Security-Aware Modeling and Analysis for HW/SW Partitioning

Letitia W. Li, Florian Lugou, Ludovic Apvrille
Embedded System Security

We can also open the door (by using the laptop) without the car key of Tesla.
SysML-Sec Methodology

Requirements

Assumptions

Attacks

Simulation Formal analysis

Simulation Formal analysis

Simulation Formal analysis

Functional view

Architectural view

Mapping view

SW/HW Partitioning

Use case view

Scenario view

SW Analysis

Structural view

Behavioral view

SW Design

Test

Deployment view
Secure HW/SW Partitioning

- Functional View
- Architecture
- Security Requirements
- Attacker
- Architecture'
- Mapping
- Functional View'
- Mapping'
- Safety/Security/Performance Evaluation
Drone Architecture

<<BUS-RR>>
Wifi

<<CPURR>>
CPUDrone

Drone::Camera
Drone::motorControl
Drone::IR

<<BUS-RR>>
BusDrone

<<MEMORY>>
MemoryDrone

<<CPURR>>
CPURemote

Drone::RemoteControl
Drone::ImageProcessing
Drone::MainController

<<BUS-RR>>
Bus0

<<MEMORY>>
MemoryRemote
Security Mechanisms
Cryptographic Configurations

- Tag indicating presence of encryption
- Operate on tagged channel
- Occupies computation time in simulation
Automatic Generation

- Time-saving and convenient
- Suggestion of basic encryption for user to enhance
- Addition of Nonces, Encryption
Unsecured Model

Camera

- captureImg
- imgData(10)

Drone Control

- missionCmd(1)
- obsData(1)
- calcStatus
- calcTraj
- motorCmd(1)
- targetData(1)
- checkArea(1)
- scanResults(1)

- calcTarget

Secured Model

Camera

- **nonceChlIP_Cam(1)**
  - chl captureImg
  - sec:nonce_IP_Cam
    - SE CC:enc_imgData
    - chl imgData(10)
      - CC:enc_imgData

Drone Control

- **missionCmd(1)**
  - chl
  - missionCmd(1)
    - [ ] [ ]
  - obsData(1)
    - chl calcStatus
    - calcTraj
    - calcTarget
    - checkArea(1)
      - motorCmd(1)
      - scanResults(1)
Performance

~1800 cycles

BUS-RR: 1%

CPURR: 52%

CPUR: 48%

BUS-RR: 0%

BUS-RR: 4%

CPURR: 52%

CPURR: 48%

CPURR: 0%

CPURR: 4%

Memory: 0%

Memory: 0%

Memory: 0%

Memory: 0%

Wifi

Drone::IR

Drone::Camera

Drone::motorControl

Drone::DroneControl

Drone::RemoteControl

Drone::ImageProcessing

Drone::BusDrone

Drone::Bus0

MemoryDrone

MemoryRemote
Performance with Added Security

~3400 cycles

<<BUS-RR>>
Wifi

<<CPURR>>
CPUDrone
Drone::IR
Drone::Camera
Drone::motorControl

<<BUS-RR>>
BusDrone

<<MEMORY>>
MemoryDrone

<<CPURR>>
CPURemote
Drone::DroneControl
Drone::RemoteControl
Drone::ImageProcessing

<<BUS-RR>>
Bus0

<<MEMORY>>
MemoryRemote
Security Analysis
Mapping Model

Intermediate Specification

Basic Blocks

Proverif Code

Results

Backtracing to diagrams

Model Transformation for Security

Lugou Modelsward2016

15

Institut Mines-Télécom

2/27/17

Modelsward 2017
Verification of model

ImageProcessing
+ processImg : Natural;

Camera
+ captureImg : Natural;

Drone::IR

Drone::Camera

Drone::motorControl

DroneControl
+ calcTraj : Natural;
+ calcStatus : Natural;
+ calcTarget : Natural;

obsData

targetData

nonceChIP_Cam

imgData

Camera
+ captureImg : Natural;

Drone::MainController

Drone::RemoteControl

Drone::ImageProcessing

<CPURR> CPUDrone

<BUS-RR> Wifi

<CPURR> CPURemote

Drone::IR

Drone::Camera

Drone::motorControl

missionCmd

droneData

MotorCommand
+ motorControl : Natural;
+ filterCommand : Natural;

RemoteControl
+ processData : Natural;
+ calcMission : Natural;

IR

+ process : Natural;
+ runScan : Natural;

scanResults

checkArea

Mapping 2

Mapping 2
Verification of Secured Model
Conclusion

- Modeling and verification of secure architectures
- Evaluation of security and impact of security on performance
- Automatic generation to secure critical communication
- Future support of code integrity, firewalls...
Questions?

Our work at:

ttool.telecom-paristech.fr
sysml-sec.telecom-paristech.fr