Arxan Application Protection for Mobile Payments and Banking

Your business can't afford to be hacked

Mobile Payment and Banking Applications Put Your Data, Reputation, and Customers at Risk

For hackers, payment information is the holy grail of online data. Protecting this sensitive data and preventing fraudulent transactions is becoming exponentially more challenging because mobile payment and banking apps are highly vulnerable. In fact, among a random sample of 55 of the most popular mobile payment and banking apps tested, 98% lacked binary protections. In addition to the obvious security risks, which leads to data theft, fraud, and brand reputation damage, 81% of payment and banking app users said they would change providers if they simply knew the apps they were using were not secure.

Top Mobile Payment and Banking App Attacks You Must Defend

Whether it's a digital wallet, P2P payment, POS system, or mobile banking application, your customers rely on your applications to empower them to transfer money, check deposits, and get business done. Hackers are targeting these high-value applications and gaining access to sensitive data, redirecting payments, and doing other nefarious things by:

- **Tampering with security logic.** Many payment and banking providers have common security modules inside their applications that provide security functionality, such as authentication. Tampering with this functionality allows hackers to bypass the controls and access sensitive data.
- **Reverse-engineering the application.** Even if you are using Mobile Device Management (MDM) and Mobile Access Management (MAM) that govern the use of the application, it is still fully exposed and vulnerable to being reverse-engineered.
- **Stealing cryptographic keys in Host Card Emulation (HCE) applications.**

Arxan Protects Your Mobile Payment or Banking App and Assures Brand Trust

Mobile payment and banking customers appreciate the technical and business value our application protection delivers.

- Prevents unauthorized access to applications
- Prevents the modification of applications, including the insertion of malicious code
- Determines whether the environment in which mobile apps are running is safe
- Prevents cryptographic key exposure for HCE

Why Choose Arxan? Your Reputation is Everything.

Mobile payment and banking customers appreciate the technical and business value our application protection delivers.

- **Security Strength:** multi-layer guard network delivers the most advanced application protection
- **Maturity:** we are protecting apps running on more than 500 million devices
- **Simplicity and Customizability:** integration is easy and security protection maps to your specific requirements
- **Service and Support:** world-class support from experts who are available when you need them
- **Trust and Stability:** financially strong company backed by top tier private equity firm; customers represent some of the world's leading brands

Arxan Automated Application Protection

DEFEND

Against reverse engineering, tampering and any manner of theft

DETECT

An attempted attack on the application code, or on another Guard

DETER

Attacks by safely exiting or silently deleting illegal assets or stealthily reporting back forensics information to a command center