Triton®
Partnership Measured in Decades...
866-787-4866
21405 B Street, Long Beach, MS 39560

atmgurus®
just ask us...

TECHNICAL BULLETIN

SUBJECT:
ATM SECURITY ALERT

TECHNICAL BULLETIN: 18-15
DATE: NOVEMBER 06, 2018

Confidential - Available to all authorized Triton distributors and third party service providers

IMPORTANT SECURITY ALERT

In light of recent reported attacks in California in which retail ATM terminals were scammed via an altered transaction reply message that effectively turned a transaction denial into a transaction approval allowing cash to be improperly dispensed, Triton Systems would like to remind customers of security features and suggested upgrades to keep your ATM portfolio safe.

To avoid man-in-the-middle attacks like those seen recently in California, Triton strongly suggests the following security features:

1. **Install high security locks.** The perpetrators in the recent attacks appear to be accessing sensitive ATM components via the top cabinet. Opting for high security locks and keys in lieu of using default locks is the first line of defense for your ATM. High security locks have unique lock/key combinations and are pick resistant. Triton offers high-security locks upgrade kits for multiple models.

2. **Enable SSL (secure socket layer) & TLS (transport layer security) protocols.** SSL provides a method to encrypt and authenticate communications between the host and ATMs connected via TCP/IP. Triton ATMs must have software version 2.4.0 or greater to enable SSL via Management Functions. Check with host processor for certificate and configuration information. Ensure host is using TLS 1.1 or later, and the ATM has the latest TLS updates installed. If using TCP/IP via a wireless communications box, check with wireless provider as well. As of October 2016, TLS updates have been preloaded onto all parts orders, repair orders, new ATMs and certified pre-owned ATMs from Triton. See Triton Technical Bulletin 18-02 for more information.

3. **Use MAC (message authentication code) if available.** MACing provides yet another method of authenticating communications between the ATM and host processor, preventing man-in-the-middle attacks. Contact host processor to verify MACing is supported and to acquire MAC Master Keys if the service is available. Entering MAC Master Keys and downloading working keys follows the same process as entering PIN Master Keys. See Triton Technical Bulletin 09-04 for more details.

For general ATM safety and security against all manner of ATM attacks, Triton also recommends the following:

4. **Perform software and security updates.** Triton periodically releases new software versions that include feature enhancements and vital security updates. Current software version can be found at the ATM via *Management Functions* > *Diagnostics* > *Terminal Status* > *Configuration Summary*. Update files and release notes can be found easily using Triton's new Software Wizard. Triton Connect users do not require a site visit and

may remotely download software updates.

5. **Additional software and communications precautions include:**

   — Triton ATMs include a firewall to block unwanted, malicious communications on the ATM TCP/IP connection. In order to enable the firewall, the operating system must be CE 5.0 or higher and the ATM software should be up-to-date. For the RL, FT and RT Xscale units, Triton offers **upgrade kits**.

   — TKM (Triton Key Management) uses cryptography to allow master keys to be loaded remotely from the host to an ATM on a public network. Once TKM is enabled at the terminal, a site visit to load master keys isn't required which allows for keys to be updated more often. Triton ATMs must have software version 2.4.0 or later, a T9 or T5 PCI keypad with firmware R2B or later, and host support.

   — Call back via Triton Connect is an option on all Triton ATMs that is designed to prevent unauthorized systems from contacting the ATM through its communication lines. When enabled, the ATM hangs up if contacted by Triton Connect, then returns the call to Triton Connect before exchanging any data.

6. **Install anti-skim card readers.** Skimming devices can be installed quickly and often go unnoticed. Triton's anti-skim card reader uses multiple methods to detect metal in or near the card reader and stops service at the terminal until skimming device is removed. **Anti-skim upgrade kits** are available for most models. See **Triton Technical Bulletin 18-07** for more details.

7. **Invest in PCI-compliant keypads.** In May of 2014, Triton began shipping our 3.1 PCI-certified T9 keypads. Triton ATMs require dual password access and tokens (permissions) from the Triton partner site, complete with challenge codes and responses, to reset a keypad tamper. Triton offers **T9 upgrade kits** for select models.

8. **Additional physical security measures include**:

   — The ARGO product line and all certified pre-owned terminals ship from Triton with an ASM (advanced security module). Triton strongly recommends installing an ASM on all fielded or legacy units to help defend against man-in-the-middle attacks that target communications between the main board and cash dispenser. **ASM Upgrade kits** are available on Triton's ATMGurus website.

   — Triton installation manuals provide step-by-step instructions for proper anchoring. All ATMs should be bolted to the floor to avoid tampering and/or theft.

   — Triton offers **close out plate upgrade kits** for legacy model ATMs to ensure that any openings on the ATM are sealed to prevent phishing attacks and unauthorized access inside the cabinet. The ARGO series was designed to eliminate these risks and does not need upgrading.

   — **Security cameras** are available on Triton's ATMGurus website, which is a good deterrent to criminal activity around your ATM. For more information on cameras and other general security measures, read **ATM Security - An FBI Perspective** on atmAToM.

   — Other top cabinet fortification includes a more robust, double CAM locking mechanism standard to Australian markets. The rules of APN stipulate that any damage must be visible if entry is attempted on the ATM. Upgrade kits can be made available to customers in other markets upon request.

9. **General Safety Practices.** Triton would like to remind customers that in addition to various software updates and hardware upgrades that help protect your ATM investments, there are some general precautions that all ATM owners and operators should employ, such as:

— Do not use default or same-number passwords, such as 1234 or 1111. Triton ATMs go out of service if master passwords are left at or set back to the default codes to protect against any fraudulent access, such as criminals accessing Management Functions to perform a denomination change, then performing normal withdrawals on a non-traceable card. The ATM can be "tricked" into thinking it is dispensing $1 bills when it is in fact dispensing higher denominations.

— Change Management Functions passwords periodically to maintain a secure environment, including master, admin, and user passwords, EPP user 1 and user 2 passwords, and EPROM access codes on Z-180 machines. This is an especially good practice to change these items when technicians or other employees with access leave.

— For dial locks, avoid using numbers 0 or 5, any numbers in a series or sequence, and do not use the numbers 0-20 for the last digit when setting your combination.

For more detailed information on ATM attacks and security measures, visit Triton's **atmAToM** to read our spotlight security blogs.

Triton Eye on Security

ATM Security – An FBI Perspective

Stay up-to-date on security concerns and products via Triton Technical Bulletins. Please ensure all vital personnel receive Triton technical and marketing communications. Customers may **subscribe** or **update preferences** from the main page of Triton's **atmAToM** blog.

If you have questions regarding this Technical Bulletin, please contact Technical Support at 1-228-575-3100, option 4 or toll free in the U.S. / Canada 1-866-787-4866, option 4. Visit www.tritonatm.com for additional information. For all ATM parts, repair, and training needs, visit www.atmgurus.com.