achelos
the experts in eID

Extended Qumate.World:

Integrated Environment for Functional Testing and Security Evaluation of Java Card™ Applets and Platform

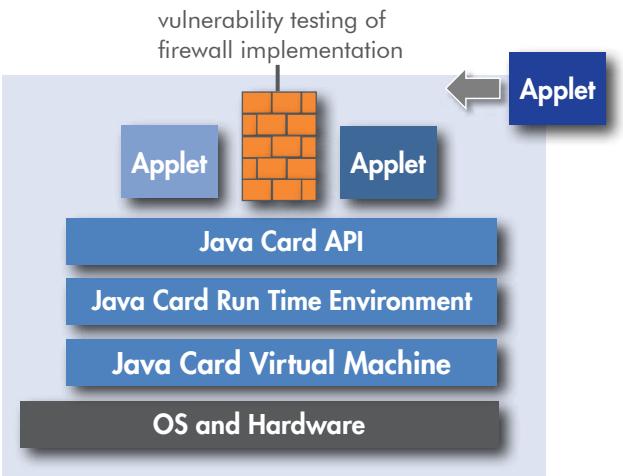
Java Card™ (JC) brings the ability for developers anywhere to write programs that drive smart card applications. While being a boon to the industry, this creates a potential for violations of card security.

Successful seizures of the SIM-Card Platforms reported recently show very clearly that the Java Card Open Platform attracts subsequently the interest of the hackers both independent individuals and employed by the commercial or government organizations. This development becomes understandable under consideration of the quantity of the yearly Java Card Shipments of 2.5 billion cards*. This requires the adequate defense measures from the issuer and users of the Java Card Open Platform based cards.

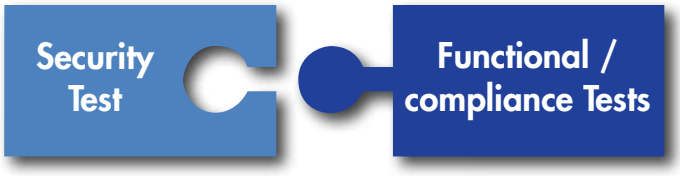
Providing a high level of security assurance, rigorous testing technology is essential

However, conventional software testing is not sufficent to discover bugs that cause security vulnerabilities. Software can be correct without being secure. Testing for security deficiencies is different from traditional software testing. Traditional bugs are found by looking for a behaviour that does not work as specified. Security bugs are found by looking for a behaviour where software does something that it was not supposed to do. Security of Java Card applets depends on the platform strength to protect its secrets and isolate its data and functionality from other applets.

Java Card Platform



Integrated extensive Java Card test suite



*JAVA CARD Forum, Bruno Basquin, Hong Kong, 20.03.2014

achelos
the experts in eID

Qumate makes Quality ... visible!
Qumate is an innovative, Java-based test management tool suite for the quality assurance of chip card systems and applications.
www.qumate-world.com

achelos' Qumate-based integrated testing and security evaluation environment and test management tool suite combines both functionality AND security tests of Java Card. achelos offers its clients complete evaluation of JC smart cards to fulfil their requirements.

This is done by running more than several hundred specially designed security tests that cover explicit and implicit security requirements of JCRE, JCVM, JC API. These Java Card specifications have been published by Oracle Corporation.

achelos will perform testing and security vulnerabilities evaluation of your JC platform and applications with its extended Qumate-based test management tool suite. Our bench takes a flexible approach by deploying and executing the tests either on the smart card platform itself or using Qumate-based simulator tools. achelos develops, runs and specifies test applets against a Java Card to identify security vulnerabilities.

With achelos' extended Qumate Framework, an evaluator can run not only a functional test suite but also the security vulnerabilities tests. It identifies potential security problems caused by deficiencies in the implementation of JCRE and/or applets. Security tests are plug-ins in the extended Qumate Framework and comprise the following tests.

Your questions:

- Is the customer's applet correct and secure or can be used for attacks (note that correct is necessary preconditon for secure)?
- Is the JC platform that the customer uses correct and well protected against attacks?
- Does the third party´s applet contain hidden malicious (i.e., it will not interfere with other applets, not damage platform)?

Tests to check :

- correctness of implementation of JCRE persistent and temporary entry point objects
- correctness of implementation of excution context switches
- correctness of implementation of atomic updates
- existence of dangling references in transient memory after the reset or applet deselection
- correctness of implementation of firewall
- correctness of implementation of transaction mechanism (checking that every access to an object acquired via the Shareable inter face is checked against the firewall rules).

achelos GmbH Vattmannstraße 1 33100 Paderborn Germany fon: +49 5251 14212-0 info@achelos.de www.achelos.com