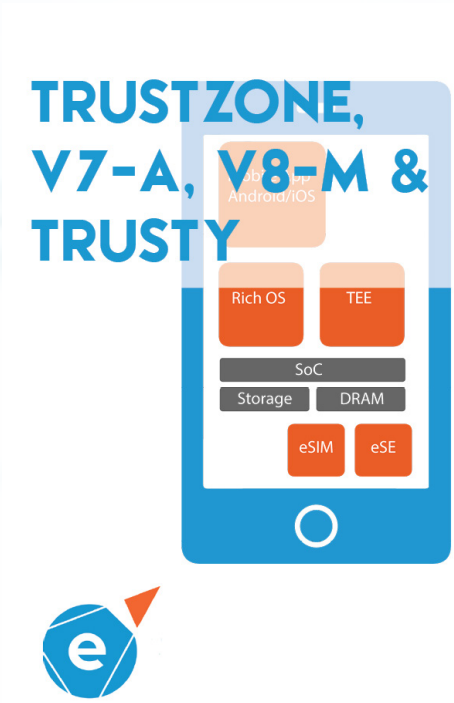
Your trusted partner in embedded security



Learn how TrustZone (ARM Security Extensions) works on ARM Architecture v7-A and v8-M, and understand in detail what composes a TrustZone v7-A secure kernel and how it interacts with the rest of the system.

TrustZone V7-A, V8-M and Trusty

Knowledge is power!

Expand your knowledge and learn from the experts. We share our expertise with you in a hands-on manner to provide a pro-active learning experience. During the training you will get examples of real-case weaknesses and understand how to attack these weaknesses. After the training, you will be able to apply this knowledge straight away to your daily work. We will show you what measures to put in place to break as well as patch these weakness, to avoid future attacks.

TrustZone, V7-A, V8-M and Trusty

About the course

TrustZone is hardware based security built into SoCs by semiconductor chip designers who want to provide secure end points and roots of trust. During this training you will learn how TrustZone (ARM Security Extensions) works on ARM Architecture v7-A and v8-M. You will learn in details what composes a TrustZone v7-A secure kernel and how it interacts with the rest of the system. You will then focus on the real world secure kernel implementation "Trusty" open-sourced by Google. You will modify Trusty in order to implement a Trusted Applet which will communicate with non-secure Linux applications.

Duration

Two days.

Target audience

Security analysts and software engineers.

Attendees will receive

The attendees will be given the presentation slides and a software package to work with.

.

Pre-requisites

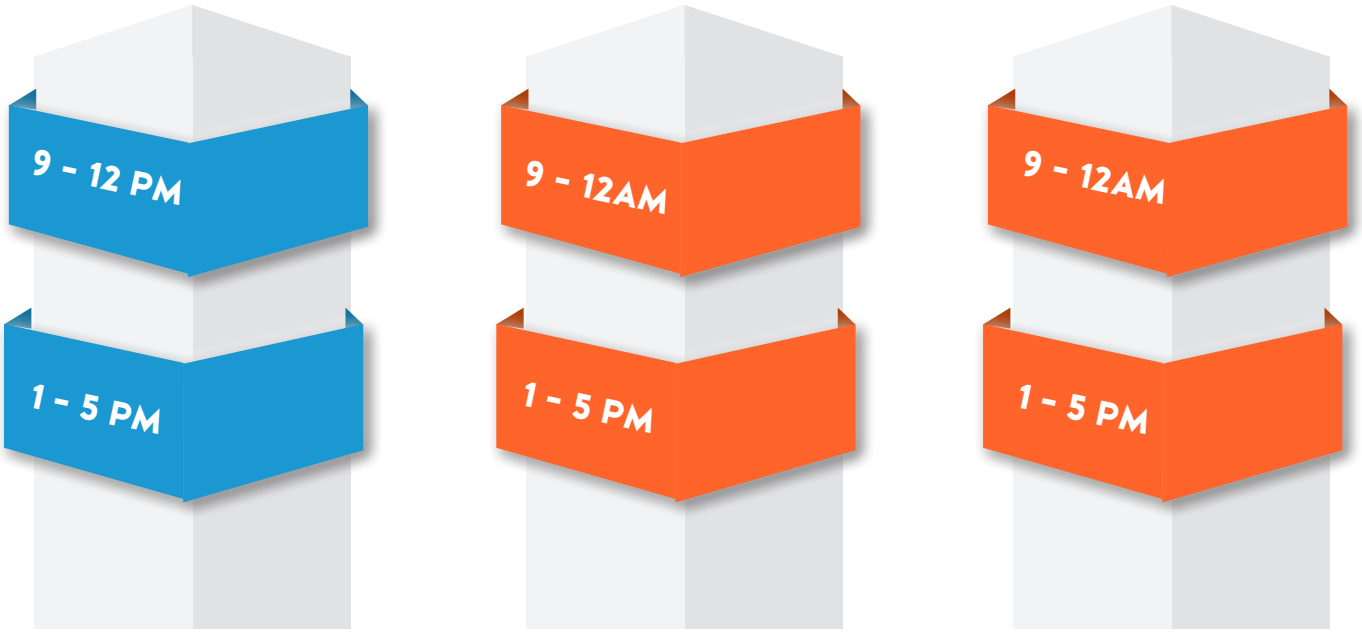
- Basic assembly knowledge
- Experience of C
- OS understanding

Benefits of training with eshard's experts

- Opportunity to work on real life cases. Since these are fairly new technologies, our experts aim to stay updated in order to share the latest knowledge.
- Access to hands-on expertise. Combined, our experts have tens of years of experience in the security field.
- We provide a balanced mix of theory and practical exercises to enhance your understanding of the technology on both levels.
- Follow this course on-site or in two locations, in Bordeaux or Marseille in France. Your call.

Course outline

Practical work Theoretical courses Challenge



Day 1

Day 1(all day):

During this part you will learn how TrustZone works and how it compares to other security solutions.

TrustZone prinicples:

- System security solutions
- ARM TrustZone principles
- Hardware & software
- TrustZone vs other solutions
- TrustZone usage examples
- Available TrustZone solutions (OP-TEE, Trusty, etc.)

TrustZone details:

- Instruction set reminder (5 minutes)
- Security Extensions on v7-A "TrustZone"
  - Secure & Non-Secure worlds
  - Virtual Memory Architecture
  - Monitor
  - IRQ handling
  - Boot process
  - Secure kernel design
- Security Extensions v8-M (in comparison to v7-A)
  - Memory Architecture
  - Secure Memory Configuration
  - IRQ handling

Day 2

Day 2 (all day):

Use Google's Trusty on wandboard (v7-A).

During the practical part, you will use a ready-to-use software package provided by eshard so that everyone works in the same environment.

At each step,you will not have to work from cratch: when necessary, code templates will be available so that you only focus on interesting tasks.

- Boot process
- Secure / Non-Secure context switch
- Implement a Trusted Applet (TA)
- Communicate with linux
- IRQ handling
- Debugging using JTAG

Upon request

Want to know more?

@eshardnews

companies/eshard

www.eshard.com
contact@eshard.com

ASIA

19 Keppel Road
#03-07 Jit Poh Building
Singapore 089058

EUROPE

1 Allée Jean Rostand Martillac
Bordeaux 33650 France

7 Rue Gaston de Flotte
Marseille 13012 France