Abstract

We present in this paper a new approach to gain access to assets of a smart card. It is based on the concept of reference forgery and array extension. We characterize the metadata of the objects and we use a weakness in the system to retrieve these data. We are able to generate arbitrary but well formed references which allow us to execute self modifying Java program inside the card. This hostile program is able to dump the complete Non Volatile Memory (NVM) memory segment.