Abstract

Smart cards are tamper resistant devices that manipulate assets in a secure way. Among the assets, one is of a particular interest the native layers. If some attacks have succeeded in getting access to the applicative layer very few of them have had access to the native layers. We propose here to use applicative programs to perform data reverse engineering in order to understand the hidden algorithms that manage the memory allocation. We are then able to generate our own fake references on objects that can be manipulated by the system as legal objects. Then, we propose a new attack called auto-forges that leads the system to interpret its own data or program as valid Java meta data. This attack provides access to new memory fragments where the native layers are stored. Getting access to this asset allows us to start the reverse engineering of these native layers.