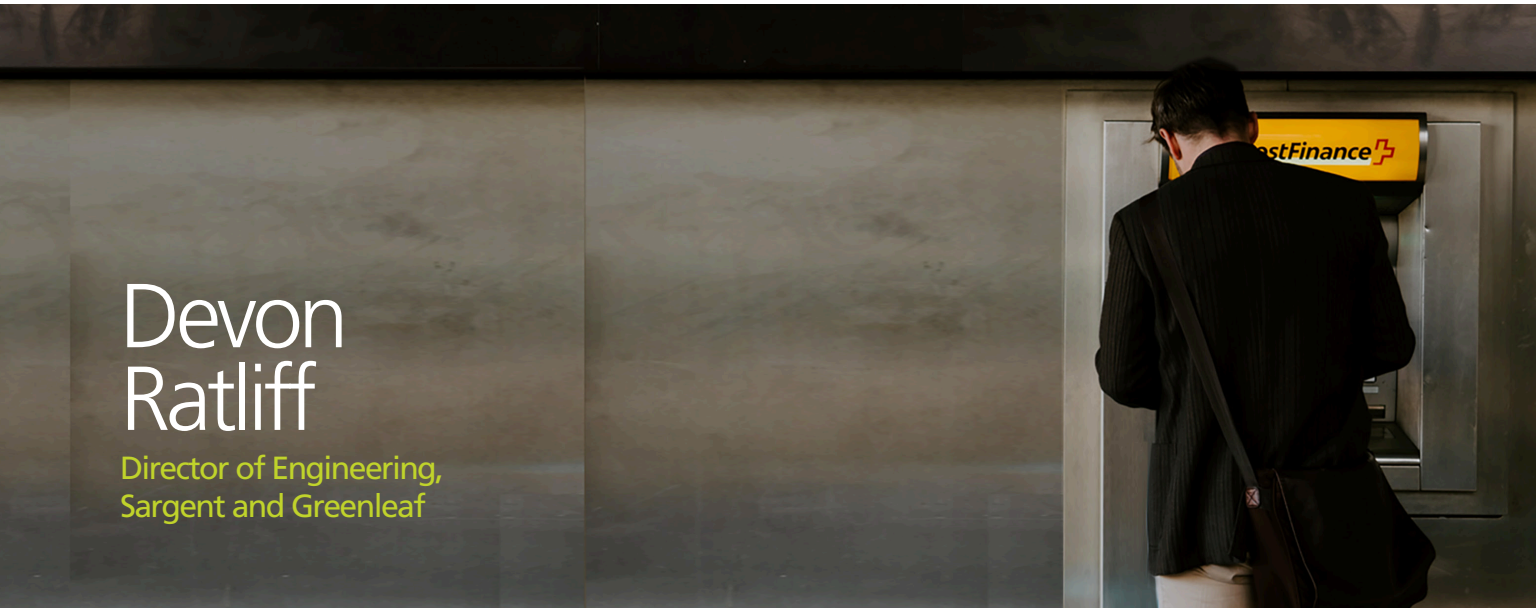
SARGENT AND GREENLEAF®

Protecting ATM Locks from Side-Channel Attacks



Devon Ratliff

Director of Engineering, Sargent and Greenleaf

Side-channel attacks, which can exploit internal electronic components of electronic locks, first emerged in 2015, and continue to grow in complexity. At a recent technology conference, security researchers presented the latest iteration of these attacks—specifically targeting ATM locks.

As one of the world's foremost manufacturers of ATM security, Sargent and Greenleaf devotes immediate and intensive response to suspected cash management vulnerabilities. In response to previous similar challenges, S&G implemented electronic hardware and internal timing changes to our A-Series and A-Series with Display locks. Our latest round of testing may give ATM owners and operators insight into how to protect their machines against side-channel attacks.

To analyze vulnerability to side-channel attacks, S&G engineers constructed scenario testing around each lock component. Specifically, we examined:

- **Availability of external connection points**
- **Electronic information stored within the lock**
- **Internal lock communication of secure information**

Our findings highlight key opportunities to thwart emerging threats.

Keypad Accessibility.

The recent attack relies on immediate access to available connection points. Making keypads with solid rings—and keeping access points behind them—may deter attackers by requiring keypad removal prior to launching side-channel attacks. Stronger deterrents such as S&G's tamper-proof keypad option add additional layers of protection to ATM security solutions.

Access Code Storage.

Rather than storing actual access codes inside the lock, tying codes to specified time windows and touch keys prevent attackers from gaining control of the system. Further, minimizing encryption information stored inside the lock can prevent side-channel attackers from initiating full encryption routines.

One Time Code Generation.

The longer hackers have to run their software to gain access, the less likely they are to meet with success. Our research shows that implementing multiple-layer code generation—such as using one-time codes, time-windows, and touch keys—substantially reduces vulnerability to random code generation breaches.

Modular Design.

Locks with modular designs support easier upgrades as new threats emerge. We tested A-Series keypads and locks, which use a four-conductor cable with flexibility to support a wide variety of scrambling devices.

S&G's engineering division remains committed to testing ATM security solutions to protect our customers and help ATM owners and operators worldwide mitigate common vulnerabilities.

Corporate Headquarters: One Security Drive • Nicholasville, Kentucky 40356 • USA • Tel. 859-885-9411, Fax 859-887-2057