

A New Approach to Secure Mobile Banking Apps

Abstract

Mobile banking applications provide significant security challenges for line of business, development and app security leaders. And application security isn't always a core competency for mobile app development managers. This whitepaper explores a new approach to mobile banking application security that is integrated at the binary and source code level.

Table of Contents

Executive Summary	3
Mobile banking apps pose enormous security challenges	4
Typical security path	5
App security tools and best practices	5
Issues with legacy app security measures	5
Rethinking mobile app security	6
Harden mobile apps once	6
Real-time visibility and analytics	7
Conclusion	7
About Arxan Technologies	8
Appendix: Additional Background	9
App security tools and best practices	9
Mobile threats prevented by Arxan Application Protection	9

Executive Summary

By the end of 2018, nearly all financial institutions will offer mobile banking services. Top business reasons for embracing mobile include retaining existing customers, meeting competitive and cost pressures, attracting new customers, and projecting market leadership in technology, according to a survey of 706 financial institutions in seven U.S. Federal Reserve districts¹. Usage lags, however, with 56 percent of institutions reporting usage rates of 20 percent or less; just eight percent reported usage rates over 50 percent, according to the survey. The number one barrier is “security concerns,” cited by 70 percent of respondents.

The purpose of this whitepaper is to help mobile banking line-of-business, development and app security leaders get executive-level context on what financial institutions are doing to secure mobile apps, and how improving those efforts can boost consumer confidence in mobile banking security.

As we find in security, there is no single “silver bullet,” so a comprehensive solution will have multiple layers. In an increasingly mobile-first world, apps are distributed via app stores and downloaded by users to what can be best described as a zero-trust environment – one in which apps are easily exploitable by attackers and, in most cases, lack proper security measures. To best secure your critical banking application, in addition to network and device security precautions, apps should be treated as an endpoint – and protection applied accordingly to prevent unprotected apps from becoming an attack vector.

Visibility is also critical for banks to adapt to the threat landscape and prevent emerging app threats from becoming widespread attacks. Unfortunately, most application protection solutions do not include real-time threat data collection, monitoring or analytics when deploying mobile banking apps in the wild. Without app feedback, there’s no way to react to attacks in a timely fashion.

¹ Federal Reserve Bank of Boston, [Mobile Banking and Payment Practices of U.S. Financial Institutions](#), Dec. 2017.

This whitepaper describes a new approach to app and endpoint security – with three transformational benefits for mobile banking apps.

- 1) Prevent reverse engineering and tampering, which could lead to breaches and app data theft, by hardening mobile apps after code is complete with a system of embedded safeguards.
- 2) Stop API compromises and theft of intellectual property or personally identifiable information with comprehensive data and key encryption using white-box cryptography.
- 3) Stay ahead of app threats and vulnerabilities with the ability for each protected app to “phone home” and provide real-time threat visibility and analytics data.

Arxan protects mobile banking and financial applications through app hardening, data and key protection, and the industry’s only real-time threat data and analytics. Implementing these capabilities improves security posture, customer trust and brand reputation. Once Arxan protections are integrated with applications, they can be automatically applied to each new revision of code – greatly reducing the effort required when updating apps for re-release.

Zero Trust Requires Closed-Loop Feedback

Zero Trust is about not trusting anything inside or outside the network perimeter. It requires verifying anything and everything trying to connect to an organization’s systems before granting access.

Because most banks can’t see application attacks coming, they are unable to optimize their response, leaving an open decision loop. Good data enables organizations to adapt defensive responses and deploy effective countermeasures.



Mobile banking apps pose enormous security challenges

Retail mobile banking is ubiquitous, according to a survey of 706 financial institutions in seven U.S. Federal Reserve districts². The report says 89 percent of respondents offer it today, and 97 percent will offer mobile banking services by the end of 2018.

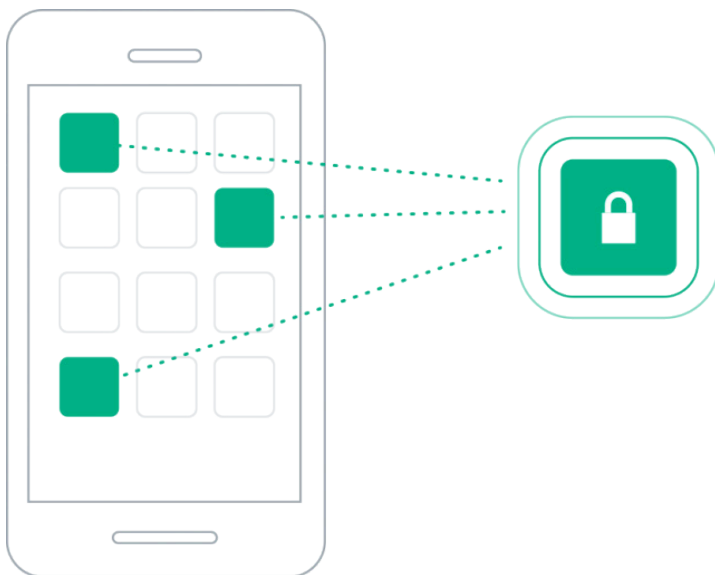
But simply offering mobile banking services does not mean people are using them. The same survey reports usage rates of 20 percent or less across 56 percent of responding institutions. Just eight percent reported usage rates over 50 percent, according to the survey³. The number one barrier is “security concerns,” cited by 70% of respondents⁴.

Security is a big concern because mobile banking apps collect key personal information and data that provide access to specific bank or payment card accounts – and to the customer’s identity. A breach can cause significant brand damage resulting in lost revenue, increased costs to address the breach and other liabilities. Customers fear the possibility of identity theft and related fallout. Many are actively reducing their exposure to risk by not using mobile banking services.

Consumers have a good reason to fear fraud due to insufficient security in mobile banking. Frequently, potential exploits in the app code are easy to expose with reverse engineering. A study of banking apps on Android™ OS found that about 60 percent did not obfuscate their source code⁵.

The resulting vulnerabilities in mobile banking apps pose a broad risk. In the first quarter of 2018, 55 percent of consumer transactions were on mobile devices and 65 percent of fraud transactions used a mobile app or browser, according to RSA. During the same period, more than 8,000 rogue mobile apps were observed by RSA⁶.

Mobile security risks are increasing everywhere, according to the Verizon Mobile Security Index 2018. About 93 percent of respondents said mobile devices present a serious and growing threat. Complacency by organizations is widespread – to which 83 percent agreed and 24 percent of those strongly agree. Respondents are especially worried about mobile threats to data and uninterrupted business operations – particularly via the Internet of Things. These disruptions were experienced last year by 27 percent of respondents⁷. Consequently, 61 percent said that their organizational spend on mobile security had increased in the past year; 10 percent said it had increased significantly.



² Federal Reserve Bank of Boston, [Mobile Banking and Payment Practices of U.S. Financial Institutions](#), Dec. 2017, p. 4.

³ Ibid., see Fig. 23: Range of Retail Customers Using Mobile Banking, p. 37.

⁴ Ibid., see Fig. 27: Most Common Barriers to Customer Adoption of Mobile Banking, p. 41.

⁵ Accenture Consulting, *Mobile Banking Applications: Security Challenges for Banks* (2017), p. 8.

⁶ RSA Fraud Report, Q1 2018, <https://www.rsa.com/content/dam/en/report-rsa-fraud-report-q1-2018.pdf>

⁷ Verizon Mobile Security Index 2018, p. 4-5, http://www.verizonenterprise.com/resources/mobile_security_index_2018_en_xg.pdf

Typical security path

For good reasons, financial services organizations comprise one of the best protected sectors against digital threats. Thanks to regulatory and industry guidance – and the experience gleaned from defending daily cyber-attacks – one might think that digital banking is on its way to achieving a perception of safety like the iconic fortified vault protecting cash and valuable assets. Based on surveys from current non-mobile users, however, the clear distrust of mobile banking security means there is more work to do. It's worthwhile to consider how mobile apps fit into the big picture of security, and why the standard path to securing mobile banking apps may provide a false sense of security.

To begin, legacy IT and network security controls are critical components vital for effective app security. This is true for on-premise and cloud hosted systems alike. In a similar manner, the broad range of potential vulnerabilities to mobile apps mirrors the complexity of all IT security. Mobile presents disparate threats, which require different technologies, solutions and processes, so there is no single “magic bullet” solution that will do it all.

With mobile app security, a multi-layer approach is required to secure the whole protocol stack. This starts with the physical and data link layers, which protect back-end and edge devices; the internet/network layer subject to IP vulnerabilities; the transport or TCP layer with its vulnerabilities; and finally, the application layers subject to vulnerabilities in HTTP and HTTPS.

App security tools and best practices

It is not uncommon for discussions about mobile banking app security to focus on a small set of externally provided safeguards (usually what a selected security vendor offers). Typical examples are device fingerprinting to ensure a mobile device is authorized for use by an authorized customer; multifactor authentication for access control to ensure the user is an authorized customer,

biometrics to ease multifactor authentication, encryption to protect sensitive data, and so forth. The idea is to build security around the app and mobile device, which in turn fit neatly into the existing IT security ecosystem. Then test the mobile app to see if security is working, and finally deploy the compiled application into the wild. The typical path for securing mobile apps includes the following tools (see Appendix for details):

- Follow Coding Best Practices
- Static App Security Testing
- Dynamic App Security Testing (DAST)
- Mobile App Security Testing (MAST)
- Interactive App Security Testing (IAST)
- Penetration App Security Testing (Pen Testing)

Issues with legacy app security measures

The tools and techniques described above (and in the Appendix) are all focused on creation of a secure mobile banking app – up to the point of compiling the code. Once shipped, visibility stops. It's impossible to know if they are truly secure and doing the job while being used by customers. And according to survey results, the state of mobile app security is not what it should be.

Legacy measures are also difficult to easily scale for a large bank. In particular, a legacy approach does not support the rapid injection of new app features for added business value. Changes to functionality in mobile banking apps occur frequently – even daily or hourly in some cases. It is very difficult if not impossible to make traditional tools scale because they must be re-applied each time changes are made to the code. Considering a large financial institution's typical portfolio of 50 to 100 customer-facing apps for mobile banking, keeping all these secure during a continuous avalanche of code changes has no realistic chance of happening with a legacy approach.



Rethinking mobile app security

Arxan offers a new approach that provides three transformational benefits for security of mobile banking apps.

- 1) Prevent reverse engineering and tampering, which could lead to breaches and app data theft, by hardening mobile apps after code is complete with a system of embedded safeguards.
- 2) Stop API compromises and theft of intellectual property or personally identifiable information with comprehensive data and key encryption using white-box cryptography.
- 3) Stay ahead of app threats and vulnerabilities with the ability for each protected app to “phone home” and provide real-time threat visibility and analytics data.

Harden mobile apps once

Arxan's approach is to add security functionality and mobile app code hardening just once, after the code is finished. It assumes “zero trust” in all devices running the app whether inside or outside of the traditional perimeter. It also assumes that coders are not security experts.

Arxan provides a spectrum of “guards,” which are code segments that provide a high level of security awareness, detection, protection, and security event data collection for analytics when an app is attacked. Once the guard network is created, follow-on protection for subsequent app releases requires minimal developer effort because of Arxan's automated re-deployment of app hardening and safeguards to each new revision of code.

Safeguards are applied once after completion of the code, and they are automatically applied with every revision. With the safeguards, all deployed apps receive continuous protection regardless of revision. Arxan's streamlined approach ensures deployment of baked-in, robust mobile banking app security for large financial institutions with multiple customer-facing apps.

FFIEC Guidelines for Banking App Security

Auditors of financial institutions look to the Federal Financial Examination Council (FFIEC) for guidance evaluating security technical controls and compliance.

The FFIEC's Information Security IT Examination Handbook, Appendix E: Mobile Financial Services addresses reduction of risk for mobile banking apps and payment systems.

Twelve technical recommendations are provided to mitigate risks.

- Policy enforcement and device fingerprinting*
- Performing security testing and secure coding practices*
- Root / jailbreak detection measures*
- Designing anti-malware capabilities into mobile apps*
- Securing back-end servers containing the mobile financial services app and customer data to prevent unauthorized users from accessing data*
- Trusted platform modules
- SSL/TLS for secure communication
- Tokenization in the context of data security*
- Authentication controls of both the user and app*

Asterisks denote where Arxan can help.

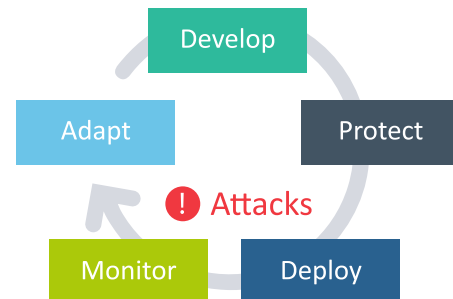
Mobile apps have many points of vulnerability that are unique and not addressed by legacy solutions. Arxan guards enable financial institutions to systematically address these many vulnerable points with technical safeguards to prevent breaches and enforce compliance. Guards offer unique advanced app security features such as:

- **Damage and repair:** Critical static data is encrypted and stored, and then replaced with a decoy version. At runtime, the guard temporarily restores the correct version for use; after which, it will optionally reinsert the decoy version to limit exposure of results in a critical range for the least amount of time possible.
- **Guard and image randomization:** Each guard can be assigned a probability of execution so that each time an attacker runs the app its behavior changes, which makes it difficult to understand and reverse engineer.
- **Multiple obfuscation modes:** A variety of obfuscation modes go beyond just renaming methods; they also perform control flow obfuscation, renaming, and reflection.

- **White-box cryptography:** A completely customized and highly secure implementation of white-box cryptography. Reverse engineering the app code is thus prevented as the crypto code is obfuscated mathematically.

Real-time visibility and analytics

In addition to enforcing security policy, guards also act like software agents by monitoring threat activity and “phoning home” with real-time threat data. Arxan Application Protection closes the loop by providing valuable intelligence into what happens to an app after it is deployed into the wild. This actionable data can be used to change the behavior of the app under attack. The data feeds into other systems, like fraud detection platforms for intelligent decision making. As a result, a financial institution gets true app security visibility via typical business intelligence and user behavior analytics platforms.






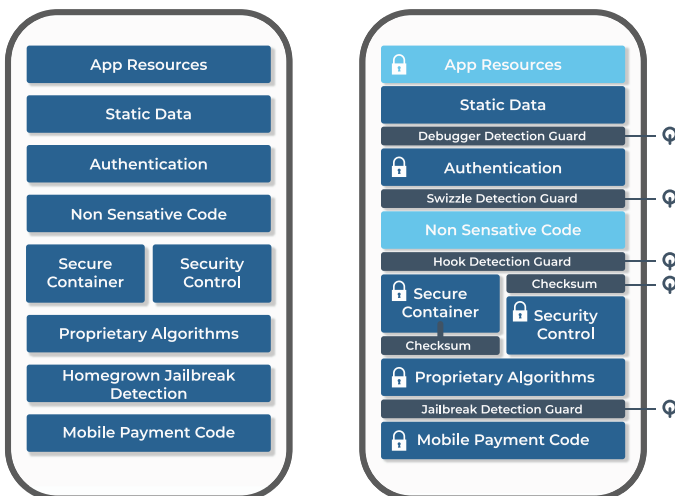
The ability to identify the most common attack vectors and targets helps developers and business stakeholders make better decisions regarding how and when to adapt their app’s security — creating a closed-loop, continuous security improvement process.

Conclusion

With the big upswing in risks for mobile banking, there is an urgent need for stronger app security. Banks and other financial institutions do not have the real-time visibility they need to continuously

Before: Unprotected App
Vulnerable to reverse-engineering, ampering, copying, and malware insertion

After: Protected, Self-Defending App
 Discrete, integrated Arxan protection
 Protected from binary attacks
 Wired for threat feedback



monitor security status of deployed apps. This data void is an enormous risk that is not being addressed by the legacy path for securing mobile banking apps. Financial institutions must harden mobile banking applications against vulnerabilities, encrypt data and keys, and ensure real-time visibility into the security posture of deployed apps. Arxan's approach supports app security requirements of the largest financial institutions. It provides broad platform support including mobile platforms, hybrid application support, desktop and server platforms. Making in-house and contract developers more efficient by providing a layer of abstraction to enable a level of security across these platforms. Our strategy is to enable once and deploy everywhere. Arxan provides security updates to software within five days of release of a new OS.

Arxan can help financial institutions meet regulatory compliance standards as well as recommendations by FFIEC. Arxan is currently the only provider of mobile app security solutions to meet standards such as ISO 13485 Medical Devices – a testament to Arxan's Quality Management; NIST FIPS 140-2: Strong Cipher Certification by the U.S. government; General Data Protection Regulation (GDPR); and various privacy requirements.

When assessing the security of mobile banking and financial applications, here are a few questions to consider:

- Is there visibility into the application's security posture in the wild?
- Is there a process to address the risk of jailbroken devices?
- Is there a process to identify high-risk users and potential app tampering?

If the answer to any of these questions is "no," then it's time for a new security approach. Arxan can help – schedule time with one of our security experts at: <https://www.arxan.com/contact>

About Arxan Technologies

Arxan, a global trusted leader providing the industry's most comprehensive application protection solutions, works with organizations looking to protect applications and to securely deploy and manage business-critical apps to the extended enterprise. Arxan currently protects more than one billion application instances across many industries including financial services, mobile payments, healthcare, automotive, gaming, and entertainment. Unlike legacy security providers that rely on perimeter-based barriers to keep bad actors out or that require device management controls, Arxan products protect at the application-level from the inside out. This approach protects the source and binary code to expand the corporate perimeter of trust. Arxan provides a broad range of patented security capabilities such as a dynamic app policy engine, code hardening, obfuscation, white-box cryptography and encryption, and threat analytics. Founded in 2001, Arxan is headquartered in North America with global offices in EMEA and APAC. For more information, please visit: www.arxan.com or follow [@Arxan](https://twitter.com/Arxan) on Twitter.

Appendix: Additional Background

App security tools and best practices

The typical path for securing mobile apps includes use of some or all the following tools:

Follow Coding Best Practices⁸ – Much of the burden of app security usually falls on coders. Their focus is functionality and speed; security is understood to be important, but often is deprioritized by business pressure to deliver better features faster. Most coders are not security experts, yet they are expected to implement lists of complex best practices.

Static App Security Testing – Coders use SAST tools that automatically examine source logic to find vulnerabilities. Examples of these errors are buffer overflows, enabling format string attacks, and integer overflows. SAST implies deep security experience of coders, for results are often noisy with too much non-prioritized data to be useful.

Dynamic App Security Testing – DAST scanning tools automatically test mobile banking apps in an operational setting. Tests disclose known vulnerabilities, such as the OWASP Top 10 and Common Vulnerability Scoring System. DAST cannot help find unknown vulnerabilities or address all use cases. Human intervention may be required to discern the best logic for testing.

Mobile App Security Testing – MAST is a partially automated scanning tool for finding vulnerabilities in non-standard configurations – the most critical being, jailbroken OSes and mobile devices. MAST is impractical because it requires many variants of the test configuration, and the process needs manual coordination.

Interactive App Security Testing – IAST uses an agent or code inside the app to enable real-time security threat data. IAST is related to Runtime App Self-Protection (RASP). IAST is useful for capturing security data in virtual apps and instances in hybrid environments and the cloud.

⁸For example, see Jaykishan Panchal, "Top 10 Mobile App Security Best Practices for Developers," <https://www.tripwire.com/state-of-security/security-awareness/top-mobile-app-security-best-practices-developers/>

Penetration App Security Testing – Pen testing is a manual or automated process to find potential app vulnerabilities. While comprehensive, pen testing also has serious issues. Manual means slow and more expensive, so pen tests are rare, typically done once a year and in conjunction with a compliance audit. Pen test results are also pegged to a snapshot of time; they do not address constant changes and potential new vulnerabilities in an agile development process.

Mobile threats prevented by Arxan Application Protection

Arxan solutions prevent exploits across a spectrum of mobile app threats. The solutions automatically block threats and centrally collect real-time data on attempted breaches. Once applied to a financial institution's final source code (and prior to compiling), Arxan protections are automatically applied to future code changes. Arxan protection ensures true app hardening, and the visibility app security teams needs to improve risk posture to emerging threats and help prevent breaches and non-compliance with:

Obfuscation Techniques – deters an attacker's ability to reverse engineer and tamper with app code by obfuscating the attacker's view of app code, its structure, and of sensitive data values

Runtime Protection – provides detection of emulation environments, and if an app is being monitored by debugging software, alerting the app and the business of pending attacks

Repair / Damage – protection that alerts the app and business of pending attacks and can repair code changes resulting from an attack; protections can also guard other protections forming an interconnected guard network

Root & Jailbreak Detection – identifies and alerts the app and business when apps are running on compromised devices

White-Box Cryptography – app level encryption of key and data in memory so plaintext cryptographic keys are never present in runtime memory.