Java Card Applet Firewall Exploration and Exploitation

Wojciech Mostowski and Erik Poll

Digital Security Group, Computing Science Department,
Radboud University Nijmegen, The Netherlands
{W.Mostowski,E.Poll}@cs.ru.nl
tel: +31–24–365–{2076,2710}

Extended Abstract

We present the results of an extensive study of current implementations of the Java Card applet firewall. Despite the imminent release of the Java Card 3.0 standard, cards with the well-established Java Card 2.x standard will stay with us for some time to come.

We report on three aspects of the Java Card firewall:

- compliance of existing Java Card implementations w.r.t. the official specification has been performed. Testing eight cards from four manufacturers revealed only minor and mostly harmless deviations from the specifications, and at least one questionable statement in the specification itself.
- using the firewall mechanism (the shareable interface object mechanism to be precise) as a way to *legally* introduce type confusion (ill-typed code) on a Java Card VM.
- finally, the protection the firewall offers against ill-typed code. As it turns out, the firewall does not provide the defence-in-depth one might hope for here. As an example we will illustrate this in an AID exploit, where ill-typed code can make arbitrary changes to the central AID registry of a card. This attack was possible on two recent Java Card smartcards currently on the market.

One of the results of our study is that despite the correct behaviour of the firewall w.r.t. the specification, firewalls could possibly be a bit more defensive.

In the presentation we will discuss our firewall compliance test and its results for our test cards, we will describe the mechanism of introducing type flaws through the SIO mechanism, and finally we will give the details of the AID attack.

Authors

The authors have been studying the correctness and security of Java Card applications for many years. The current work is part of the PINPAS Java Card project, in collaboration with the Technical University of Eindhoven and Brightsight (formerly TNO-ITSEF), both from the Netherlands, and ST Microelectronics in Belgium.