escrypt
SECURITY. TRUST. SUCCESS.

Security trainings

Standard security trainings and coaching

Learn and understand automotive security

ESCRYPT is a leading provider of IT security solutions in embedded systems and of consultancy and services for enterprise security and IT-protected production. Particularly in the area of automotive security and automobile series production, ESCRYPT solutions are used today millions of times over. We channel our years of experience in embedded security, gained during numerous industry projects, to provide practical examples and the latest technological developments.

Your advantages

- We have more than 15 years of experience in automotive security
- Our trainings are based on numerous customer projects and include up-to-date-knowledge about the industry and its development
- All our trainers have a background in IT security and years of practical experience with insights from various customer projects
- Upon completion, each participant receives a certificate of attendance

Designed to suit your needs

- Wide range of topics that cover theoretical as well as practical aspects
- Including discussions, real-world examples as well as best practice solutions
- Offered worldwide and when possible in local language
- In-house trainings at your location, in one of our offices as well as online sessions
- Individual training concepts on request
- Recommended group sizes from 8 to 12 participants

	Training	Description	Duration
Basic	**Secure product design**	Fundamentals of information security including technical and organizational aspects for product development.	2 days
	Security testing	Introduction to security testing methods for the entire lifecycle.	1 day
Advanced	**Secure connected products**	Advanced security aspects of connected products explaining best practices to secure communication.	1 day
	Automotive security	A holistic view on automotive security with best practices for hardware and software in modern automotive systems.	2 days
	ISO 21434 security engineering and management	Introduction to ISO/SAE 21434 cybersecurity management and engineering activities for the entire lifecycle in context of UNECE R155.	2 days
Coaching	**Security risk analysis**	Why, when, and how to perform a security risk analysis. We support you to create a security risk analysis for one of your own systems.	3 days
	Security testing strategy	Develop a strategy how to approach security testing for your organization and products.	1 day

"I'm a product manager and wanted to learn about different security principles and cryptographic tools. Mission accomplished – the training was great!"

Participant of ESCRYPT's
secure connected products training

"After the training I know much more about automotive security. Especially the information on secure connected vehicles and secure networking will help me in my work."

Participant of ESCRYPT's
automotive security training

BASIC TRAINING

Secure product design

Training topics

- Get to know different aspects of security (e.g., theory vs. practice, challenges)
- Learn and understand security basics (e.g., basic terminology)
- Find out how to set up a secure software development lifecycle
- Establish fundamental knowledge about cryptographic tools, algorithms, and protocols
- Understand important aspects of access control (authentication and authorization)
- Learn to apply main security principles
- Secure coding module option: comprehend secure coding techniques
- Risk analysis module option: learn how to apply a risk-based approach towards security (e.g., economic security)

Target group

- Product managers and project managers who need to establish a solid understanding about general security principles, processes and tools that are necessary for secure product design
- System engineers and system architects who are responsible for developing and analyzing security requirements and for defining security concepts

Requirements

- Basic technical understanding of mathematical and information technology on engineering level
- No security background is necessary

Duration:
2 days / 16 hours

Languages:
German / English / Chinese / Japanese / Korean

Location:

- ESCRYPT site
- customer site
- conference hotel
- online

Day 1

Security basics

- Discussion of recent IT security threats
- Different aspects of IT security
- Basic terminology
- Generic security framework

Secure software development

- Economic security
- Security activities for a software development process
- Conventional software development
- Agile software development

Cryptographic primitives

- Benefits and limitations of cryptography
- Fundamental cryptographic principles
- Symmetric and asymmetric tools and algorithms
- Cryptographic protocols
- Application and practical advices

Day 2

Access control: authentication

- Password-based authentication and secure password management
- Multi-factor authentication
- Implementation aspects

Access control: authorization

- Permission management and access control lists, role-based access control
- Capabilities and secure session management

Security principles & concepts

- Security principles (defense in depth, keep it simple, least privilege)
- Security concepts (trust boundaries, separation of duties, error and exception handling)

Secure coding

- Secure coding in the development process
- Weaknesses, vulnerabilities and attack references
- Best practices in defensive coding and secure coding guidelines

BASIC TRAINING

Security testing

Training topics

- Get to know the motivation, challenges and limitations of security testing
- Find out how to thoroughly consider security testing in the product development lifecycle (e.g., testing activities in the different phases of the lifecycle)
- Get an overview of different security testing methods and understand the differences
- Learn and understand the basic principles of security testing
- Learn and understand what to target in the security testing in which testing setup (e.g., systems, devices, components, interfaces)
- Get to know how to handle identified weaknesses and which mitigation options exist
- Understand the requirements for security testing from the most prominent standards and regulations
- Interactive exercises to strengthen understanding of individual topics

Target group

- Product managers, project managers, test managers, and security managers who need to establish a solid understanding about security testing methods and how to apply them throughout the development lifecycle
- System engineers, system architects and testers who are responsible for the execution of test strategies

Requirements

- Technical understanding of systems/products and system/product development
- Basic understanding of IT security is helpful

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ESCRYPT site
- customer site
- conference hotel
- online

Day 1

Introduction

- Real-world example: Why is practical security testing important?
- Security testing in UNECE WP.29 and ISO/SAE FDIS 21434

When to test in the product development lifecycle

- Introduction of a general testing lifecycle form the start in the “analysis phase” until the end in the “phase-out”
- Recommendation of security testing activities for each lifecycle phase
- Considering continuous integrated security testing during development

Security testing methods and principles

- Blackbox vs. greybox vs. whitebox testing
- Security testing methods:
  - Penetration testing
  - Vulnerability scanning
  - Functional security testing
  - Code analysis
  - Fuzzing
  - Hardware / side channel attack testing
- General security testing principles

What to test in the automotive environment

- Overview of security relevant entities, systems, protocols, components, etc. in the automotive vehicle and surrounding environment
- Potential attack points and paths in a modern connected vehicle
- Different testing scopes and testing setups with advantages and disadvantages
- Different aspects of system, device, component and network testing
- How to handle third party components in security testing

Handling of findings and testing resources

- Process for the handling of findings with mitigation options
- Security testing resources with their challenges and competence requirements

Example pentest report and evaluation methodologies

- Important aspects of a security test report
- Investigation of an ESCRYPT example test report with example findings and ratings
- Discussion on different rating methodologies: CVSS, ESCRYPT proprietary rating, ECVSS

ADVANCED TRAINING

Secure connected products

Training topics

- Understand distinct security aspects regarding connectivity
- Get to know important aspects of advanced access control
- Establish an overview knowledge of secure protocol configurations and pitfalls
- Learn the basics about protocols for the internet of things
- Comprehend the threats to interfaces and how to alleviate them
- Find out the basics about web services and possible vulnerabilities

Target group

- Product or project managers who need to establish a solid understanding how secure products are properly secured
- Product engineers who are responsible for analyzing and defining security requirements and for defining security concepts

Requirements

- Basic technical understanding of mathematical and information technology (engineering level)
- Basic technical understanding of cryptography and IT security (i.e., knowledge from secure product design or equivalent)

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ESCRYPT site
- customer site
- conference hotel
- online

Day 1

Connectivity basics

- Connected systems and architectures
- Security in the internet protocol stack
- Advanced access control, public key infrastructures

Secure communications

- Secure IP-based communication protocols
- Secure TLS configuration
- IoT technologies: Wi-Fi, Bluetooth, BT Low Energy, NFC, ZigBee

Interface protection

- Attacks on external interfaces
- Securing interfaces

Web services

- Types and uses cases
- Access control
- Command injection

ADVANCED TRAINING

Automotive security

Training topics

- Get to know current aspects of automotive security
- Discover a holistic view on automotive security
- Understand the challenges and possibilities to develop secure ECUs
- Get to know the challenges and possibilities of secure networking
- Learn about the challenges and possibilities of secure connected vehicles
- Gain an overview of the most important automotive safety standards

Target group

- Product or project managers who need to establish a solid understanding about automotive security principles for secure design of ECUs, the on-board network or connected vehicle services
- Automotive product engineers who are responsible for analyzing and defining security requirements and for defining security concepts

Requirements

- Basic technical understanding of automotive systems on engineering level
- Basic technical understanding of cryptography and IT security, i.e., knowledge from secure product design or equivalent

Duration:
2 days / 16 hours

Languages:
German / English

Location:
- ESCRYPT site
- customer site
- conference hotel
- online

Day 1

Introduction to automotive security

- Overview of automotive threats
- Review of recent successful attacks

Holistic automotive security

- Security as a process
- Security stages for a holistic security model

Secure ECU design

- Software
- Case study: AUTOSAR
- Hardware
- Case study: SHE
- Trust anchors, key handling, and supply chain security

Day 2

Secure on-board networking

- Automotive network buses
- Network security measures
- Case study: SecOC
- Secure network architectures

Secure connected vehicles

- Automotive IoT use cases
- Protection of external interfaces

Automotive security standards

- Security activities in the automotive lifecycle
- UNECE WP.29 & ISO 21434

ADVANCED TRAINING

ISO 21434 security engineering and management

Training topics

- Learn the building blocks of ISO/SAE FDIS 21434 compliant security engineering
- Get an overview how ISO/SAE FDIS 21434 helps you to meet the requirements of the UN regulation 155
- Understand the risk-based approach of ISO/SAE FDIS 21434 to product security
- Learn from our firsthand expertise for the ISO/SAE FDIS 21434 through dedicated case studies
- Get to know more about security engineering during the concept phase (incl. cybersecurity relevance assessment, goals & concept)
- Find out about the importance of security engineering in the development phase (incl. cybersecurity DIA, design, implementation and V&V)
- Benefit from our knowledge about cybersecurity in production, operations, maintenance and decommissioning

Target group

- Security manager, product manager or project manager
- System engineer, software engineer, hardware engineer, developer

Requirements

- Basic technical understanding of automotive systems on engineering level

Duration:
2 days / 16 hours

Languages:
German / English / Japanese

Location:
- ESCRYPT site
- customer site
- conference hotel
- online

Day 1

Introduction to security engineering

- Motivation based on common challenges
- Context of the UNECE WP.29 regulation
- ISO/SAE FDIS 21434 overview

Governance and ecosystem

- Cybersecurity Management System (CSMS)
- Security in the supply chain

Risk management

- Risk assessment methodology

Day 2

Risk management (continued)

- Continuous cybersecurity activities including cybersecurity monitoring, vulnerability analysis and management

Concept and development

- Project-level cybersecurity management
- Security goals and concept
- Cybersecurity validation

Production and operation

- Production security
- Incident response and patch management
- Decommissioning

Outlook

ADVANCED COACHING

Security risk analysis

Coaching topics

- Learn and understand how security risk analyses contribute to efficient and effective risk management, e.g., in the context of IOS/SAE FDIS 21434
- Get to know one methodology of security risk analyses
- Carry out a security risk analysis for one of your systems

Target group

- Product and project managers who need to understand the methodology of a security risk analysis in the context of the product development process
- Security managers who are responsible for conducting security risk analyses during the product development process

Requirements

- Basic knowledge of product development processes
- General understanding and awareness of security risks
- Overview and description of the system that is to be evaluated

Duration:
3 days (spread over approx. 3 month)

Languages:
German / English

Location:

- ESCRYPT site
- customer site
- conference hotel
- online

Workshop 1

- Why to perform a security risk analysis?
- Introduction to the security risk analysis methodology
- What are the valuable assets of your target of evaluation?

Workshop 2

- Lessons learned and results from workshop #1
- Threat analysis based on attack trees
- Assessment of attack potentials based on common criteria

Workshop 3

- Lessons learned and results from workshop #2
- What could possibly go wrong?
  - Damage scenarios
  - Damage potential assessment
- Risk handling
- Security needs
- Discussion and Q&A

In-between the workshops, the customer team completes the steps of the methodologies, while the ESCRYPT trainer provides support and reviews.

ADVANCED COACHING

Security testing strategy

Coaching topics

- Get to know the motivation, challenges and limitations of security testing
- Find out how to thoroughly consider security testing in the product development lifecycle (e.g., testing activities in the different phases of the lifecycle)
- Get an overview of different security testing methods and understand the differences
- Learn and understand the basic principles of security testing
- Learn and understand what to target in the security testing in which testing setup (e.g., systems, devices, components, interfaces)
- Get to know how to handle identified weaknesses and which mitigation options exist
- Create a first draft of a security testing strategy during the workshop
- Understand the requirements for security testing from the most prominent standards and regulations

Target group

- Product managers, project managers, test managers, and security managers who need to establish a solid understanding about security testing methods and how to apply them throughout the development lifecycle.

Requirements

- Technical understanding of systems/products and system/product development
- Basic understanding of IT security is helpful
- If available, an overview of the own security testing strategy

Duration:
1 day / 8 hours

Languages:
German / English

Location:
- ESCRYPT site
- customer site
- conference hotel
- online

Training

- Real-world example: Why is practical security testing important?
- Security testing in UNECE WP.29 and ISO/SAE FDIS 21434
- When to test in the product development lifecycle
- Security testing methods
  - Penetration testing
  - Vulnerability scanning
  - Functional security testing
  - Code analysis
  - Fuzzing
  - Hardware / side channel attack testing
- General security testing principles
- What to test in the automotive environment
- Handling of findings and testing resources

Workshop

- Status quo of security testing
- Which testing methods are already established? What's being used today?
- What is currently working well and where are the gaps?
- Which testing methods and tools do we want to use in the future?
- When and to what extend do we need to test?
- Who is responsible for which testing artefacts?
- What could a future security testing strategy look like?

Topics and leading questions can be tailored to customer needs.

Ready to train you worldwide

Bangalore Berlin
Bochum Gothenburg
Lund Munich Plymouth
Pune Saint-Ouen Seoul
Shanghai Stuttgart
Sunnyvale Torino Warsaw
Waterloo Wolfsburg
Yokohama York

ESCRYPT 2021/06

Any questions?

Please contact us any time.

info@escrypt.com
Phone: +49 234 43870-200
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.