# BGSW- SJCE Academy Connect

## Secure Logging overview

Naveen Kumar S H

Bosch
Global
Software
Technologies
alt_future

# Security Features overview

## CIA - RECAP

### Confidentiality

Confidentiality mechanism guarantees the secrecy of the transmitted information by guaranteeing that the message isn't unveiled to an unapproved client/user.

### Availability

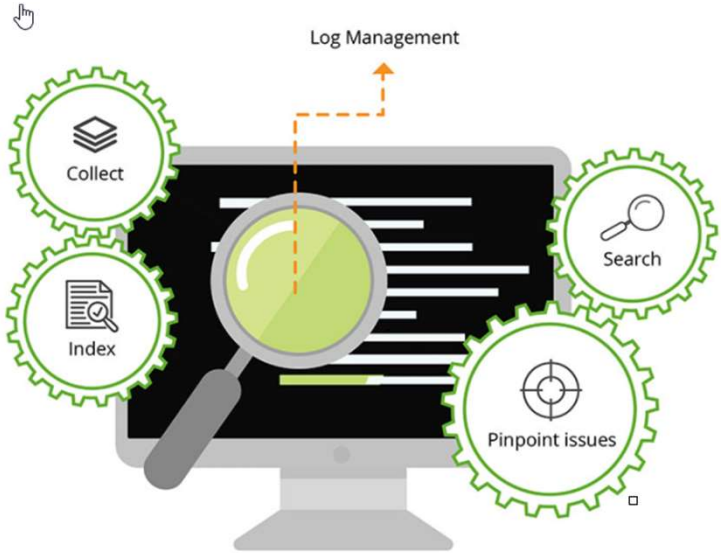
Availability ensures information assets such as session key and applications are accessible by the authorized users.


### Integrity

Integrity assurance (often also referred as data integrity) of a message provides the receiver with an assurance that the data has not been modified during transmission.

# Secure Logging

## High level view




Generally, logging systems store events and information to enable an analysis at a later time . Logging systems storing security related events may be used to:

1. Detect if a system has been compromised
2. Identify and analyze how the system got compromised
3. Retrace what the attacker did

# Secure Logging

## Secure monitoring

Security monitoring: Keeping an eye on the fleet

No matter how high the level of protection against cyberattacks established during development, it will inevitably diminish over the course of the vehicle's service life. For that reason, vehicles and vehicle fleets will require an active, ongoing security approach in the future, one that monitors known risks and attack vectors and also identifies and mitigates new risks. Especially because when UN regulation R155 comes into force, type approval will become contingent upon furnishing proof of appropriate risk management throughout the vehicle lifecycle..

Obtaining a meaningful picture of the overall threat situation requires examination of several areas and action on several levels. Two key components are necessary: first, embedded in-vehicle attack detection in the form of an intrusion detection system (IDS); and second, a vehicle security operations center (VSOC) in the backend, where the attacks are aggregated and evaluated to prevent scaling of attacks across the entire fleet.

# Secure Logging

## Intrusion detection system (IDS)

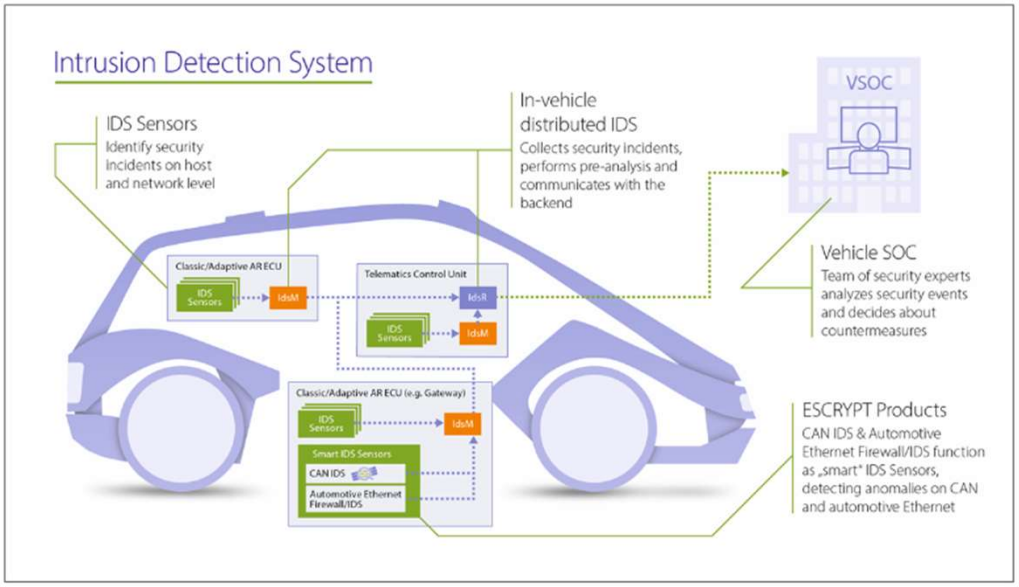
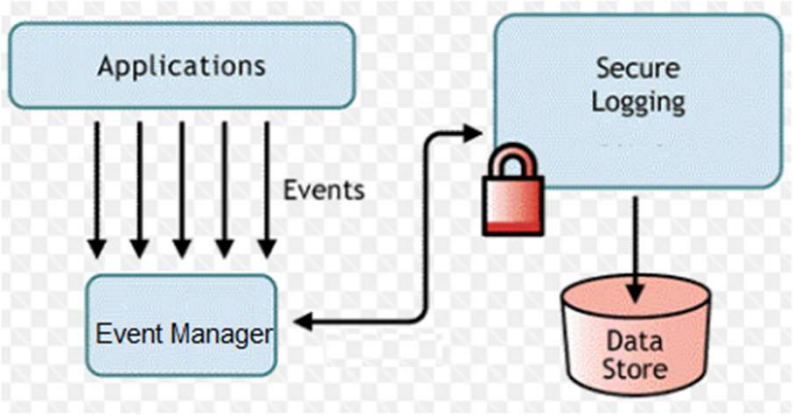



Figure 1: Distributed system for intrusion detection in the vehicle – from the IDS sensor to the IDS manager to the IDS reporter.

Truly effective security monitoring calls for attack detection that is embedded deep in the distributed system. In particular, to detect local attacks on a specific vehicle, intrusion sensors – integrated into the E/E architecture of the individual vehicle – are indispensable. As a result, two important tasks emerge: first, investigate right from the vehicle development stage what potential vulnerable points could exist in the E/E architecture; and second, incorporate this knowledge into a consistent monitoring concept based on a distributed intrusion detection system (IDS) in the vehicle's internal network.

# Secure Logging

## Summary




Safety and security relevant events are stored securely. The stored event entries are protected against any further manipulation and against unauthorized read-out.

*Secure Logging* may also provide protection against unauthorized read out to make reverse-engineering and future attacks more difficult. If attackers do not know what is logged, it is more difficult for them to find out.

The logging mechanisms and the logged data should be protected against unauthorized manipulations to avoid false claims.

# Secure Logging

## References

UDS – Automotive & Embedded Info (wordpress.com)

Security monitoring: Keeping an eye on the fleet | ESCRYPT

# Thank you!

Bosch
Global
Software
Technologies
alt_future