WHITE PAPER

The Security Flaws Leaving Financial Mobile Applications Vulnerable

Authors:
Joe Jeanjaquet, Senior Director of Applied Technologies
Aron Seader, Senior Director of Core Engineering
David Schoenberger, Chief Innovation Officer

February 10, 2021

Document ID: ECLYPSES – 1532395320 -223

Contents

Introduction

Cyber risks are hardly infrequent, but there is an alarming number of them in the world of mobile applications – especially those in the financial services sector. While many financial institutions use security solutions to protect their perimeter, a startling number do not shield their mobile apps from an attack.

According to an Intertrust report[2], 77% of financial apps have at least one serious vulnerability that could lead to a data breach. With financial mobile apps being more susceptible than ever (especially in the wake of the COVID-19 pandemic), it has become essential for firms to know what types of security flaws are out there and why it is critical to properly secure these vulnerable applications.

"77% of financial apps have at least one serious vulnerability that could lead to a data breach."
-Intertrust report

The Problem

More troubling is the fact that most of these mobile applications have more than one high-risk vulnerability that leaves their data exposed and users vulnerable to future attacks. According to Payments Journal[1], "Unfortunately, most finance-related apps we assessed failed to fully protect user security and privacy. A remarkable 263 (70%) scored a D or an F in security and privacy, meaning they contained at least two high-risk vulnerabilities that leak sensitive data or leave users vulnerable to network attacks."

What are the types of security flaws found in financial mobile applications?

- **Bugs and improperly implemented code** allow a cyber attacker access or control
- **Weak encryption and poor key management** can lead to data loss, even the best encryption algorithms can fail if not properly handled
- **Unsecured authentication tokens and API keys** allow for apps to interact with third parties with weak security
- **Insecure data storage** allows malicious users or malware to inspect data storage
- **Zero-day attacks** can allow cyber attackers access to sensitive data stored on the mobile device

According to the Aite Group[4], one of the most important elements for banking apps is encryption, yet 80% had weak or incorrect implementation.

Mobile application vulnerabilities can cause substantial problems for financial institutions, such as data exposure. This is because financial mobile apps store and process personal data, such as bank credentials, personal identification information, credit card numbers, and other valuable data. This data exposure can lead to cyber criminals stealing funds, confidential information, identity fraud, and access to financial institution networks.

> "One of the most important elements for banking apps is encryption, yet 80% had weak or incorrect implementation."
> -Aite Group

Check Point Research[3] reported one of the largest mobile breach reports of 2021, which disclosed 13 popular Android apps that exposed the data of as many as 100 million users. These mobile app developers failed to secure third-party cloud services, which exposed personal data including emails, chat messages, passwords, and photos. While these cyber criminals are stealing from financial organizations and their clients, the financial organization's reputation is also suffering, there is a loss in customer confidence, and a strong possibility of facing regulatory fines and damage payments.

What Can Financial Institutions Do to Improve Mobile App Security?

To ensure that their financial mobile apps are as secure as possible, it is best to deploy a security solution that protects valuable data at the application level.

Mobile app developers should take a proactive approach and add Eclypses MTE technology as a foundational part of security design, as using it protects data the moment it is created. MTE technology replaces data with instantly obsolete random streams of values and restores it on the other side. By securing at the application level, MTE technology:

- Verifies each endpoint connection
- Requires no change to the user experience
- Minimal impact on system resources
- Secures data inside the application
- Allows you to stop trusting the operating system and communication protocol

Conclusion

With more transactions and exchanges happening on mobile applications than ever before, cyber attacks are inevitable and will continue to increase. Mobile app developers and organizations need to take a step back and make application-level security a priority.

“Financial apps need to take responsibility for the security of data within their mobile applications and stop relying on the operating system and communication protocol to take care of it for them. Data needs to be secured by the application so only that application and the server it communicates with have access to the data, eliminating the need to trust things they don’t control,” comments Aron Seader, Senior Director of Core Engineering at Eclypses.

For a free consultation on your financial mobile application security, email contact@eclypses.com.

Sources

Reed, B. (2021, October 11). *Many Finance Mobile Apps Fail to Protect Data.* Payments Journal. Retrieved January 10, 2022, from https://www.paymentsjournal.com/many-finance-mobile-apps-fail-to-protect-data/

Security, H. N. (2021, June 7). *Most mobile finance apps vulnerable to data breaches.* Help Net Security. Retrieved January 27, 2022, from https://www.helpnetsecurity.com/2021/06/09/mobile-finance-apps/

Sharma, M. (2021, May 20). *Android apps put data of 100 million Google Play Store users at risk.* TechRadar. Retrieved January 27, 2022, from https://www.techradar.com/uk/news/android-apps-put-data-of-100-million-google-play-store-users-at-risk

The Vulnerability Epidemic in Financial Services Mobile Apps. (n.d.). Https://Info.Digital.Ai/Aite-Research-Financial-Mobile-Apps.Html. Retrieved January 27, 2022, from https://info.digital.ai/aite-research-financial-mobile-apps.html

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

contact@eclypses.com
www.eclypses.com
(719) 323-6680