Automotive Security Challenges in Autonomous Driving Systems

Presenter: Hoyong Lee

Seoul, Korea, 29.06.2017

Agenda

- Security Constraints
- Evolution of Automotive
  - Digital Revolution
  - Advanced Driver Assistance Systems (ADAS)
  - Autonomous Driving (AD)
- Security
  - Automotive Security Today
  - Autonomous Driving Attacks
- Security Measures
  - Security for the Complete System
  - Use Cases of Automotive Security Solution
- About Escrypt

info@escrypt.com

escrypt
Embedded Security by ETAS

- Security is usually only one concern of many others
  - that interdepend
  - that may conflict
  - that becomes forgotten
  - …

Security Constraints

- Security is often hard to sell
  - For customers, well-implemented IT security measures (in contrast to most other features) are (if done good) invisible and without any apparent functionality.
  - Very often, security is more a basic expectation that an important feature.
- Security is often difficult to build adequately
  - Prevent undersized, but also oversized security solutions.
- Security is often too late
  - Need for security is often regarded first, when the system is already broken.
  - Adding security afterwards is seldom easy, cost efficient, timely, … if possible at all!
  - Security experts need to be involved from the start!

info@escrypt.com

Security Constraints

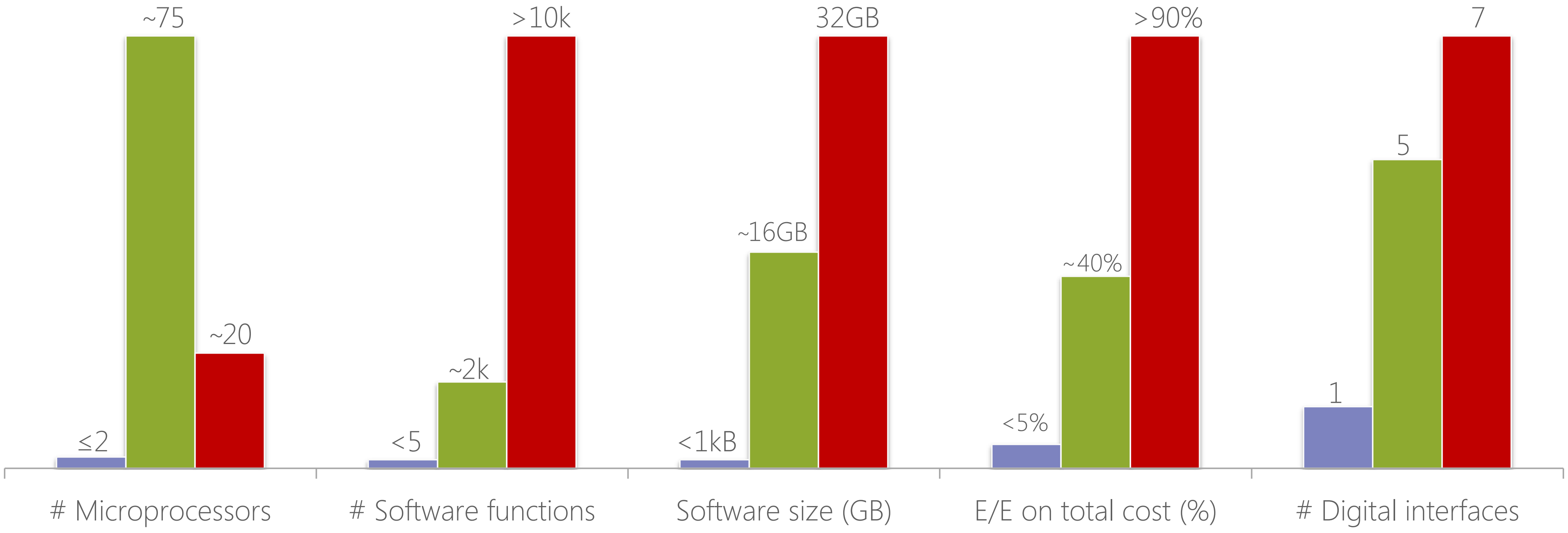
- Security…
  - … is not (only) cryptography
    The latest "biclique cache timing sub-key attack" on AES in 99,99% will not be the weakest link (and hence the preferred attack path) for your security solution!
  - … is more than technology
    Vulnerabilities in organizational aspects, processes and policies are equally dangerous and important!
  - … does not add up
    A weak, a medium, and a strong protection measure do not add up to a more than a strong measure in total, but remain weak!

Security is only as strong as the weakest link in the chain!

The Digital Revolution of Modern Cars

A Comparison

Car 1981 Car 2014 Smartphone 2014

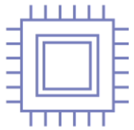


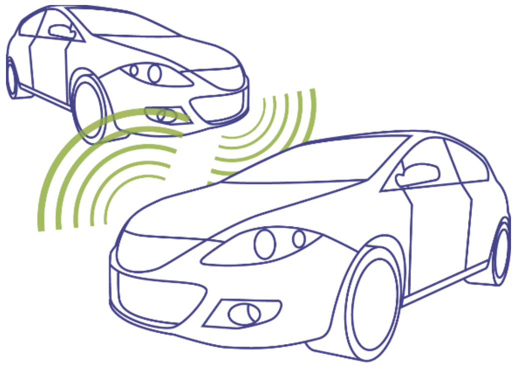
info@escrypt.com

ADAS

Consequence of the Digital Revolution

- Digital Revolution allows for **Advanced Driver Assistance Systems (ADAS)**
- ADAS rely on **important improvements** in:
  - sensor technologies (e.g. movement sensors or cameras)
  - Processing capacity
  - Algorithms

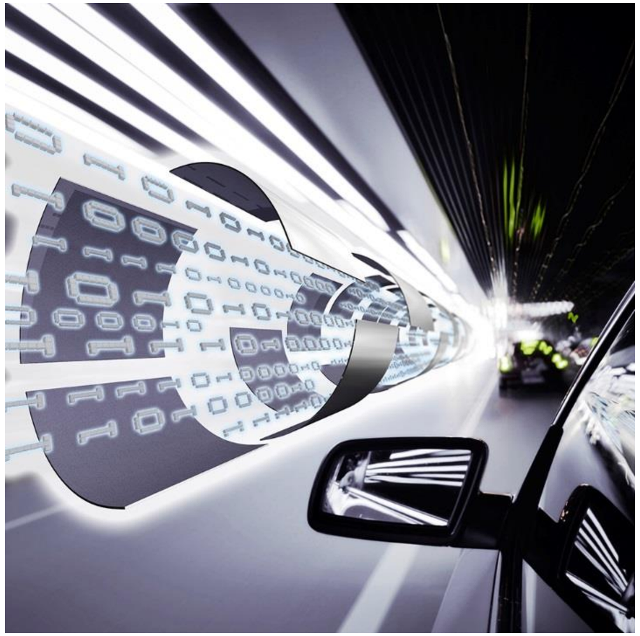




info@escrypt.com

From ADAS to Autonomous Driving

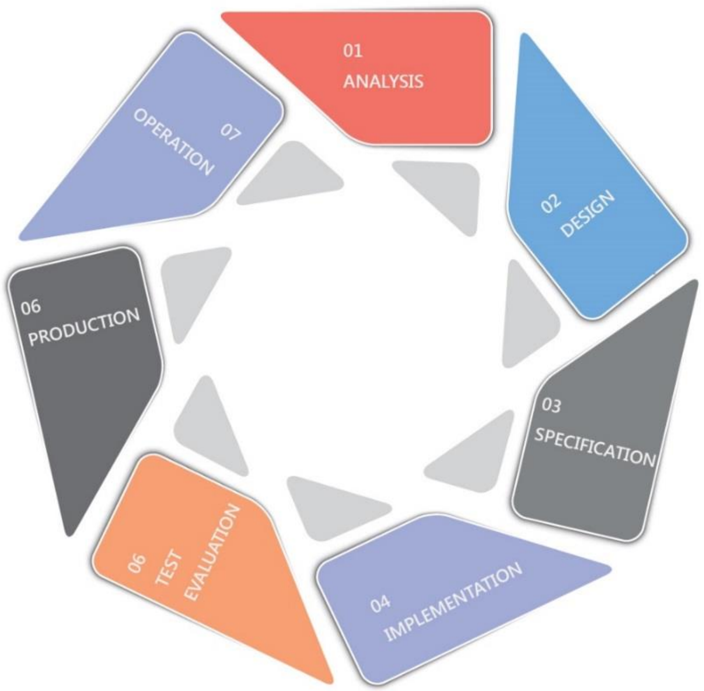
- The integration of different vehicle components and progresses in C2X allow for Autonomous Driving (AD)



- No human intervention, i.e. vehicle control is totally performed by IT systems -> liability in case of accident
- No backup control of the vehicle

info@escrypt.com

- Safety issues: plausibility tests and redundancy
- IT Security is crucial and should be performed during the whole lifecycle of the product



Automotive Cyber Security Today

Exemplary Automotive Attackers & Attacks

- Thieves…
  - steal valuable car parts (e.g., airbag, infotainment)
  - steal complete cars (e.g., 18.800 in 2013 in Germany)
- Owner or driver…
  - manipulate vehicle data records (e.g., odometer, electronic data recorder, or digital tachograph)
  - manipulate (legal or safety) car settings (e.g., no TV while driving lock, exhaust system, chip tuning)
  - infringe licenses or underlying business models (e.g., illegal navigation CD copies, feature activation codes)
- OEMs and suppliers…
  - steal business secrets (e.g., engine control maps)
  - do counterfeiting and piracy (e.g., fake spare parts)
- Third party function providers…
  - exceed their given authorizations (e.g., unauthorized access to onboard resources, user data espionage)
- Hackers, viruses, malware…
  - steal personal data (e.g., contacts, calls, logbook, vehicle location, images captured by the video camera)
  - sabotage driving safety (e.g., interfere with ABS, ESP, steering control)
  - Modify street maps
  - Manipulate GPS signals
  - Spoof V2X messages

Property

Brand image

Business models

Legal regulations

Know-how

Reliability

Driving safety

Personal privacy

info@escrypt.com

Automotive Cyber Security Today

Example: The Fiat Chrysler Hack

- Published attack by Miller and Valasek (2015)
  - Works on many cars by Fiat Chrysler Automobiles
- Prerequisites
  - Car's IP address is the only information needed
  - No special hardware required, only common notebook
- Attack path and vulnerabilities
  - Contact cellular radio over internet (insufficiently secured external interface)
  - Open SSH session (insufficient access control)
  - Control the infotainment unit (Uconnect) over internal D-BUS (no secure onboard communication)
  - Flash infotainment unit with modified firmware (no platform security)
  - Send arbitrary commands over CAN bus (no secure onboard communication)

info@escrypt.com

Automotive Cyber Security Today

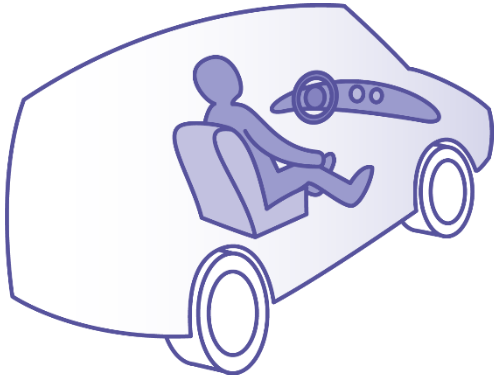
Example: The Fiat Chrysler Hack

- **Impact**
  - Full control over comfort features
    - Heating, infotainment…
  - Full control over the car's steering behavior
    - disable brakes, lights…
    - control acceleration and in some special cases even the wheel
  - Full surveillance
    - Track GPS route, speed etc.

- **Consequences**
  - Affects all FCA cars with the Uconnect unit built btw. late 2013 and early 2015
  - Led to recall of 1.4m vehicles
  - Extensive press coverage and negative publicity for FCA
  - Note: Attack was found by researchers and reported to FCA months before publication

info@escrypt.com

- **Published** attack by Jonathan petit (2015)
- **Prerequisites**
  - Some special hardware (emitters) is required:
    - light sources
    - radio signal sources
- **Attack path and vulnerabilities:**
  - Install emitters in the vehicle or on its proximity
  - Use the emitters to send controlled signals in order to jam or blind the vehicle's sensors
- **Affected Sensors**
  - LIDAR, Camera

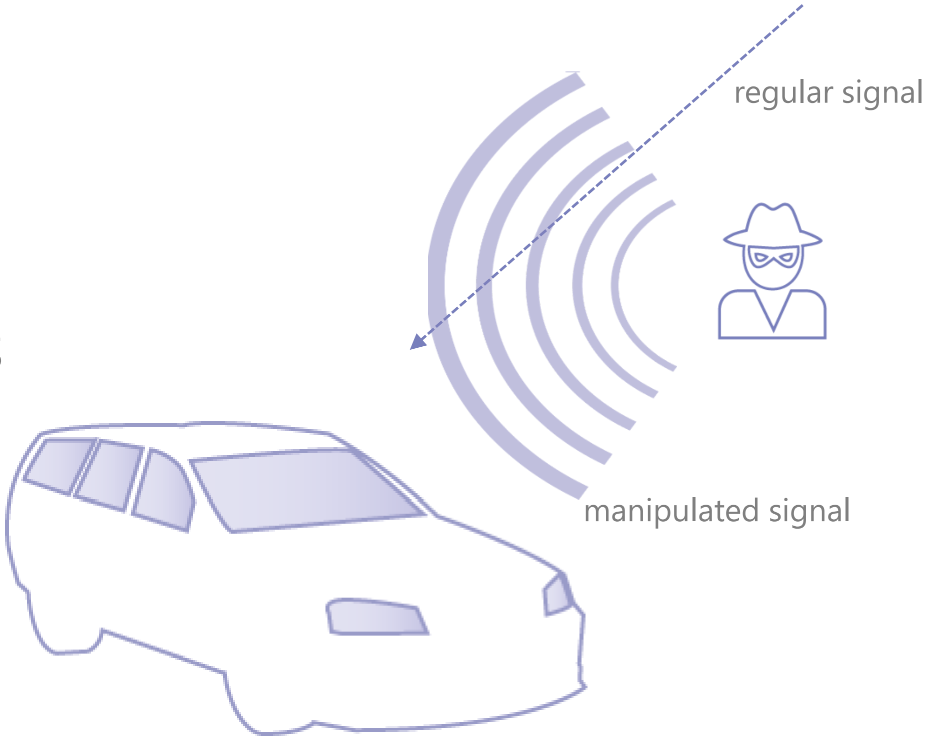


info@escrypt.com

Autonomous Driving Attacks

Example: Tricking the Sensors

- Impact
  - Objects and obstacles are not correctly detected or tracked
  - Lost of location reference
- Consequences
  - This attack was only implemented in the lab
- Countermeasures:
  - Redundancy of cameras and other techniques
    -> specially important for AD systems



Autonomous Driving Attacks

Example: Tracking the Vehicles

- Published attack by Jonathan petit (2015)
- Prerequisites
  - Manipulation of the in-vehicle processing unit
  - Manipulation of the infrastructure
- Attack path and vulnerabilities:
  - Location and driving data from vehicles is transmitted to data centers -> spoof and track
  - This data can be collected by an attacker in-vehicle (by using malware) or in the infrastructure
- Affected Interface
  - 802.11p

info@escrypt.com

Autonomous Driving Attacks

Example: Tracking the Vehicles

- Impact
  - Full surveillance
    - Collecting location and other information from the vehicle or from the infrastructure
    - Location of the vehicle at different times
- Consequences
  - This attack was only implemented as a proof-of-concept
- Countermeasures:
  - Encryption of the signals
  - Anonymous credentials
  - Usage of Pseudonyms

info@escrypt.com

- **Published** attack by Shepard et al. (2012)*
  - This attack was performed on UAVs (unmanned aerial vehicle), i.e., drones
- **Prerequisites**
  - Hardware: radio frequency front-end
  - Software: special techniques developed to spoof the GPS signal
- **Attack path and vulnerabilities:**
  - An attacker receives the civil GPS signal
  - Manipulation of the civil GPS signal
  - Jam the *real* GPS signal with the manipulated one

*Source: Daniel Shepard et al., *Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle*

escrypt
Embedded Security by ETAS

- Impact
  - Hijack a civil drone by spoofing the civil GPS signal
- Consequences
  - Civilian UAVs are vulnerable to sophisticated attackers
  - Allegedly Iran has managed to capture an American drone by jamming the drone's communication
- Countermeasures:
  - improve civil GPS security by using cryptographic and non-cryptographic defenses

info@escrypt.com

escrypt
Embedded Security by ETAS

Increasing digitalization and connectivity have increased the security need of modern cars dramatically

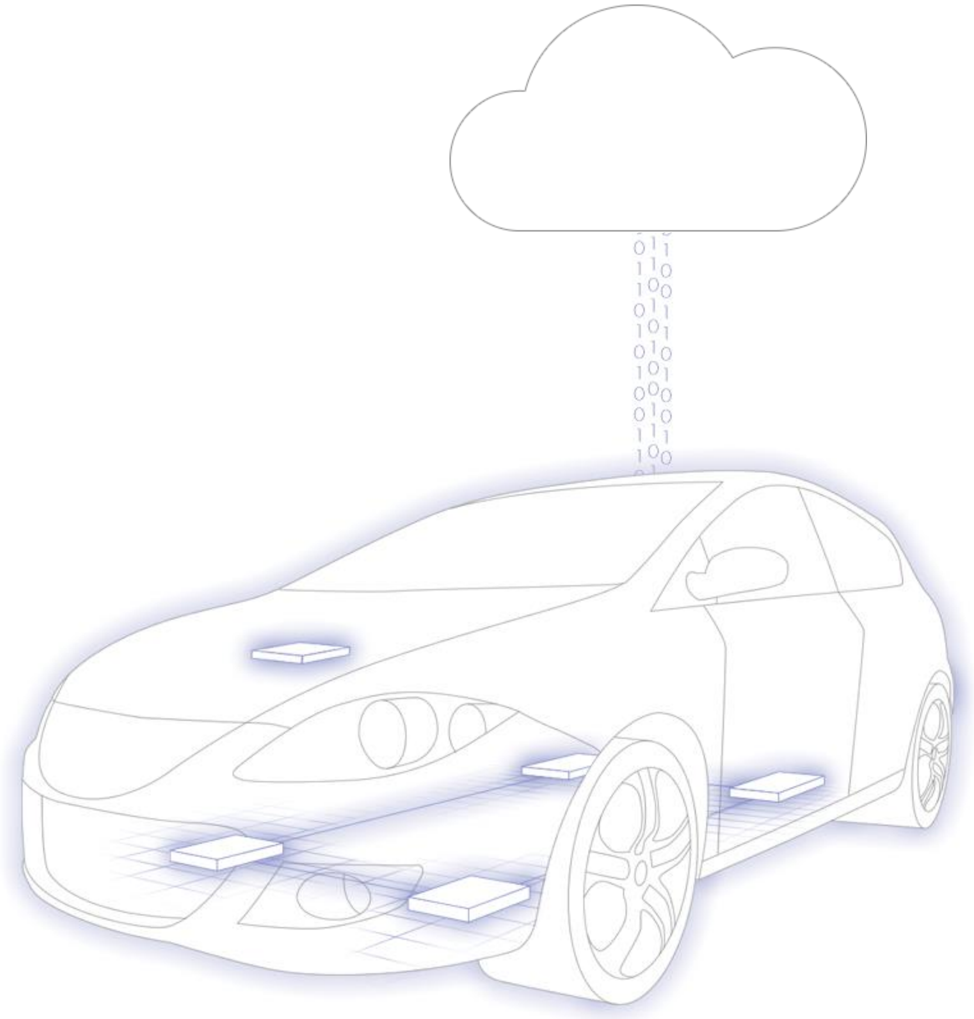
Autonomous Driving relies entirely on the intervention of digital components, which need to be carefully protected against attackers

Common vulnerabilities that are often exploited:

- Only one layer/level of security (if broken, the complete system is broken)
- Implementation flaws
- Outdated security measures
- Insufficient key management and protection
- Insecure onboard communication
- Insecure external interfaces
- No platform security
- …

info@escrypt.com

- **Secure** ECU
- **Secure** Onboard Network
- **Secure** E/E-Architecture
- **Secure** connected vehicle



Threats

- Unauthorized access to, manipulating or copying of software and data
- Privilege escalation
- Side-channel attacks
- Physical manipulation

Security Solution

- Ensuring authenticity, integrity and confidentiality of software and data by modern cryptography
- Access authorization managed by Secure OS, Secure MMU, One-Time-Token etc.
- Logical/physical partitioning of software and data of different security levels, e.g. through virtualization or HSM
- Secure Boot

info@escrypt.com

Security for the Complete System

Secure Onboard Network

escrypt
Embedded Security by ETAS

Threats

- Unauthorized creation, counterfeiting, repeating of messages
- Eavesdropping
- Use of forged message receiver or sender identity, time stamps, message sequences

Security Solution

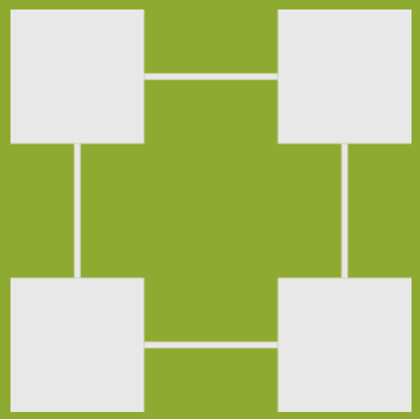
- Authentication of sender and receiver
- Ensuring authenticity, integrity and confidentiality of messages
- End-to-end security
- Granular, restrictive access authorization management
- Logical/physical separation of network areas

info@escrypt.com

escrypt
Embedded Security by ETAS

Threats

- Insufficient separation and insufficient access control with regard to data, functions of different security/safety classification



Security Solution

- Logical/physical separation of vehicle sections through central gateways
- Firewalls
- Intrusion Detection and Response System (IDS und IRS)
- Secure software development based on the principle „security by design"

info@escrypt.com

Security for the Complete System

Secure connected vehicle

Threats

- Manipulation, counterfeiting, eavesdropping, replaying, of messages, data or software by other vehicles, devices, infrastructure or via Internet
- Misuse of external access and usage authorization

Security Solution

- Authentication of sender and receiver through modern cryptography and PKI
- End-to-end security for the communications channels
- Firewalling, Intrusion Detection and Response for all external interfaces
- Isolation of and access control for all 3rd party applications
- Cryptographically secured Software Updates OTA

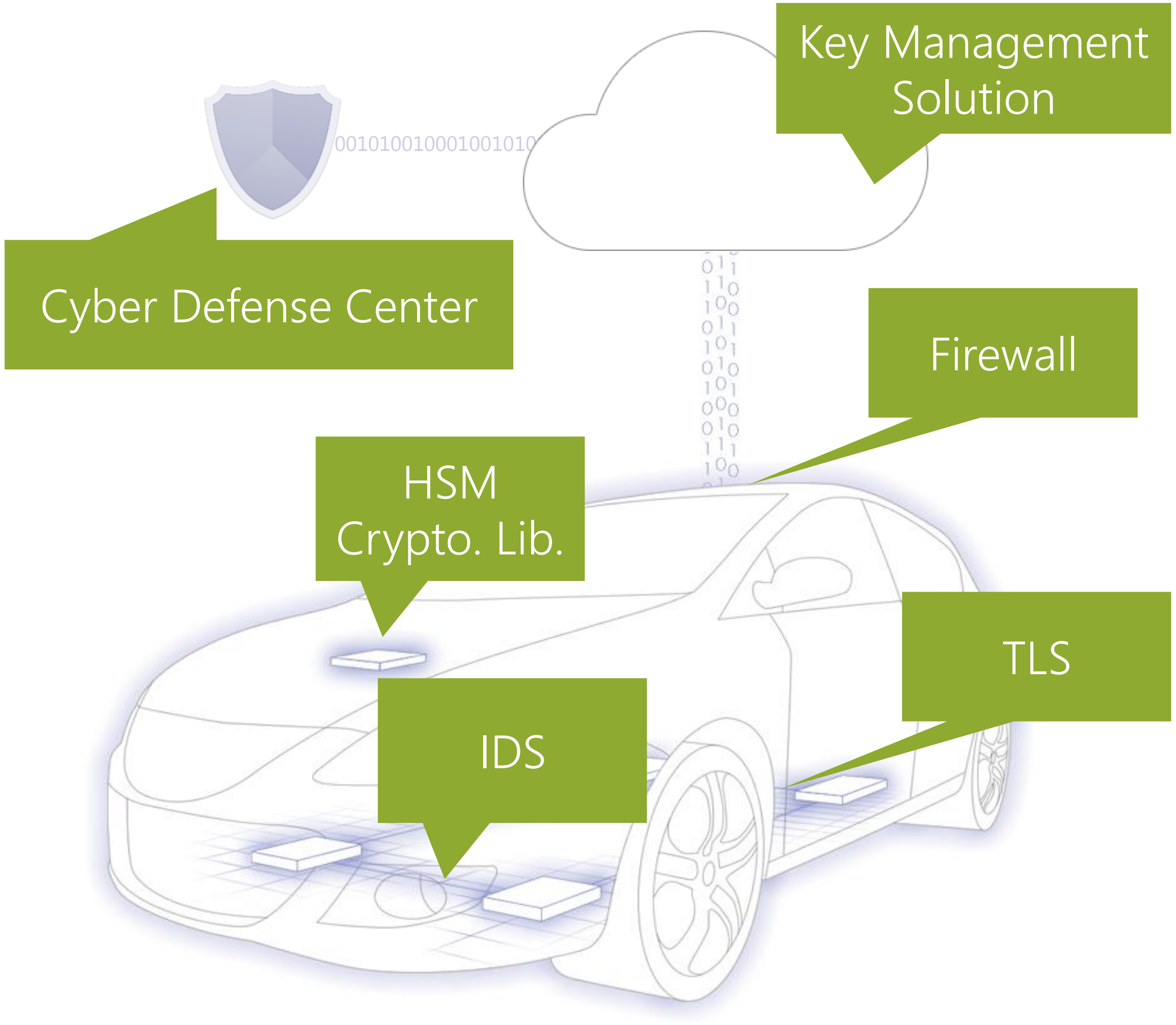
info@escrypt.com

Secure ECU
Protect integrity of ECU software and data
Hardware based security mechanisms

Secure Onboard Network
Protect integrity and confidentiality
of critical in-vehicle signals

Secure E/E-Architecture
Use separation and securely configured gateways
to protect functional domains of E/E architecture

Secure connected vehicle
Automotive firewalls and security standards
for external interfaces



info@escrypt.com

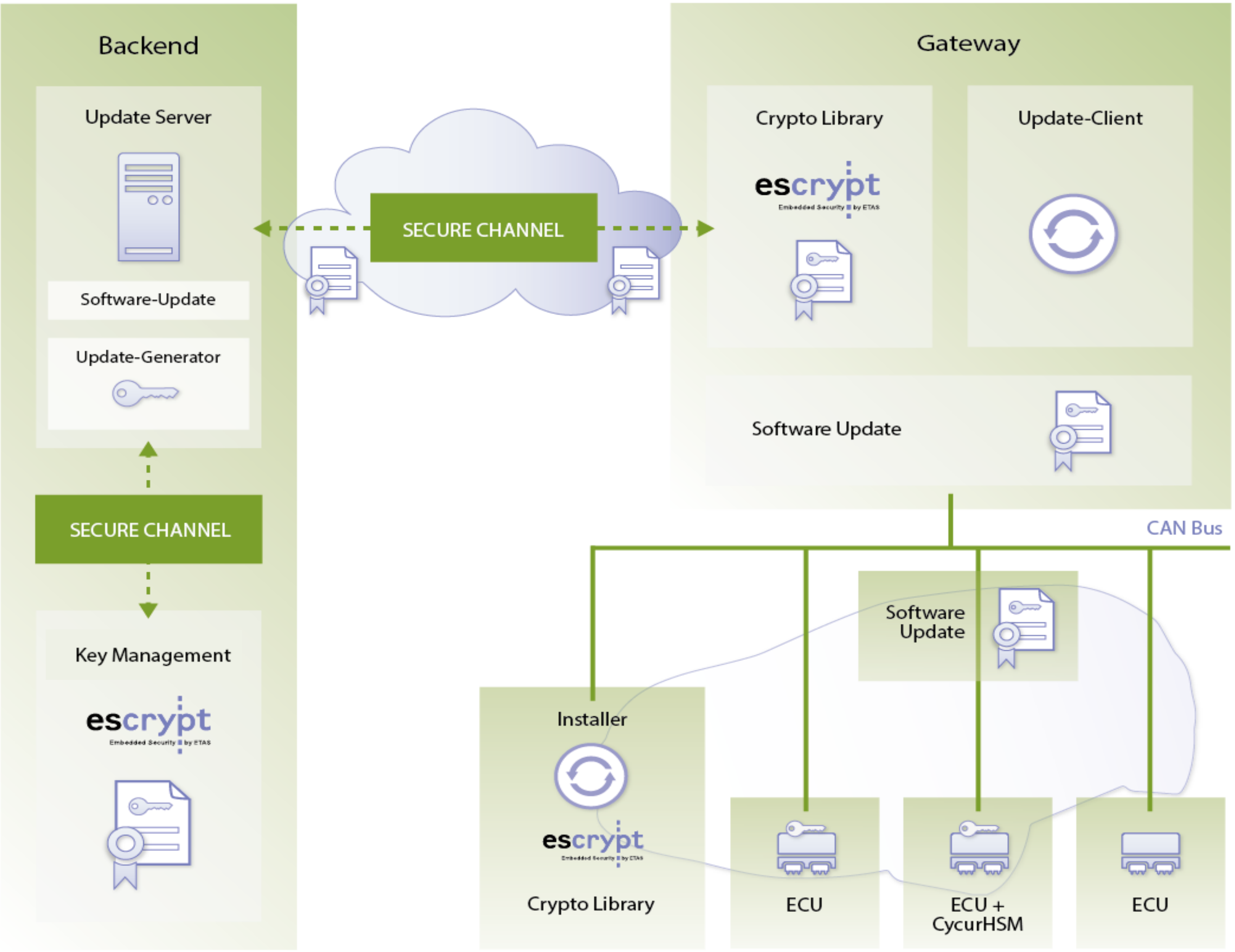
Key Management Solutions

Use Case

Secure Software Updates
Over-the-Air (OTA)

Customer Benefits

- Secure and cost-efficient firmware updates eliminating recalls
- Increases update reaction times and broadens update coverage
- Fully auditable and reliable logs of update activity



info@escrypt.com

escrypt
Embedded Security by ETAS

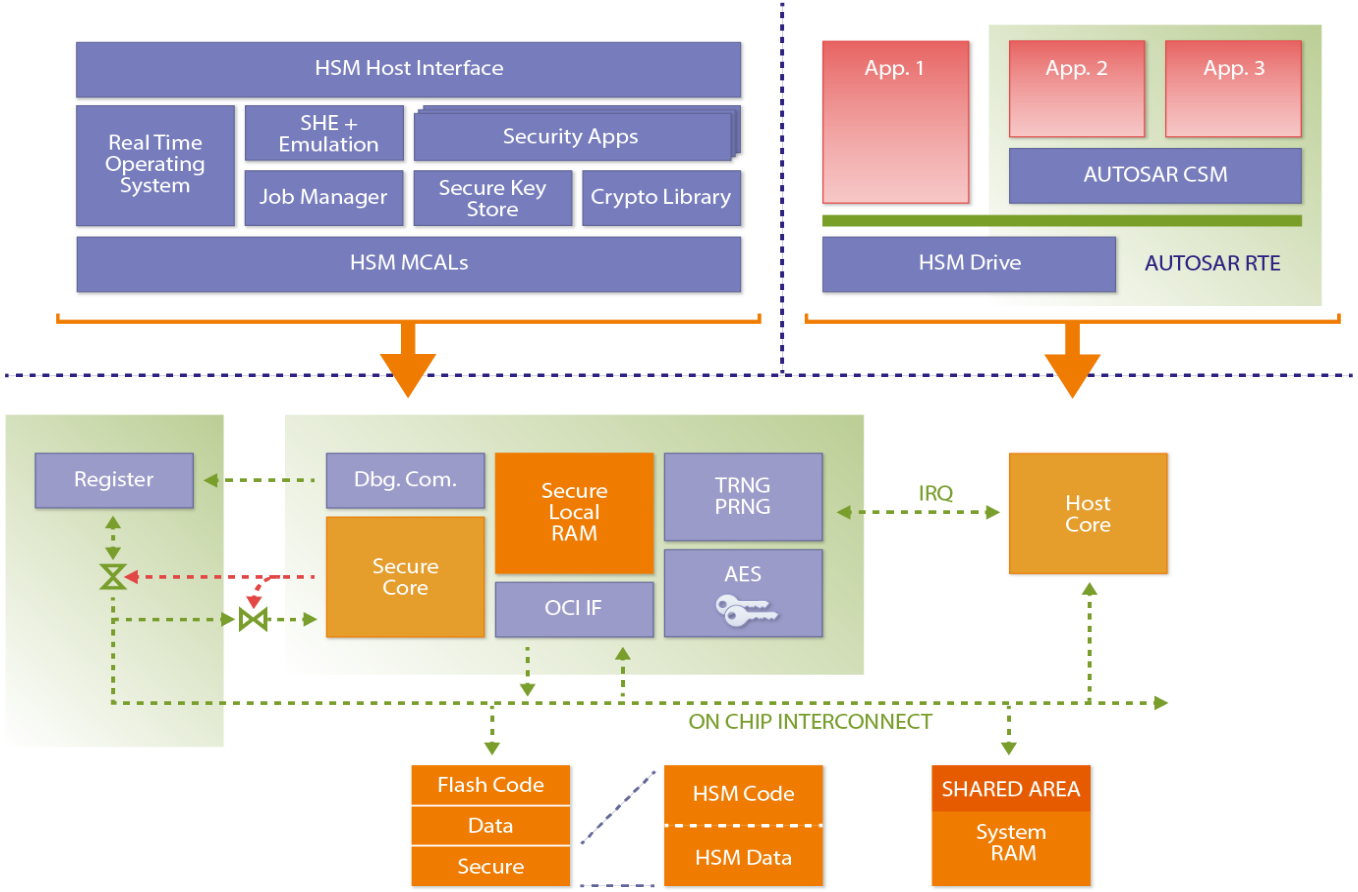
Plug & Play Integration of Hardware Security Modules

Use Case

Integrating Hardware Security Modules (HSM) requires the creation of a second independent software environment in the control unit

Customer Benefits

- Turnkey software solution with well-defined interfaces makes the development complexity manageable
- Encapsulating security functions, leaving the application developer free to concentrate ensuring ECU functionality



escrypt
Embedded Security by ETAS

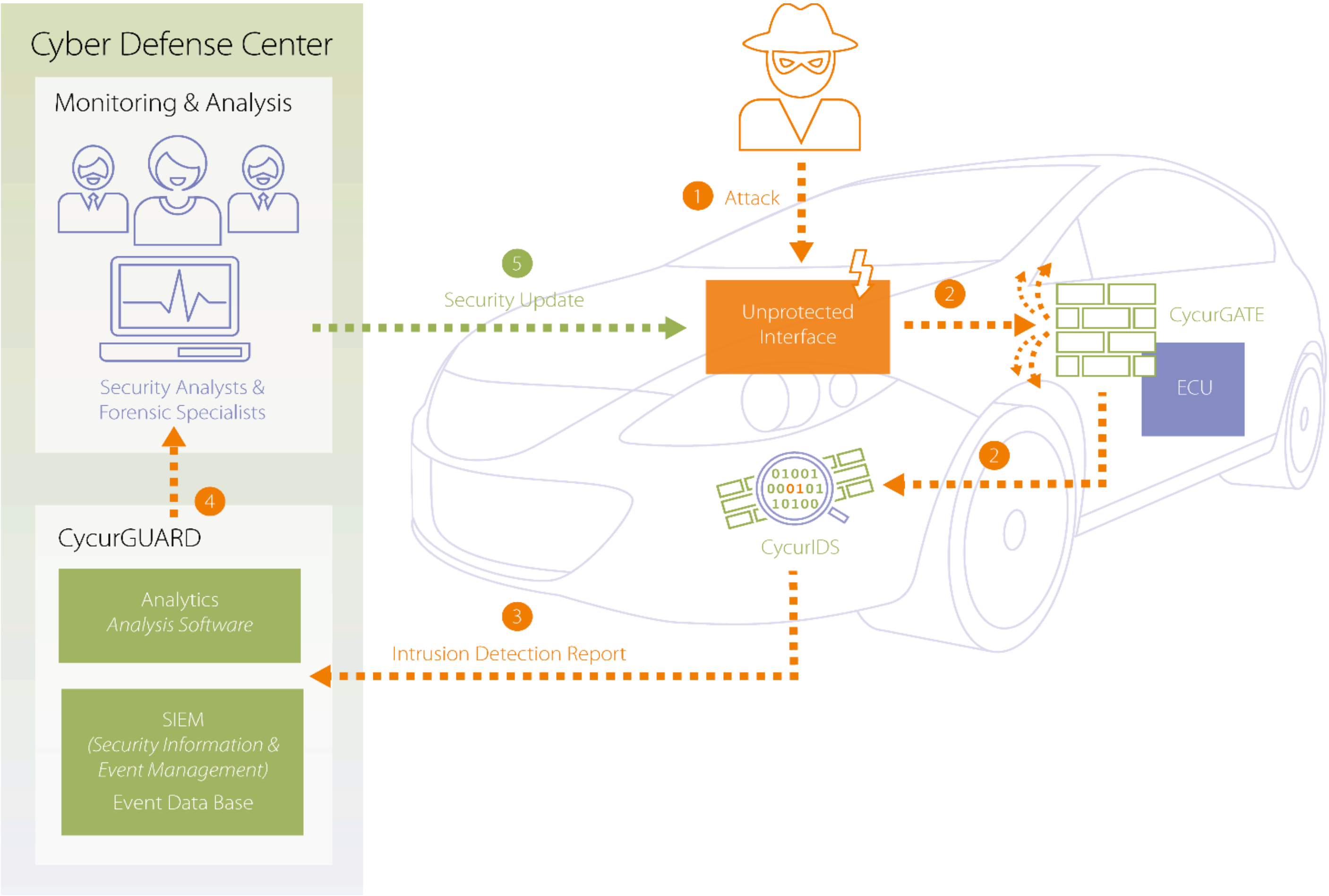
Automotive Intrusion Detection and Prevention System

Use Cases

Detect intrusions in vehicles' network, analyze and assess potential intrusions, manage and roll out counter measures

Customer Benefits

- Timely detect and react on ongoing cyber security attacks
- Overview of cyber security welfare of vehicle fleet
- Cost-efficient further development of cyber security
- Fulfillment of (future) legal requirements, especially in the US



Corporate Profile

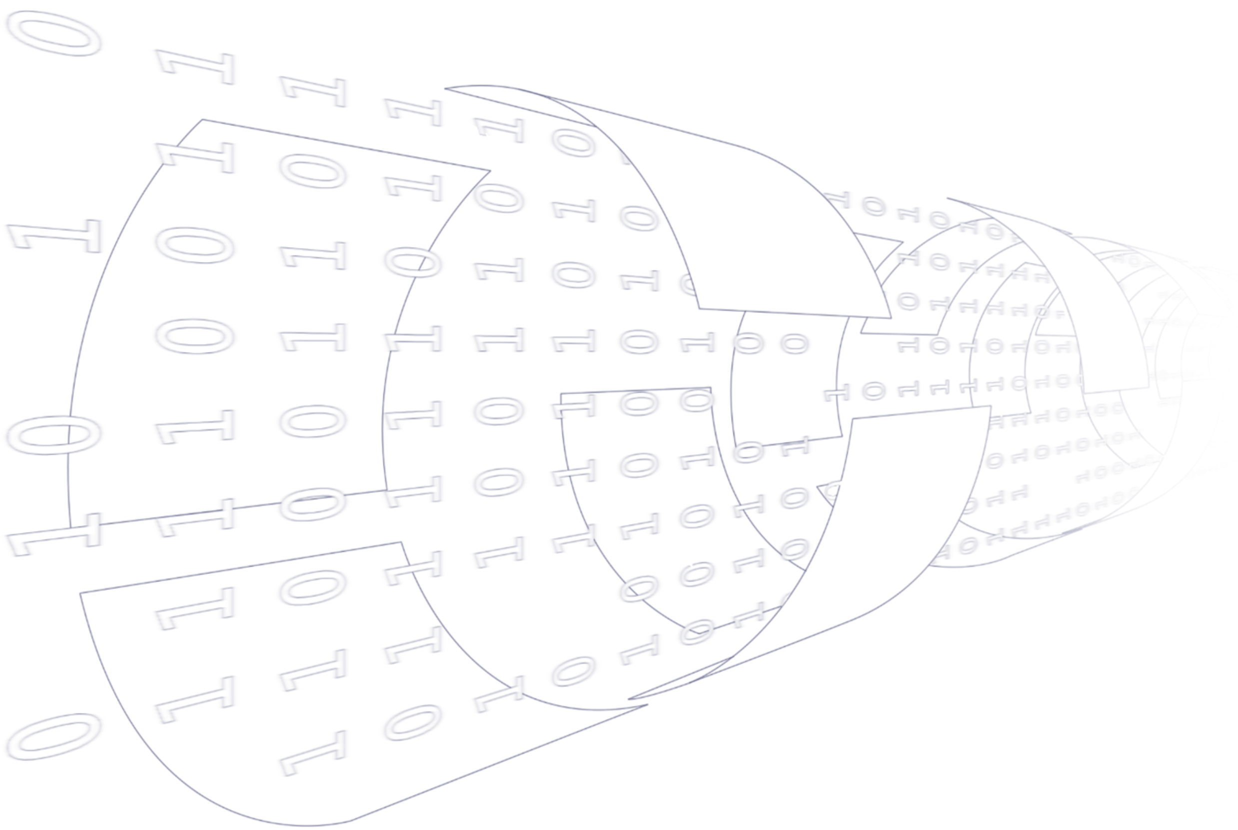
ESCRYPT GmbH

Founded in:	2004
Shareholder:	100 % ETAS GmbH
Headquarters:	Bochum, Germany
Employees:	150 security experts world-wide
Management:	Martin Ridder, Dr. Thomas Wollinger

Portfolio

ESCRYPT provides a variety of products and services to protect and secure devices, applications, business models, and back-end infrastructures.
ESCRYPT's products are applicable to all industries with a need for embedded security.

- Security consulting and services
- Security products
- Tailored security solutions
- Supporting infrastructure



Corporate Profile

Service Wherever it is Needed

Europe

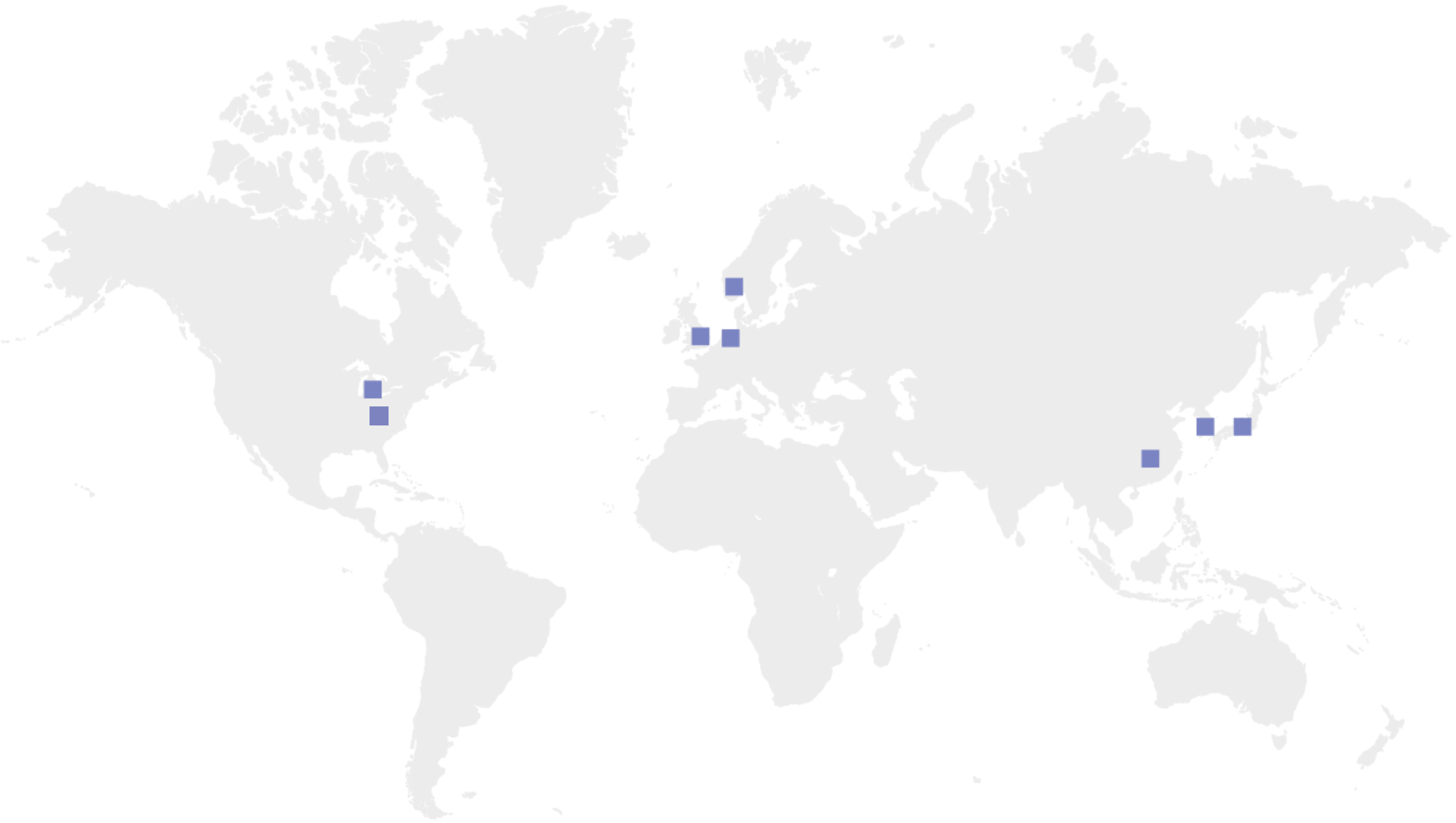
Germany: Berlin, Bochum, Munich, Stuttgart, Wolfsburg
UK: York
Sweden: Lund

Asia

China: Shanghai
Japan: Yokohama
Korea: Seoul

Americas

USA: Ann Arbor
Canada: Waterloo



ESCRYPT - Embedded Security KOREA

4F, ABN Tower, Pangyo-ro 331, Bundang-gu
Seongnam-si, Gyeonggi-do, 13488
Rep. of KOREA

Phone: +82 31 326 6200
Fax: +82 31 326 6209

info@escrypt.com
www.escrypt.com