# SECURITY BY DESIGN

Peter Lieber

# AGENDA

1. A brief introduction

2. The STRIDE Framework built in EA itself

3. Problem Statement(s) (with a little focus on Automotive)

4. Innovation: Security-by Design with ThreatGet

5. Live is Life

6. Conclusion

# PETER LIEBER

- Parallel Entrepreneur
  - Sparx Systems Central Europe
  - Sparx Services Central Europe
  - LieberLieber Software
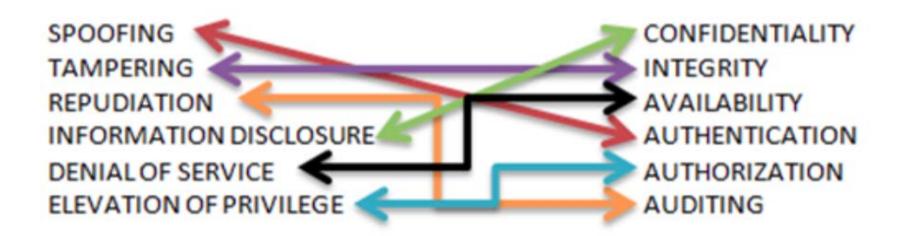
- President Österreichischer Gewerbeverein
- (www.gewerbeverein.at)
- President Verband Österreichischer Software Industrie
- (www.voesi.or.at)

# THE STRIDE THREAT MODEL
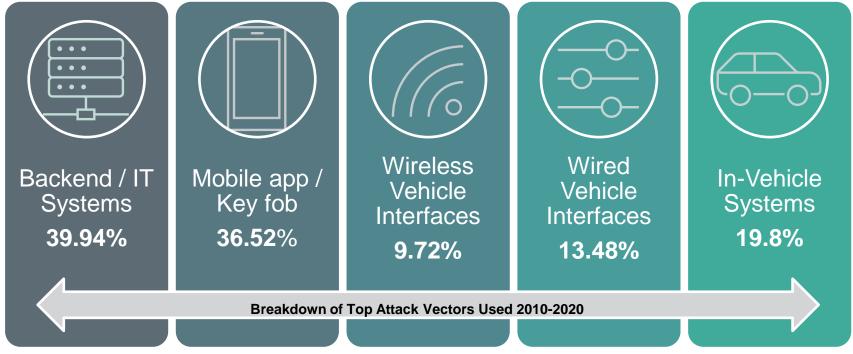
Is a Framework of security risks developed

SPOOFING          CONFIDENTIALITY
TAMPERING         INTEGRITY
REPUDIATION        AVAILABILITY
INFORMATION DISCLOSURE     AUTHENTICATION
DENIAL OF SERVICE       AUTHORIZATION
ELEVATION OF PRIVILEGE     AUDITING

# AUTOMOTIVE SHOWCASE

# CONNECTED VEHICLES ARE HERE TO STAY

By 2025, connected vehicles will comprise nearly 86% of the global automotive market



Upstream Security Global automotive Cybersecurity Report 2021

# AUTOMOTIVE CYBERCRIME IS ON THE RISE

**THREAT GET**

Backend / IT Systems
**39.94%**

Mobile app / Key fob
**36.52%**

Wireless Vehicle Interfaces
**9.72%**

Wired Vehicle Interfaces
**13.48%**

In-Vehicle Systems
**19.8%**

**Breakdown of Top Attack Vectors Used 2010-2020**

Upstream Security Global automotive Cybersecurity Report 2021

14/07/2022

# 2015 - SUMMER OF CAR HACKS



THREATGET

**THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE**

Security researchers Charlie Miller and Chris Valasek. WHITNEY CURTIS FOR WIRED

**Security researchers hack a car and apply the brakes via text**

Vulnerability revealed in diagnostic dongles used for vehicle tracking and insurance that lets them take control using just an SMS
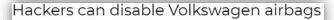
Car dongle hack was demonstrated on a Corvette, but any vehicle with the diagnostic dongles attached could be vulnerable. Photograph: Charles Rex Arbogast/AP

**Hackers can disable Volkswagen airbags**

As if Volkswagen didn't have enough to worry about with the emissions scandal, European security researchers have demonstrated a proof-of-concept exploit that can allow an attacker to covertly disable airbags (and other systems) in the German manufacturer's autos. Unlike the more dramatic wireless hacking demonstration of Jeep vehicles that caused a massive recall, this particular exploit requires actual contact with the car, either via a compromised laptop or malicious USB device connected to the vehicle's diagnostics port. To demonstrate the hair-raising potential of this exploit, the hackers were able completely disable the airbag, but have the onboard software continue to report the system as functioning properly. For now, the hackers limited their hacking to this proof-of-concept, but they believe that

Home / Car Tech

NEWS
**BMW cars found vulnerable in Connected Drive hack**

By Martyn Williams
Senior Correspondent, IDG News Service
JAN 30, 2015 12:30 PM PST

# UNECE WORLD FORUM FOR HARMONIZATION OF VEHICLE REGULATIONS

- UNECE WP29 defines requirements for type approval
- Members are:
    - Type approval authorities
    - Certification bodies
    - OEM and Tier 1
- Two new regulations on:
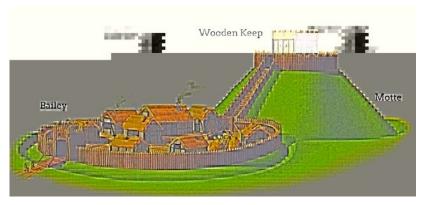    - **Cybersecurity**
    - Software Updates

# SECURITY-BY DESIGN

## Innovation through Threat Modeling with ThreatGet

# HOW DOES THREAT MODELING WORK?

- **Structured process**
  - Check system for threats



https://www.castlesworld.com/tools/motte-and-bailey-castles.php

# HOW DOES THREAT MODELING WORK?

- **Structured process**
  - Check system for threats

- **Systematik approach**
  - Vulnerabilities & Threats



https://www.castlesworld.com/tools/motte-and-bailey-castles.php



https://deadliestwarrior.fandom.com/wiki/Huo_Chien

# HOW DOES THREAT MODELING WORK?

**THREATGET**

- **Structured process**
  - Check system for threats
  - Fixing the identified problems

- **Systematik approach**
  - Vulnerabilities & Threats



https://www.castlesworld.com/tools/concentric-castles.php



https://deadliestwarrior.fandom.com/wiki/Huo_Chien

# HOW DOES THREAT MODELING WORK?

- **Structured process**
  - Check system for threats
  - Fixing the identified problems
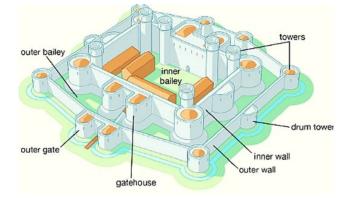
- **Systematik approach**
  - Vulnerabilities & Threats
  - Update Vulnerabilities & Threats



https://www.castlesworld.com/tools/concentric-castles.php
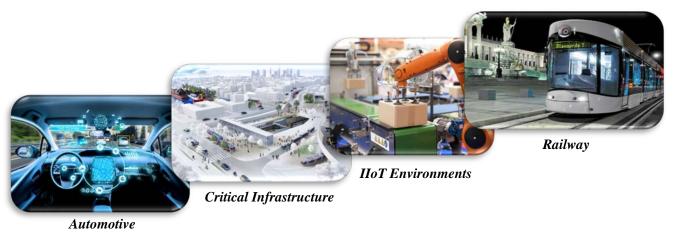


https://www.pbs.org/video/1812-niagara-frontier-fort-george-cannon-firing/

# CYBER SECURITY MODELING
# WITH METHODOLOGY- THREATGET

- ThreatGet is a tool based on Sparx Systems Enterprise Architect that helps in the design phase of many projects to search for potential threats:

*Railway*

*IIoT Environments*

*Critical Infrastructure*

*Automotive*
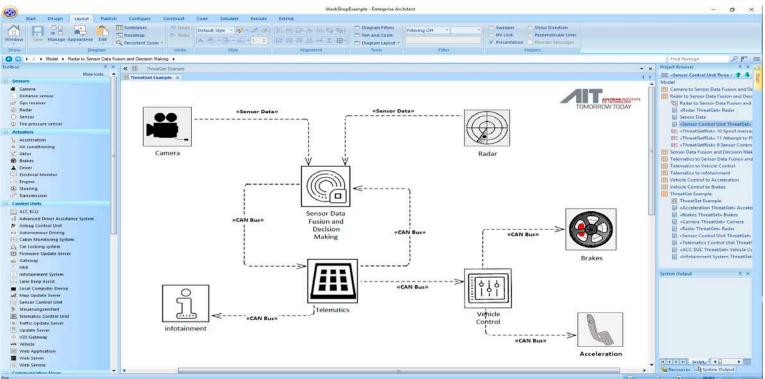
The barrier to change is not too little caring; it is too much complexity.

Bill Gates
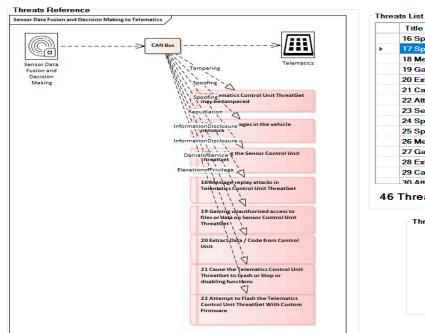
# THREATGET

# CREATING RISK ANALYSIS AUTOMATICALLY

# RISK ASSESSMENT

# THREAT MODELLING



- System Modell
- Security propertiesn
- Automated analysis
- Found threat with impact
- Risk Management Support
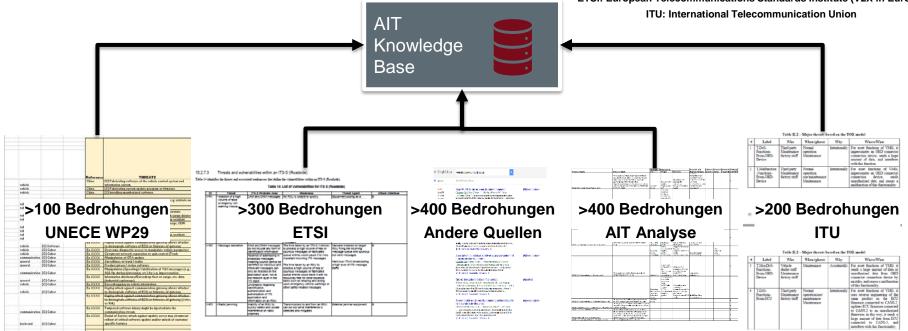
# THREAT INTELLIGENCE – AUTOMOTIVE EXAMPLE

UNECE WP29: World Forum for Harmonization of Vehicle Regulations
ETSI: European Telecommunications Standards Institute (V2X in Europe)
ITU: International Telecommunication Union

AIT Knowledge Base

>100 Bedrohungen
UNECE WP29

>300 Bedrohungen
ETSI

>400 Bedrohungen
Andere Quellen

>400 Bedrohungen
AIT Analyse

>200 Bedrohungen
ITU

# THANK YOU!

www.threatget.eu