



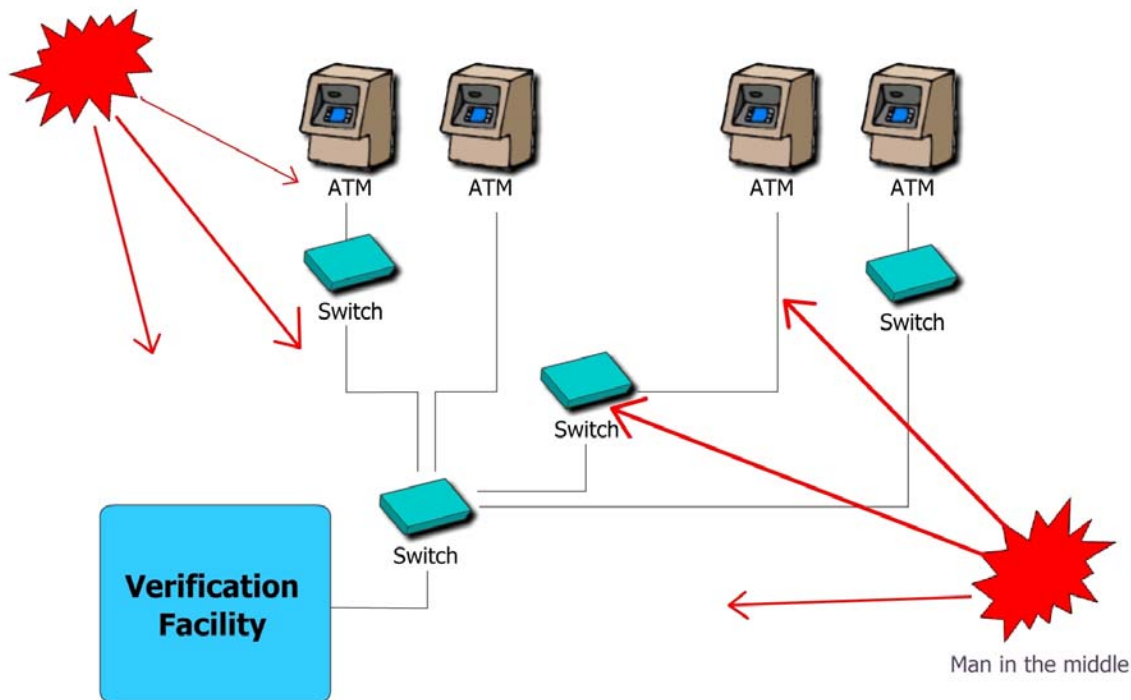
# PrivateServer Switch-HSM



Secure  
Simple

In the world of financial transactions and payment systems, cardholders, either of mag-stripe cards or chip-cards, are required to enter their PIN (Personal Identification Number) when using their credit/debit/cash cards to authenticate them to the issuing bank or to financial institutes. The customer's PIN can be verified offline at the Point-of Sale terminal, or can be verified online while the transaction takes place.

When using an ATM (Automated Teller Machine), the PIN verification is typically done online, vis-à-vis the card-issuing financial institution's server. To enable online PIN verification, a PIN code typed at an ATM and the account number related to the inserted card must be transmitted through several computer and communications gateways, or Switches, prior to reaching its final destination at the issuing bank for verification.



At the ATM, the information is packed and encrypted and is then passed through the network. At each gateway node (Switch) there is usually a Hardware Security Module (HSM) that decrypts the data from the ATM and then re-encrypts it, using a key this node shares with the next Switch. The function that these Switches perform is called "PIN Translate". Recent academic research has discovered a major security flaw within the HSM's implementation of the standards, relating to the PIN Translate function. The research, conducted on how "*HSMs Implementing the Standard Relating to the PIN Translate API*", concluded that insiders of Switch facilities can quite easily exploit and use the functionality that the HSM supplies to expose PIN codes entered by customers at the ATM.

This inherently extends the liability of all financial institutes that are responsible for the maintenance of these HSMs located at the Switch locations, especially where tourists make withdrawals from ATMs in countries with relaxed security policies.

PrivateServer Switch-HSM

**PrivateServer  
Switch-HSM**

## The Vulnerability

The exposure of customer PIN codes is enabled due to vulnerabilities in the standards defining the PIN Processing formats and PIN translation function when using an HSM for PIN processing. A hacker, or Switch insider, can manipulate the encrypted data that comes from the ATM, sending it repeatedly to the HSM - each time with different parameters. In doing so – the attacker can expose the PIN codes encrypted by the ATM. An attacker can also use an existing set of PIN-processing functions that are not absolutely required for the Switch's ongoing operations. These additional sets of functions are simply a part of the general functionality of HSMs for PIN-processing applications. These functions were not traditionally considered to be vulnerable, since they were regarded as sensitive only together with access to the Issuer keys. It was a surprise to learn the functions could be used in an attack for exposing the PIN codes in the Switches even without having access to the Issuer keys..

Attacks taking advantage of the vulnerabilities are described in detail in **the academic paper [The Unbearable Lightness of PIN Cracking](#)\*** presented at the [Financial Cryptography and Data Security 2007](#) conference.

Security guru Bruce Schneier commented on the PIN vulnerability paper on his website [www.schneier.com/blog/archives/2006/11/attacking\\_bankc.html](http://www.schneier.com/blog/archives/2006/11/attacking_bankc.html):

## Attacking Bank-Card PINs

*By Bruce Schneier,  
November 17, 2006*

"... the paper describes an inherent flaw with the way ATM PINs are encrypted and transmitted on the international financial networks, making them vulnerable to attack from malicious insiders in a bank.

One of the most disturbing aspects of the attack is that you're only as secure as the least trusted bank on the network. Instead of simply trusting your own issuing bank to be secure against insider fraud, you have to trust every other financial institution on the network as well. An insider at another bank can crack your ATM PIN if you withdraw money from any of the other bank's ATMs."

\* The report was published by Odelia Ostrovsky, an academic in the Computer Science Department of Tel Aviv University and a product manager of Israeli cryptography firm, ARX (Algorithmic Research), and Dr. Omer Berkman, a lecturer at the Academic College of Tel Aviv Yaffo's School of Computer Science.

## **Solving the PIN Vulnerability at the Switch**

### **The Challenge**

Switches are usually owned and operated by third-party companies – and not directly by the cardholder’s bank or financial institution. The issuing entity has neither control over employees at the Switches’ locations, or over the HSM environment that defines the way the HSM is used. Switch insiders can take advantage of the weaknesses in the standard and use the relevant HSM to conduct an attack, for example, on a foreign bank. Many of the Switches use low-grade security solutions to perform the “translate” operation. Furthermore, even known secure solutions such as the HSM’s found in today’s marketplace, do not offer sufficient protection against the attacks described above.

In addition to the unnecessary extra functionality that downgrades the security of common HSM’s, there is another major issue that needs to be addressed: commonly used formats. HSM’s must support each of the approved formats for packing a PIN, and since one of the approved formats is a very weak format (ISO-1) - but can still be used in the HSM – it downgrades the entire system security to the level of the weakest format – even if the original format used by the ATM and by the issuer was the more secure one (ISO-0). Until the weak formats are removed from the list of approved formats for online transaction that must be supported by HSM’s, attackers can change the PIN codes formats between the different formats, exposing the PIN code.

Some HSM’s allow for the disabling or enabling of unnecessary functions. This could have been a basic solution to the problem. Alas, since each Switch is a stand-alone facility that is not under the supervision of the issuing bank, the malicious insider of a specific Switch can re-enable a weak function and use it to expose customer PIN codes.

Hackers exposing PIN codes in Switches will be able to use fabricated cards along with the corresponding PIN code to steal money from any financial card issuing institution, even outside of the country where the Switch is located – something that may dramatically decrease the chances of their being caught.

Once there is a suspicion that such an attack took place, all the Switches along the network from the ATM to the issuing bank are considered potentially vulnerable.

Marking certain Switches as vulnerable may pose a threat, and a serious risk for the relevant banks. This may become a major barrier for such banks to offer ATM services to either foreign citizens or foreign banks.

## The Solution

To prevent the described attacks, modifications should be applied to the standard that defines the handling and verification of the PIN codes. However, until such time that this takes place, and the modifications are approved by the relevant bodies, clear and strict security-related measures must be taken to prevent the PIN exposure.

The required steps are mainly related to HSM-functionality within the Switch facility. To be considered a fully-functional and security-hardened solution, the Switch-HSM should have the following capabilities:

1. **Centralized key management** – keeping all involved keys inside the HSM and having a mechanism to tightly control the keys uploading process to the HSM. In this manner, dummy keys cannot be used and loaded to the HSM without dual the control of reliable security supervisors. **If the keys are kept in a database outside of the HSM and then forwarded to the HSM as a parameter of the PIN translation function, then a dummy key can easily be used by an insider to then exploit and expose the PIN.**
2. **Disabling functions not required by the Switch** – for example, “Calculate\_PW” and “Calculate\_offset”. Unnecessary functionality should not exist at all on the Switch HSM and therefore cannot be enabled.
3. **Prevent encrypted data from the ATM from being entered repeatedly into the HSM** - this mechanism must identify encrypted data that was already processed by the Switch HSM and thus refuse to accept it again for additional processing. In this way the attacker will not be able to get information about the PIN code was entered at the ATM.
4. **Prevent re-formatting the PIN block into weak structures** – Although according to the current standard, PIN translation functions can also re-format the PIN block from one ISO format to another, the Switch HSM should disallow such reformatting in order to prevent the attacker from exploiting this weakness and gaining information about the customer PIN.

A Switch using an HSM that can protect the PIN code from being divulged **will not be accused** and **will not be liable** for cash withdrawals occurring as a result of Switch-based PIN attacks. Such Switches will be seen as a more attractive node to issuing banks, ATMs and other Switches.

## How the PrivateServer Switch-HSM Solves the Problem

The **PrivateServer Switch-HSM**® is a dedicated, FIPS 140-certified, hardware solution that supports the functionality required by Switches for financial transactions. The **PrivateServer Switch-HSM** is equipped with the following capabilities that help solve the security vulnerabilities within Switches:

1. The **PrivateServer Switch-HSM** does not include any unnecessary functionality that might be exploited by the Switch's insider to expose PIN codes. The HSM is delivered with the required function only and does not contain the implementation of the other set PIN Processing functions.
2. The **PrivateServer Switch-HSM** has mechanisms that ensure that encrypted data that was processed by the HSM at the Switch once cannot be processed by the HSM again.
3. The **PrivateServer Switch-HSM** contains a secured key management that supports all VISA and MasterCard requirements. The keys are securely stored inside the HSM and the HSM manages the key access rights and user access rights mechanisms. Each user can be allowed to perform a certain number of operations and might use a certain list of keys. Even if an insider of a Switch will be able to access all the functionality available on the HSM – they will not be able to trick the HSM for malicious purposes.
4. Keys inside the **PrivateServer Switch-HSM** can be defined as non-extractable and thus, working according to VISA and MasterCard regulations, ensures that these keys cannot be exposed.
5. PIN block formats considered to be weak, such as ISO-1 or ISO-2, can be excluded.
6. The **PrivateServer Switch-HSM** includes advanced security mechanisms such as Secure Session, tight access control of keys and internal auditing.

Combined, these mechanisms make the **PrivateServer Switch-HSM** a robust and highly secure solution for Switches, protecting against PIN-related attacks that might reveal PIN codes of any payment transaction sent to the issuing financial institution, through a specific Switch.