

Riscure Training Academy

2018 Course Calendar



Your partner for
Expert Security Knowledge
in Embedded Device Security

It is only possible to deliver robust hardware and software when security is part of your development process. To test your products you can use the specialized tools and services of Riscure. To embed security in your product lifecycle, you need to invest in your talent. Riscure Training Academy helps your development team accelerate the learning of the latest attack and mitigation techniques. We achieve this by adding three main ingredients to every course: a view from an attacker's perspective, detailed knowledge of the security landscape relevant for your industry, management and collaboration approaches to deliver secure software and devices. Our courses condense years of experience of our security team, hundreds of successful security evaluation projects and in-depth research on device security to deliver exactly these three requirements to your company and your development team.

Learn more about Riscure Training Academy at www.riscure.com/training/
Get in touch with us via trainingacademy@riscure.com

Embedded Systems Security

This introductory course covers the most relevant attacks and protection methods for embedded devices. The main goal is to broaden your horizon and offer an answer to the important question: "Is my embedded device secure?". If the answer is a positive one, this course helps you build the argument for why this is the case. If on the other hand, the answer is a negative one, this training gives you a plan on how to start implementing security. The recommended course for security experts looking for an essential overview of embedded systems security.

2018 Availability: Open Training in November



Vulnerability Identification and Code Hardening

This course is a comprehensive introduction to the art and practice of code auditing and code hardening. The main objective of the training is to enable developers to find vulnerabilities in their code by covering the what, why and how of code auditing and code hardening strategies. The training is highly practical with many C language examples which illustrate the concepts discussed during the training.

2018 Availability: Open Trainings in May and November, US Roadshow in June



ARM Reverse Engineering

The ARM Reverse Engineering training for software applications helps you understand how attackers take a piece of software apart and analyze its inner workings. The training will give you a solid overview of the techniques to navigate, instrument and analyze binary code. This course is aimed at development professionals who implement countermeasures.

2018 Availability: Open training is over, only on request



Fault Injection: Essential and Advanced

Fault Injection is an art of hardware hacking, where a disruption of a normal device operation helps to reveal secrets or bypass security mechanisms entirely. An approach often overlooked by hardware and software developers, it is becoming even more important as the software protection methods are getting more robust. During this course you learn how to inject faults for the purpose of security testing and you will apply these techniques in practice on real-world targets. This course is offered in two different types: Essential is focused on the general concepts of Fault Injection and Advanced explores the topic in a deeper detail for experienced hardware security professionals.

2018 Availability:
Essential: Open Trainings in March, June, October
Advanced: Open Training in September



Introduction to Software Exploitation

In this course we cover the most common mitigation techniques and the different approaches to bypass them. We additionally touch upon less common mitigation techniques that try to address these shortcomings.

2018 Availability:
Open Trainings in April and December



NEW! Hardening Secure Boot Workshop

Secure Boot is a common concept that ensures proper initialization and operation of a device. The compromise of a Secure Boot often leads to a full compromise of any security mechanism. This is a practical one-day workshop where we discuss and analyze common mistakes that lead to Secure Boot weaknesses.

2018 Availability: 1 day workshops in May and November, US Roadshow in June



Side Channel Analysis: Essential and Advanced

This course provides the foundation knowledge and skills to evaluate the resistance of chips and devices to Side Channel Analysis. The main objective of the three day training is the methodology of applying SCA to a wide range of devices from the very simple, unprotected smartcards to implementations protected with advanced countermeasures or complex embedded applications. This course is offered in two different types: Essential is focused on the general concepts of SCA and Advanced explores the topic in a deeper detail for experienced hardware security professionals.

2018 Availability:
Essential: Open Trainings in March, June, October
Advanced: Open Training in September



HCE Security Certification Master Class

The content of this online training is a distilled version of the lessons learned by our security evaluation team throughout the 50+ mobile payment security evaluation projects we executed in the last 3 years. The course includes lessons and quizzes on requirements, the evaluation process itself, HCE architecture, attack models and attacks versus countermeasures, common pitfalls and mitigation strategies.

2018 Availability: Online



White Box Cryptography

Software crypto plays a large role in securing for instance content and mobile payments, but how does it stand up to local attackers with full control over a device? After taking the course, you will know how to attack software obfuscated ciphers, without spending endless time in de-obfuscation and reverse engineering.

2018 Availability: On Request



Introduction to Smartcard Security

This is a three day practical introduction to all relevant attacks for smartcards. We focus on logical, side channel security and fault injection issues and introduce secure programming patterns, providing an understanding of the security requirements which can be taken into account when developing or evaluating smart card security.

2018 Availability: On Request



NEW! Embedded Security for Automotive

Modern cars are digital devices, controlled with multiple ECUs and millions of lines of software code. They are the frontline of modern embedded device development. With respect to unique safety requirements and rapid development of V2V communications automotive security benefits from the expertise of other embedded applications. The Embedded Security for Automotive is brought to you by embedded device security veterans, with years of expertise in securing payment and content protection application. In this training you will look at an automotive solution from an attacker's perspective. You will learn how ECUs can be hacked and identify ways to apply this knowledge to your product and make it more robust. As a result, you will obtain the expertise to make effective security-related decisions throughout the entire development lifecycle of a vehicle electronic system.

2018 Availability: US Roadshow in May and June



Riscure Training Academy – 2018 Open Training Calendar

Course Title	Duration	Dates
ARM Reverse Engineering	3 days	5-7 February
Introduction to Side Channel Analysis	3 days	5-7 March
Introduction to Fault Injection	2 days	8-9 March
Vulnerability Identification and Code Hardening	2 days	30 April - 1 May
Hardening Secure Boot workshop	1 day	2 May
Introduction to Side Channel Analysis	3 days	4-6 June
Introduction to Fault Injection	2 days	7-8 June
Advanced Fault Injection	2 days	5-6 September
Introduction to Side Channel Analysis	3 days	15-17 October
Introduction to Fault Injection	2 days	18-19 October
Vulnerability Identification and Code Hardening	2 days	5-6 November
Hardening Secure Boot Workshop	1 day	7 November
Embedded System Security	3 days	19-21 November
Software Exploitation and Mitigation Techniques	3 days	10-12 December
Riscure Training Academy Roadshow, Detroit, US		
Embedded Security for Automotive	3 days	13-15 June
Vulnerability Identification and Code Hardening	2 days	18-19 June
Hardening Secure Boot Workshop	1 day	22 June
Open training – Asia		
Embedded Security for Automotive	3 days	collocated with ESCAR Asia
2018 NEW courses		
Hardening Secure Boot Workshop	1 day	2 May, 7 November
Embedded Security for Automotive	3 days	14-16 May
Advanced SCA- Deep Learning	2 days	3-4 September
Introduction to Software Exploitation	2 days	16-17 April

Riscure offers NEW training courses, customization packages and pricing models for our corporate customers. Please ask for more details: trainingacademy@riscure.com

riscure