Security, the new safety requirement

riscure

January 29, 2019
Speaker: Rafael Boix Carpi

About me

- Principal Trainer & Security specialist at Riscure (The Netherlands)

- Riscure provides training, tooling, security evaluations and consultancy on hardware and software solutions
  - Automotive
  - Smart-cards / secure elements / ...
  - Hardened crypto implementations
  - Mobile payment solutions
  - Pay-TV / Content-Protection / ...
  - TEEs / White-box-crypto / secure boot...

Agenda

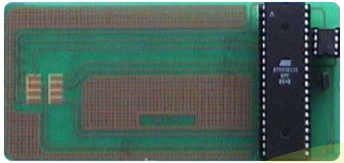
- Events that shaped automotive security
- Why security is required to ensure safety
- How to start securing automotive systems

A bit of car hacking history…

…and a message of hope :)

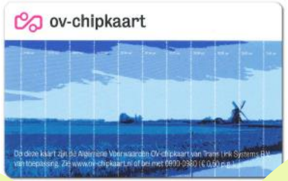
Before car hacking...

1997: Satellite TV hack wars



Nowadays: I'll deliver a free week of training @ Riscure if you show me a **hacked cable TV decoder** that can decode **today** a cable/satellite signal from Europe :)

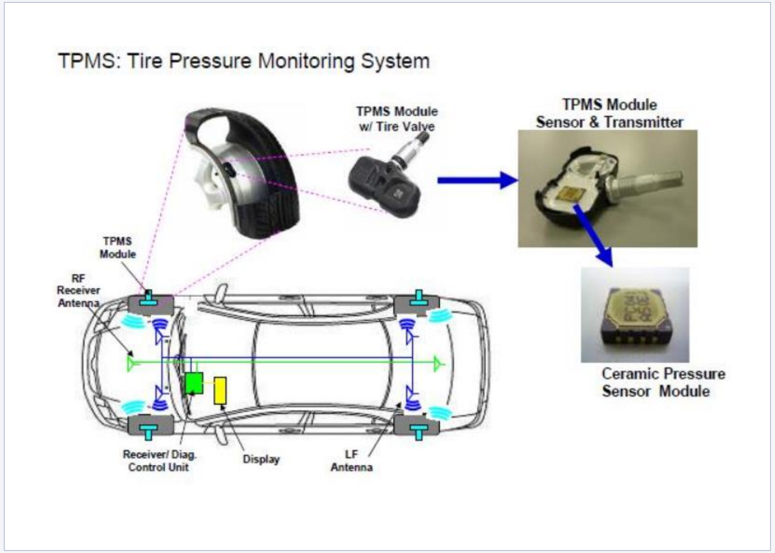
- Vulnerable to attacks
- Logical (SW only)
- Physical / remote
- No tamper evidence



Car hacking: history repeats itself

Pre-2015: there are publications about hacking ECUs

- Impersonating ECUs (e.g. brake ECU) with CAN messages
- Hacking the TPMS (tire pressure monitor) with RF signals
- Hacking key fob (car key remote control)


TPMS: Tire Pressure Monitoring System
TPMS Module w/ Tire Valve
TPMS Module Sensor & Transmitter
TPMS Module
RF Receiver Antenna
Ceramic Pressure Sensor Module
Receiver/ Diag. Control Unit
Display
LF Antenna

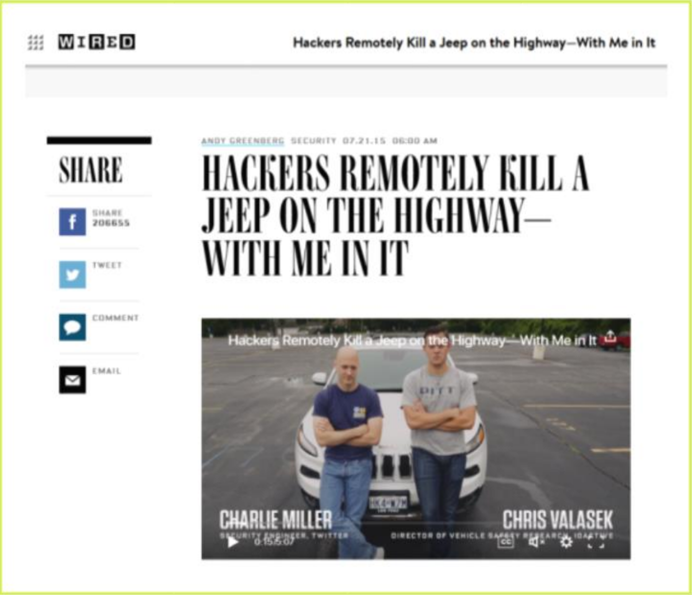
src: https://web.wpi.edu/Pubs/E-project/Available/E-project-091115-154458/unrestricted/MQP_piscitelli_arnold_2015.pdf

Car hacking:
history repeats itself

2015: the game changes

WIRED magazine article (2015)

- Remote attack
- Targeting safety-critical ECUs
- Presented also in DEFCON and BlackHat



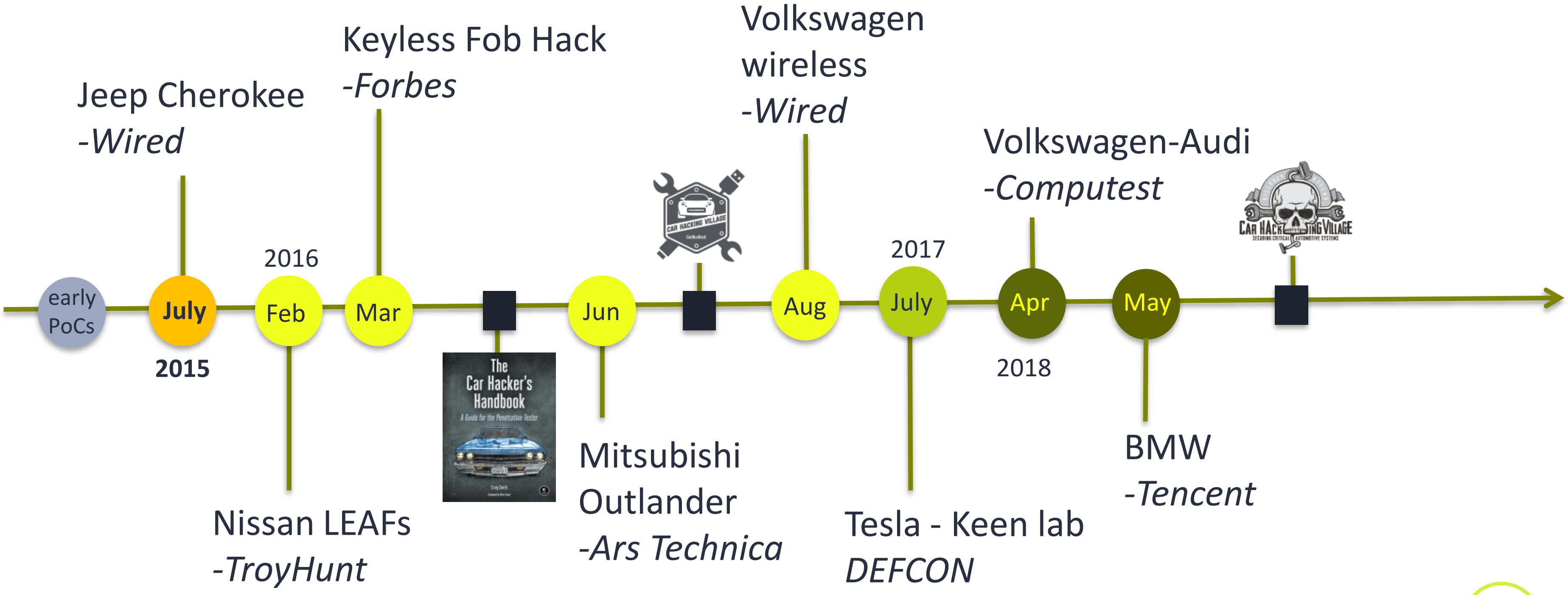
WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

SHARE
SHARE 206655
TWEET
COMMENT
EMAIL
Hackers Remotely Kill a Jeep on the Highway—With Me in It
CHARLIE MILLER
SECURITY ENGINEER, TWITTER
CHRIS VALASEK
DIRECTOR OF VEHICLE SAFETY RESEARCH, IOACTIVE
0:15:5:07

Car hacking: timeline



early PoCs

2015 July: Jeep Cherokee *-Wired*

2016 Feb: Nissan LEAFs *-TroyHunt*

Mar: Keyless Fob Hack *-Forbes*

Jun: Mitsubishi Outlander *-Ars Technica*

Aug: Volkswagen wireless *-Wired*

2017 July: Tesla - Keen lab *DEFCON*

2018 Apr: Volkswagen-Audi *-Computest*

May: BMW *-Tencent*

The Car Hacker's Handbook
A Guide for the Penetration Tester
CAR HACKING VILLAGE
CAR HACKING VILLAGE
SECURING CRITICAL AUTOMOTIVE SYSTEMS

Consequences

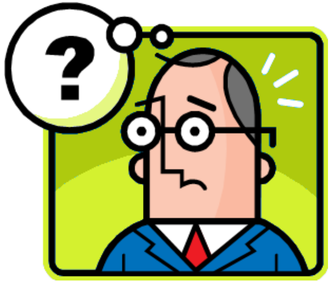
- Recalls, online services gone offline, etc... costs **LOTS** of money
- Incident response plans put in place
- Automotive industry **awareness** of cybersecurity needs
    - OEMs publicly announcing cybersecurity plans
    - SAE, ISO, govt. agencies issue new cybersecurity regulations
    - ...

The automotive industry is changing:
<u>security is needed</u>

The “trick question” #1

How do you implement security in an automotive system?

- Think for 10 seconds



Did you think about…

- Who is the attacker? What can the attacker do?
- What are the assets to protect?
- Are there many attack paths for the same goal?
- What does it actually mean to implement security?
  - *What is the difference between safety and security?*

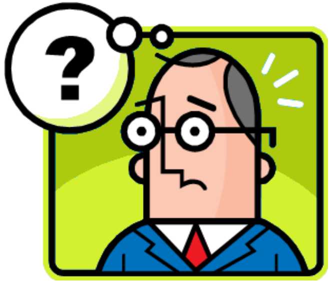
The “trick question” #2

How do you implement security in your product(s)?

- Think for 10 seconds

But…

- Is there any standard process to implement security?
- Where does security fit in the V cycle?
- How much does it cost? And what do you get?



A message of hope

Perfect security doesn’t exist…

…*good enough* security does

Why is security required in order to have safety in automotive systems?

Safety engineering

src: https://www.driving.co.uk/car-clinic/check-safe-car-using-euro-ncap-crash-test-scores/

Goal of safety engineering

- Input/State/Output of E/E systems always **<u>known and predictable</u>**

Challenging safety

- Ensure specifications hold in reality (lots of testing)

OEMs & regulations enforce functional safety

- ISO 26262 (2011)
- Well-established processes e.g. FMEA

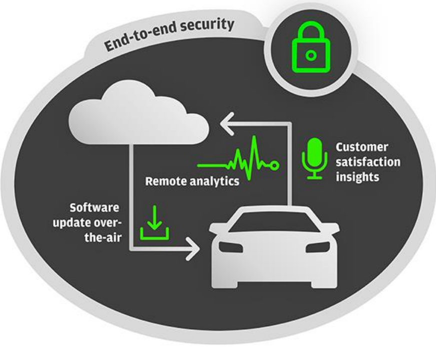
Automotive trends

Electric

Connected

Autonomous

Shared



OTA Update

Modern auto landscape

Cars were **stand alone** systems, like an **off-line** network.

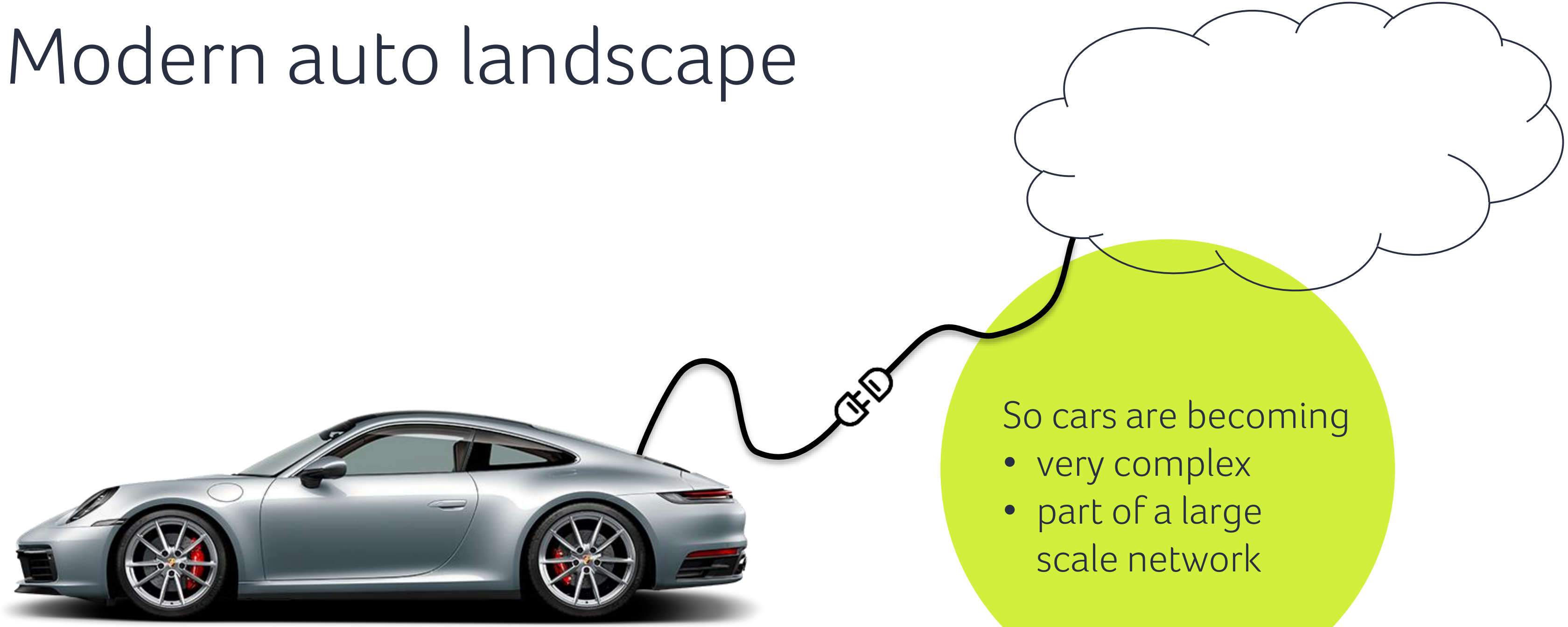
Modern auto landscape

Then, we decided to connect them…

…and added a ton of driver assistance systems:

adaptive cruise control anti-lock braking system automatic parking blind spot monitor
collision avoidance system crosswind stabilization cruise control driver drowsiness detection
driver monitoring system emergency driver assistant forward collision warning
high beam assist hill descent control intelligent speed adaptation intersection assistant lane centering
lane change assistance lane departure warning system navigation system night vision parking sensor pedestrian protection system rain sensor surround view system
tire pressure monitoring traffic sign recognition turning assistant vehicular communication systems wrong-way driving warning

Modern auto landscape



So cars are becoming

- very complex
- part of a large scale network

…and added a ton of driver assistance systems:

adaptive cruise control anti-lock braking system automatic parking blind spot monitor
collision avoidance system crosswind stabilization cruise control driver drowsiness detection
driver monitoring system emergency driver assistant forward collision warning
high beam assist hill descent control intelligent speed adaptation intersection assistant lane centering
lane change assistance lane departure warning system navigation system night vision parking sensor pedestrian protection system rain sensor surround view system
tire pressure monitoring traffic sign recognition turning assistant vehicular communication systems wrong-way driving warning

Safety vs Security

Goal of security engineering

- Ensure some component/system property (e.g. data confidentiality) **cannot be compromised** by a given attacker

Challenging security

- Attack component/systems to compromise their security properties (usually leaving the system in undefined state)

Security is a different aspect of E/E systems

- Security protects from threats, not hazards
- No standardized processes yet
- Standards are guidelines (SAE J3061) or WIP (SAE J3101, ISO 21434, ...)

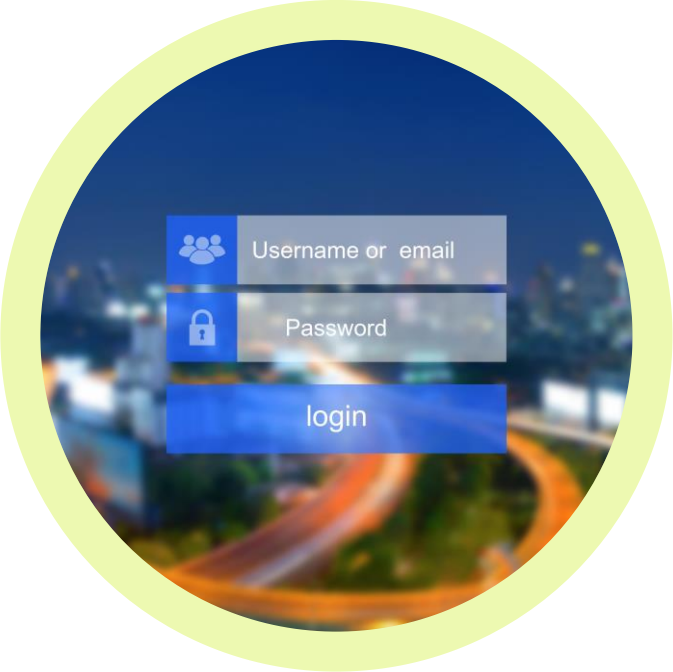
src: Santiago Cordoba, Security Analyst @ Riscure

Safety vs Security: ECU diagnostics password

Safety requirements

- Password check function should work as intended
- Password check function code should not crash with unexpected/malformatted input
- ....

Hardcoded, predictable password is fine



Security requirements

- Password should not be "guessable"
- Data protected by password / password function should not be available to unauthorized users
- .....

Hardcoded, predictable password is <u>unacceptable</u>

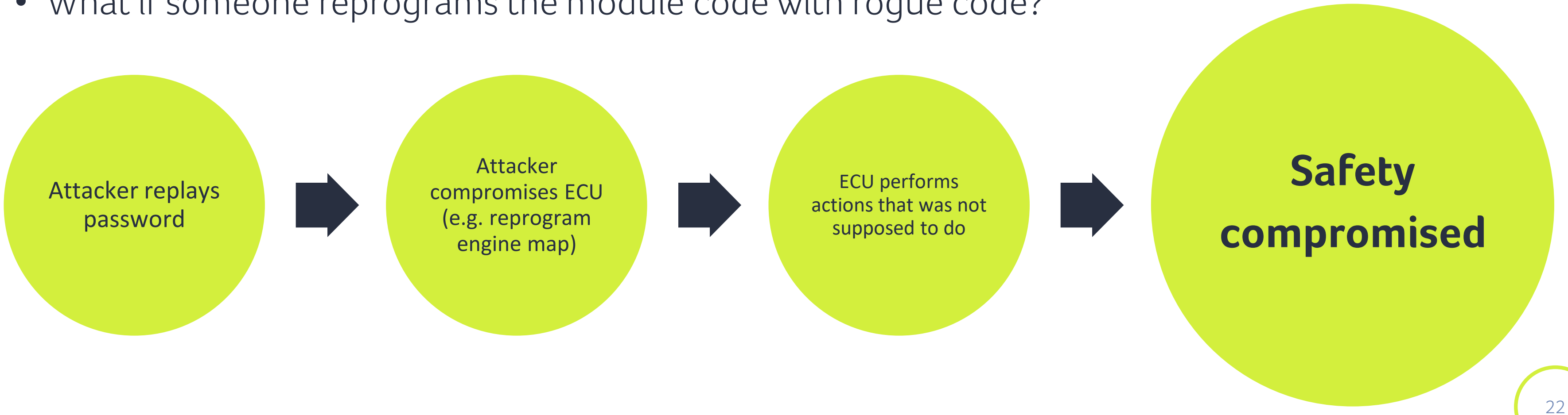
Safety vs Security: ECU diagnostics password

Conflicting safety-security requirements

- **In case of doubt: safety wins → hardcoded, predictable password**

However…

- What if the password was the diagnostics password for an engine module?
- What if someone reprograms the module code with rogue code?



Attacker replays password
Attacker compromises ECU (e.g. reprogram engine map)
ECU performs actions that was not supposed to do
Safety compromised

Safety != Security

Security is a **requirement** for safety

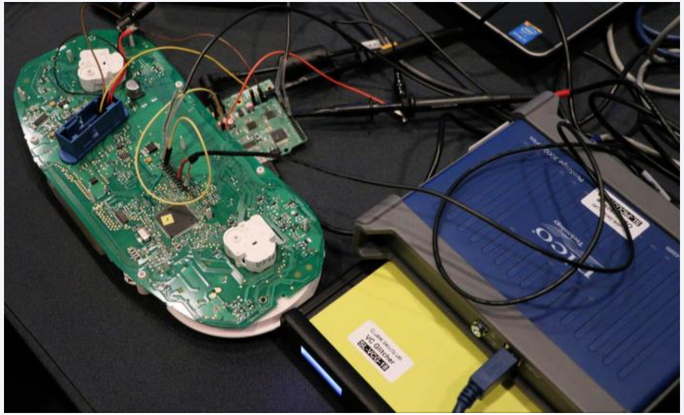
How do I start securing my system?

Security: the unfair, hard game for developers

Attacker only needs **one** way in
Developers need to **identify** and **protect** all ways in

Many people / parties involved
Complex products: 100M lines of code in a car
Tight **deadlines & budgets**

Functionality vs. Reality
“It was not meant to be used like that”
Wrong **assumptions** on security wording meaning
Lack of system **overview**
Lack of **good** secure development **habits**



Src https://woodworking.stackexchange.com/questions/3869/what-do-i-need-to-know-to-use-a-claw-hammer-effectively

Threat modelling

Defines context for discussing security:

- Security and its actors
- Attackers (threats)
- **Assets**
- Exploits (attacks)
- Defense

Foundation to start implementing security

Difficult task if you never did it before
...and *still not easy* even if you’re experienced

Threat Assessment & Risk Analysis (TARA)

Given a certain security context, a TARA process:

- Defines what can happen to a system because of described attackers
- Structurally estimates & rates the risk of different attacks
- Proposes defenses for the considered attacks in a structured way

Automotive TARA has some unique characteristics

- Proper asset identification & rating (required for TARA) usually gets less attention
- Many variations
- Reuse of safety processes

Threat Assessment & Risk Analysis

Some popular references in automotive for preparing & performing a TARA

Microsoft STRIDE & DREAD (~2007)

STRIDE reused often, DREAD abandoned in 2008

Common Criteria (CC)

Common Methodology for Information Technology Security Evaluation (CEMV3.1R4 Appendix B)

EVITA (started ~2009) (deliverable 2.3 appendix B,C)

Uses CC, also uses ISO 26262 (ASIL)

Seems to be popular in Europe

MITRE CJA & TARA (2013)

Cyber Threat Susceptibility Analysis & Cyber Risk Remediation Analysis

Seems to be popular in USA

HEAVENS (2016) (Document D2 Security Models)

Builds on EVITA, uses STRIDE

Example TARA process: MITRE TARA

Input

- TARA scope (assets & relevance, e.g. from CJA)
  - This could be issued e.g. by OEMs to Tier-1s

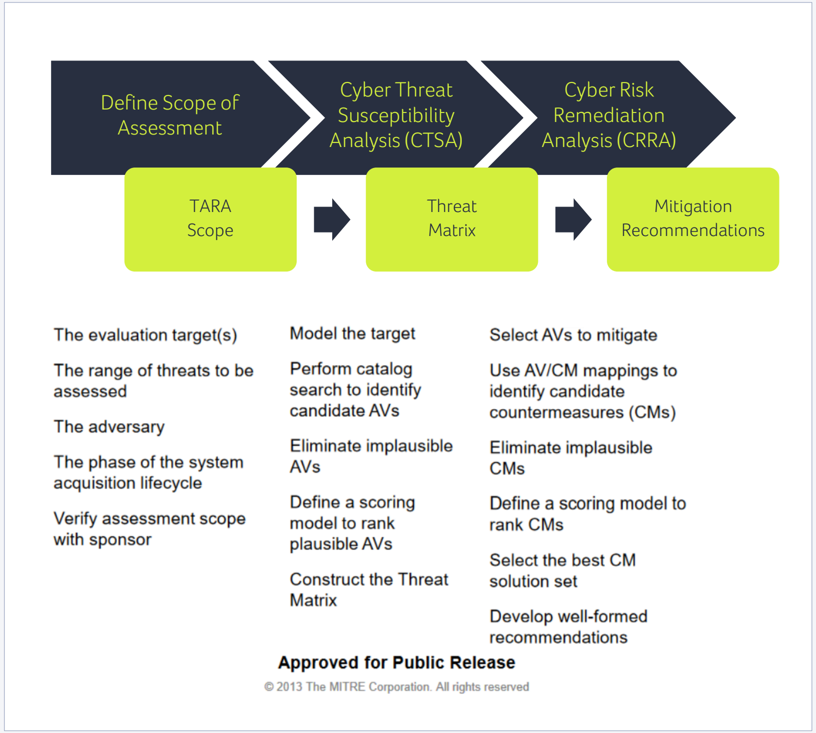
Output

- Threat matrix (from CTSA)
- Recommendations for countermeasures (from CRRA)

Requirements

- List of all attacks and attackers
- List of all countermeasures
- **Fully understanding your system and its context**

MITRE TARA full description:
https://www.mitre.org/sites/default/files/pdf/11_4982.pdf



Define Scope of Assessment

Cyber Threat Susceptibility Analysis (CTSA)

Cyber Risk Remediation Analysis (CRRA)

TARA Scope

Threat Matrix

Mitigation Recommendations

The evaluation target(s)

The range of threats to be assessed

The adversary

The phase of the system acquisition lifecycle

Verify assessment scope with sponsor

Model the target

Perform catalog search to identify candidate AVs

Eliminate implausible AVs

Define a scoring model to rank plausible AVs

Construct the Threat Matrix

Select AVs to mitigate

Use AV/CM mappings to identify candidate countermeasures (CMs)

Eliminate implausible CMs

Define a scoring model to rank CMs

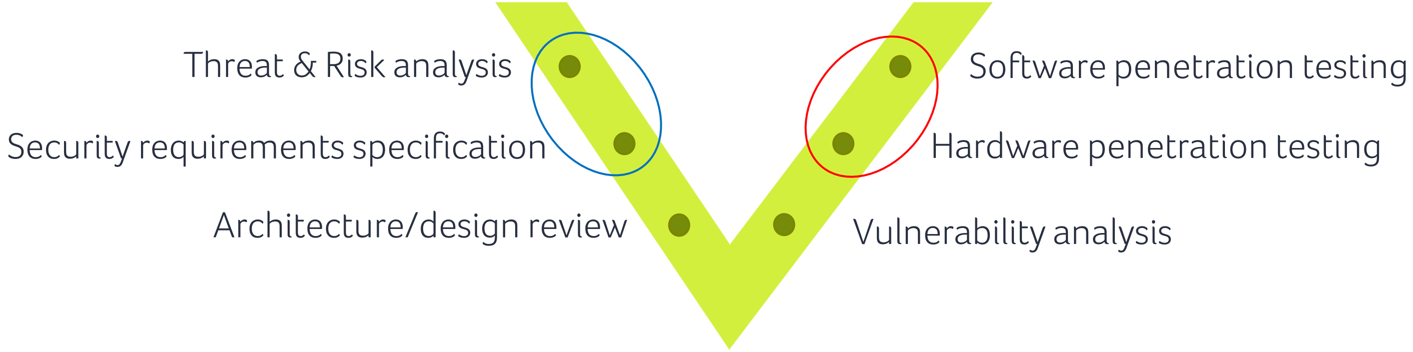
Select the best CM solution set

Develop well-formed recommendations

Approved for Public Release

How does TARA fit in my development cycle?

Security activities in Product development cycle



Threat & Risk analysis
Security requirements specification
Architecture/design review
Software penetration testing
Hardware penetration testing
Vulnerability analysis

TARA or not?

TARA is key to enable security…

…but **requires clear scope & asset definition**

… and **needs to be adapted to your company**

Summary

A message of hope
It is possible to have good enough security

Safety != Security
Security **is a requirement** for safety

TARA or not?
TARA is **fundamental** to security, only if done right

I want to learn more!

Automotive ONLINE

Starting March 2019, join now!

https://www.riscure.com/training/

Wrap-up

Thank you for your attention!

Q&A time ☺

References and links

Threat Assessment and Remediation Analysis (TARA) Methodology Description, MITRE Technical Papers, MITRE. Link: https://www.mitre.org/publications/technical-papers/threat-assessment--remediation-analysis-tara

Crown Jewels Analysis (CJA), MITRE Systems Engineering for Mission Assurance, MITRE. Link: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

EVITA - Deliverable D2.3, deliverables from EVITA project. Link: https://www.evita-project.org/deliverables.html

Deliverable D2 (**HEAVENS**), HoliSec project. Link: https://autosec.se/holisec-results/

STRIDE & DREAD, Microsoft SDL. Link: https://www.microsoft.com/en-us/securityengineering/sdl/

Common Methodology for Information Technology Security Evaluation (CEMV3.1R4 Appendix B), Common Criteria. Link: https://www.ipa.go.jp/security/jisec/cc/documents/CEMV3.1R4.pdf

"Safety!=Security", Riscure, presented at ESCAR 2017. Link: https://www.riscure.com/publication/safety-not-equal-security/

Mentioned car hacking articles in timeline

2015

- Hackers remotely kill a Jeep in the highway–with me in it – Wired

2016

- Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs – TroyHunt
- Hackers break the connected Mitsubishi Outlander hybrid wide open – ArsTechnica
- A New Wireless Hack Can Unlock 100 Million Volkswagens – Wired
- Thieves Can Crack Open Audi, BMW, Ford Cars With Simple Keyless Fob Hack – Forbes

2017

- Tesla Model S & X hacks by Keen lab – DEFCON

2018

- New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars - Tencent
- Car Hack project Volkswagen/Audi - Computest

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
inforequest@riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road, Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com

Further questions/information:

Rafael Boix
Principal Security Specialist
E-mail: rafael@riscure.com
Twitter: @rafabxc

www.riscure.com

riscure

driving your security forward