Q-NET Security Use Case: ATM Protection

The Problem

Encrypting and authenticating data in ATM networks is an industry standard practice. Hardware Security Modules (HSM) are the leading solutions in the ATM space. But these tend to be decades-old solutions with aged operating systems and weak encryption schemes that enable ATMs to fall victim to modern and sophisticated attacks, such as jackpotting.

The Solution

Q-Net Security (QNS) snaps seamlessly onto legacy ATM networks with a solution built to last decades. The retrofit takes minutes and does not require any software agents, server upgrades, patches, or network modifications, and is compatible with existing HSMs. The solution provides 256-bit symmetric encryption that exceeds NSA / NIST post quantum compute standards and therefore safe from exascale and quantum computing attacks of tomorrow. The QNS solution is silicon-based and impervious to security holes in operating systems that are being exploited by hackers with increasing frequency.

How Does it Work?

Small bump-in-the-wire devices are installed inside each ATM. The installation is simple: if you know how to connect a printer, you can install a QNS solution. The connections are managed through a central module – the QNS Policy Manager – that has proven to require no advanced training and be self-explanatory. Deployments at other financial institutions have literally taken only minutes.

What is the Special Sauce?

The founders of QNS have a distinguished history of fundamental innovation, including significant roles in building the first personal computer, inventing modern computer networking, developing security for magnetic swipe technology, and pioneering the field of heterogeneous computing. The QNS approach moves away from a general-purpose computer architecture to a special-purpose architecture that makes it impossible to hack. There is no way to install or execute software on a QNS device, nor is there any IP address to connect to it, rendering cybersecurity attacks futile.

Value Proposition

- ***Install quickly and economically***: protects any ATM with no changes needed to existing ATM software or network; no regression testing required
- ***Cut network expenses***: can safely use the public Internet or LTE; no costly private networks required
- ***Lower operations costs***: use doesn't require advanced personnel; no external key management or additional IP addresses required; never need to update or patch
- ***A futureproof investment …*** prolong the useful life of existing equipment; solution designed to protect network for decades

Just Try It!

QNS solutions have been deployed in high-value networks of some of the most important financial services companies in the world. QNS can perform a proof-of-concept in just a morning or afternoon. We welcome the opportunity to show how easily a QNS solution retrofits into your network, and to demonstrate that it is the strongest commercially available network cybersecurity solution on the market.

Q-Net Security