ARXAN
guarding your IP™

Mobile App Security for the Financial Services Ecosystem

Multi-platform and Device Application Protection

android
Windows Mobile
iPhone
RIM

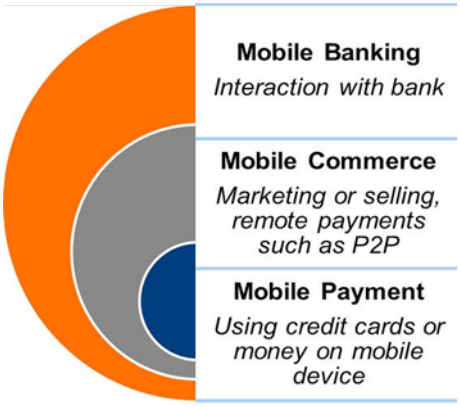
Individual banks should be able to increase their revenues and cut costs if they successfully exploit the convenience of mobile, its potential to drive digital commerce, and the opportunity it represents to target the unbanked in emerging markets.

--McKinsey and the European Financial Management and Marketing Association (EFMA) 2011

Mobile Apps are Vulnerable

Attacks against all major mobile platforms - including Android, Apple iOS, Blackberry, Windows, – are growing both in number and in sophistication. As the financial industry continues to undergo significant change from rapid mobile expansion, industry players must compete to ensure customer satisfaction and loyalty. As financial institutions and retailers differentiate by deploying new mobile services, such as mobile P2P transactions, remote deposit, balance transfers and payment, the underlying software applications that reside in or communicate with mobile devices are subject to attack.

Mobile Financial Applications Enable Services throughout the Ecosystem



Financial apps are subject to various hacker threats due to inherent vulnerabilities that can be exploited via **reverse-engineering** or **tampering** attacks. Additionally, open-source platforms, such as Android, that currently have the highest growth/adoption rates are at greater risk! Nonetheless, any jail broken mobile device can result in hackers gaining root access to mobile applications in order to **analyze security logic, insert malware, subvert authentication /access controls or steal intellectual property (algorithms or keys).**

In this new attack paradigm, the stakes are high as app developers throughout the ecosystem as threatened by a loss of control and exposed to high risk consequences; including the provider's reputation, financial loss and customer loyalty on mobile and traditional services.

Mobile Application Security is Required

Deploying anti-virus, anti-spam, device monitoring or other network and firmware oriented solutions do not provide industry players with a complete security solution. **In addition to device and data security, the financial industry must deploy complementary protection at the application layer.** Specifically, publishers of mobile applications must safeguard applications INTERNALLY with layered protections, using a variety of security techniques that are resistant to attack.

Arxan Protects Financial Services Mobile Apps Anywhere, Anytime

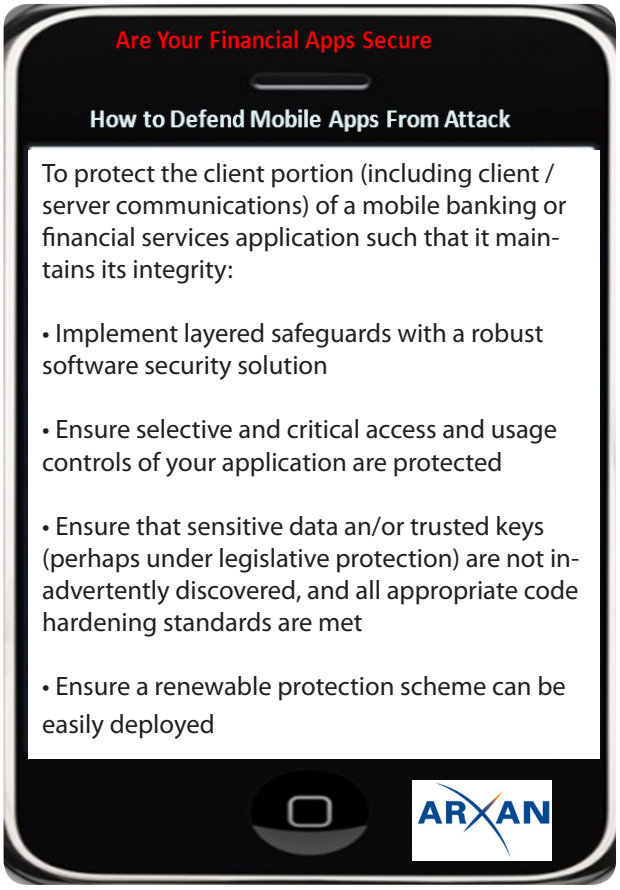
Arxan is a leading provider of software security solutions that protect applications from attack in distributed or un-trusted environments. Arxan's proven security for mobile, embedded, desktop and server environments protect financial services software against with best of breed anti-tamper and anti-reverse engineering technology.

Arxan's mobile software security solutions offers multi-layered protection which includes a variety of security technologies including static and dynamic defenses such as: **obfuscation, anti-debug, repair, self-healing and anti-tamper to ensure durability, resiliency and performance in the field.**

ARXAN
6903 Rockledge Drive, Bethesda, MD 20817 | T 301.968.4290 or 877.445.1350 | F 301.968.4291 | www.arxan.com

Among Smartphone owners the number of banking users has risen by 40 percent since August 2010. Also, in March 2011, 20 million mobile users across the five leading European markets (UK, France, Spain, Germany and Italy), … accessed their bank account via a mobile phone in March 2011.

- comScore, Inc. (LONDON, UK, 2011)



The value of Arxan's security includes:

- Cross-platform (mobile, desktop, embedded, server) security from a single reputable vendor
- Multi-programming language protection (C, C++, .NET, Java, etc.)
- Military-grade security (both static and dynamic alerting capabilities)
- Binary based (non-intrusive to the software development lifecycle)
- Proven, and highly configurable products

Example use cases for banking and finance include:

Reverse Engineering & Code Modification

1. Prevent binary/data analysis
2. Obscure program interfaces
3. Protect business logic
4. Harden password routines

Preventing Discovery of Sensitive Keys

1. Protecting encryption keys
2. Protecting hashes
3. Protecting passwords

About Arxan Technologies

Our advanced software protection solutions secure ISV, digital media providers' and enterprise applications to proactively defend the integrity of code and business models. We defend, detect, alert and react to attacks through a threat-based, customizable approach. Proven, durable and resilient, Arxan's offerings support a full range of application protection needs, from commercial software to military grade assurance. Founded in 2001, Arxan Technologies has offices in Bethesda, Md., San Francisco, and West Lafayette, Ind. For more information, please visit **www.arxan.com.**

Our Solutions

Arxan's patented defense-in-depth protection is a proven, low-impact application security solution to protect code, keys and data. Through our award winning **GuardIT®, EnsureIT™, TransformIT™ and BindIT™** products, as well as Professional Services expertise, we effectively prevent software attacks.

ARXAN

6903 Rockledge Drive, Bethesda, MD 20817 | T 301.968.4290 or 877.445.1350 | F 301.968.4291 | www.arxan.com