21405 B. Street, Long Beach, MS • 866-787-4688 • www.triton.com • www.atmgurus.com

August 24, 2021
Bulletin 21-03

2021 Triton Security Update

Triton understands how paramount security is to your business, so we make it our business to ensure that Triton ATMs have the best protection possible. Increased risks make it difficult for the industry to stay ahead of the criminal element. Therefore, we would like to take a moment to review our ongoing commitment to keeping Triton ATMs safe.

Windows CE™

There were many factors considered while assessing platforms to power the operating system of Triton ATMs. The decision was to go with Windows CE for several reasons;

CE uses less computing resources, meaning lower-cost hardware, without sacrificing functionality. As a result of the low cost, Triton can offer our customers standard software updates at no charge.

Windows CE is an embedded platform so it can be easily tailored to specific requirements and functionality.

Triton has access to much of the CE operating system source code and can provide updates beyond Microsoft™ support.

The majority of security updates provided by Microsoft are for Internet Explorer issues. Triton ATMs do not use Internet Explorer (Microsoft Edge™) and it is removed from our customized operating system.

Triton ATMs currently run a proprietary, locked-down version of Microsoft Windows CE 4.1, 5.0, 6.0 or Compact 7. The operating system is customized by Triton to add additional security beyond what is provided by Microsoft.

Triton ATMs are locked down by not providing any access to the OS or internal storage except through our ATM software interface. Software can only be installed by loading a software update which must be digitally signed by Triton.

Triton ATMs use the Windows CE "Trusted Environment" to verify the authenticity of all software. Every component is signed with Triton's private key which must be verified by the operating system before executing. In this manner, the ATM is protected from executing software not created or approved by Triton.

As part of the Triton customization, all system tools have been removed from the operating system that an attacker might use to access or manipulate the system, including File Explorer, Windows Desktop, Internet Explorer, Command Shell, ActiveSync, and Remote Desktop.

Triton regularly monitors all security updates provided by Microsoft. To date, Triton has never had to install a Microsoft provided update for any security reason. Triton will continue to monitor our ATMs for security issues beyond support by Microsoft and provide updates.

In the event a security issue is identified on an operating system that is no longer supported by Microsoft and cannot be addressed by Triton, an upgrade path to a newer operating system version will be provided. This upgrade could include a hardware upgrade as well. Costs for any hardware/software updates will be determined at that time.

Software and Security Updates

Check that you have the most current software version running on your ATM fleet. Triton periodically releases new software versions for all of our ATM models that include feature enhancements, as well as vital security updates to protect your investment. These updates are easily found on our website, just follow the instructions. If you have Triton Connect, you can load/update software remotely. Additionally, unlike traditional Financial Institution ATM manufacturers, software only updates from Triton are available free of charge, and all coding is written and tested in our America-based labs.

MACing

MAC stands for Message Authentication Code, which provides a method to be certain that messages between the ATM and the host are authentic and unmodified, thus preventing man-in-the-middle attacks and bogus hosts or ATMs. The first step is to contact your Host/Processor to verify if they support MACing. The Host/Processor will provide MAC Master Keys that must be loaded at the ATM just like PIN Master Keys are loaded. A Key Download is performed at the ATM and MAC Working Keys are sent from the Host/Processor to the ATM. The Host/Processor can then enable MACing.

Secure Socket Layer (SSL/TLS)

Like MACing, SSL/TLS also provides a method for the ATM to authenticate the host and additionally provides encryption and integrity between the Host and the ATM connected via TCP/IP (either hard wired, or with a wireless communication box). You will need Triton software version 2.4.0 software or later for the ATM to be SSL capable. The Host/Processor will provide you with configuration information to allow you to set up your ATM to communicate SSL with their network. Additional certificate updates may need to be loaded on the ATM because of Triton's validation of certificate authority and dates (confirm with your host processor).

If the ATM does not verify that the certificate was issued by a trusted authority, then the ATM does not authenticate the host, and an attacker can insert themselves between the ATM and the host as a man-in-the-middle, or the attacker can stand-in as a fake host. Unbeknownst to the card-holder, the attacker can eavesdrop on all communications, for example capturing the card's track-2 data. And if no other authentication technique is employed (such as MACing), the attacker can also modify the communications, such as changing the transaction's dollar amount or converting a declined result to approved. It can be argued that there is no risk of an attacker inserting themselves, that's why SSL is being used in the first place — the very use of SSL is an admission of the risk of a malicious interloper.

Anyone can generate their own certificate, containing any arbitrary data. It takes just a few seconds using the free software OpenSSL. If an ATM does not verify that the certificate is current and was issued by a trusted authority, then the ATM cannot differentiate an attacker's bogus certificate from a host's legitimate certificate.

Triton has been told by our customers that this feature makes a Triton more difficult to operate in the field. Security is not always convenient. When making decisions between convenience and security, Triton will always err on the side of security. We hope that our customers understand this as we work to keep your portfolio safe.

Malware and Jackpotting

Two lines of defense prevent unauthorized software from making its way onto Triton ATMs.

Both lines of defense use the same technique, namely the ATM verifies that the software has been digitally signed by Triton using Triton's private key. If the digital signature is incorrect, then the ATM does not accept the software. This ensures that only legitimate software, authorized by Triton, can run on the ATM.

1. Before a software update is installed, the ATM verifies the load file's signature, and only proceeds with the installation if the signature is correct.
2. The ATM uses the Microsoft Windows CE operating system's Trusted Environment which verifies the signature of every program before it is allowed to run.

An attacker cannot generate a correct signature, because only Triton holds Triton's private key. Thus, malware cannot be imported into the ATM because the encapsulating load file's signature would be incorrect. Malware cannot run on the ATM because Windows CE's Trusted Environment would not execute a program whose signature is incorrect.

Firewall

Triton's ATMs include a firewall to block unwanted communications on the ATM's TCP/IP connection. The firewall defends against malicious attempts to remotely access the ATM. It also helps the ATM to pass a PCI DSS vulnerability scan. You can verify the settings for firewall in the management functions.

Default Passwords

Make sure to change management passwords periodically and keep control of them in a secure environment. It's also a good business practice to change them when technicians leave. This includes Management Function passwords (Master, Admin, Users), EPP User 1 and User 2 Passwords, and EPROM Access Codes on Z180. Note that the ATM will not go in service until default passwords are changed.

Denomination Changes

Triton ATMs require access to the cash vault to modify the denomination setting. This prevents an attacker from changing the denomination to a smaller amount than what is actually in the dispenser. Information is also logged to the ATM journal during a denomination change to indicate if a failure occurred, as well as the user who was logged in at the time.

Anti-Skim Card Reader

Skimming devices can be added to card readers so quickly they can easily go unnoticed. Triton's anti-skimming device works by detecting metal near or on the card reader. If metal is detected, the ATM automatically goes out of service, logs the event in its journal, and advises Triton Connect. When the skimmer is removed, the ATM automatically recovers. The anti-skim card readers also employ,

- Magnetic Field Interference in which a jamming signal is emitted to disrupt a detected skimmer's reading of a magnetic stripe.
- Encryption at Magnetic Head – Magnetic stripes are encrypted at the very first point at which they are read, defending against a skimmer inside the ATM's cabinet.
- Encryption of EMV Chip Card APDU – Data exchanged with an EMV chip card is encrypted on the card reader's cable, defending against a skimmer inside the ATM's cabinet.

PCI v3.1/v5

All new Triton ATMs ship with our PCI 5 certified keypad, the T10.

Triton follows the letter of the law for PCI. For a Triton ATM, a tamper, resulting from removing the keypad cannot be reset without dual access to the Triton partner site to then go through the process Triton has set for reactivation.

Some manufacturers may have settings in management functions that allow keypads to be removed without tampering. We believe this is a potential security risk and may not meet PCI as intended. You should verify with your manufacturer that they do not allow this in the field.

Triton Key Management (TKM)

TKM uses cryptography to allow Master Keys to be loaded remotely from a host to an ATM over a public network. This will allow the keys to be changed more often and will not require a site visit to load keys once TKM is enabled. The Host must support TKM the ATM must have version 2.4.0 or later software, as well as a T5 PCI Keypad with Firmware R2B or later, or a T9 or T10 PCI Keypad. In addition, the Host provides a Host ID, and TKM must be enabled on the ATM.

With upcoming PCI 5 keypads, the host must support SHA 2 in order to also support TKM. Check with your Host for support timelines. This allows ATM owners, especially those with large ATM portfolios or those that operate in markets that require that master keys be changed frequently, to save time and money while improving security.

TKM verifies the host ID that Triton issues to each host. This keeps impersonator or rogue hosts from loading the attacker's keys to the ATM.

Triton Connect Call Back

Call Back is an option in the Triton Connect set up on the ATM. If Call Back is enabled, when Triton Connect contacts the ATM, the ATM will hang up and call Triton Connect back before data is exchanged. This feature is designed to prevent unauthorized systems from contacting your ATM through the communication line. This function is always enabled when using SSL and when performing a software download.

Bolt the Cabinet/Level 1 Vault

Physical security requires that the ATM be bolted securely to the floor. Triton installation manuals provide step by step instructions for proper bolting.

There is also a level 1 safe option for Triton ATMs.

High Security Locks

High security locks have unique keys for each lock and are pick resistant to UL437. Triton Part Number 06100-08029 is configurable for high security locks for ARGO, ARGO FT, Traverse, FT5000, RL5000, 8100, RL2000, RT2000, RL1600, 9700, 9100. These locks can be ordered in any number of unique keyed solutions (a unique set of locks for all your ATMs, for select customers, or even down to the ATM level).

All manufacturers have default keys that work on all their ATMs. High security locks are the first line of defense to keeping your mainboard secure.

EMV

Triton developed EMV upgrade kits for our legacy products including RL2000, RL1600, RL5000 X1 and X3, FT5000 X1 and X3, RT2000 X1 and X3 (10.4” LCD only), 9100, 8100, 9700, and 9600. Our current product line of ARGOs, Traverse and ARGO FT are standard with EMV and fielded units also have upgrade paths to support EMV. You can find EMV upgrade kits here.

Advanced Security Module

With the release of the ARGO product line in 2013, Triton introduced a new security module to improve the security of communications between the ATM's mainboard and cash dispenser. The Advanced Security Module (ASM) and updated software are available for legacy ATMs as well. Triton strongly suggests that this hardware/software upgrade be loaded on all your machines to help defend against man-in-the-middle attacks between your ATM's mainboard and dispenser.

The Triton ASM uses a software key to secure the communication traffic between the mainboard and the security module which resides in the safe with the dispenser. The software key is unique per ATM using a key exchange between the ASM and the mainboard of the ATM. Initiating the key exchange requires Master User credentials for the specific ATM as well as access to the vault. Synchronization is required anytime the mainboard or the ASM are replaced.

Cameras

Installing a camera to help deter thieves at your ATM location is an option. All ARGO ATMs are equipped with a camera mount housed in the control panel.

Close Out Plate

Triton released the Close Out Plate Kit for legacy ATMs in 2014, which will ensure that the openings on your ATM are sealed tight. When adding the close out kits, the cables also need to be rerouted. The number of kits required depends on the business hour cabinet or level one vault in question. The ARGO was designed to eliminate these risks and does not need upgrading.

Enhanced Control Panel Security

Entails a more robust double CAM locking mechanism. This ensures that if an attempt is made to break into the cabinet, the damage will be easily seen.

Projects in the pipeline for 2H 2021/2022

NFC – The cardless option will be available for all ARGO ATMs and will offer an EMV transaction and the security you are used to having with a Triton.

Anti-Skim Card Reader – To combat deep insert skimming, we will be adding features to the anti-skim card reader.