On Avoidance of Attacks Against the PIN Error Counter of Smart Cards

Zoltán Kincses

Smart cards are generally considered as secure tokens, applicable for storage of long cryptographic keys or usable as keys themselves in different security mechanisms. However usually the access ability or usage of the internal data depends on the knowledge of a short PIN code. Counting the attempts of use with invalid PIN codes usually protects the card against simple brute force attacks.

If this PIN error counter can be somehow circumvented, an easy way opens to access data in the card without proper knowledge of the PIN code. The full paper of this detailed abstract describes attack methods - classical and newly invented also -, and suggests appropriate defensive measures.

Basic standards or programmer's guide supplied with developer kits describe the role and the mechanism of CHV (Card Holder Verification) and AUT (Authentication) bytes in a smart card environment. The access control can be maintained through the management of asset of codes, which are commonly referred to as PIN (Personal Identity Number) codes. In general, the access of the data stored in a smart card is controlled by these PIN codes (PIN as basic code, PIN2 as security code, PUK as unlock code, and other more specific codes, like operator code for higher security access to the chip or even supervisor code).

Smart cards have their well-defined methods to handle the PIN management, from storage of these codes, through change possibility, till the counting of bad attempts.

When the smart card's PIN management system asks for a code to be entered, the presented code is compared with the stored one. If the given code does not match with the stored one, then the operating system will increment the counter of bad attempts. After reaching the maximum number of allowed bad attempts, the OS will deny further attempts by blocking the code. The card can be used only after entering the unblock code. After receiving the correct code, the counter will be reset to initial value.

Analysing the security of the system from the PreDeCo (Preventive-Detective-Corrective) control's point of view, the existing and the missing protection measures can be discovered. This way the weakest points in the security of the implemented system are easily identified. The preventive control against the user access is asking the PIN code. The detective control is the counter of attempts and the corrective is the usage of an unblock code. From an attacker's point of view, however the preventive control is the counter of attempts, but if this control can be circumvented, there is no detective or corrective control.

The question is how it is possible to avoid or block the increment of the counter. The chip must be operational for reading the data and compare the entered and the stored code, while it must not be able writing the new counter value into memory. One is the manipulation of algorithm execution from outside and another is monitoring and manipulation of power consumption. Both have a simple protection method.

The new attack method is the 'low temperature attack'. The aim is to reach that temperature state of the chip when it is able to process reading functions, but it is unable to process the writing functions. Protection measures will be presented against this type of attack, and this protection can be applied in any other systems also, where the written data can be read back for control purposes.

In general, the suggested scheme - that is, the application of a secondary backup counter for checking the correct increment of the error counter - can be applied in all cases when the success of a memory write operation affects the security of the system.