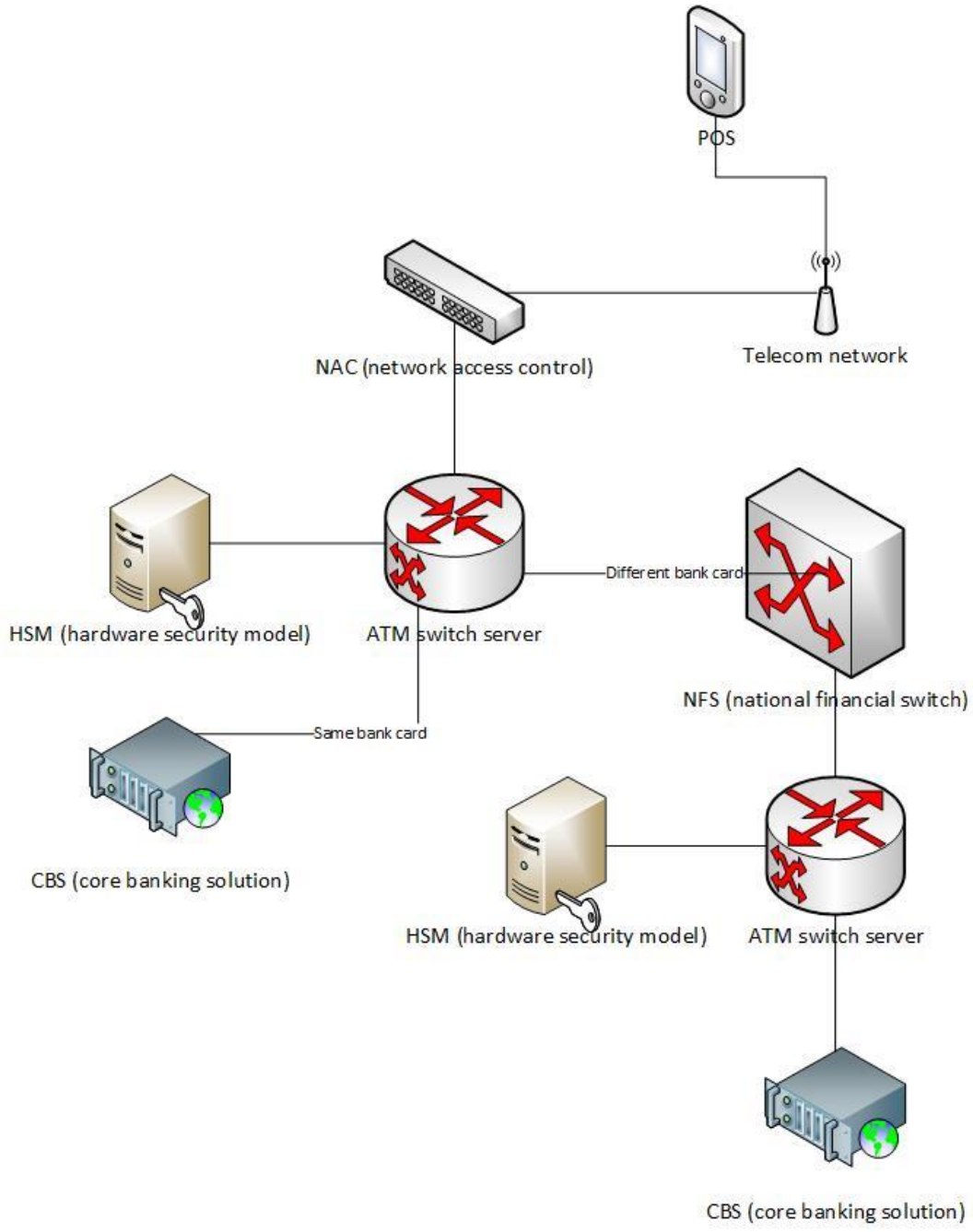
What is POS?

POS stands for Point of Sale. POS device process the transaction between customer and merchant for any service or product purchase.

It is the combination of hardware and software where POS application is used to perform all the transactions related operations by communicating backend server and management application is used to manage or configure the POS device including its services.

How Does POS Transaction Work?



1. Customers insert the Card into the POS device and enter the PIN.
2. POS device sends the card details along with the PIN to the ATM Switch server via NAC. NAC validates the identity of the POS device and allows access to appropriate servers during the initial setup.
3. If the card belongs to the same bank, the ATM switch will verify the PIN with the help of the HSM server and send the request to CBS server on successful verification of the PIN. If the PIN is invalid request will go back to POS device to re-enter the PIN.
4. If the Card belongs to a different bank, the request will go to NFS (National Financial switch) server and NFS server will send the request to ATM switch + HSM server of the different bank where the ATM PIN gets validated. ATM switch server will send the request to the CBS server on successful validation of the PIN.
5. CBS (Core banking system) check the sufficient amount in cardholder account. CBS deduct the purchase amount from cardholder account and the same amount is credited to the merchant account.
6. The CBS server sends the response back to ATM switch and ATM switch sends the response back to POS device with a successful transaction.

We have understood the transaction workflow in the above section. Now let's move ahead to the POS device security testing.

Will cover the POS device security testing into the following phases.

1. POS secure configuration review.
2. POS application testing.
3. POS network penetration testing.

### 1. POS secure configuration review:

POS device comes with the default configuration. It's default configuration settings must be changed before deploying into the production environment. A default configuration includes device access management, encryption methods, FTP service configuration, etc.

Review all the default configuration settings and other parameters to make sure that it has been configured properly while doing secure configuration review of the POS device.

- **Physical security:**
  Inspect the surrounding of POS device to make sure that there is no rogue camera and NFC card reader is placed to capture the card details.

  - **POS skimmer:**
    POS skimmer is placed over the card swipe mechanism to capture the customer card details from the magnetic stripe. Check the card swipe mechanism of the POS device to make sure that no skimmer has been placed.

  - **POS device – PIN pad skimmer:**
    PIN pad skimming / key-logging is used to capture the customer card PIN. An attacker installs the keypad overlay on the POS device that looks like the same as real POS device keypad. Check the keypad of the POS device to make sure that no skimming or key-logging device has been placed.

- **Network connectivity of POS:**
  The POS network must be segregated and no other user should be able to connect to the same Wi-Fi or LAN Network. Check the network connectivity of the POS device.

- **Default credentials on Device:**
  The device is using the default username or password for hardware administration. Check for the default device password which is used to administer the device.

- **Encryption:**
  The device can send data on Wifi/LAN channel. Check the encryption setting available on the POS device to make sure that it is enabled and properly configured.

- **Insecure Data Storage:**
  The device can store the data on the Memory card or in the device itself. Check for the configuration files whether it is stored in an encrypted format or not.

- **Cleartext services:**
  Check for the cleartext services enabled on the device such as FTP service which is used to download the device firmware from the server for the firmware upgrade. Cleartext services should be disabled on the device.

- **Logs:**
  Check for the device logs.

- **Missing Patches:**
  The missing patches address vulnerabilities which may allow unauthenticated remote code execution, privilege escalation, denial of service, and confidential information disclosure. Check for the latest updates.

- **Sensitive data exposure without authentication:**
  POS device has the feature to print reports of the device details and the transaction details containing sensitive information such as firmware version details, payment details, etc. Try to access the device reports feature without authentication.

- **Device update settings:**
  Check the device update setting for the latest updates.

- **The password policy:**
  Check the password policy applied on the device.

2. **Application testing:**

Application testing is an important activity to find out various application-level vulnerabilities. SoftPay application is used in the POS device to carry out all the payment related operations including online-sale, offline-sale, refund, etc.

In this section, will cover various application level and logical vulnerabilities:

- **Cleartext traffic:**
  Connect your laptop to the POS network segment and ensure that the laptop IP address and gateway address of the POS device must be the same. You can edit the POS gateway address under the device settings menu and restart the POS device. Check the cleartext traffic by initiating the request from the POS device and capture the traffic using Wireshark on the laptop.

- **Refund of amount:**
  Try to refund the amount more than the purchase amount.

- **Privilege escalation:**
  Application has 3 different privilege levels like Clerk, Manager, and Superuser. Try to access the manager functions/data using clerk account.

- **Check PIN validation for the transaction:**
  Try with the invalid PIN for the transaction during product purchase.

- **Data manipulation:**
  Try to manipulate the data by intercepting the traffic.

- **Sensitive Information Disclosure:**
  POS device generates the transaction receipt on the successful payment of the product/service. Check for any sensitive information such as account number and card details on the generated transaction receipt. The card details should be masked on the generated transaction receipt.

- Try the POS transaction without the PIN.

- Try to perform the offline sale transaction without or wrong approver code.

## 3. Vulnerability assessment and penetration testing.

Vulnerability assessment and penetration testing is the important activity to identify the network level vulnerabilities as POS device connects to the backend server in the segregated environment of the bank for various transaction operations.

Connect your laptop to the POS network by obtaining IP details of the POS device under the device settings menu and check the network connectivity with the POS device. Perform the full TCP and UDP ports scan on the POS device using Nmap tool to identify the open ports and the Nessus vulnerability scan on the POS device to identify the vulnerabilities on the POS device.

There are very limited and other services running on the POS device.

- **Operating system version:** Try to enumerate OS version details and verify for any vulnerabilities.
- **FTP service:** This service is used to download the updates from the server and upload device files. Check for the FTP vulnerabilities.
- **SNMP service:** SNMP service is used to manage the POS device centrally. Check for the SNMP vulnerabilities.
- **Management portal:** Check for the access to the management portal.
- **POS application:** Check for the application version vulnerability.