Personal Identification Number (PIN) Entry Device Approved by International Security Standard

GOTO Masao, KIKUCHI Shigehisa, HOKOTA Hiroya, MORITA Makoto

Abstract

Up to the present, the credit settlement system has evolved entirely in the context of IT and it has thus established itself as a key social infrastructure. However, recent technological innovations, social structural changes and the increasing social awareness of information value and personal information security have made it necessary for the credit settlement system to utilize more advanced security technologies.

NEC Infrontia has recently developed a personal identification number (PIN) entry keypad, called the "PINpad" and has acquired the approval of the PCI (Payment Card Industry) standard, which is the international standard for PIN-pad security.

Keywords

credit settlement, security device, PCI standard, PINpad, PIN, PCIPED, IC card

1. Introduction

The number of credit cards issued in Japan has grown by 25% over the last decade, and the amount of credit has increased by 86% in the same period. Under this trend of dissemination and expansion, however, abuse methods have also diversified and advanced. To deal with this issue, the Japanese credit card industry has enhanced its efforts for promoting the use of IC cards since 2003 in order to improve the security standards of credit settlements.

As a result, the protection of the personal identification number (PIN) using a PIN entry keypad (PINpad) has become a critical factor in IC card credit settlement procedures. Recently, we have succeeded in developing the high-security PINpad and have obtained the approval of the PCI (Payment Card Industry) standard for the first time in Japan, which is the international standard for the security of PINpad devices, as well as that of credit card companies. The product is described in detail below. [*1]

2. Background to the PCI Standard

The PCI standard defines the physical and logical security requirements for the devices used in entering the PIN required for IC card credit settlements.

Briefly the history up until the establishment of the standard is as follows. It was in 2000 that an independent standard for PINpad devices was conceived and it was in 2004 that the international PCI standard was established. Since Japanese brands joined the standard in the fall of 2005, PCI standard approvals also became popular in Japan.

The PCI SSC (PCI Security Standard Council) was organized by participation of key members from five international brands and in 2008, the PIN Entry Devices Program was defined in terms of PINpad security requirements and was enforced as the PCI PED (PIN Entry Devices) standard.

The PINpad incorporates the latest technologies and original improvements in order to meet the requirements of the PCI standard, such as safe use against external attacks by preventing the theft of important information.

3. PCI Standard Requirements Summarized

The security requirements for the PINpad can be classified into the following four categories.

(1) Physical Security Core Requirements

Security requirements for the PINpad hardware.

[*1] Since this device is security equipment, please note that some of the information cannot be opened to the public or described in details.

(Items related to defense and detection of physical attacks)

(2) Logical Security Core Requirements

Security requirements for firmware.

(Items related to the defense of PIN and PIN block against hacking and alterations)

(3) Online Requirements

Security requirements for online PIN entry.

(4) Offline Requirements

Security requirements for offline PIN entry.

4. Merchandise Specifications

Table shows the specifications of the newly developed PIN-pad product.

Photo 1 and **Photo 2** respectively show external views of the PINpad, for the model without the magnetic card reader and one with it.

Table PINpad specifications.

Item		Specifications
Display	Device	LCD (Backlight controlled by commands)
	Number of characters	8 Japanese full-width characters × 4 lines (128 × 64 dots)
	Type of characters	JIS Level 1
	Display size (mm)	Display area: Approx. 41(W) ×Approx. 24(H)
Keyboard	Layout	Telephone set layout
	Numeric keys	Numeric keys × 10 (0-9), Function keys × 4, Enter key × 1, Cancel key × 1
	Power key	Not provided
Buzzer sounds		Key entry tones, alarm tone
IC card reader		ISO/ICE7816 compliant, EMV4.0 certified.
Magnetic card reader		JIS1(ISO tracks 1 and 2), JIS2
Security		Conforming to JDCPA (Japan Debit Card Promotion Association) terminal guidelines, Conforming to JAMPA (Japan Multi-Payment Network Promotion Association) terminal guidelines, Approved by PCI Standard (Version 1.3A)
Settings		Contrast (5 steps), buzzer volume (3 steps), register (fixed), buzzer period (variable)
Interfaces		RS232,USB
Cable lengths		RS232 and USB, standard 2 meters
Installation		Handheld type
Dimensions (mm)		Approx. 190(W) × Approx. 70(D) ×Approx. 30(H) (Model with magnetic card reader: Excluding the privacy screens)

Photo 1 Model without magnetic card reader (without privacy screens).

Photo 2 Model with a magnetic card reader (with privacy screens).

5. Technologies Applied, Features

5.1 The Physical Technologies and Their Features

The functions necessary to meet the physical requirements are resistance to attacks and detection of attacks received.

(1) Technology for Detecting Attacks

The mechanism required for detecting an attack is to install multiple switches and sensors and to erase the sensitive information (PIN, encryption key, etc.) immediately when any one of them is activated (**Fig.**).

This device also has functions for detecting physical attacks such as an opening of the case, removal of a circuit board or cutting of a circuit board by various means. One of the known environmental attack techniques is the low-temperature attack on the memory. This device detects such an attack by incorporating a temperature sensor IC.

(2) Technology for Resistance to Attacks

In order to reduce the probability of receiving attacks, this device is designed to eliminate unnecessary clearances and spaces wherever possible (**Photo 3** , **Photo 4** and **Photo 5**).

Personal Identification Number (PIN) Entry Device Approved by International Security Standard

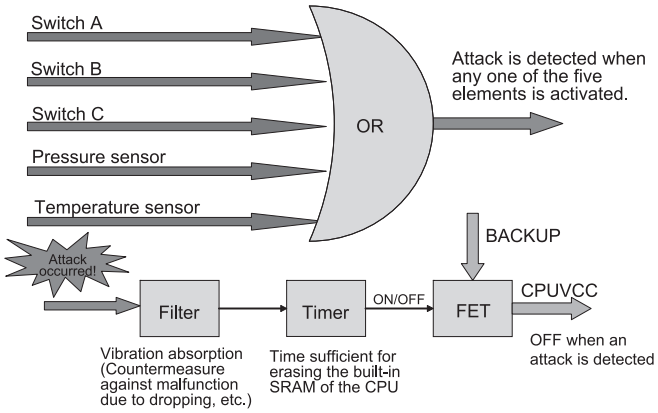

Fig. Attack detection method.

Photo 3 Elimination of clearance for inserting two IC cards.

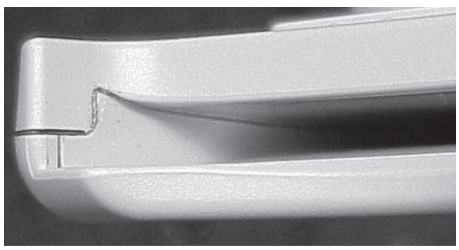

Photo 4 Elimination of space for entering a skimming device inside.

This measure is taken to eliminate the possibility that an attacker may insert a skimming device between the IC card and the case if the IC card insertion slot has a clearance exceeding the thickness of a card.

The device is also designed to retain evidence of an attack by using a curved line, instead of straight one, in the case engaging section. This is because a curved engagement section is difficult to open and leaves evidence of opening if an attacker attempts to open the case by cutting into the engagement section of the case.

Photo 5 Visible card insertion slot that can show the presence of a skimming device at a glance.

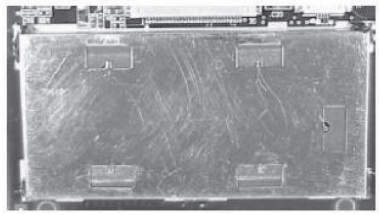

Photo 6 Internal protection with a built-in case shielding for attack detection.

The main issue in the circuit design is to protect the part that saves the sensitive information (memory) so that internal sensitive information is not illegally accessed in a direct attack of the memory. This device achieves protection of the main circuitry including the memory by shielding it with a case that has a built-in attack detection circuit (**Photo 6**).

5.2 Logical Technologies and Their Features

The functions necessary to meet the logical requirements are

1) Impossibility for the attacker to know or guess the PIN
2) Impossibility of overrun even when the PINpad receives unexpected communication data (The attacker attempts to trigger unexpected operation by causing overrun.)
3) Impossibility for a third party to insert a malicious program into the PINpad
4) Deletion of sensitive information when an attack is detected

This device fulfils the above requirements with the technologies as described below.

(1) Impossible for the Attacker to Know or Guess the PIN

The PINs entered by users are not output from the PINpad. The entered data is encrypted every time a key is pressed and it is saved as sensitive information. It is then deleted when it becomes redundant (after the PIN has been output to the IC

card) or when the timeout is reached after start of the key entry.
The above operations minimize the retention of PINs in the PINpad. Even when they are retained, they are encrypted to reduce the risk of PIN thefts by attacks.
The key entry tone generated during PIN entry is always identical and the display shows meaningless characters (asterisks) in order to prevent the PIN from being guessed from the key entry tone or display.

(2) Impossibility of Overrun Even When the PINpad Receives Unexpected Communication Data

A special defense program that can deal with data other than the command data specified in accordance with the specifications in the form of completely meaningless data is incorporated in order to prevent attacks that attempt to cause program overrun by sending a large amount of data or unexpected data.

(3) Impossibility for a Third Party to Insert a Malicious Program in the PINpad

Each PINpad is given a unique encryption key for use in firmware rewriting, and a hash value is assigned to the firmware information to prevent it from being altered by a third party.

(4) Deletion of Sensitive Information When an Attack is Detected

Sensitive information is deleted when an attack is detected. Any data containing sensitive information is cleared immediately after use and not left in the memory. Data containing sensitive information is not used in an external memory that is not protected by a shield case with built-in attack detection circuitry.
In addition, sensitive information is checked periodically. If it is found that the information has changed, an attack is identified and the information is deleted immediately.

6. Conclusion

In the above paper, we discussed the device development of the PINpad approved by the PCI standard for the first time in Japan.

As the PCI approval of the device has led to market evaluation of its superiority, we have already shipped about 50,000 units for use in POS-connected IC card credit settlement systems of major mass-sales stores as well as for OEM supply to major manufacturers.

Against a background of progress in technological innovation, the techniques of attachment are also advancing each year and the required security levels are changing. Accordingly, the PCI standard was upgraded from Version 1.3A to 2.0 on April 1, 2008 and it now incorporates the achievement of more advanced security levels as product requirements.

Based on the expertise that we have acquired in the development of the present device, we will endeavor to further improve our technology so that it will be able to clear even higher security standards and will help in continuing to expand our market presence.

References

1) Statistics of Japan Consumer Credit Industry Association
2) "Payment Card Industry (PCI) PIN Entry Device (PED) Testing and Approval Program Guide," Version 1.0, December 2007
3) PCI POS PED Security Requirements v1.3
4) PCI POS PED DTRs v1.3
5) EMV Integrated Circuit Card Specifications for Payment Systems (c)1994-2004 EMV Co, LLC ("EMV Co"). All rights reserved.
6) ANS X9.24-2004 Retail Financial Services Symmetric Key Management (c)2004 Accredited Standards Committee X9, Inc. All rights reserved.

Authors' Profiles

GOTO Masao
Expert,
3rd Product Development Group,
i Appliances Division,
NEC Infrontia Corporation

KIKUCHI Shigehisa
Manager,
3rd Product Development Group,
i Appliances Division,
NEC Infrontia Corporation

HOKOTA Hiroya
3rd Product Development Group,
i Appliances Division,
NEC Infrontia Corporation

MORITA Makoto
3rd Product Development Group,
i Appliances Division,
NEC Infrontia Corporation