Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Crypto Chip-Set Security

Learn via: **Classroom**

Duration: **3 Day**

Overview

The biggest challenge for professionals working on design and development of crypto chip-sets is to be continuously up-to-date regarding the attack methods and their mitigation. Serving them, this course explains various physical and logical attacks on security chips, possible countermeasures and best practices.

Regarding physical attacks, the passive attacks are detailed through optical reverse engineering and various side channel analysis methods, while active attacks are discussed with special emphasis on fault injection, Focused Ion Beams and hardware Trojans. The very powerful passive and active combined attack (PACA) type is introduced through the practical example of RSA implementations. Discussion of logical attacks not only covers practical attacks against specific cryptographic algorithm implementations, but also the relevant programming bugs and mitigation techniques like buffer overflow or integer problems are introduced.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

Developers, architect and testers of secure hardware components.

What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Have a practical understanding of cryptography
- Understand the requirements of secure communication
- Understand essential security protocols
- Understand some recent attacks against cryptosystems

Outline

- IT security and secure coding
- Requirements of secure communication
- Practical cryptography
- Security protocols
- Simple physical attacks and protections
- Passive physical attacks
- Active physical attacks
- Passive and active combined attacks
- Special security functions – Requirements and solutions

- Principles of security and secure coding