Security of the Java Card Platform

Guillaume Bouffard (guillaume@bouffard.info)

1 Description of Training Class

During this training, participants will learn how the Java Card platform works. They will learn how to design a secure Java Card Virtual Machine. They will then focus on a real Java Card implementation reproduce several exploits which gives full control over the Java Card platform.

- **Duration**
  2 days
- **Targeted Audience**
  Security analysts
  Software engineers
- **Attendees will receive**
  Slides copy
  Software package
- **Pre-requisites**
  Basic assembly knowledge
  Java programming
  Basic OS understanding

2 Covered in this training

- **Theory (1/2 day)**
  Java architecture and Java Card architecture
  The Java Card file format
- **Security of the Java Card Platform (1 day)**
  Java Card security mechanisms
  Attacks against the Java Card platform
- **Practical (1/2 day)**
  Simple Java Card Hello World
  Exploit on real card

- **Theory (1/2 day)**

  During this part, participants will learn how the Java Card platform works.

  Java architecture
  Java Card architecture
  The Java Card file format

- **Security of the Java Card Platform (1 day)**

  During this part, participants will discover the Java Card security mechanisms and attacks against the Java Card platform. Some counter-measures will also be introduced.

  Java Card Byte Code Verifier
  Java Card Firewall
  Software attacks against the Java Card platform
  Combined (physical and logical) attacks against the Java Card platform

- **Practical (1/2 day)**

  During the practical, trainees will use a ready-to-use software package so that everyone works in the same environment with the same tools. At each step, trainees won't have to work from scratch, code templates will be available so that they do not spend time on uninteresting tasks.

  - Day 1 afternoon – Discover tools
    Implementing a simple Java Card Hello World applet and loading it on a real smart card. Sending several commands and handling smart card answer.
  - Day 2 afternoon – Exploit on real card
    Exploiting a real smart card upon a several software attacks to characterizing a Java Card virtual implementation.