Typical Attack Techniques for Compromising Point of Sale PIN Entry Devices

Steven Bowles, Ben Cuthbert, and Wayne Stewart

Payment Assurance Lab
EWA-Canada
Ottawa, Ontario, Canada
{sbowles, bcuthbert, wstewart}@ewa-canada.com

Abstract

This paper intends to provide insight on vulnerabilities that are commonly found in the current generation of Point of Sale PIN Entry Devices (PEDs). These vulnerabilities can be exploited using unsophisticated techniques to expose PINs and cardholder data. To mitigate these risks, the paper will highlight several considerations that could be employed at the PED's design phase.

1 Introduction

Payment card fraud is a growing epidemic. Visa International estimates that their annual fraud costs have reached $2.77B worldwide. Device manufacturers have made substantial strides in improving the security of their solutions, but vulnerabilities that can be exploited still exist.

1.1 Magstripe versus Smartcard

Currently there are two classes of payment cards; magnetic stripe and integrated circuit cards.

Magnetic stripe (magstripe) based payment systems are prevalently used in North American credit and debit implementations. Magstripe solutions can be used as 2-factor mechanisms that combine user account information from the magnetic stripe of a credit or debit card with the secret PIN entered by the user through a secure PIN Pad (it should be noted that most credit systems do not require the use of PINs to authenticate transactions). These data elements are combined within the PEDs secure processor and encrypted. The resulting cryptogram is used within the financial network to authenticate the transaction. As it is easy to read and copy a magstripe card, the security posture can be strengthened by employing PINs that are kept secret.

Integrated circuit card (ICC or Smartcard) based payment systems also provide for the same sort of 2-factor mechanism. With Smartcards, the card is a secure processing platform. The secret PIN is entered through the PIN Pad and passed to the card where it is verified. The card replies with a PKI-based authentication string that is sent along with the financial transaction. Currently, Smartcards are considered to be extremely difficult to copy. As the security posture can be less reliant on the secrecy of the PIN, PINs are quite often sent to the Smartcard in plaintext.

1.2 Scope

This paper is focused on the exploitation of PEDs supporting magstripe transactions as to determine plaintext magstripe data, PINs, and/or secret key values.

Attacks on Smartcard implementations are not discussed as it require additional consideration of how to compromise, capture, or copy the Smartcard.

2 Typical Vulnerabilities

A Threat Agent's goal is to gather sets of magstripe data and the associated PINs (if required) in order to make fraudulent cards that can be used to complete fraudulent financial transactions. If it is not possible to get this information directly, acquiring knowledge of the secret key values stored in the PED would allow for the decryption of intercepted packets of transaction data.

In order to gain access to any or all of this information, a Threat Agent must find weaknesses in the layered security design of a PED that can be exploited. Typical vulnerabilities include:

- Ineffective tamper-evident seals that cover case seams or screws;
- Openings that can be used to conceal penetration attempts or malicious circuitry;
- Surface mounted display covers that are attached to the device with weak glues or epoxies;
- Any security relevant components (i.e. RAM chips, switches, or inter-PCB connectors) that are easily accessible;
- Conductive traces from the PIN Pad that are easily accessible; and
- Use of weak epoxies to cover security relevant circuitry.

2.1 Identifying and Exploiting Weaknesses

When conducting an attack, the typical goals of a Threat Agent are to: disable or bypass any relevant active tamper response mechanisms (i.e. not all active tamper response mechanisms are of concern, depending on the planned attack); defeat passive tamper mechanisms; intercept key entry information from the PIN Pad; and/or determine cryptographic keys.

Mainly all attacks on PEDs can be modeled in a 4 step methodology:

1. **Enumeration** of a PEDs sensitive components and physical safeguards to aid in planning an attack;
2. **Gaining Access** allows for the proving, refinement, and packaging of a theoretical attack;
3. **Exploiting** a PED with the developed attack vector to record sensitive data; and
4. **Covering Tracks** by effectively hiding the malicious modifications.

2.1.1 Enumeration

Vulnerabilities in a PED can be inferred through the examination of several sources available to a test laboratory; schematics, PCB layout drawings, component datasheets, and manual inspection and measurements with voltmeter, ohmmeter and oscilloscope.

In this step, consideration of the following PED design issues can be used to identify exploitable vulnerabilities:

1. Identify components and PCB traces that could provide access to sensitive information;
2. Determine where the active tamper detection sensors are, what they protect, and how they trigger;
3. Determine if any of the tamper detection mechanisms can be disabled or bypassed from openings in the device (i.e. ventilation, Smartcard Reader, etc.);
4. Look over the device to see if there are any areas available that can be cut into and covered up;
5. If locations to cut into the device were found, make sure that the cuts won't trigger a tamper response. If the cuts won't trigger a tamper response, evaluate whether or not it is possible to disable any or all tamper response mechanisms from these cuts; and

6. Determine if any cuts or openings allow access to security relevant traces or components (i.e. PIN Pad traces).

This enumeration of the PED's vulnerabilities can then be used to evaluate the feasibility of successfully attacking these points to gather sensitive information.

2.1.2 Gaining Access

Once a theoretical attack is devised, a procedure must be developed and refined such that the exploit can be executed economically and efficiently (according to PCI; $25k USD and 10 hrs.). This step would also include the development of any specialized tools or circuitry required to gain access to the sensitive data once exposed.

2.1.3 Exploiting

Once the attack vector has been planned, it must be possible to insert the required malicious hardware and/or software needed to monitor or record the targeted sensitive data. Depending on the complexity of the attack, a Threat Agent may require a significant amount of practice to refine the technique. Retries of this nature can be frustrated if the PED enters into a severe non-operational state (i.e. won't remain powered-up without the entry of authenticated keys or a password) once the tamper response mechanisms have been triggered.

2.1.4 Covering Tracks

As the acquisition of cardholder data requires the participation of a non-colluding user, it must be possible to reassemble a compromised PED with original or replacement parts such that the exploit is not noticeable to the casual observer. This fourth step needs to be considered when developing the attack. For example, if an exploit is making use of an opening under a removable cover, where the opening needs to be widened, care should be taken to ensure that a edge is left that can be used for reattaching the display cover once the exploit has been implemented.

2.2 Tools and Techniques

A Threat Agent looking to exploit the vulnerabilities of a PED will make use of a number of tools, both common and complex. This analysis is focused on some of the more useful, easy to acquire tools and their potential uses.

A *hand-held rotary tool* plays a significant role in many attack strategies. This type of tool can be used to access internal areas by cutting the case, removing internal case material in order to access security relevant components, and for the removal of large/hard epoxies.

Adhesives are commonly used to hold switches shut and hold other pieces in place.

A *dental pick* is primarily useful for its ability to scrap away epoxies from components or out of conductive vias in a PCB. They are also useful in the application of adhesives that are used to keep tamper response switches closed. As well, a dental pick in conjunction a small amount of epoxy can be used to place malicious wires and components into tight spaces.

Conductive epoxy can be applied to a PED to short out component contacts and act as a 'cold weld' for heat sensitive applications and tight areas. As well conductive epoxy provides an easy method of attaching wires to traces that have been revealed by scrapping off the PCB's conformal coating.

In order to make connections with small conductive vias on a PCB, *Magnet wire* can be sharpened and inserted into these holes. Sometimes a pair of pliers is required to work in tight spaces.

3 Design Considerations to Mitigate Risk

In order to mitigate common vulnerabilities in PEDs, the following suggestions on PED design should be considered:

- Run keypad/active tamper response mechanism traces on the middle layer(s) of a PCB;
- Place keypad/active tamper response mechanism vias in inaccessible areas (i.e. underneath the chip that they are inputs to, close to active tamper response mechanisms, at the button pad);
- Keep active tamper response mechanisms independent of each other as long as possible. If the tamper response logic must be combined into one signal, do this only in a secure area and make sure this single trace is well protected;
- Try to place active tamper response traces and chip pins away from traces and chip pins that carry the signal similar to that used for 'NO TAMPER DETECTED' signals (i.e. if a trace/chip pin carries a high signal when an attack is detected, keep that trace/chip pin away from ground traces/chip pins);
- Ensure that items on, or in the device, that are not meant to be removed, cannot be removed without triggering a tamper response mechanism;
- Do not rely only on passive mechanisms such as epoxy or tamper evident seals/labels;
- Avoid placing removable covers on the device. Removable covers give access to areas on the device that can be cut away and evidence of the cuts will be hidden when the cover is back in place;
- Try to design the device so that every aspect of the device increases the security of the device;
- Do not allow physical access to the internals of the device for any reason.
- Do not allow the device to be reset and/or reused after a physical attack has been attempted. Design the device so that any physical access to the internals of the device will cause physical or logical damage to the device to the extent that it is inoperable and won't remain powered-up;
- Design active tamper response mechanisms that use conductive pucks to require a constant pressure applied to them to be effective; and
- Use tamper detection switches that are small and require a fair amount of pressure to keep the switch closed.

4 Conclusion

Despite improvements to the design of PED security features, vulnerabilities still exist that can be exploited by Threat Agents using simple techniques. These vulnerabilities can be mitigated during the PEDs design phase.