NCR Secure Whitepaper:

Solution: Dispenser Security Solution – September 2018

Protects against – Black Box Attacks

Description

Dispenser Security Solution (DSS) is a software countermeasure against black box attacks. A black box attack is one in which an attacker unplugs the currency dispenser communications cable from the ATM PC Core, and re-connects it to a controller which has the capability to send dispense commands. This controller could be a bespoke electronic subsystem, or it could be a laptop. The generic term for any type of controller is a 'black box'.

DSS works by enforcing encryption of the sensitive commands to the currency dispenser. Any command that results in the movement of cash is deemed sensitive, and is encrypted. The encryption protocol is designed such that a new encryption key is derived for each command therefore preventing replay attacks. The initial encryption key is generated by the currency dispenser during the initial bring live of the ATM, ensuring that each dispenser uses a unique key. The algorithm and key size used is AES 128.

The initial key exchange of this generated key is controlled by the Dispenser Protection level. This is a customer defined authentication setting which governs the circumstances under which the dispenser will share an initial key with the PC Core. Authentication is required to ensure that unauthorised personnel cannot force a key exchange, because if a key exchange is performed with a black box attached, then the black box will be able to send the requisite encrypted commands to the dispenser to facilitate an attack.

There are three levels of Dispenser Protection, described as follows;

Protection Level S1 / S2	Authentication Function
xxxx-F325 / F625 Level 1 USB Protection	Level 1 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software
xxxx-F326 / F626 Level 2 Logical Protection	Level 2 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software, and that a valid NCR USB Service Dongle is presented to the PC Core.
xxxx-F327 / F627 Level 3 Physical Protection Mandatory level to protect against Black Box attacks.	Level 3 authentication requires that the PC Core is running valid NCR APTRA XFS Currency Dispenser Software, and that safe access is demonstrated by performing the appropriate authentication sequence.

Considerations for setting Dispenser Protection Level

The initial protection level must be specified when the ATM is purchased. There is a mandatory feature in the ATM configuration which must be chosen, F325, F326 or F327 for S1 dispenser, F625, F626 or F627 for S2 dispenser. This will set the protection level on the dispenser as it leaves the factory.

It is possible to change the protection level in the field should that be required, and there are two possible methods to achieve this. A CE physically present at the ATM can use SYSAPP to change the level, or it is possible to send the new settings remotely using software distribution.

However, one very important point about changing the settings is that the protection level can be *increased* simply by setting the command in SYSAPP or remotely, but it is not possible to *decrease* the level unless the current level authentication is provided. In other words, to move from level 3 to level 2 or level 1, then physical access to the safe must be demonstrated, and to move from level 2 to level 1, a CE USB service dongle must be inserted. In practice therefore, decreasing the protection level is not possible using

remote methods since there must be a physical presence at the ATM to toggle a cassette and insert the dongle.

Required setting for Dispenser Protection

For protection against black box attacks, the Dispenser Protection level **MUST** be set to **Level 3, Physical Protection**.

Required software version for Dispenser Protection

General guidance for dispenser driver software is that it should always be upgraded to the latest version. The dispenser is a critical component of ATM security, and prompt patching of dispenser software should be planned as part of an FI's overall endpoint security strategy. Following a Black Box attack in Brazil in July 2014, NCR modified the DSS protocol, upgraded the encryption algorithm from DEA to AES, and introduced a 'no-roll back' function into the firmware. The no-roll back function means that an attacker cannot mount a Black Box attack by simply rolling back the firmware to a version that could be exploited.

As of May 2018, the software version of DSS included in the USB Currency Dispenser component released in APTRA XFS 06.06.00, (release 8th June 2018), was again updated. This software includes important security fixes, including resistance to 'endoscope attack' and misuse of diagnostic dispense. (Please see NCR Security Alerts for details of these attacks.)

In September 2018, the APTRA XFS Dispenser Security Update 01.00.00 was released, which also includes critical security updates.

Dispenser platform software is available from NCR Professional Services via the NCR Download Centre, and is free to customers on Software Maintenance.

Required setting for Dispenser Authentication Sequence

Dispenser Protection includes a function that will allow configuration of the Dispenser Authentication Sequence, and this parameter must be set correctly to maintain protection. The Dispenser Authentication Sequence is the action which authorises a key exchange for dispensers set to Level 3 Protection. (This setting is not applicable to dispensers not set to Level 3.)

Authentication Sequence Options for Level 3 Dispenser Protection:

S1: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBCurrencyDispenser/Operational Parameters/Dispense Authentication Level	
Sequence 1: dword:00000000 (Default)	Remove bottom cassette **OR** Insert bottom cassette **OR** Toggle switch on control board Action must complete within 60 seconds of command
Sequence 2: dword:00000001 **(Minimum Recommended Level)**	Remove bottom cassette **AND** insert bottom cassette, **THEN** remove purge bin **AND** insert purge bin Full sequence must complete within 20 seconds
Sequence 3: dword:00000002	(Rack out dispenser **AND** Remove bottom cassette **AND** Insert bottom cassette **AND** Toggle switch on control board **AND** Toggle switch back again **AND** Rack in dispenser) Sequence must complete within 20 seconds

S2: HKEY_LOCAL_MACHINE/SOFTWARE/NCR/APTRA Self-Service Support (NCR Features)/USBMediaDispenser/Operational Parameters Dispenser Enable Level	
Sequence 1: dword:00000001 (Default, Recommended)	Remove bottom cassette **AND** insert bottom cassette only Action must complete within 60 seconds of command, cassette must be replaced with 10 seconds of removal
Sequence 2: dword:00000002 Note: Available in APTRA XFS 6.06 only	Remove bottom cassette **AND** insert bottom cassette, **THEN** remove purge bin **AND** insert purge bin Action must complete within 60 seconds of command, sequence must complete within 20 seconds

The authentication sequence only applies to Currency Dispensers set to Level 3 Protection. Any Currency Dispenser not set to Level 3 Protection is already vulnerable to Black Box attack, and this setting will provide no further protection unless Level 3 protection is configured.

The authentication sequence level can be increased remotely. The authentication sequence can be decreased only if the current authentication sequence is performed. (e.g. to move an S2 Currency Dispenser from Sequence 2 to Sequence 1, it will be necessary to remove and insert the bottom cassette, then remove and insert the purge bin, within one minute after issuing the command.

For the S1 Currency Dispenser, Sequence 2 is the MINIMUM RECOMMENDED LEVEL, and this setting MUST be configured along with Level 3 Protection.

Operational Considerations

The implications of setting a protection level must be considered. While the initial key exchange happens at ATM bring live, there are other lifecycle circumstances which will necessitate a new key exchange. These are;

- Software Rollback
- Software Ghosting
- Hard disk swap
- Core swap
-

Software Rollback or Ghosting effectively replace the entire software contents of the hard disk, and will cause the dispenser encryption key to be erased. Therefore, on an ATM set to level 2 or level 3, a 'Prepare for Ghost' command must be issued prior to replacing the software. This is an encrypted command that will ensure that the current encryption key is preserved, thus removing the requirement for physical access at the ATM.

In the case of a hardware swap, due to either an upgrade or repair due to failure, then it should be recognised that if the protection level is set at level 3, then the CE will require safe access in order to complete the upgrade or repair.

Summary: Minimum requirements to protect against Black Box Attacks

1. Deploy the latest version of Dispenser Platform Software. NCR apply critical security patches to the dispenser platform software, and it is imperative that customers maintain their platform software to the latest version. The minimum version which must be used is **APTRA XFS Dispenser Security Update** 01.00.00

2. Set the Dispenser Protection Authentication level to **Level 3, Physical Protection**.

3. For S1 dispensers, set the Dispenser Authentication Sequence to Level 2 (Dispense Authentication Level = dword:00000001)

Anything less than these three requirements will NOT protect the ATM against Black Box Attacks.

First Issue Date: 30 October 2014
Update for recommended software versions: 14 September 2018