From Requirement to Standard Security Test
A brief introduction to the world of security testing

Christian Folda (Test Architect)
## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Cyber Security Introduction</td>
</tr>
<tr>
<td>3</td>
<td>Security Testing Introduction</td>
</tr>
<tr>
<td>4</td>
<td>Example</td>
</tr>
</tbody>
</table>
Since 1871 with headquarters in Hanover, Germany
Sales of €44 billion
235,473 employees worldwide
554 locations in 61 countries

Sales by division in %
- Chassis & Safety: 22%
- Tires: 26%
- Interior: 21%
- Powertrain: 17%
- ContiTech: 14%

Status: December 31, 2017
# Continental Corporation
## Five Strong Divisions

<table>
<thead>
<tr>
<th>Chassis &amp; Safety</th>
<th>Powertrain</th>
<th>Interior</th>
<th>Tires</th>
<th>ContiTech</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle Dynamics</td>
<td>Engine &amp; Drivetrain Systems</td>
<td>Instrumentation &amp; Driver HMI</td>
<td>PLT, Original Equipment</td>
<td>Air Spring Systems</td>
</tr>
<tr>
<td>Hydraulic Brake Systems</td>
<td>Hybrid Electric Vehicle</td>
<td>Infotainment &amp; Connectivity</td>
<td>PLT, Replacement Business, EMEA</td>
<td>Benecke-Hornschuch Surface Group</td>
</tr>
<tr>
<td>Advanced Driver Assistance</td>
<td>Contract Manufacturing</td>
<td>Commercial Vehicles &amp; Aftermarket</td>
<td>PLT, Replacement Business, APAC</td>
<td>Industrial Fluid Solutions</td>
</tr>
</tbody>
</table>

---

PLT – Passenger and Light Truck Tires
Interior Division
Our Business Units & Product Portfolio

Instrumentation & Driver HMI
- Instrument clusters
- Full digital clusters
- Integrated Interior Platform
- Display solutions
- Head-up displays
- Haptic controls
- Interior camera

Infotainment & Connectivity
- Radios
- Infotainment
- Connectivity & telematics
- Software & connected solutions

Body & Security
- Body control modules
- Access control systems
- Power closures
- Door control units
- Intelligent Glass Control
- Seat comfort systems
- Tire information systems
- Gateways
- Power stabilization
- Lighting control units
- Advanced antenna electronics
- Smart device Integration

Commercial Vehicles & Aftermarket
- Tachographs and telematics
- Visual and haptic human-machine interface
- Chassis, body and transmission electronics
- Spare parts, wear parts and tools
- Original equipment services
- Services and diagnostics for the independent aftermarket, fleets and vehicle manufacturers
- Key as a Service
- In-Car Data as a Service
- eHorizon as a Service
- City-Data as a Service
## Agenda

1. Introduction
2. Cyber Security Introduction
3. Security Testing Introduction
4. Example
Cyber Security Introduction

Definition Cyber Security

"Cybersecurity, computer security or IT security is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators, whether intentional or accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods."
New threats, new needs…

Out-of-Vehicle

Minor crimes
Car theft
Invasion of privacy
Compromise safety

Inside Vehicle

Prevent
Understand
Respond

Holistic Security Concept

ARGUS CYBER SECURITY

ARGUS

03-Apr-2019
C. Folda © Continental AG
Cyber Security Introduction

Attack Vectors

- Physical Access
  - Long-Range Wireless Access
  - Short-Range Wireless Access
  - Remote Attack Interfaces
  - In-Vehicle Attack Interfaces

- Indirect Physical Access
  - Distance

From Requirement to Standard Security Test
Public
03-Apr-2019
C. Folda © Continental AG
Cyber Security Introduction

Threats & Security Measures on ECU

- Disable software functions
- Manipulate keys
- Manipulate software
- Inject wrong key
- Eavesdrop message
- Unauthorized diagnosis access
- Disturb communication
- Unauthorized software update
- Steal software
- Extract secret keys
- Manipulate messages
Cyber Security Introduction

Threats & Security Measures on ECU

- Eavesdrop message
- Disturb communication
- Steal software
- Extract secret keys
- Manipulate messages
- Unauthorized software update
- Unauthorized diagnosis access
- Inject wrong key
- Manipulate keys
- Disable software functions
- Manipulate software

Confidentiality
- Steal Software
- Eavesdrop message
- Extract secret keys

Integrity
- Manipulate Software
- Manipulate messages
- Manipulate keys

Authenticity
- Unauthorized software update
- Inject wrong key
- Unauthorized diagnosis access

Availability
- Disturb communication
- Disable software functions

Confidentiality
- Integrity
- Authenticity
- Availability
Agenda

1. Introduction
2. Cyber Security Introduction
3. Security Testing Introduction
4. Example
Security Testing Introduction

Why Security Testing

Intended Behavior
Security Testing Introduction
Why Security Testing

Implemented Function of an ECU

Intended Behavior

Missing or Incorrect Functionality
Security Testing Introduction
Why Security Testing

- Missing or Incorrect Functionality
- Side-Effect Behavior
- Implemented Function of an ECU
- Intended Behavior
Security Testing Introduction

Goals of Security Testing

› Define the Level of Security for the Project
  › What are the attacker Profiles
  › What are the Security assets
  › ...
› There is no 100% Security!
› Fleet Attacks should be prevented
› The Goals of Security Testing:
  › ensure that chosen Level of Security is reached
  › Test for known Attacks on used technologies
  › Detect unwanted side behavior or Vulnerabilities

SRC: Screen from Zimperium presentation video “Xiaomi Scooter Hack”
https://youtu.be/ASygXa8UVYk
Security Requirements
Origin of Requirement

Classic Project Requirements
- Sources: Stakeholder requirements, TARA results, security measures
- Ex: „The product must be secure against „CAN ID 0 DoS“

Research
- Sources: conferences, articles, security research
- General research results from public or private research facilities on general or specialist topics
- Includes also “well known” attacks
- Ex: HSM Chip Security, Heartbleed, Spectre …

Incidents
- Sources: Incidents in the Automotive - or IT Market, Penetration Test Reports, CVE’s
- Successful attacks in the Automotive and IT Market, Company related incident report
- Ex: Internal Pentest reports, Used chip get’s cracked, Used cryptography get’s cracked
Security Requirements
Forging a Requirements Set

› Goal: All the requirement sources described must be translated into a consistent set of requirements.

1. Select all matching Requirements (filter)
2. Remove Duplicates
3. Apply the Requirements
Security Testing
Definition of Test Types

Penetration Test
- The classic Penetration Test
- Performed by a company external or Project independent Team
- Highly skilled Tester
- Creative Testing with 'loose' definition of Scope
- Mostly done at the end of the Development or after big releases
- Validates the Test Process and Verifies the product Security

Standard Security Test
- An 'in between' of classic Testing and Penetration Testing
- Performed during Development in the normal Test process
- Very clear defined Test Cases/Test Scripts for testing
- Can be executed by "normal" Test Engineers
- Checking for generally known Vulnerabilities, Implementation errors
- Verifies the Product Security
Security Testing
Why Standard Security Test

Consistent Quality
Reduce Scope in Pentest
Automated Testcases
Executed in The Project
Fail Faster
Security Testing

Security Testing Process

Development Process without Security Testing

Development Process with Penetration Testing

Development Process with Standard Security and Penetration Testing

From Requirement to Standard Security Test

Public

03-Apr-2019

C. Folda © Continental AG
Security Testing
Conclusion

- Missing or Incorrect Functionality
- Side-Effect Behavior

Implemented Function of an ECU

Intended Behavior
Security Testing

Conclusion

- Missing or Incorrect Functionality
- Side-Effect Behavior
- Standard (Positive) Testing
- Standard Security (Positive) Testing
- Implemented Function of an ECU
- Intended Behavior
Security Testing

Conclusion

- Missing or Incorrect Functionality
- Side-Effect Behavior
- Standard (Positive) Testing
- Standard Security (Positive) Testing
- Standard Security (Negative) Testing
- Implement Function of an ECU
- Intended Behavior
- Vulnerability Assessment and Penetration Testing

From Requirement to Standard Security Test
Public

03-Apr-2019
C. Folda © Continental AG

25
Security Testing
Conclusion

› Penetration and Standard Security Tests influence each other over Security Requirements

› Example:

› The First Penetration Test has a very open Scope and has some findings

› These findings are translated to Security Requirements, Test Goals and Test Methods

› These new Requirements are covered afterwards with Standard Security Tests

› The next penetration Test Scope can be reduced and let the Penetration Test to focus on a more detailed level

© Continental AG
## Agenda

1. Introduction
2. Cyber Security Introduction
3. Security Testing Introduction
4. Example
Example Scenario

› Scenario:
  › Let’s assume we are developers of specific TLS libraries and deliver different Variants and Systems to our Customers
  › Heartbleed is not discovered yet

› Incident:
  › An internal Penetration Tests finds a Security Vulnerability in the Heartbeat functionality in our products (Heartbleed)
  › They deliver a Test report and steps how to reproduce it
Example
What is Heartbleed

SRC: Webcomic Series XKCD @ https://xkcd.com/1354/
Example Approach

1. Analyze the Report

2. Define and write Security Requirements

   “The Server must not report with more characters than the requested String has”

3. Create automated Security Testcases to avoid to deliver this vulnerability again

<table>
<thead>
<tr>
<th>Positive Test</th>
<th>Security Test 1</th>
<th>Security Test 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• result = tls_heartbeed(&quot;hat&quot;, 3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>if result == &quot;hat&quot;:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pass()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>else:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• result = tls_heartbeed(&quot;hat&quot;, 500)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>if len(Result) != 3:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>else:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pass()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• result = tls_heartbeed(&quot;hat&quot;, 0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>if len(Result) != 3:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>else:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pass()</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thanks for your attention!

Questions?
Business Unit Body & Security
In global reach and proximity to our customers

North America
- Detroit (USA)
- Troy (USA)
- Guadalajara Tijera (Mexico)
- Nogales (Mexico)
- Tlaxcala (Mexico)
- Jacutinga (Brazil)
- Guarulhos (Brazil)
- São Paulo (Brazil)

South America
- R&D / Sales
- Production

Europe
- Regensburg HQ (Germany)
- Bebra (Germany)
- Ingolstadt (Germany)
- Markdorf (Germany)
- Hildesheim (Germany)
- Rosenheim (Germany)
- Vienna (Austria)
- Toulouse (France)
- Vila Real (Portugal)
- Frenstat (Czech Republic)
- Sibiu (Romania)
- Timisoara (Romania)
- Iași (Romania)
- Novi Sad (Serbia)

Asia
- Chongqing (China)
- Shanghai (China)
- Suzhou (China)
- Tianjin (China)
- Changchun Moonlake (China)
- Yokohama (Japan)
- Singapore (Singapore)
- Icheon (South Korea)
- Bangalore (India)
- Manila (Philippines)