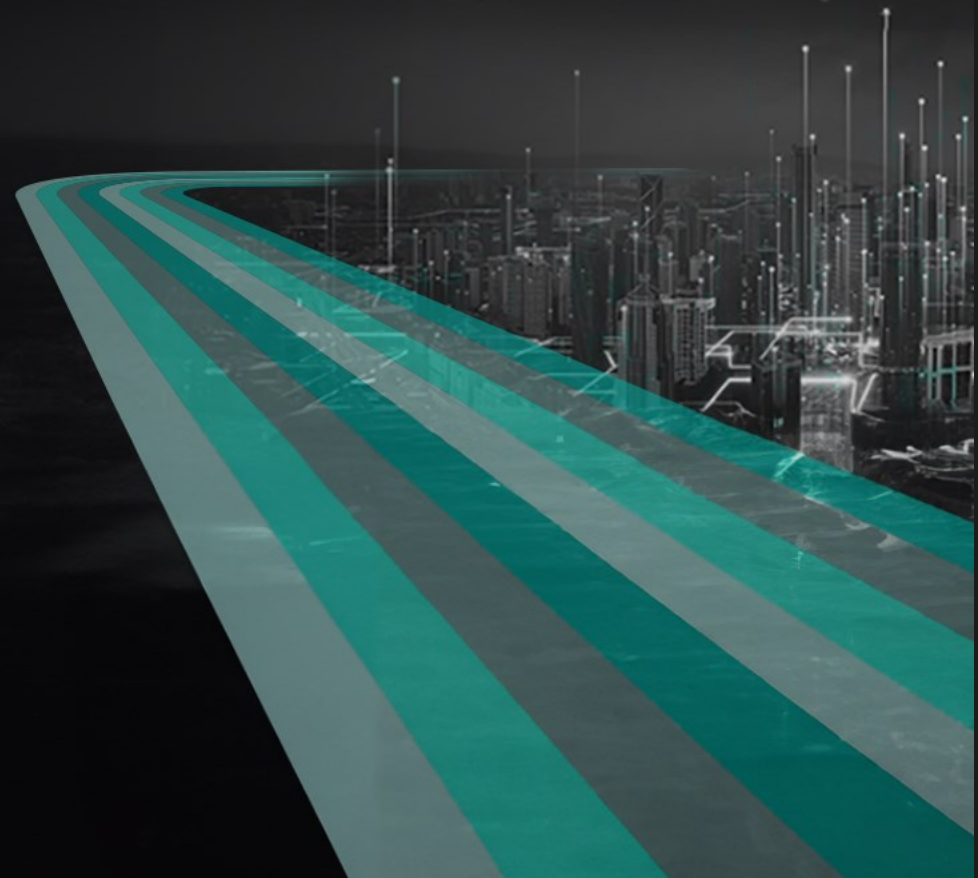
2
Wind River Linux For Automotive Security

3
Use Cases

WNDRVR

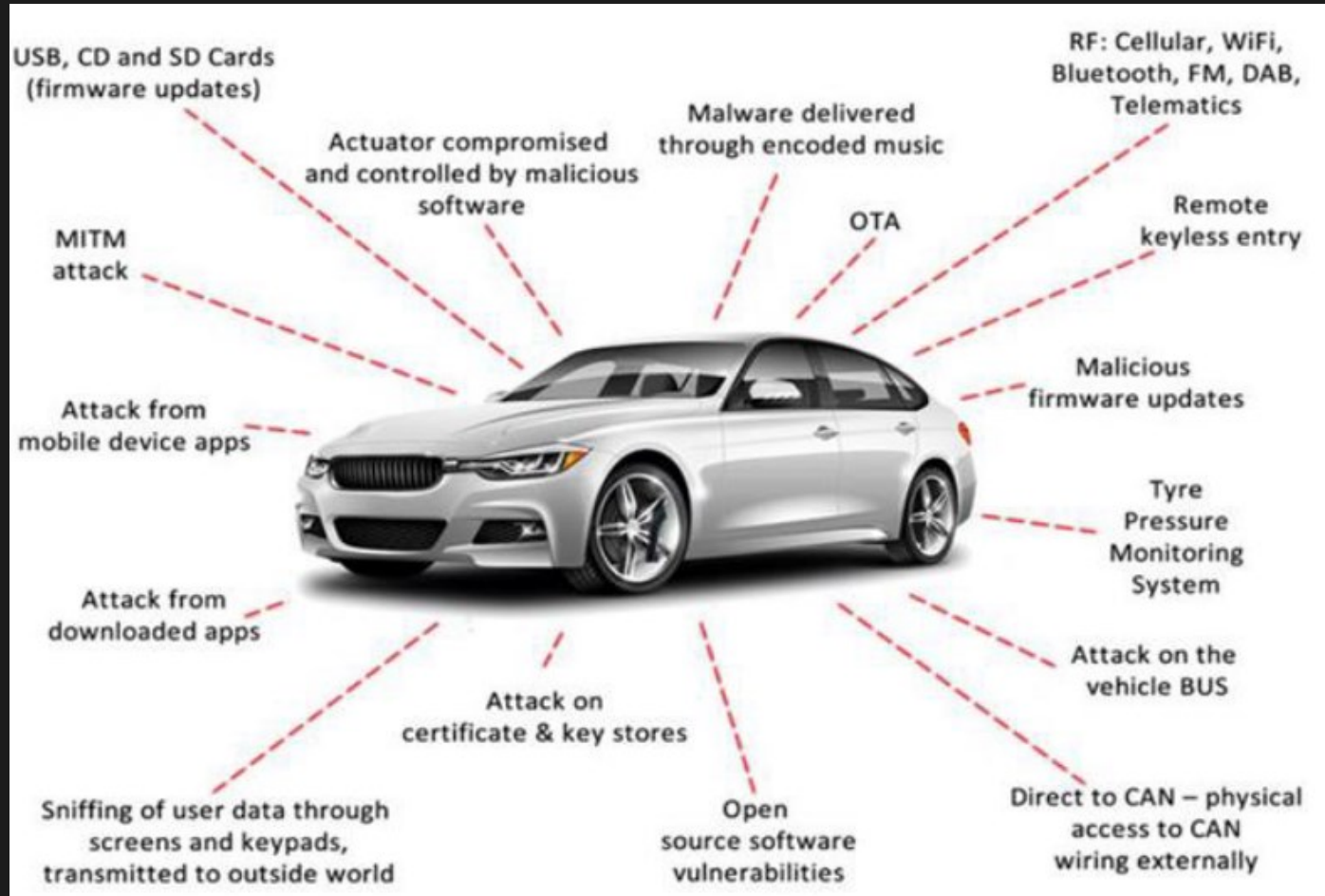
Automotive Security Overview

- Security Challenges
- Security Regulations and Standards
- CIA Triad
- CIA implication for Automobile



Security Challenges

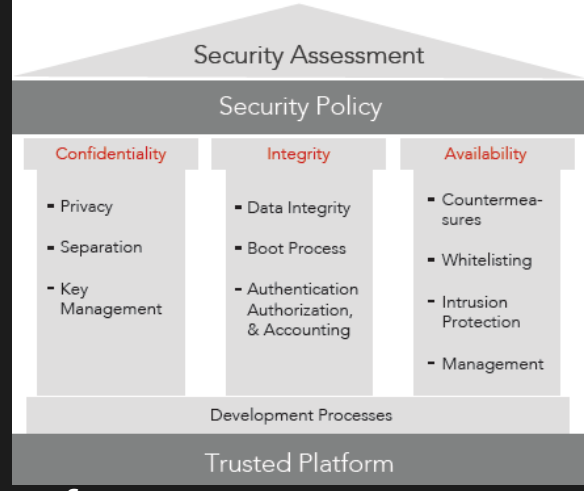
- More connected vehicles, more vulnerabilities
  - Connected Vehicles: 230M (2021) -> 571M (2025)
  - Cybersecurity Risks
    - Remote hacking, malware attacks, and unauthorized access, personal information (vehicle occupants) leakage
  - Maintain the security of the vehicle throughout its lifecycle
- Complicated software, huge code base
  - ADAS, Infotainment, AI algorithms, …
- The attack surface of a connected vehicle



Security Regulations and Standards

- **ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering**
  - Provides guidelines for establishing a cybersecurity framework for vehicles **(**risk assessment, threat modeling, and defining cybersecurity processes throughout the vehicle's lifecycle**)**
- UN Regulation No. 155, “Cyber security and cyber security management systems”
- **GDPR (General Data Protection Regulation) Compliance**
  - Applies to vehicles operating in the European Union
- **Collaboration with Industry Standards**
  - e.g Auto-ISAC (Automotive Information Sharing and Analysis Center) facilitate the sharing of cybersecurity threat intelligence and best practices
- SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
  - developing cybersecurity processes, strategies, and measures to protect vehicles from cyber threats, unauthorized access, and malicious activities

CIA Triad



- 3 pillars of information security
- The term "**information security**" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) availability, which means ensuring timely and reliable access to and use of information

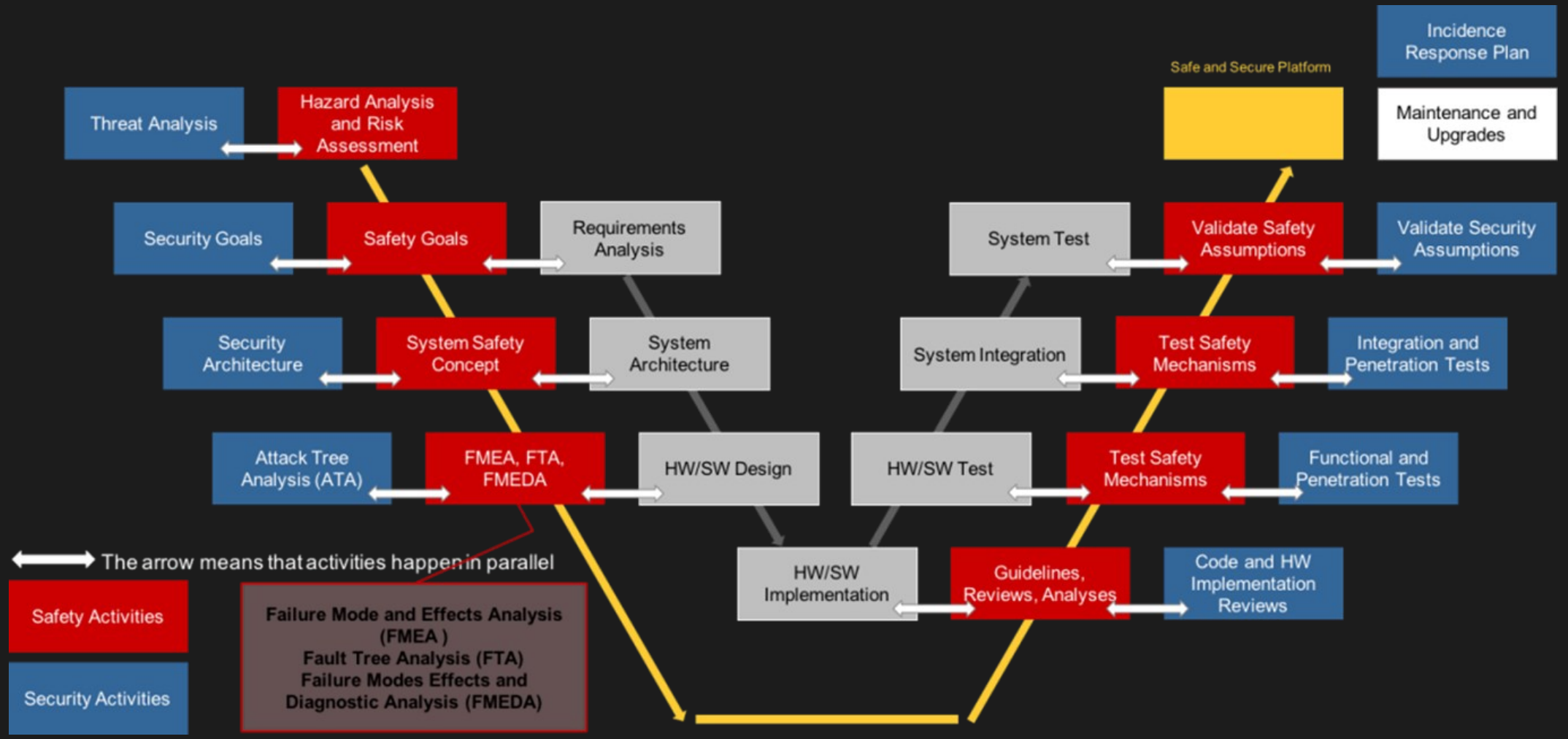
CIA implication for Automobile

- Confidentiality
  - Protecting personal data like driver profiles, contact information, location data, and even biometric information
  - Securing communication channels for over-the-air software updates, navigation services, and entertainment streaming
  - Securing safety-related information, such as sensor data from cameras, radar, and LiDAR systems
- Integrity
  - Prevents unauthorized tampering with boot process, software, firmware, or configuration settings within the vehicle's Electronic Control Units (ECUs)
  - OTA updates to enhance features, fix bugs, and address security vulnerabilities
  - Vehicle diagnostics and usage statistics
- Availability
  - Fundamental for individual mobility, emergency services, mobility services like ride-sharing, and public transportation etc.
  - Stranded vehicles can inconvenience occupants and may require costly rescue operations

Wind River Linux For Automotive Security

- Security Development Lifecycle versus Safety
- Confidentiality
- Integrity
- Availability

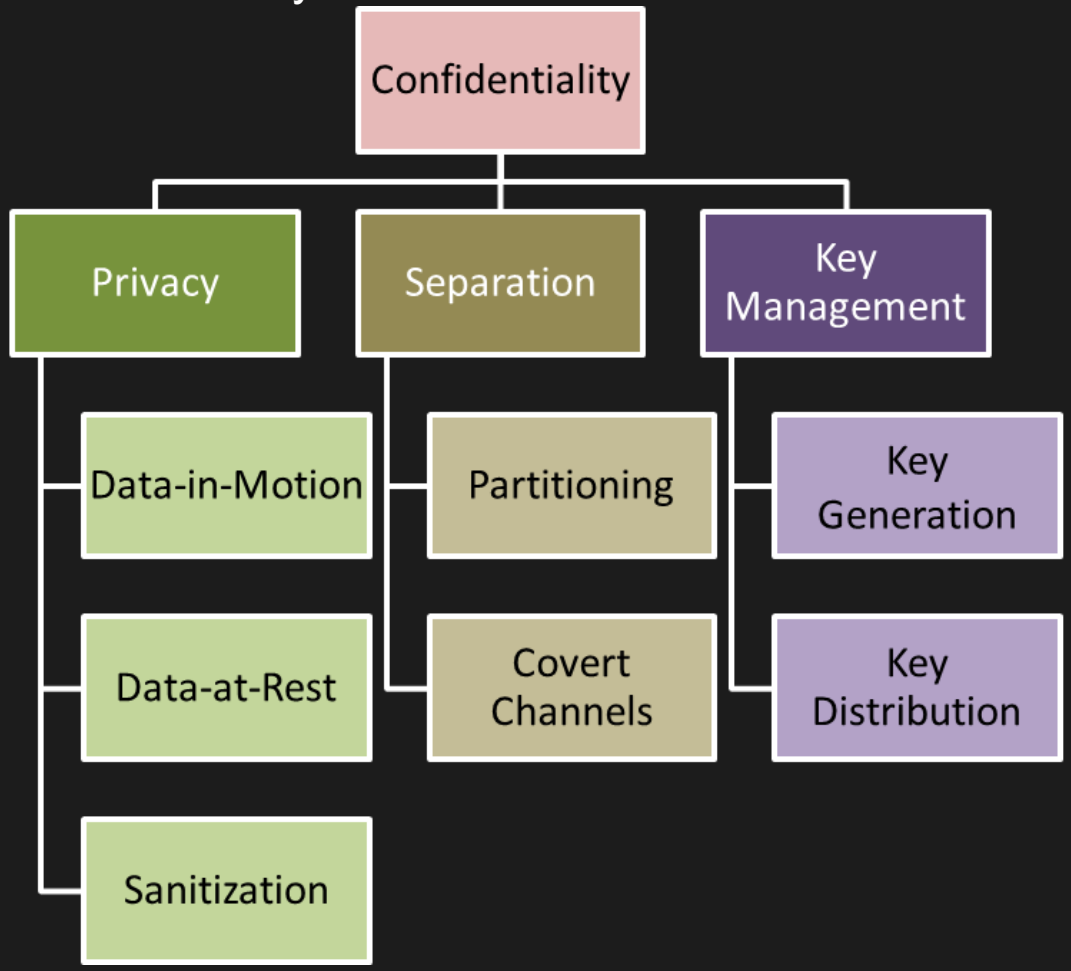
Security Development Lifecycle versus Safety



WNDRVR

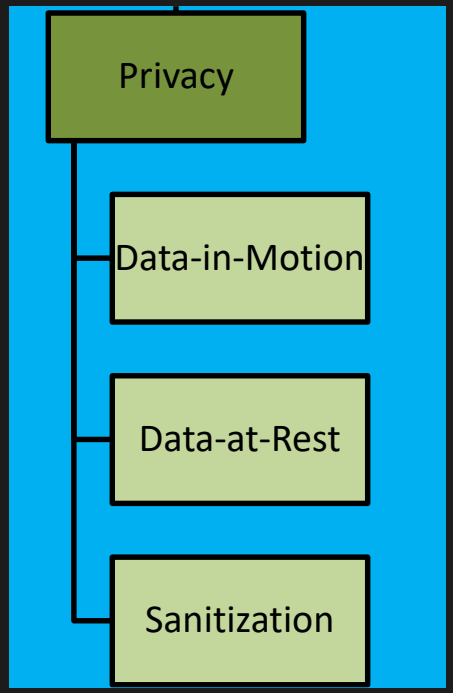
Confidentiality

- Decomposition of Confidentiality



Confidentiality – Privacy

- Privacy is implemented using cryptography
- **Symmetric —** use the same key for encryption and decryption
- **Asymmetric —** uses a pair of keys as part of the cryptographic function
  - Public key – known to any party
  - Private key – known only to one party
  - The public key is mathematically related to the private key
    - mathematically infeasible to determine the private key from the public key
  - For privacy, encrypt with the public key
    - can only decrypt with the private key
- Related Open Source Software
  - OpenSSL/OpenSSH/GnuPG/strongSwan/ipsec-tools/vsftpd (data-in-motion)
  - LUKS for Full Disk Encryption (FDE)/HSM for keys and credentials (data-at-rest)
  - shred/hdparm (sanitization)

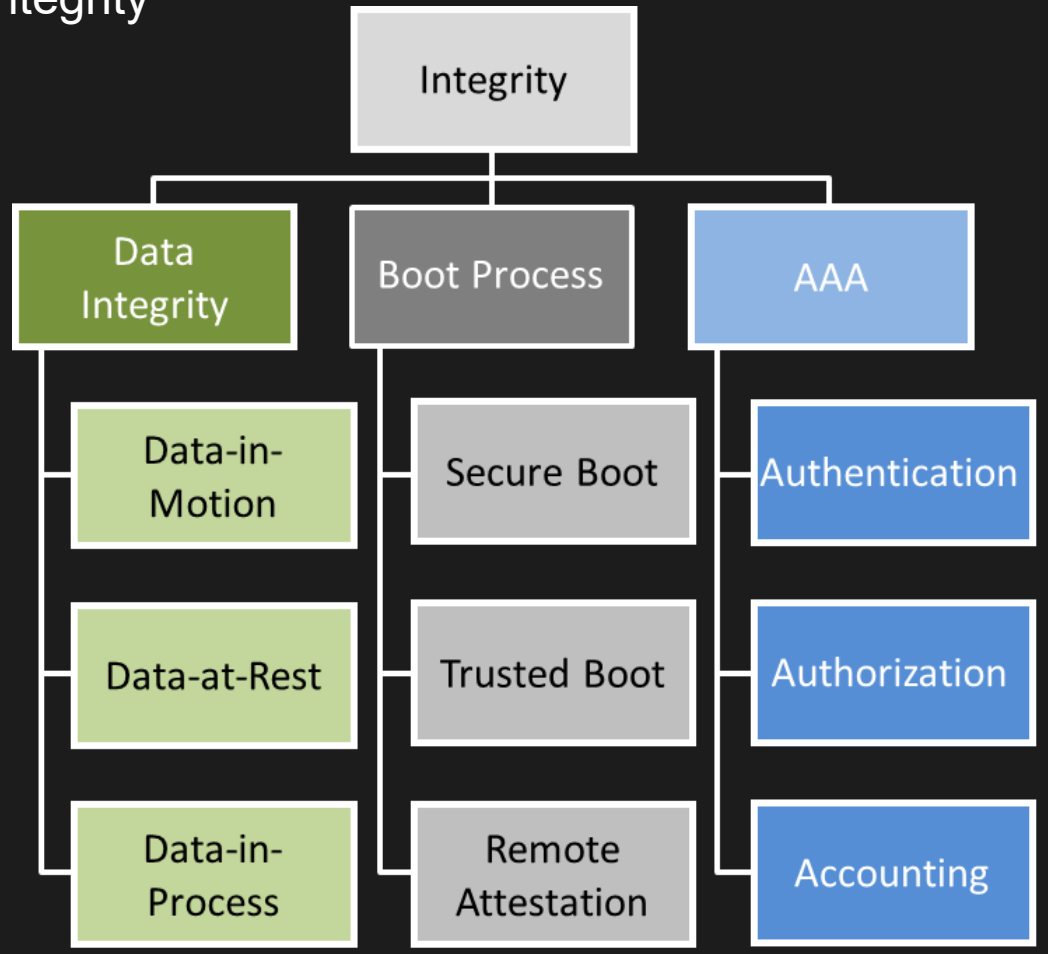


Confidentiality – Others

- It is the key that provides the privacy to the ciphertext
  - Random number generator (RNG)
  - Certification of algorithms (e.g FIPS 140-2 certified module)
  - Establish a secure communication path for key distribution
- Separation
  - Partitioning is used to create enclaves to protect the data within each VM
  - Detect and monitor covert channels that transfer information and violate the system's security policy
- Related Open Source Software
  - haveged/libjitterentropy/Libksba（Key Generation)
  - keyutils/PKI/IKE (Key Distribution)
  - Libvirt/refpolicy-mls/vlan (Partitioning)
  - Iptables (Covert Channels)

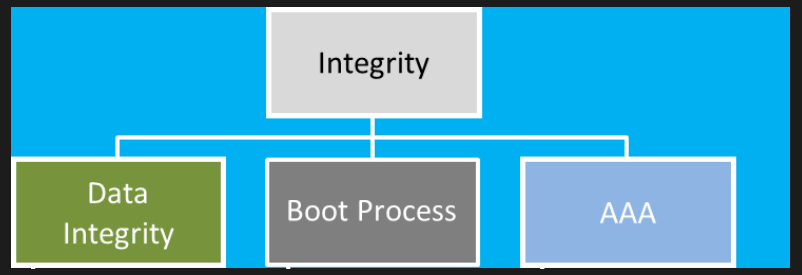
Integrity

- Decomposition of Integrity



Integrity

- Assurance of data is not modified
  - Over a network
  - Stored on the device
  - While being processed



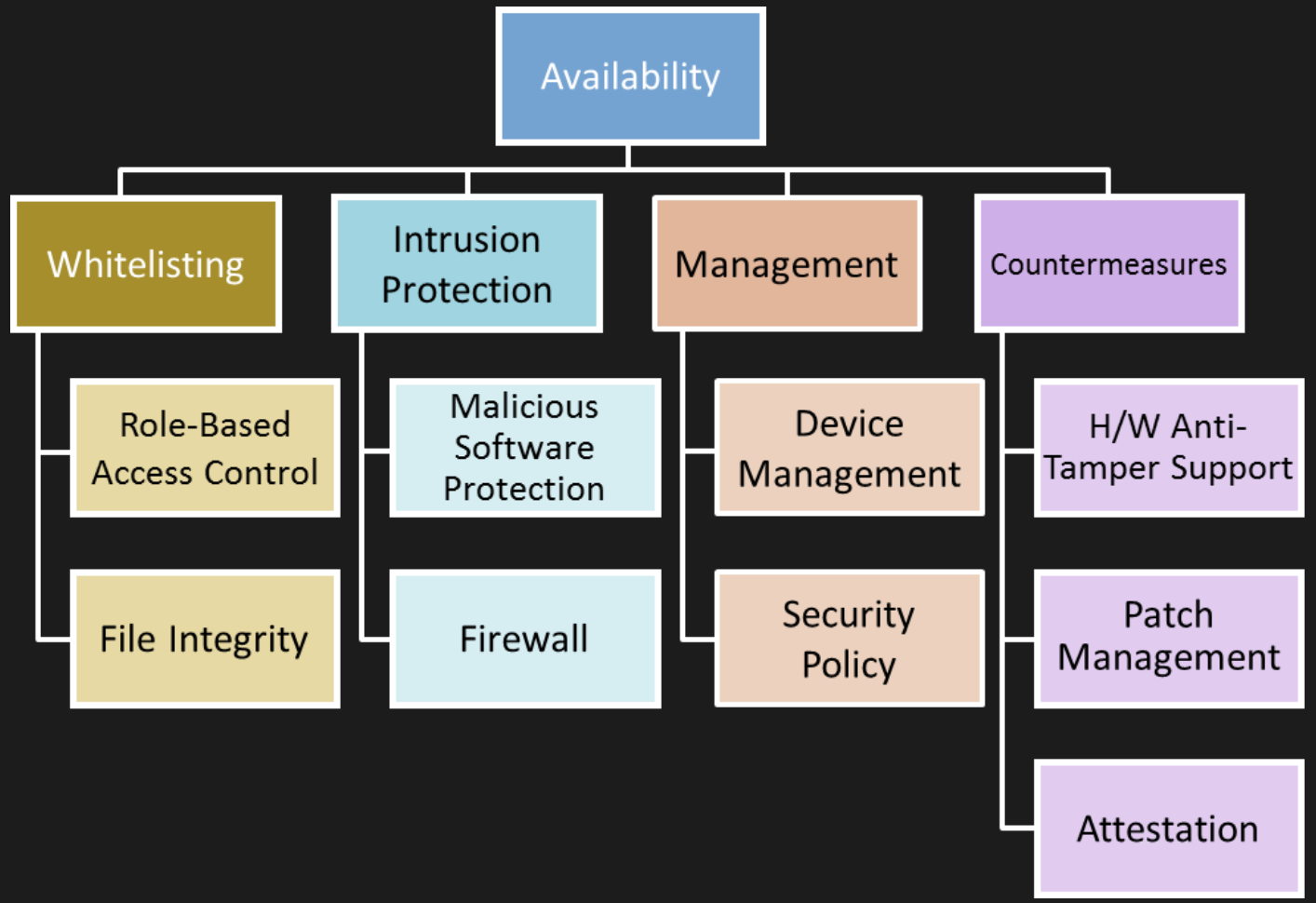
- Know what the device booted
  - Secure boot is purely hardware driven
  - Trusted boot is software driven with hardware assist
  - Remote attestation allows a trusted device to present reliable evidence to remote parties about the software it is running

- Within the device
  - Verification of the process / task / partition making the system call
  - Determination of the request is allowed
  - Logging of security-related events

- Related Open Source Software
  - openssl/anspass/fuse/trousers (Data Integrity)
  - efibootmgr/mokutil/OPTEE/tpm_quote-tools (Boot Process)
  - Libpam/oath/openldap/freeradius/polkit/audit/rsyslog/sysklogd/syslog-ng (AAA)

Availability

- Decomposition of Availability



Availability – Guideline

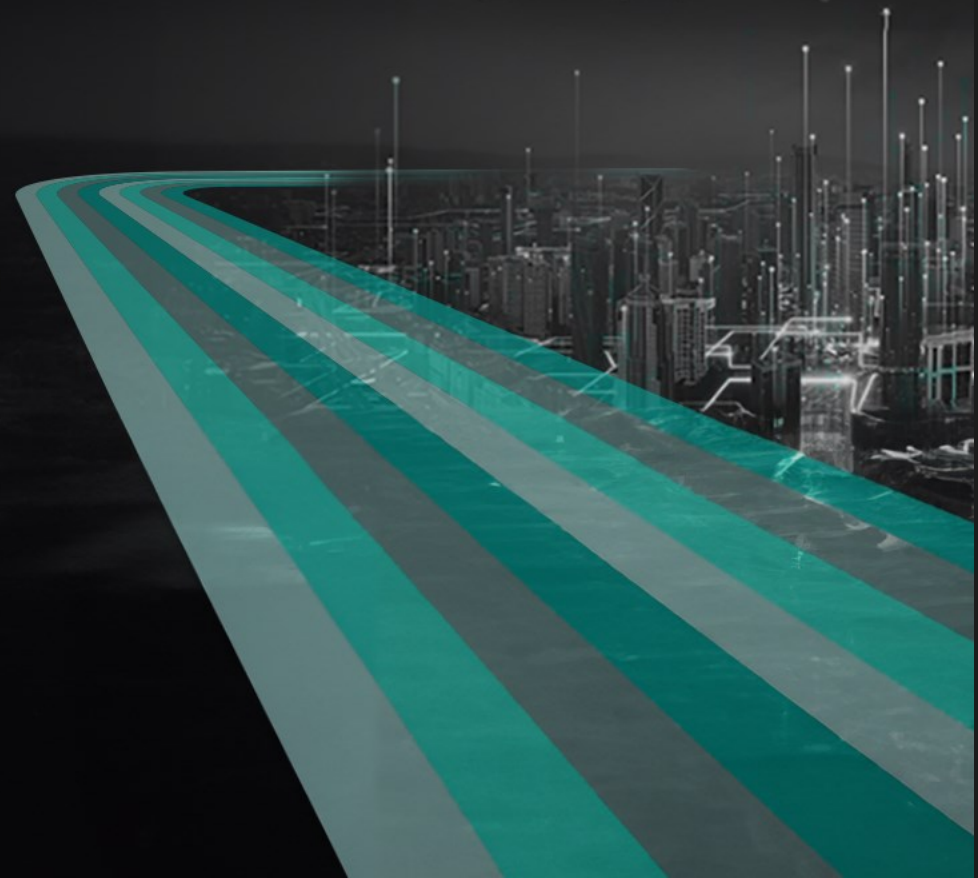
- Use the Principle of Least Privilege
- Use a firewall to block all unused ports, protocols, etc.
- Provide a path to updating the software on the embedded device
- Provide hardened memory protections
- Enable a mechanism to ensure that what is running on the embedded device is what is expected

Availability – Configuration

- WHITELISTING
  - Acl/SELinux/AppArmor/IMA
- INTRUSION PROTECTION
  - Detection & Prevention
  - Ebtables/iptables/Samhain/snort
- MANAGEMENT
  - Active control and analysis of domain controllers
  - Software updates/Security Audit Log analysis/Security Policy updates
- COUNTERMEASURES
  - An action taken to reduce or neutralize a danger or threat
  - Dnf/docker/mcelog/Zabbix/nagios

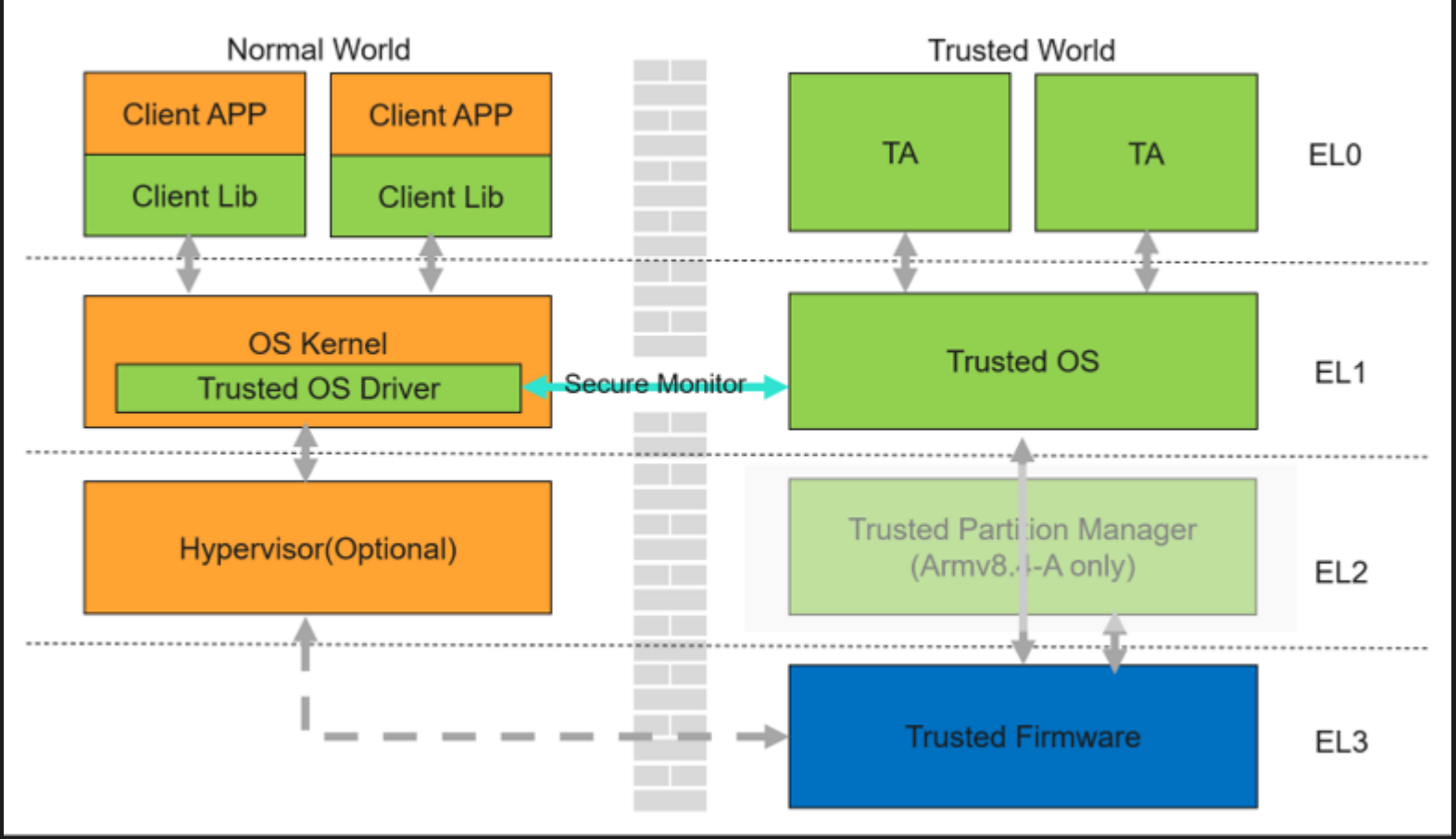
Use Cases

- OPTEE
- SELINUX
- CVE

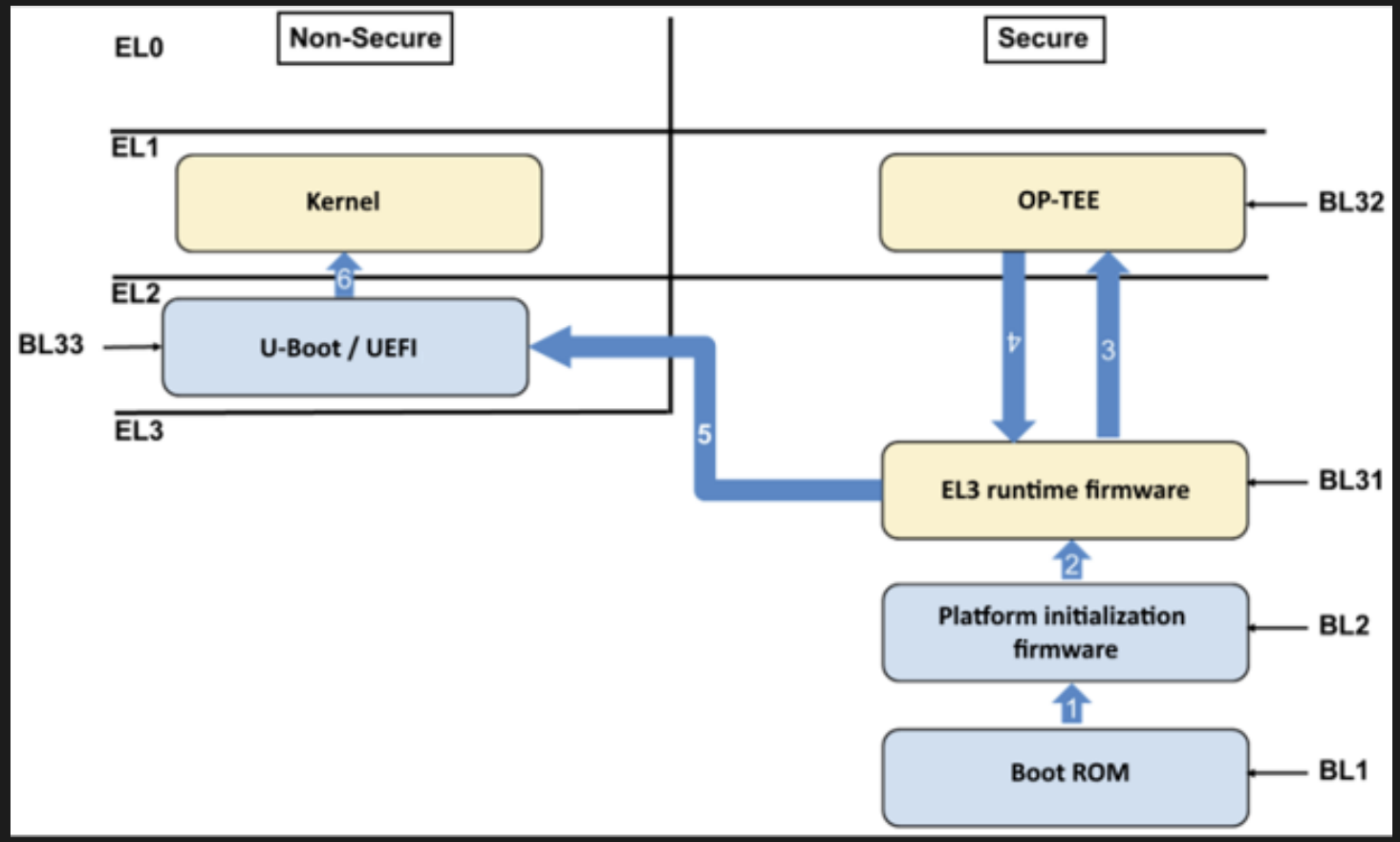


OPTEE

- OS Kernel: Wind River Linux/ Trusted OS: OPTEE (Open Portable Trusted Execution Environment)

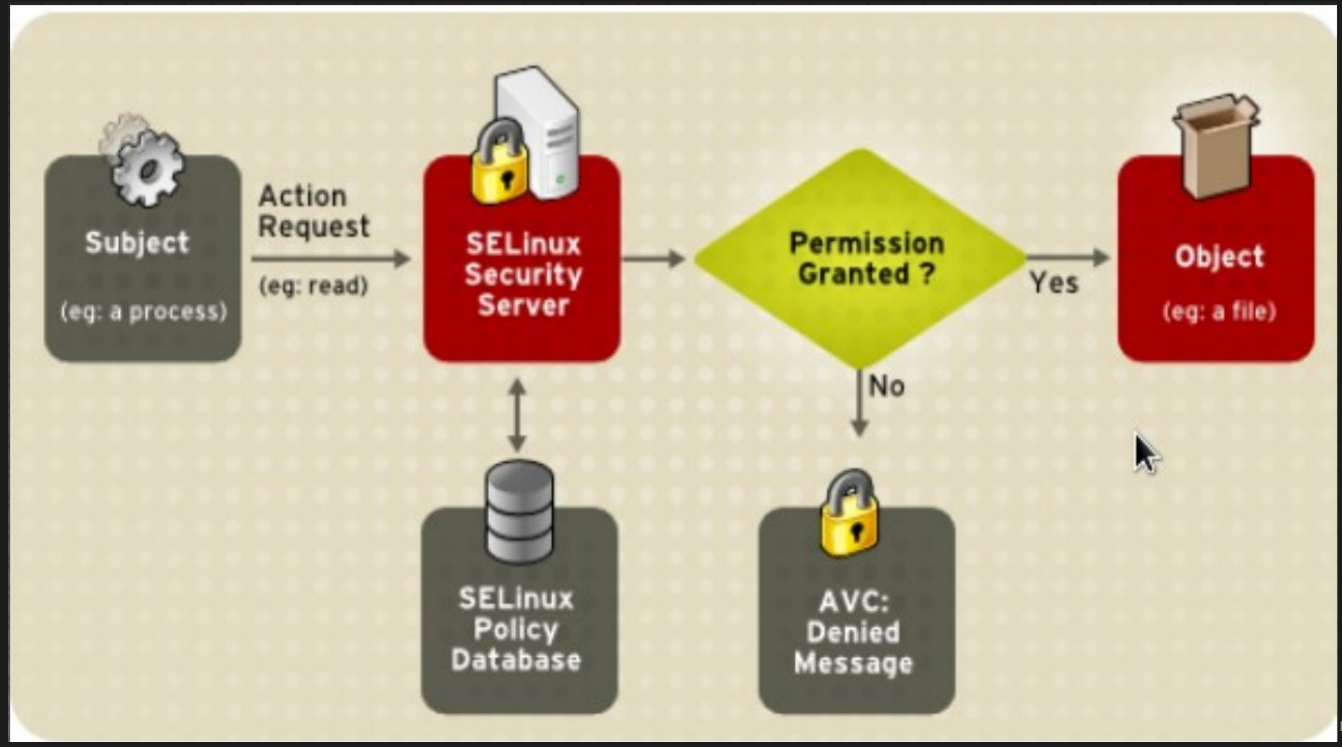


OPTEE BOOTUP

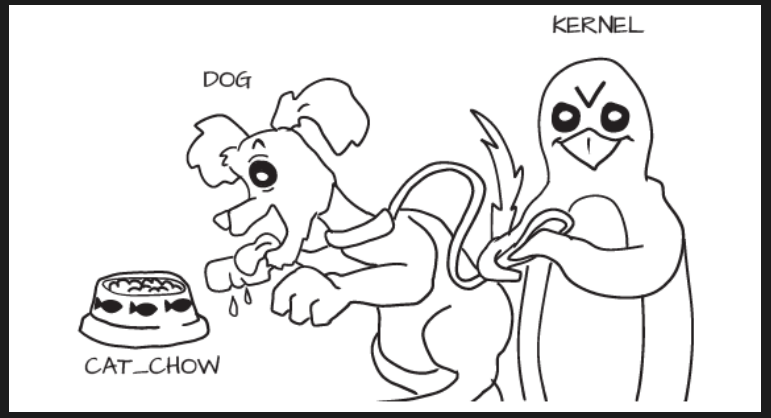


WHAT IS SELINUX

- A labeling system
- Every subject (process/user) has a label
- Every object (files, directories, network ports, ipc, process etc.) on the system has a label
- The SELinux policy controls how process/user labels interact with other labels on the system
  - Denied if not specific rule defined
  - Label = security context
  - USER:ROLE:TYPE:LEVEL
  - system_u:system_r:haval_t:s0-s15:c0.c1023
- The kernel enforces the policy rules.



POLICY RULES



- Statement: COMMAND SOURCETYPE TARGETTYPE:CLASS PERMS;
  - allow staff_t etc_t:file { open read getattr ioctl lock};
  - Read: allow process labelled with staff_t type to open/read/.. files labelled with etc_t type
  - Also call Type Enforcement
- COMMAND
  - allow, dontaudit, auditallow, neverallow ..
- CLASS
  - file, dir, sock_file, tcp_socket, process ..
- PERMS
  - read, open, write ..
- SOURCETYPE/TARGETTYPE
  - Defined as needed =>
- m4 macro language

```
########################################
#
# Declarations
#

type haval_t;
type haval_exec_t;
init_daemon_domain(haval_t, haval_exec_t)

#permissive haval_t;

########################################
#
# haval local policy
#
allow haval_t self:fifo_file rw_fifo_file_perms;
allow haval_t self:unix_stream_socket create_stream_socket_perms;
```

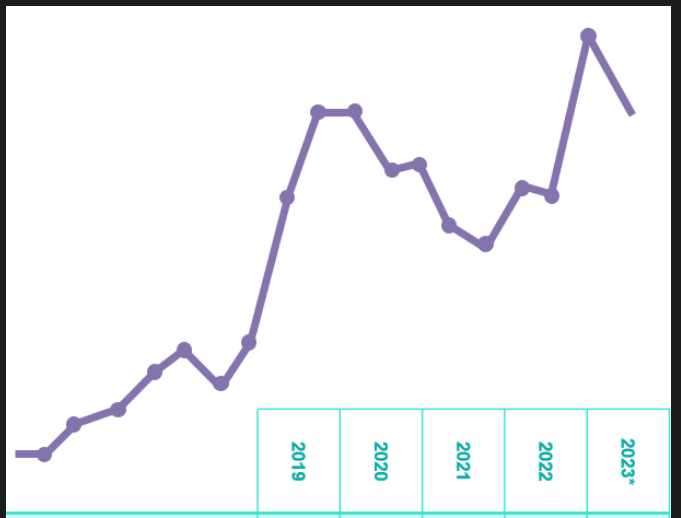
WRL LTS SELINUX

- Policy source
  - RELEASE_2_20210203 https://github.com/SELinuxProject/refpolicy/tree/RELEASE_2_20210203
  - +Yocto patches: https://git.yoctoproject.org/meta-selinux/tree/recipes-security/refpolicy/refpolicy?h=hardknott
  - + WRL patches: ./layers/wrlinux/wrlinux-distro/dynamic-layers/selinux/recipes-security/refpolicy/refpolicy-wr
- SELinux Policy Types
  - refpolicy-mls (default) => 408 modules, TE+MLS
  - refpolicy-standard => 408 modules, TE
  - refpolicy-minimum => 26 core modules, subset of refpolicy-mls, TE+MLS
  - refpolicy-targeted => 408 modules as refpolicy-mls, only constrain service domains, unconfined for login users
- Policy name => check sestatus

```
root@qemuarm64:~# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             wr-mls
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested (insecure)
Max kernel policy version:      33
```

CVE (Common Vulnerabilities and Exposures)

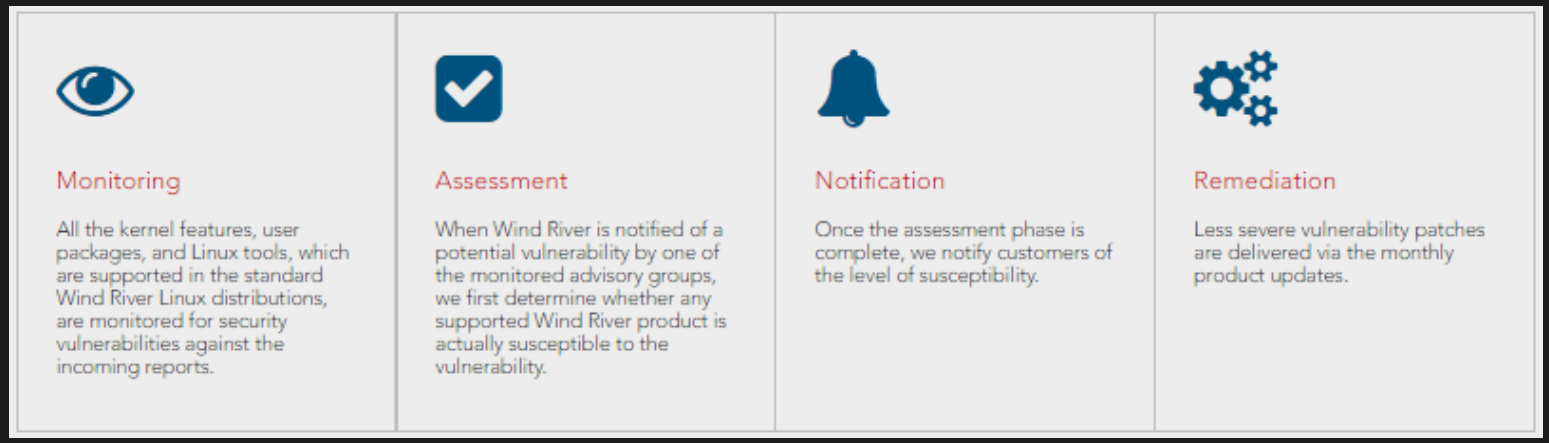
- Exported vehicles require security scanning
  - Blackduck/tencent security/360 security
- Product Security Incident Response Team (PSIRT)



	2019	2020	2021	2022	2023*
Monitored	17788	18551	20277	25191	link
Assessed as non-vulnerable	17356	18002	19357	24820	link
Investigated and notified	1139	929	1288	2020	link
Delivered fixes	805	576	765	1102	link

* Click the links for latest data. Source: Wind River CVE Database

What we do for standard products that are active!!



WNDRVR

Summary

- More connected vehicles, more concerns on security in vehicles
- CIA (Confidentiality, Integrity, Availability) is golden standard to analyse and enforce automotive security
- Wind River Linux follows CIA Triad to implement and harden security for intelligent ECU controllers in vehicles
- Wind River gathers strong security capability in serving AUTO customers in the journey toward developing secure and safe vehicles

WNDRVR