THALES

A Systematic Approach to Securing Automotive Systems

Stuart Soltysiak and Pali Surdhar

Introduction

The evolution of the car into a connected vehicle is presenting the automotive industry with similar challenges to the Internet of Things (IoT)

- Distributed ecosystem of vehicles, infrastructure and other processing Things
- Data collection, collation and communication by Things with each other and back-end data systems
- Much of the collected data can be considered sensitive – from many perspectives:
  - Vehicle safety and performance
  - Personally Identifiable Information
- Reliance on cloud infrastructures to support scalability and performance for data processing
- Multiple and disparate sources for creation and supply of components

It is therefore ever more important that security is considered from a complete systems perspective

- Essential to have trust for the protection of data
  - At rest
  - In transit
  - Undergoing processing

Automotive Industry

The automotive industry has several important aspects that affect security:

- Long lifespan of systems in service
- Long lead times to deliver new features/platforms into service
- Cost efficiency
- Complex supply chain
- IoT like architecture
- Increasing dependence on software
  - On board
  - Infrastructure (Cloud, Mobility solutions)

Software continues to eat the world - major disruptors

- Electric cars
- Connected cars
- Connected services
- Vehicle becomes a platform – laptop on a car

Supply Chain Issues

There is a complex supply chain to take into account

- Many suppliers per manufacturer
- Connected car technologies expand the supply chain beyond the vehicle to include the supporting IT systems (in their entirety – cf. system lifecycle considerations)
- Recent report indicates only 10% of suppliers worry about security[1]
- Vulnerabilities in a supplier component are exploitable across large product range – it is worse than a localised safety problem
- Suppliers and manufacturers have a shared responsibility for security – now acknowledged by UK Government guidance[2]

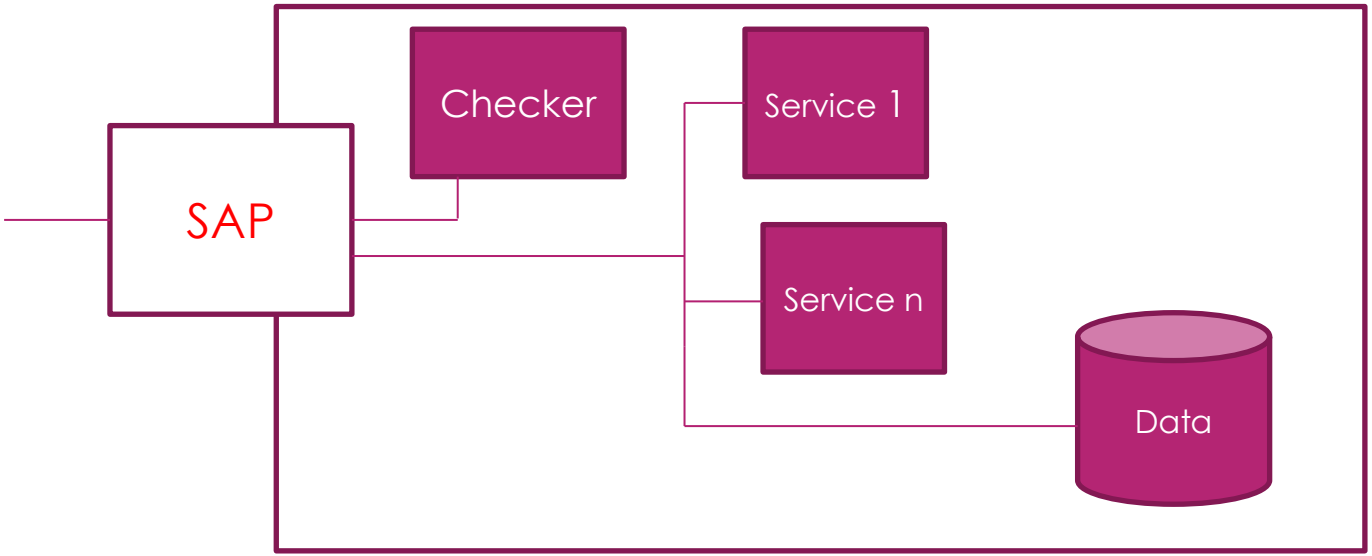
1. C. Bordonali, S. Ferraresi & W. Richter: Shifting gears in cyber security for connected cars. McKinsey & Company, February 2017
2. UK Government Guidance "The key principles of vehicle cyber security for connected and automated vehicles", 6 August 2017

Design Considerations

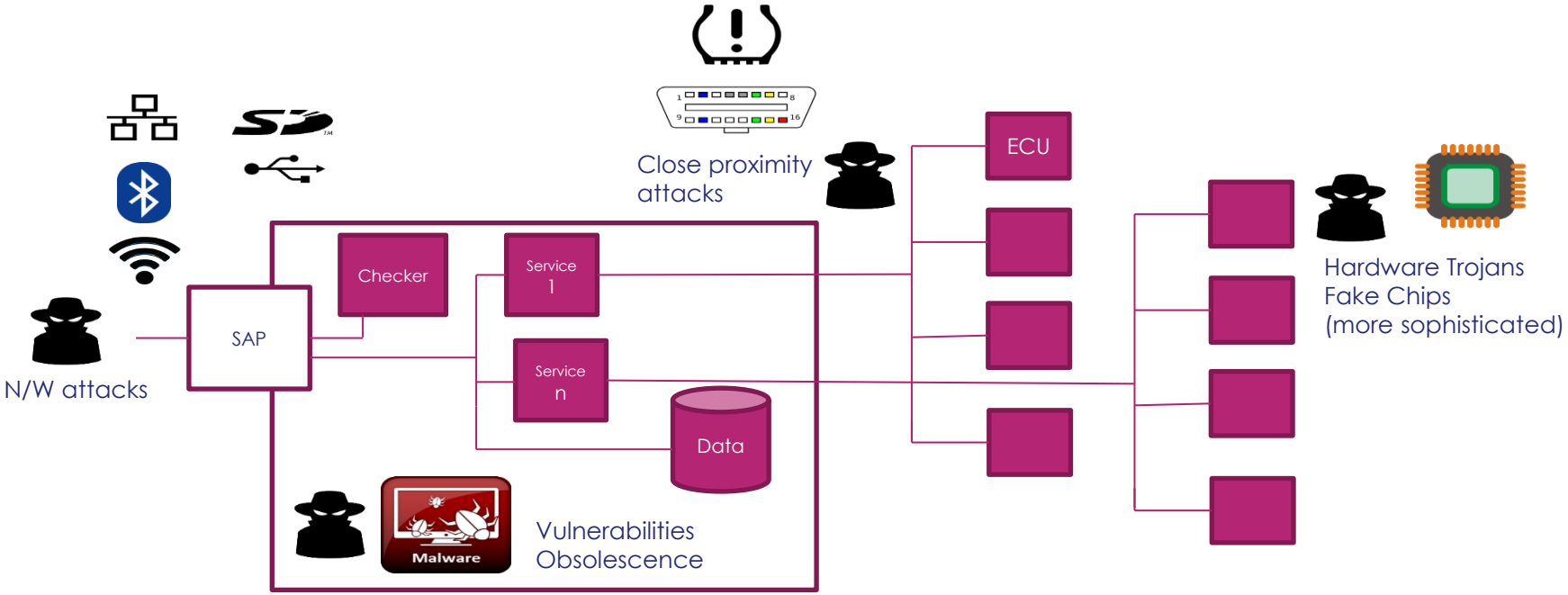
- The need for a holistic approach to security
- Security boundary
- Root(s) of Trust
- Open source software
- Design for update
- Newer architectures
  - Virtualisation – how long until ‘Docker in car’?
  - Orchestration
- Support for mobility

Traditional Security Patterns

Single Access Point and Checker



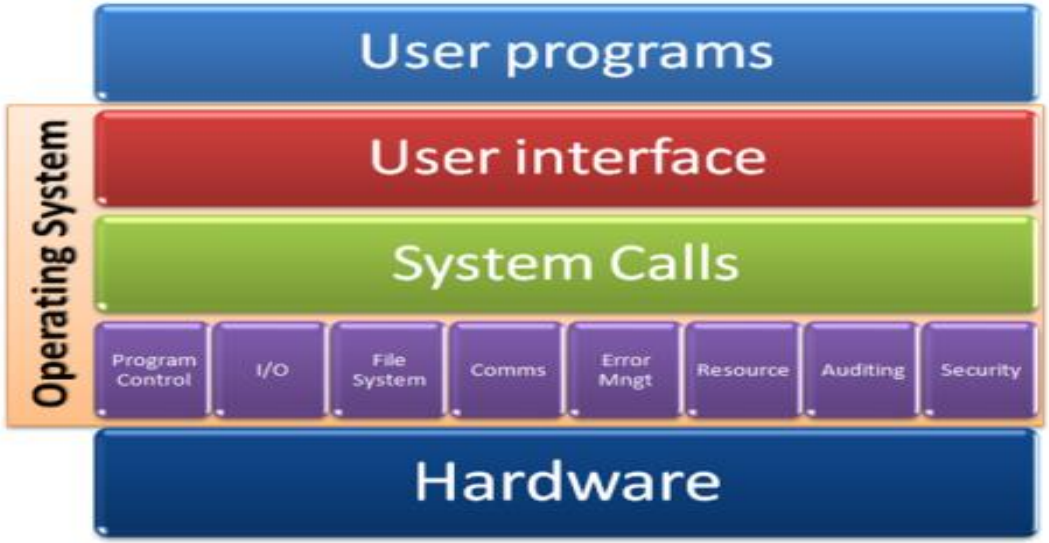
Threat Landscape



OPEN

THALES

Full Stack Security



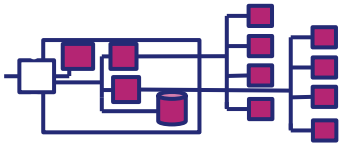
Access controls
Audit and Monitoring

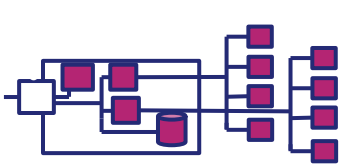
Privileges
Stack Protection
Shared Code
Crypto
Stored Data

Entropy source
Emissions
Firmware Integrity

Attack One, Attack All?

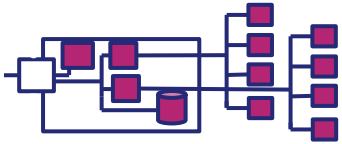
Consumer Applications
PII
Aggregation



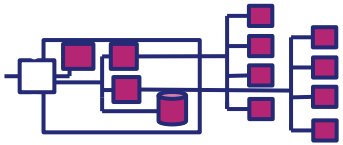


H/W + S/W
attacks

Supply Chain
Provider Trust
Third Party Code



Supply Chain



OPEN

THALES

Countermeasures?

The need for a holistic approach to security

Start with understanding the system

OPEN

THALES

System Security Analysis – Overview

Pragmatic approach aligning security modelling with systems modelling

Full system context: functional behaviour and operational process views

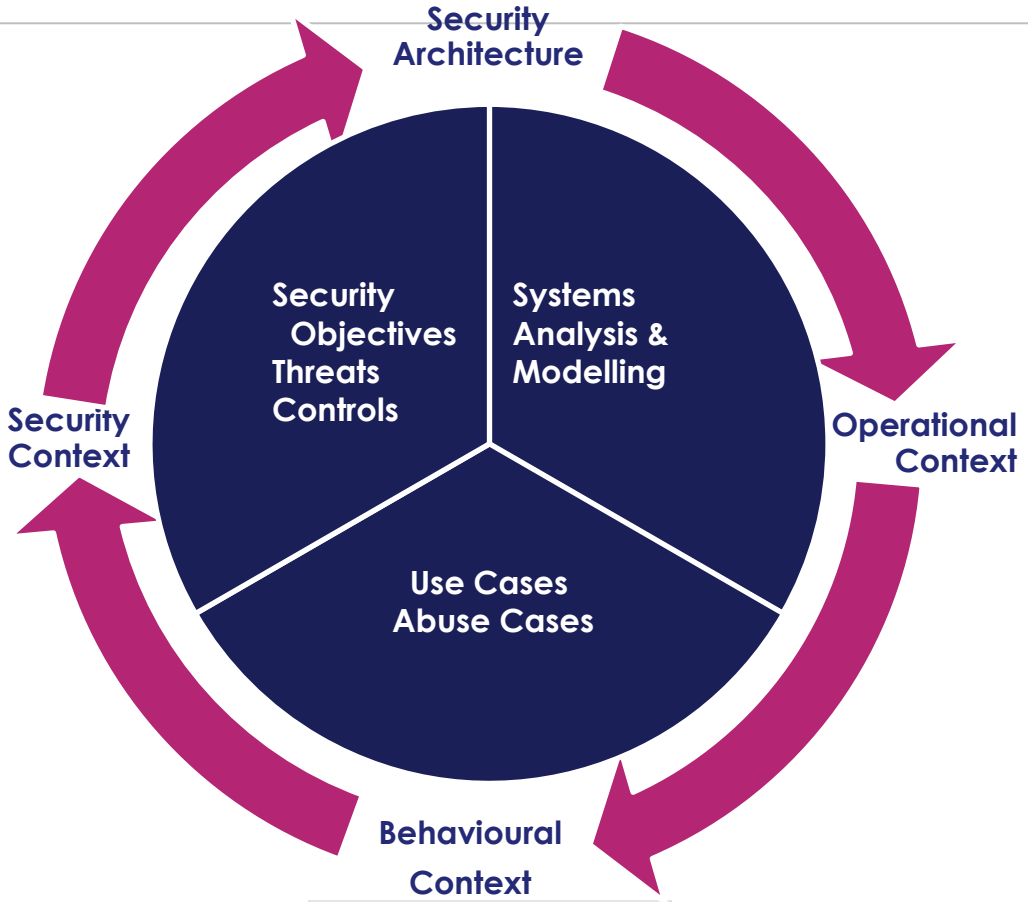
Iterative approach, identifying

- Key system elements and interactions
- Security objectives
- Threats and controls

Underpinned by use of a modelling tool

- Incremental refinement of underlying systems and security models
- Builds re-usable domain-specific threat intelligence
- Supports security accreditation

Systematic Approach to Security



OPEN

THALES

Attack One, Attack All?

Malicious Code Protection

Consumer Applications
PII
Aggregation

User Identification & Authentication

Device Identification & Authentication

Service Identification & Authentication

H/W + S/W attacks

Separation of Duties

Least Privilege

Supply Chain
Provider Trust
Third Party Code

Cryptographic Key Establishment & Management

DoS Protection

Trusted Path

NW attacks

Transmission Confidentiality & Integrity

IS Monitoring Tools & Techniques

Available on the App Store

Personnel Security Policy

Security Awareness & Training

Secure Development Lifecycle

Application Partitioning

Supply Chain

Baseline Configuration

Configuration Change Control

Component Authenticity

Access Control Policy

Physical & Environmental Protection

Maintenance Policy & Procedures

Audit Monitoring, Analysis & Reporting

Benefits of a Systematic Approach to Security

Higher quality of system security:

- A structured framework in which to explore the security landscape of a system – preventing ad-hoc or patchy analysis

Effective demonstration of system security coverage:

- The model provides a powerful basis for formal and informal security analysis. We can easily review whether security objectives are met and to what extent threats are mitigated by the implemented controls

Knowledge transfer and education:

- Developing the model with all engineers grows security knowledge and skills across all engineering disciplines; it builds a security mindset into the early phases of the development lifecycle

Longer-term commercial benefit:

- Artefacts and knowledge generated by development of the model can be re-used to evaluate changes in the environment, system functionality or deployment – removes the need for bespoke security analysis activities

Compliance:

- Threats and controls aligned with standards (e.g. ISO 27005, OWASP, NIST Controls, Open Security Architecture, Cloud Security Alliance) allows coverage and compliance to be reviewed easily, and provides supporting evidence for system certification and assurance activities

Thankyou

We welcome your questions and feedback