Adi Karahasanovic

Cyber Security Consultant | M.Sc.

Combitech AB, Sweden

Automotive Cyber Security

ADAPTING THREAT MODELING METHODS FOR THE AUTOMOTIVE INDUSTRY

Based on a paper published on the 15th ESCAR Conference 2017 and can be found in the download area at *www.escar.info*

CONNECTED SOCIETY

- Global Digitalization
- Internet of Things (IoT)
  - Smart homes
  - Smart meters
- Smart Grids
- Industrial Internet of Things
  - Smart manufacturing
  - Local and Global Clouds
  - Suppliers and OEM in constant contact

COMBITECH

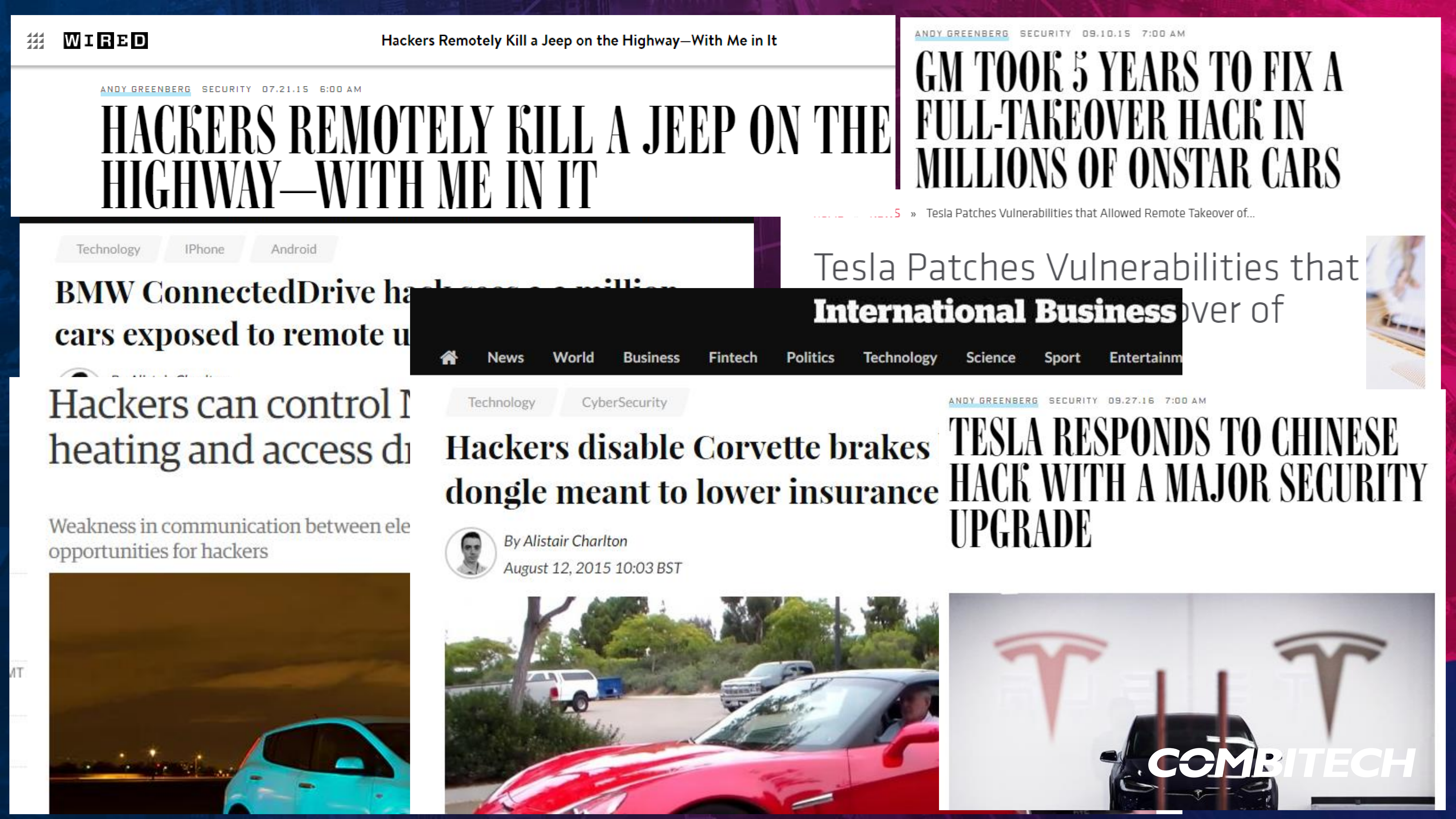
CONNECTED CAR

- Automotive industry is rapidly changing
- 380 million connected cars by 2021

- Vehicles today
  - Wi-Fi
  - 4G\LTE
  - Bluetooth
  - Over-The-Air updates
  - Remote diagnostics
  - Infotainment center

- Vehicles tomorrow
  - Vehicle-2-Vehicle
  - Vehicle-2-Infrastructure
  - Autonomous driving
  - Cloud based services

COMBITECH



WIRED

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

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

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

ANDY GREENBERG SECURITY 09.10.15 7:00 AM

GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS

» Tesla Patches Vulnerabilities that Allowed Remote Takeover of...

Tesla Patches Vulnerabilities that ...over of

Technology IPhone Android

BMW ConnectedDrive h...
cars exposed to remote u...

International Business

News World Business Fintech Politics Technology Science Sport Entertainm

Hackers can control ...
heating and access d...

Weakness in communication between ele...
opportunities for hackers

Technology CyberSecurity

Hackers disable Corvette brakes ...
dongle meant to lower insurance ...

By Alistair Charlton
August 12, 2015 10:03 BST

ANDY GREENBERG SECURITY 09.27.16 7:00 AM

TESLA RESPONDS TO CHINESE HACK WITH A MAJOR SECURITY UPGRADE

COMBITECH

SECURITY CONCERNS

- Exposing a car to the Internet makes it vulnerable to cyber attacks
- No safety without security
- CAN bus
- Infotainment system
- 3rd party applications
- Security as an afterthought
- Cost

COMBITECH

THREAT MODELING

- Three main approaches:
  - Attacker-centric approach
    - **Intel's TARA (Threat Agent Risk Assessment)**
    - Cyber Kill Chain
    - OODA
  - Asset-centric approach
    - PASTA
    - OCTAVE
    - ETSI's TVRA
  - Software-centric approach
    - **STRIDE**
    - DREAD

TARA

- TARA – Threat Agent Risk Assesment
- Focus on the attacker
- Domain experts, On-line survey and Research
- On-line survey – 12 respondents (Security Experts from Automotive industry)
- Tim Casey, Intel Security – Founder of TARA method

- Adaptations:
  - New threat agents (Intel Security, Healthcare & ENISA)
  - Outcome attribute extended
  - Threat agent attributes adapted
  - New methods and impact levels

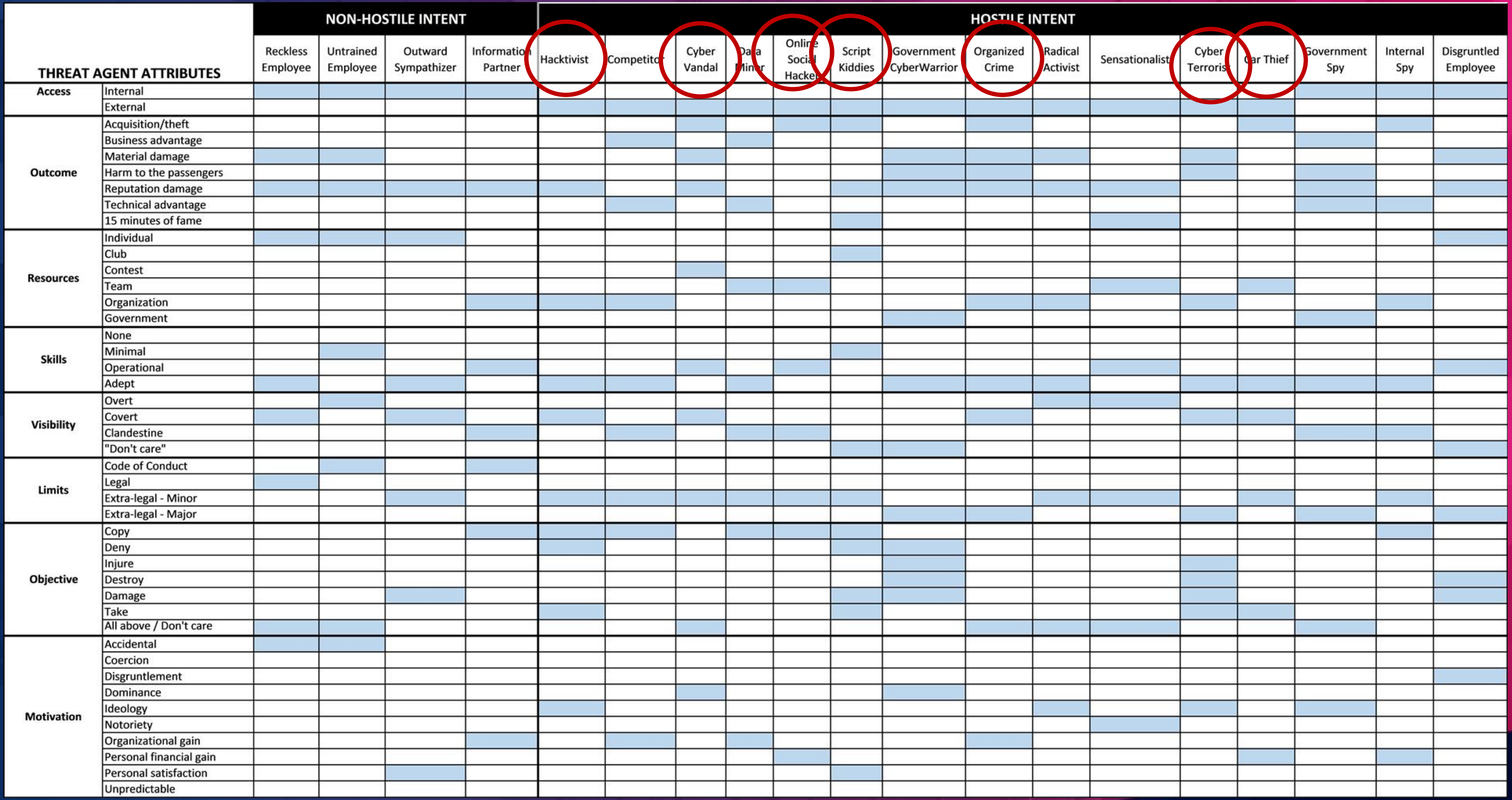
TARA - Methodology

1. Measure current threat agent risks
2. Distinguish threat agents with elevated risk level
3. Derive primary objectives of those threat agents
4. Identify methods likely to manifest
5. Determine the most important collective exposures
6. Align strategy to target the most significant exposures

TARA – results

- Three libraries for Automotive industry
- TAL – Threat Agent Library
  - 19 threat agents profiles and 9 different attributes
- MOL – Methods and Objectives Library
  - 5 attack methods and 5 impact levels
- CEL – Common Exposures Library
  - 18 most vulnerable attack surfaces
  - Completely customized

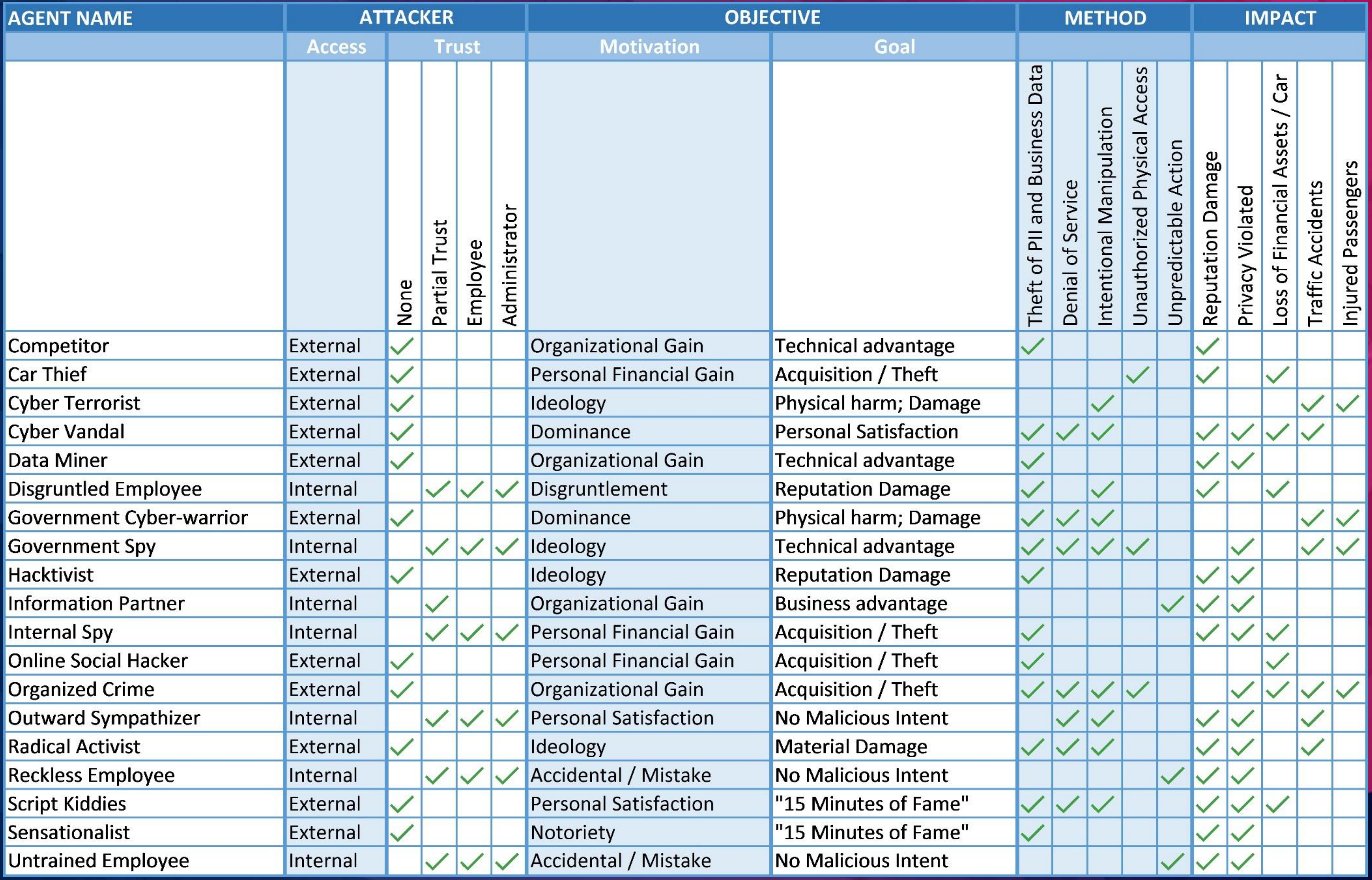
Threat Agent Library – Automotive industry



THREAT AGENT ATTRIBUTES		NON-HOSTILE INTENT				HOSTILE INTENT														
		Reckless Employee	Untrained Employee	Outward Sympathizer	Information Partner	Hacktivist	Competitor	Cyber Vandal	Data Miner	Online Social Hacker	Script Kiddies	Government CyberWarrior	Organized Crime	Radical Activist	Sensationalist	Cyber Terrorist	Car Thief	Government Spy	Internal Spy	Disgruntled Employee
Access	Internal	■	■	■	■													■	■	■
	External					■	■	■	■	■	■	■	■	■	■	■	■			
Outcome	Acquisition/theft							■		■	■		■				■		■	
	Business advantage						■		■									■		
	Material damage	■	■					■				■	■	■		■				■
	Harm to the passengers											■	■			■		■		
	Reputation damage	■	■	■	■	■		■			■	■	■	■	■			■		■
	Technical advantage						■		■									■	■	
	15 minutes of fame										■				■					
Resources	Individual	■	■	■																■
	Club										■									
	Contest							■												
	Team								■	■					■		■			
	Organization				■	■	■						■	■		■			■	
	Government											■						■		
Skills	None																			
	Minimal		■								■									
	Operational				■			■		■					■					■
	Adept	■		■		■	■		■			■	■	■		■	■	■	■	
Visibility	Overt		■											■	■					
	Covert	■		■		■		■					■			■	■			
	Clandestine				■		■		■	■								■	■	
	"Don't care"										■	■								■
Limits	Code of Conduct		■		■															
	Legal	■																		
	Extra-legal - Minor			■		■	■	■	■	■	■			■	■		■		■	
	Extra-legal - Major											■	■			■		■		■
Objective	Copy				■	■	■		■	■	■								■	
	Deny					■					■	■								
	Injure											■				■				
	Destroy											■				■				■
	Damage			■							■	■				■				■
	Take					■					■					■	■			
	All above / Don't care	■	■					■					■	■	■			■		
Motivation	Accidental	■	■																	
	Coercion																			
	Disgruntlement																			■
	Dominance							■				■								
	Ideology					■								■		■		■		
	Notoriety														■					
	Organizational gain				■		■		■				■							
	Personal financial gain									■							■		■	
	Personal satisfaction			■							■									
	Unpredictable																			

COMBITECH

Methods and objectives library – Automotive industry

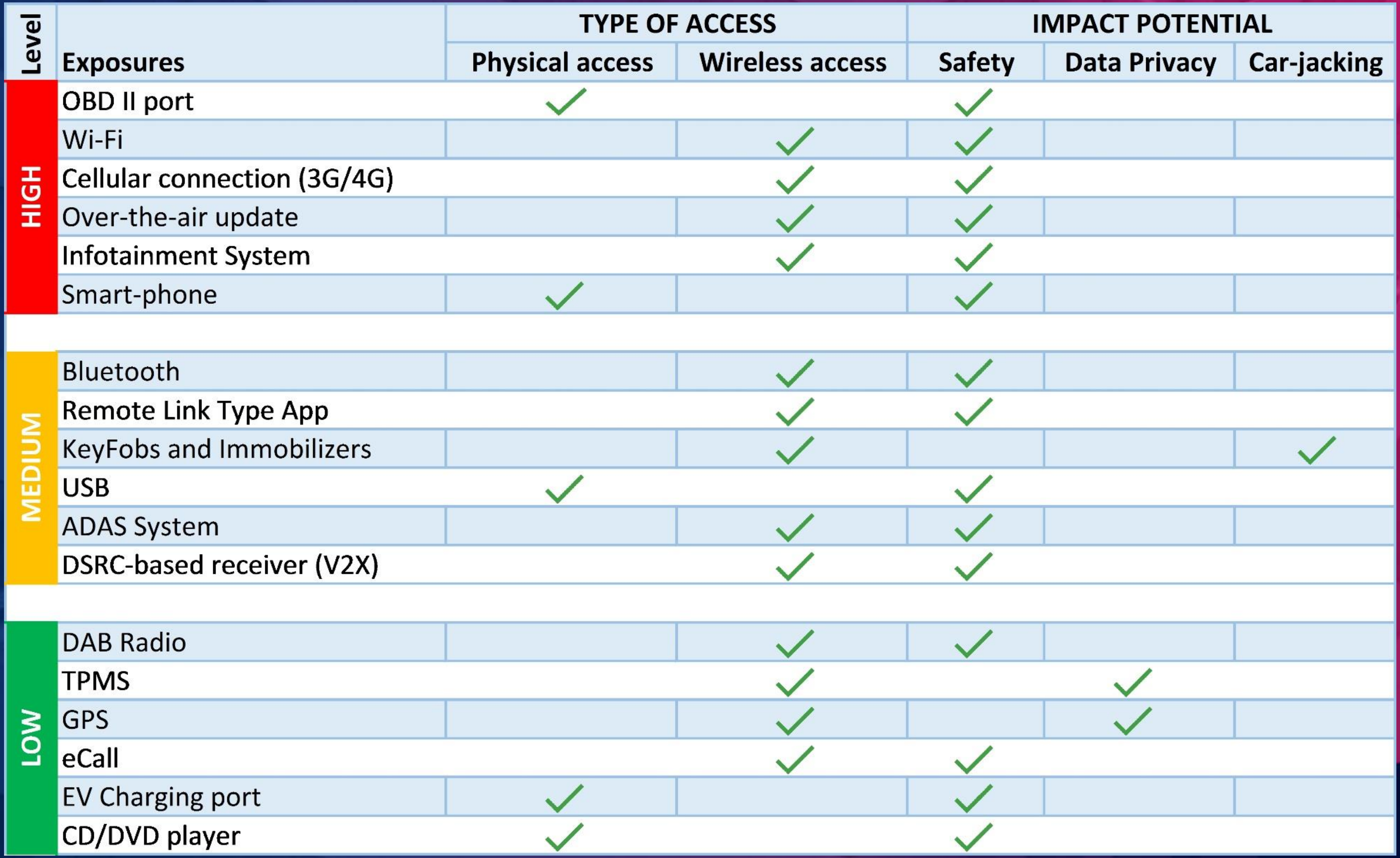


AGENT NAME	ATTACKER					OBJECTIVE		METHOD					IMPACT				
	Access	Trust				Motivation	Goal										
		None	Partial Trust	Employee	Administrator			Theft of PII and Business Data	Denial of Service	Intentional Manipulation	Unauthorized Physical Access	Unpredictable Action	Reputation Damage	Privacy Violated	Loss of Financial Assets / Car	Traffic Accidents	Injured Passengers
Competitor	External	✓				Organizational Gain	Technical advantage	✓					✓				
Car Thief	External	✓				Personal Financial Gain	Acquisition / Theft				✓		✓		✓		
Cyber Terrorist	External	✓				Ideology	Physical harm; Damage			✓						✓	✓
Cyber Vandal	External	✓				Dominance	Personal Satisfaction	✓	✓	✓			✓	✓	✓	✓	
Data Miner	External	✓				Organizational Gain	Technical advantage	✓					✓	✓			
Disgruntled Employee	Internal		✓	✓	✓	Disgruntlement	Reputation Damage	✓		✓			✓		✓		
Government Cyber-warrior	External	✓				Dominance	Physical harm; Damage	✓	✓	✓						✓	✓
Government Spy	Internal		✓	✓	✓	Ideology	Technical advantage	✓	✓	✓	✓			✓		✓	✓
Hacktivist	External	✓				Ideology	Reputation Damage	✓					✓	✓			
Information Partner	Internal		✓			Organizational Gain	Business advantage					✓	✓	✓			
Internal Spy	Internal		✓	✓	✓	Personal Financial Gain	Acquisition / Theft	✓					✓	✓	✓		
Online Social Hacker	External	✓				Personal Financial Gain	Acquisition / Theft	✓							✓		
Organized Crime	External	✓				Organizational Gain	Acquisition / Theft	✓	✓	✓	✓			✓	✓	✓	✓
Outward Sympathizer	Internal		✓	✓	✓	Personal Satisfaction	No Malicious Intent		✓	✓			✓	✓		✓	
Radical Activist	External	✓				Ideology	Material Damage	✓	✓	✓			✓	✓		✓	
Reckless Employee	Internal		✓	✓	✓	Accidental / Mistake	No Malicious Intent					✓	✓	✓			
Script Kiddies	External	✓				Personal Satisfaction	"15 Minutes of Fame"	✓	✓	✓			✓	✓	✓		
Sensationalist	External	✓				Notoriety	"15 Minutes of Fame"	✓					✓	✓			
Untrained Employee	Internal		✓	✓	✓	Accidental / Mistake	No Malicious Intent					✓	✓	✓			

COMBITECH

Common Exposure Library – Automotive industry

- Based on the On-line Survey and confirmed by security experts from the industry



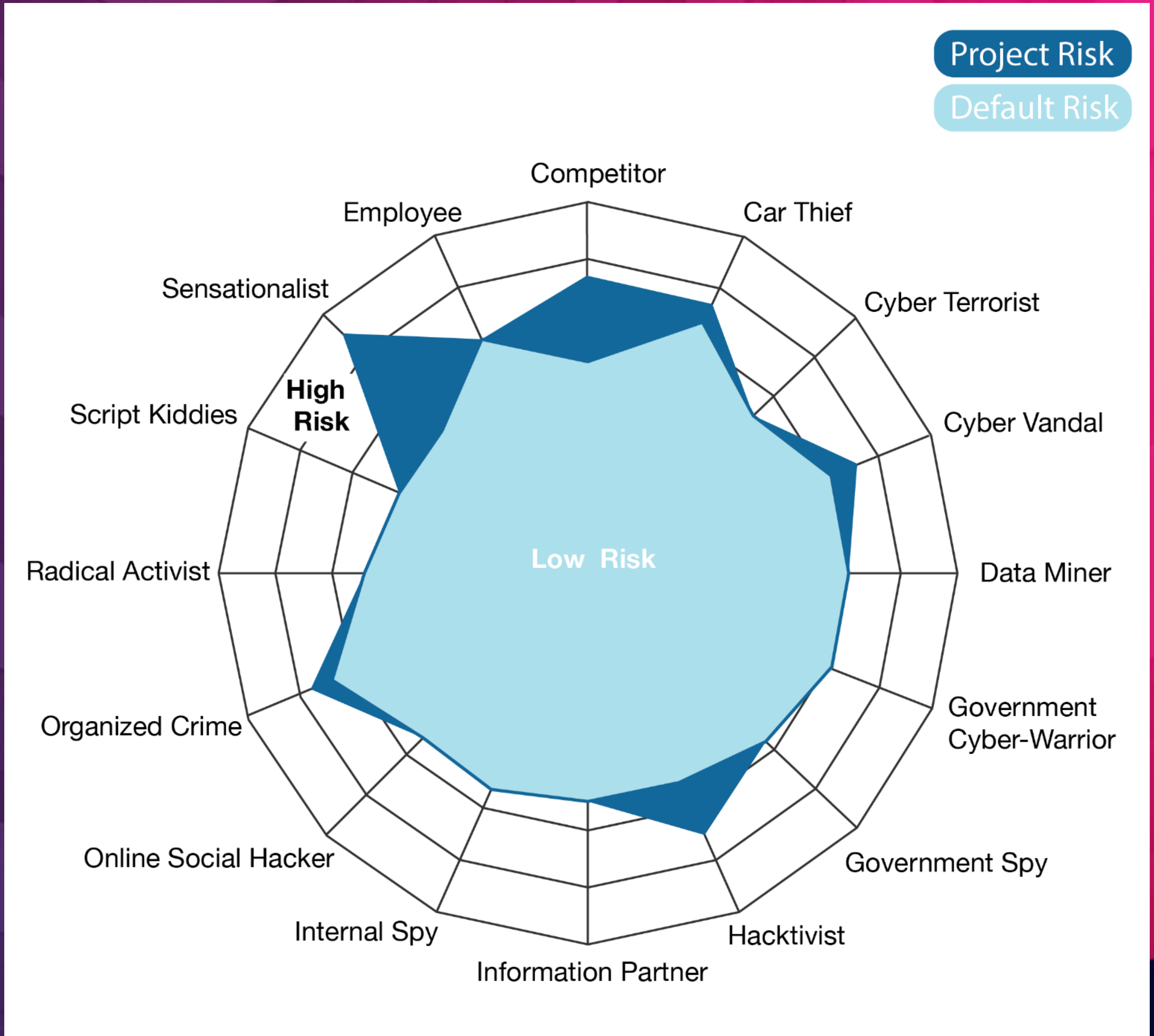
Level	Exposures	TYPE OF ACCESS		IMPACT POTENTIAL		
		Physical access	Wireless access	Safety	Data Privacy	Car-jacking
HIGH	OBD II port	✓		✓		
	Wi-Fi		✓	✓		
	Cellular connection (3G/4G)		✓	✓		
	Over-the-air update		✓	✓		
	Infotainment System		✓	✓		
	Smart-phone	✓		✓		
MEDIUM	Bluetooth		✓	✓		
	Remote Link Type App		✓	✓		
	KeyFobs and Immobilizers		✓			✓
	USB	✓		✓		
	ADAS System		✓	✓		
	DSRC-based receiver (V2X)		✓	✓		
LOW	DAB Radio		✓	✓		
	TPMS		✓		✓	
	GPS		✓		✓	
	eCall		✓	✓		
	EV Charging port	✓		✓		
	CD/DVD player	✓		✓		

Threat agent comparison

Risk comparison

- Default risk – IT Services
- Project risk – Connected Car

- Highest ranking threat agent
  --> Sensationalist
  (at the moment)



COMBITECH

STRIDE

STRIDE :

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

- Domain experts from Combitech, Arccore & NCC Group
- **Target: AUTOSAR Interior Light Example**
- Data Flow Diagrams (DFD)
- Microsoft Threat modeling tool 2016
- **Template** for the Automotive industry (NCC Group)

STRIDE - Methodology

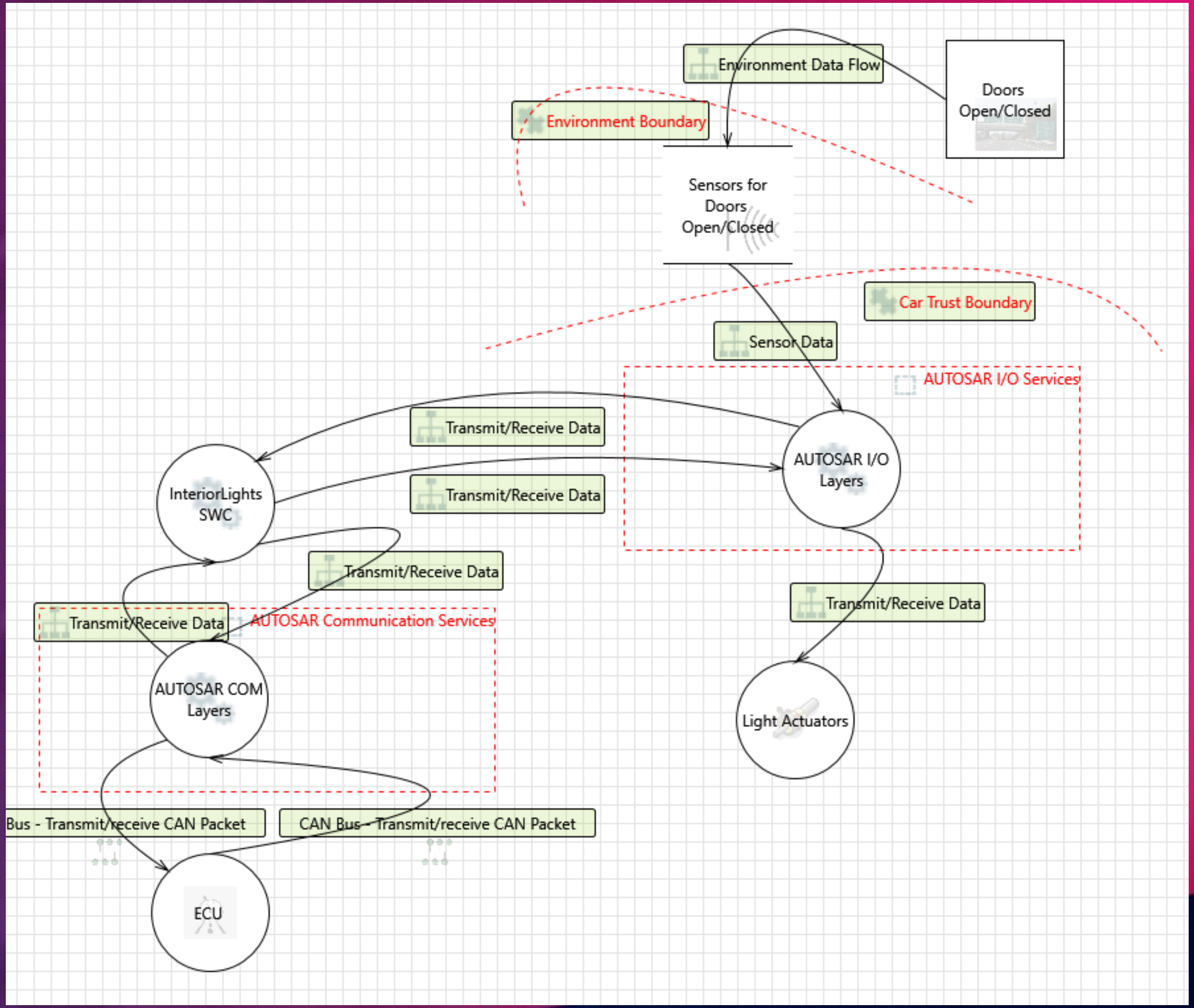
1. Analyze the Interior Lights example
2. Create a DFD diagram
3. Generate threats using MS Threat modeling tool
4. Analyze threats
5. Test one threat from each category in a simulated environment
6. Suggest security measures to mitigate threats

STRIDE – Data flow diagram

- Typical communication flow in AUTOSAR
- Interior Light Software Component (SWC)

- MS Threat Modeling tool 2016
  - Automatic threat generation
  - STRIDE per-interaction

- **NCC Group template further developed**



COMBITECH

Stride - results

- 74 threats found
- 17 not applicable
- 57 need further investigation
- A threat from each STRIDE category was found

Validation

- Verify threats found by the STRIDE method
- One threat from each STRIDE category
- Hardware from Arccore simulates a small CAN network
- Interior Lights SWC simulated with sensors and actuators
- GOAL – double check the results of the MS Threat modelling tool

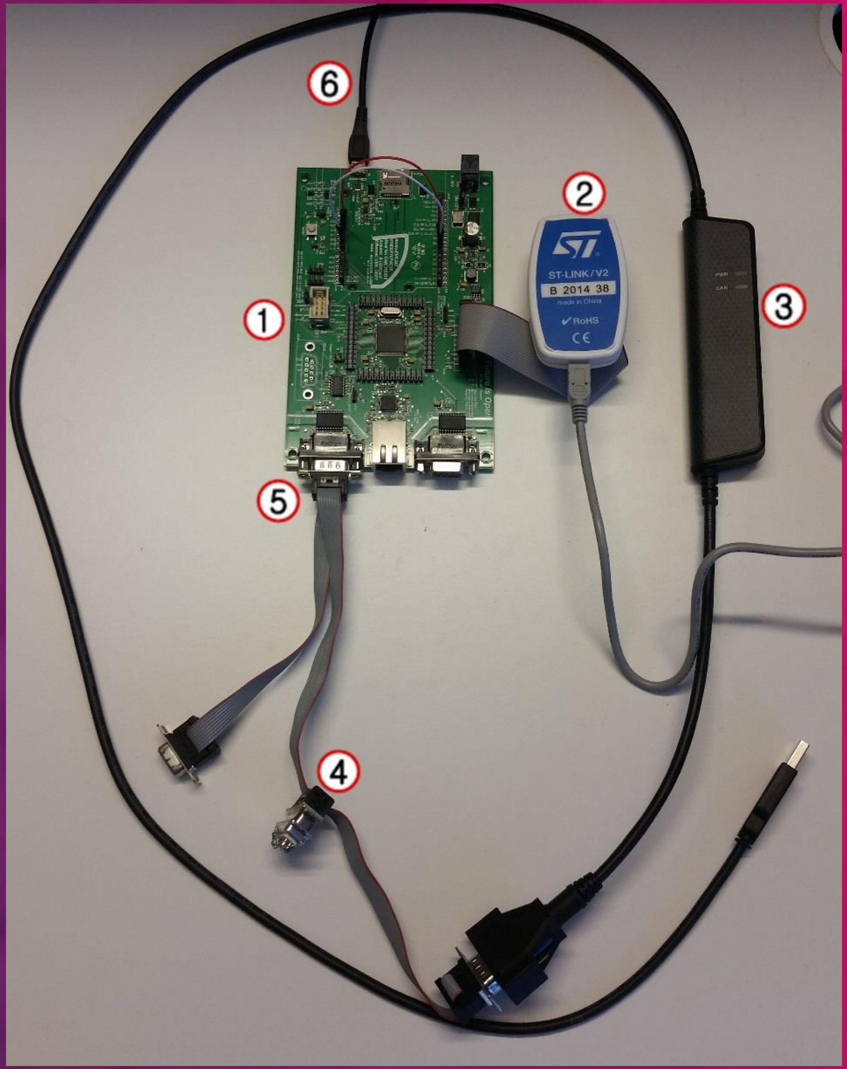
Arccore Hardware board

HARDWARE:

1. STM32 Arctic hardware board
2. ST-Link v2 Debugger
3. Kvaser Leaf Light v2
4. Capacitors
5. CAN-port 1
6. Mini USB power supply

SOFTWARE:

- Arctic Studio
- WinIDEA
- BusMaster



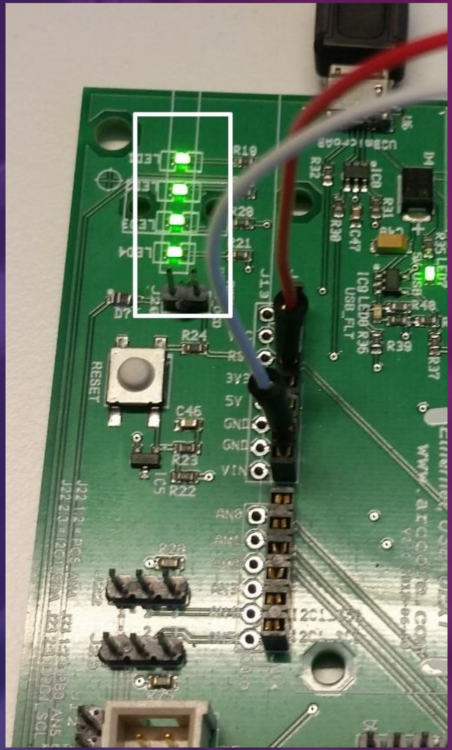
COMBITECH

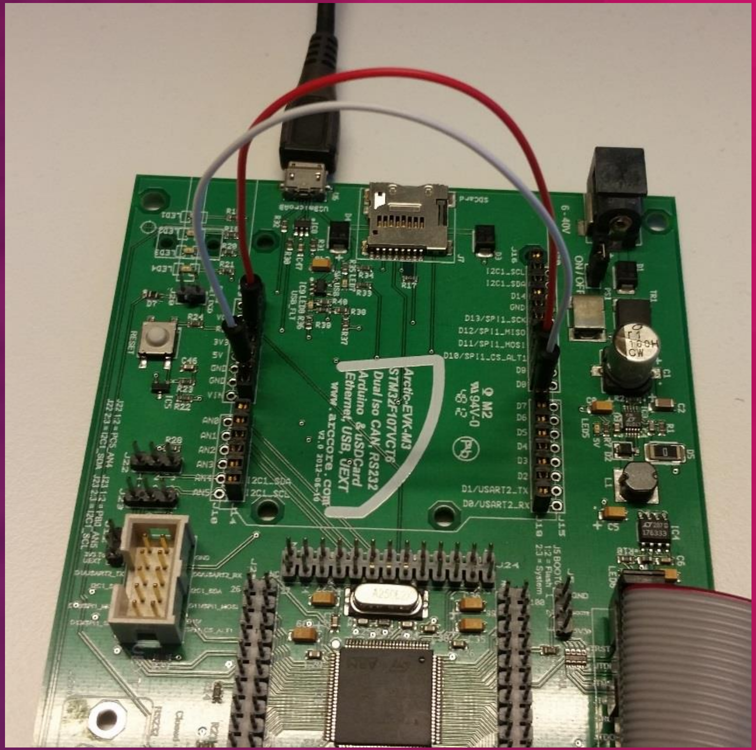
Arccore Hardware board

- Interior Lights Indicator
- 4 LEDs

- 2 wires simulate doors open/close

- One threat from each STRIDE category tested





Results

- The Interior Light SWC – VULNERABLE !
- A threat from each STRIDE category verified
- Security concepts violated:
    - Authentication
    - Integrity
    - Non-repudiation
    - Confidentiality
    - Availability
    - Authorization

- SecOC module – Authentication, Replay & Integrity

Conclusion

- Automotive industry needs more methods for threat detection
- Apply experiences from computer industry
- STRIDE and TARA sucessfully adapted and applied to the connected car
- Template from the NCC Group a good starting point
- TAL, MOL & CEL can be further developed and adapted by each car OEM
- Security needs to be incorporated from the start and not as an afterthought

Based on a paper published on the 15th ESCAR Conference 2017 and can be found in the download area at *www.escar.info*

COMBITECH