

Security training courses

For 20 years Brightsight has been spreading security knowledge around the globe to support its customers in their security challenges. Everyone interested in payment device security, smart card security or Common Criteria evaluations is welcome to attend.

Which courses do we offer?

The topics of these security training courses include two days of Common Criteria evaluation, one day of payment device security, two and half days of smart card security. Our experts will present the trainings in a workshop model that allows room for discussion and specific questions from the participants. The courses will start at 9:00 am and will finish at 17:00, including two short coffee breaks and one hour for lunch. The courses take place at our office in Delft, The Netherlands.

Who should attend?

Key personnel who should attend include risk and fraud managers, marketing and product managers of security products and smart cards in particular, hardware and software developers. The workshops are targeted at the smart card industry, the embedded security industry and industries deploying smart cards such as banking, transport, ID (e-passport), telecom and conditional access (Pay TV) industries. People, already having five or more years of experience in the topics offered in these security training courses, will probably appreciate a more detailed course in stead, which can be offered on request.

Why apply for security training at Brightsight?

For 20 years Brightsight has been involved in security including performing security evaluations, supporting developers in their development, defining security requirements for our customers and providing security training. The comprehensive training courses are the condensation of our security knowledge gathered in the hundredths of projects we have been involved in. Brightsight is globally recognized as a partner in security approval by the smart card industry. Furthermore, Brightsight plays a leading role in the Standardization Committee of Common Criteria.

For more information please dial +31 15 269 2500 or send email to info@brightsight.com



Common Criteria for Developers

Course objectives

- Understanding of the essence of Common Criteria
- Understanding of the CC requirements commonly requested in smart card and PED related markets
- Understanding of the process of an evaluation and the impact on the developer

This course will provide

- Brightsight Certificate of Attendance
- Course manual containing useful information
- 2 hours consultancy, free of charge

Day 1 // Essence of the Common Criteria

Summary of the CC

This part provides a general overview of the Common Criteria. It summarizes this complex standard to its essence, focussing on the (hidden) structure of the standard and how it is actually used. Although the technical terms of the CC will be mentioned, the focus is on understanding the standard, not on repeating all the CC-jargon.

Important questions will be answered, such as: what is an evaluation, why would one use the Common Criteria for evaluation,

what are the various roles in the evaluation and certification, why is it so hard? We then discuss what the developer has to do for an 'average' evaluation: EAL 4. It also discusses the differences with EAL3 and EAL5.

Unless requested otherwise, examples from the smartcard and PED industry will be used throughout the course.

Day 2 // The developers practice Protection Profiles and Security Targets reading guide

The Common Criteria language used in Protection Profiles and Security Targets is difficult to understand and intended mostly for the evaluators. In this part we will teach you how to read PPs and STs.

We will use the EuroSmart Protection Profile (BSI-PP-0002) for smart cards to illustrate this topic, as it is one of the most widely used Protection Profiles.

Markets and their popular CC requirements (Protection Profiles) summarised

In theory the Common Criteria allow expression of almost any set of security requirements in PPs and STs. In practice industries have established de facto standard requirements. In this part we will

explain these requirements (e.g. the popular PPs) of the following industries:

- > Smartcards (e.g. the Java Card PPs and the e-Passport PP (BSI-PP-0017))
- > PED (e.g. APACS PP)
- > (other markets available on request)

We will also cover the (sometimes well hidden) pitfalls of these PPs and where they are hidden.

Common Criteria evaluations: what you need to know before you start

In this block we explain how the evaluation process looks like from the point of view of the Developer and the Sponsor, in terms of risks in the process. The typical high and low points of the evaluation will be covered, with the emotional stress it will typically have. This will give a good understanding of what common pitfalls and milestones are so that they can be recognised and hopefully avoided.

The Common Criteria courses do not require prior knowledge of the Common Criteria or other evaluation methodologies, although general knowledge of IT security is preferred.

Course objectives

- Understanding of smart card security from a business and risk point of view
- Understanding of smart card security threats
- Understanding of smart card security attack techniques
- Understanding of generic smart card security (countermeasure) techniques
- Understanding of smart card security evaluation process

This course will provide

- Brightsight Certificate of Attendance
- Course manual containing useful information
- Opportunity to ask questions to globally recognized smart card security experts
- Lab tours providing insight in how smart card security is put to the test on a daily basis at Brightsight
- 2 hours consultancy, free of charge

Day 1 // The hardware side of Smart Card Security

Hardware security threats

Smart cards can be seen as a hardware platform (IC, chip) that runs software. From a security point of view this separation can also be made, although some security threats involve both hardware and software. This session will explain hard security threats such as reverse engineering, mechanical probing and Focused Ion Beam manipulation. After a theoretical discussion a hardware security expert will demonstrate the threats in one of our labs.

Perturbation security threats

Perturbation attacks are hardware manipulations applied to disturb

the software running on a smart card. Most common threats are power supply manipulation and light manipulations (which involves exposing the chip surface of a smart card to light) during the operation of applications running on the card. The goal of these types of manipulation is to retrieve secret data from the card or to circumvent security measures present in the software to achieve fraudulent use of the card. After in-depth discussion about these threats, both types of perturbation will be demonstrated by one of our experts in the lab.

Day 2 // Side-channels and contactless smart card security

Side channel security threats

This day will start off with another type of smart card security threat that involves both hardware and software sides of the card. Smart cards may leak secret information through side channels such as power consumption or electro magnetic emanation. These threats involve both hardware and software aspects of a smart card. Side channel threats will be explained in detail, both from a hardware and software point of view. Furthermore, different forms of side channel analysis of smart cards will be demonstrated in one of our labs.

RF ID and contactless card security threats

This part of the course will focus on the specific security threats that involve the use of RF or contactless card technology. Privacy violation, identity theft and virtual pick pocketing are threats that worry a lot of people in the industry. First the hardware security threats will be addressed which will also be compared to the existing threats

Smart Card Security

for contact technology. Secondly, software and protocol related security threats will be discussed in detail. This session will be closed by some demonstrations in our lab clearly visualizing the implication and reality of RF ID and contactless card security issues.

Day 3 // The software side of smart card security

Software security threats

Without a doubt the security of smart card software plays a vital role in protecting the assets stored on the card. The most commonly used types of cards are either Native Operating System or JavaCard Operating System enabled. Both types of cards have common security threats to counter, but additionally they also need to resist specific OS related threats. Besides this, application related security threats will be discussed in detail as well. Furthermore, commonly known software countermeasures will be addressed as well.

The smart card security courses do not require prior knowledge about smart card security, although general knowledge about smart card technology is preferred.

Course objectives

- Understanding of PCI PED approval process, requirements and evaluation
- Understanding of PED and terminal security from a business and risk point of view
- Understanding of PED and terminal security threats
- Understanding of PED and terminal security attack techniques
- Understanding of generic PED and terminal security countermeasures
- Understanding of PCI PED in relation to other payment schemes
- Understanding of other PCI security processes such as Encrypted PIN Pads, Unattended Payment terminals, Mobile Payments, IP and Wireless enabled terminals, Host Security Modules and ATMs.

This course will provide

- Voucher for 500 euros discount on PCI PED Evaluation at Brightsight
- Brightsight Certificate of Attendance
- Course manual containing useful information
- Opportunity to ask questions to globally recognized PED and terminal security experts
- 2 hours consultancy, free of charge

Pin Entry Device and Terminal Security

Introduction

This course starts with an overview of PED security, including the functionality of a PED and PIN, multi applications, threats and countermeasures.

PCI PED Approval Process

Describes the different aspects of the PCI PED Approval Process including the documents, the evaluation, the review and approval by PCI and how to handle changes and modifications of PCI PED approved products.

This part also contains a Questions & Answers session of commonly asked questions about the PCI PED Approval Process.

PED Attack Techniques

Provides detailed information about techniques that would allow access to a PED for key tapping or bug or skimmer insertion.

PED Defense Techniques

Elaborates on the “why” and “how” of countermeasures that need to be implemented on PED’s both from a physical and logical point of view.

PCI PED versus other payment

schemes, such as German (ZKA), Dutch (Currence formerly known as Interpay) and British (APACS) Points out the main differences between PCI PED and the other

schemes, focusing on the security requirements, and, the possibilities to re-use evaluation efforts for multiple approvals amongst the different schemes.

New PCI Approval Processes

Closes the day with another existing PCI approval area (Encrypting PIN Pads) and areas under development, such as Unattended Payment Terminals, Mobile Payments, IP and Wireless enabled terminals, Host Security Modules and ATMs.

The PED and terminal security course does not require prior knowledge about PED or terminal security, although general knowledge about PED and terminal technology is preferred.