verimatrix™

Protecting Financial Services Mobile Apps

App Guardian: How XTD Safeguards Financial Service Providers' Mobile Security

Introduction

In the digital age, our interactions with financial institutions, merchants, and governments have changed significantly. Mobile phones have become the preferred way to access digital services, and we now have millions of unmanaged devices connecting to enterprise systems. The challenge for Chief Security Officers (CSOs) and Chief Information Officers (CIOs) is to ensure the security of their systems and apps, and to provide access to core services.

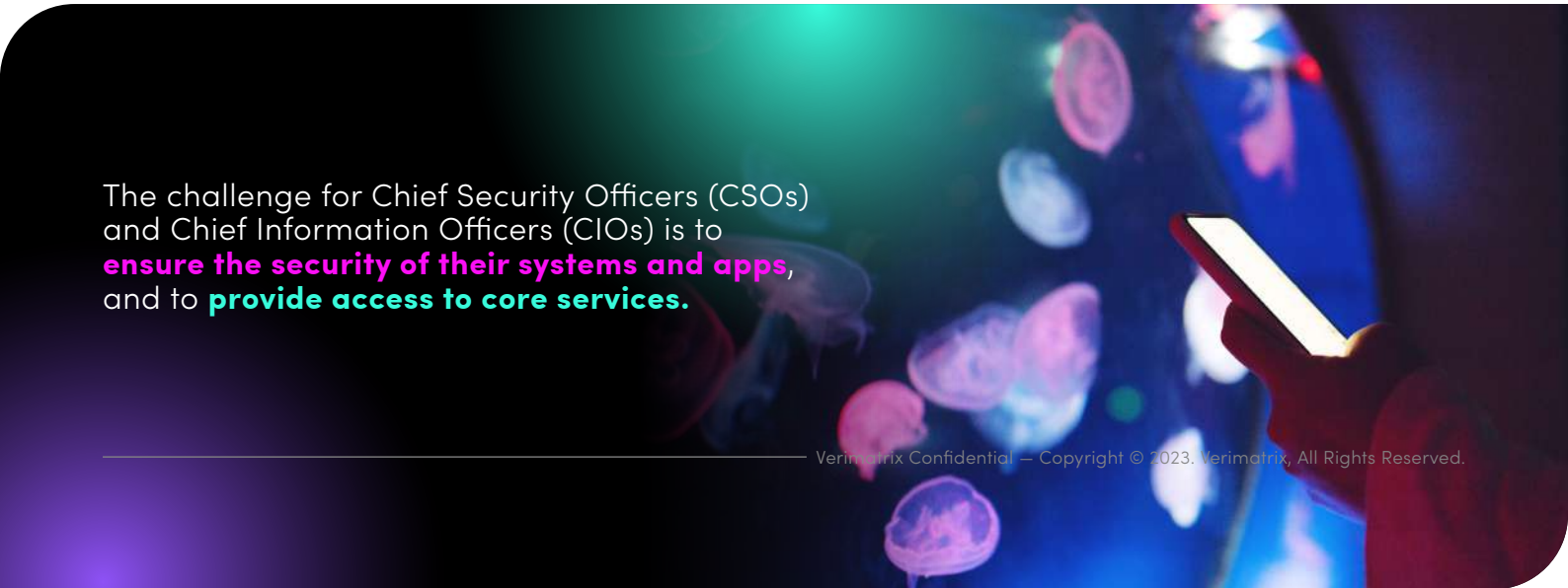
This paper will examine the mobile app security landscape, how threats are evolving, and how in-app security is essential in the face of these threats. But before delving into the intricacies of mobile app security, it is important to understand the evolution of the consumer.

Mobile Tribes

Historically, humans lived in tribes with constant and instant communication with everyone they knew and trusted. But as society became more connected, this link with our immediate "tribe" broke down, and our friends and family spread around the globe. The mobile phone, however, has put us back into constant and instant communication with our tribe.

Gen Z and millennials are becoming an increasingly important group for merchants and financial institutions to attract, but they are notoriously less loyal than previous generations, and they are mobile-first. They use their mobiles to communicate with their tribes, plan their shopping, manage their data, finances, and make their payments.

In order to address this move to a mobile-first world, Financial Service Providers and merchants are developing and deploying mobile apps to engage this new breed of consumer. However, providing access to backend systems through apps and capturing sensitive data requires a trusted mobile experience. For Gen Z and millennials, loyalty will be based on brands inserting themselves into their mobile tribes.

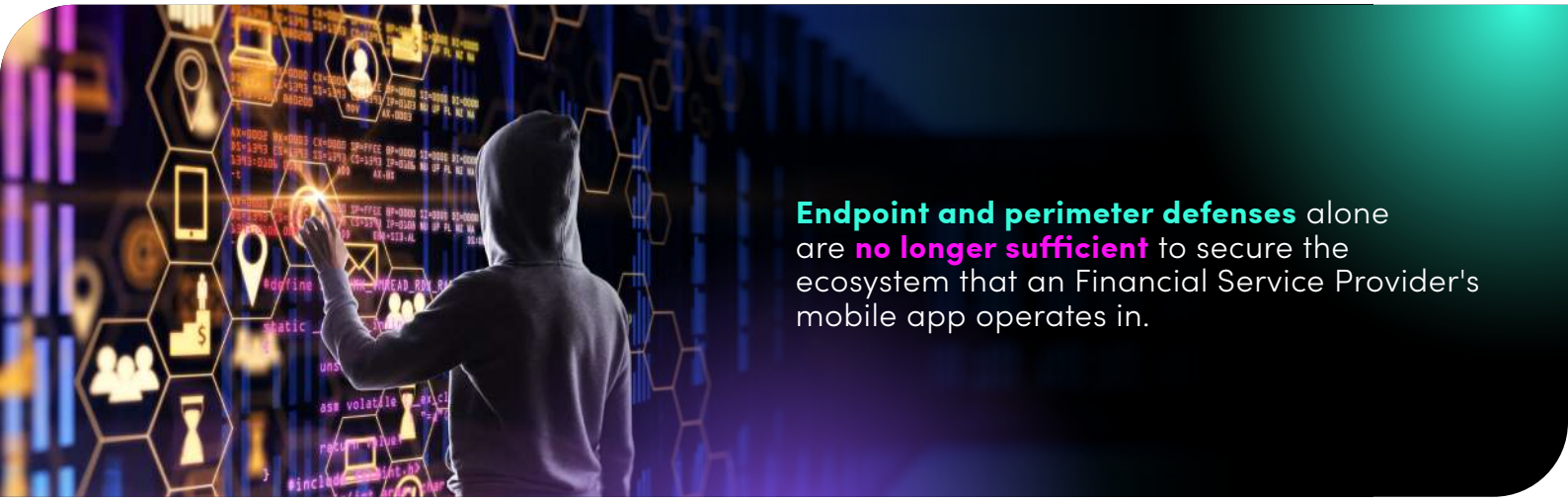


The challenge for Chief Security Officers (CSOs) and Chief Information Officers (CIOs) is to **ensure the security of their systems and apps**, and to **provide access to core services.**

The Extended Threat Surface

This shift to mobile and app-based service provision presents quite a challenge to Financial Service Providers. Traditional "bank-grade" security was akin to building a castle, with secure walls, drawbridges, and secure points of entry, with sentries and defenses against known attackers. Like these castles, data processing centers were secure buildings with cameras, restricted access, security guards, firewalls, and APIs to admit good traffic and block bad traffic.

However, endpoint and perimeter defenses alone are no longer sufficient to secure the ecosystem that a Financial Service Provider's mobile app operates in. The option for enterprise IT departments to lock down enterprise mobiles with agents to control their contents and use is not viable for consumer mobiles. A consumer's mobile device can't be locked down and is, in effect, an unmanaged device. Financial Services Providers must find another way of securely providing their services. Protecting APIs is not enough; it leaves Financial Service Providers blind to the mobile device.



Endpoint and perimeter defenses alone are **no longer sufficient** to secure the ecosystem that an Financial Service Provider's mobile app operates in.

The Pseudo-managed Conundrum

The mobile device brings enormous benefits in providing people access to financial services, but it also extends the threat surface. This environment and the threats need to be understood, managed, and controlled to provide a secure trusted service. A Financial Services Institution must adopt a risk-based approach to security and move from a world of trust to one where they "never trust, always verify."

There are challenges in securing mobile apps. The level of security and controls required in an app will vary depending on the services that the app provides and the data it uses. While some mobile devices provide hardware-backed security, such as a Trusted Execution Environment (TEE), these are not ubiquitous, and app developers need to build appropriate security defenses for the lowest device and operating system their apps will be deployed on.

Financial Service Providers are grappling with a conundrum: how to ensure that their mobile apps offer the same level of security as their managed devices, even though consumers' mobile devices are unmanaged. This means that Financial Services Institutions must build "pseudo-managed" control points directly into their apps in order to provide the necessary level of assurance.

Think Like Hackers to Build Better Security

But how can they design in this crucial security? First things first: Financial Service Providers must gain a deep understanding of the threats and vulnerabilities that are inherent in the ecosystem their app will operate in. Armed with this knowledge, they can then identify which control points and countermeasures are necessary to truly secure their service. In other words, to achieve true security, Financial Services Institutions must think like hackers, anticipate their moves, and build in the necessary safeguards to prevent them from succeeding. It's not an easy task, but it's essential in today's digital age.

Mobile applications are vital as they store and transmit sensitive data. To ensure that external actors cannot access and misuse this data, developers must protect it. However, various actors have different motivations for compromising an app's security. Children may do it for fun, while academics may do it to research mobile security and improve data protection. On the other hand, criminals may do it for small or large-scale gains. To prevent security breaches, developers need to understand the attackers' techniques and build appropriate security architectures.

Mobile app security vulnerabilities have remained constant over time, with many weaknesses listed in the Open Web App Security Project's (OWASP) top 10 critical security concerns for both web and mobile apps. The OWASP produces a Mobile Application Security Verification Standard that outlines the controls and countermeasures necessary for building secure mobile apps.

Benefits of Layered Cybersecurity

Securing against threats requires a layered approach to security. Developers need to design the app with a "trust nothing, verify everything" approach to ensure the security of app data. They must consider the appropriate use and protection of encryption keys, secure cryptography functions, and whitebox/SE/TEE when persistent storage of sensitive data is required. Mobile apps rely on their host environment, which is unmanaged and untrusted, and this should be taken into account when designing their security. The app must include sufficient control points to allow informed decisions about whether to allow or not allow traffic from the mobile app.

Adding security to an existing app is difficult, and some countermeasures such as code obfuscation can be applied as a security wrapper, but this is only one layer of protection. Data encryption and secure comms are complex, and only by designing security with a holistic view can a Financial Service Provider build appropriate defenses. App lifecycles and a Financial Service Provider's back-end system play a critical role in assessing and enforcing security. As threats evolve, so must the app defenses.

To provide access to its services, a Financial Services Institution must ensure that the device and app are secure and operating as intended. The app designers must ensure that the app is running in a trustworthy environment, that the mobile has not been subject to jailbreaking/rooting, or running in emulation, and that zero-code injection or hooking is present. The app must contain tamper detection and countermeasures, and it also needs external monitoring to extend the threat defense.

Seek Out Cyber Expertise

Expertise in security systems and mobile app security technologies may or may not be wholly within a Financial Service Provider's core competencies. Fortunately, the software security industry can provide tools and services to help Financial Services Institutions develop and maintain secure apps and services. Software security companies monitor threats and develop best practices, tools, and services to counter known threats as the threat landscape evolves. They can provide expertise in design, packaged countermeasures, attestation services, and PEN testing.

A Financial Service Provider must decide whether to engage with these companies and to what level, depending on in-house expertise and capabilities and the amount of control a Financial Service Provider wishes to have. An important part of this decision is whether to source technology tools or engage with an enterprise-grade cybersecurity solution for protecting mobiles and mobile apps. Once a Financial Services Institution determines the appropriate level of security for its services, it can then decide the level to which it builds or buys the defense tools to reduce its risk to an acceptable level. The key is designing with a holistic view, considering threats as they evolve and building appropriate defenses.

In today's world, security is of utmost importance, especially in the financial industry where a breach in security can result in disastrous consequences. In order to prevent such incidents, Financial Services Providers need to be proactive and have a well-planned and adaptive security architecture in place. This involves understanding potential attacks and the required security baseline to predict and prevent future attacks by deploying appropriate countermeasures.

Focus on Holistic Security Solutions

The security architecture must be designed to produce secure apps and systems that are properly hardened to prevent both known and theoretical attacks. Monitoring the perimeters of these systems and apps is crucial to detect and contain any incidents that occur, and responding with appropriate measures and changes in the security design.

The continual monitoring and analysis of security threats form the core of a virtuous cycle of security, with attestation and analysis being key components. By constantly analyzing the security threats and feed the app development lifecycle, Financial Services Providers can produce updates in the app design, device monitoring, and attestation systems alongside their feature set.

In order to achieve this, Financial Services Providers need to adopt a holistic approach to security. The mobile app should not be seen in isolation but as part of the Financial Service Provider's system. System security design should include the mobile, turning it from an unmanaged and untrusted high-threat environment into a pseudo-managed first line of defense in a layered approach to security.

The Dawn of Extended Threat Defense

Securing mobile apps is complex and evolving, and requires a well-planned and adaptive approach. Building in-house capabilities is advantageous, but it is necessary to have external expertise to maintain a secure service that is constantly evolving and updating. The Adaptive Security model developed by Gartner emphasizes the need for an enterprise threat detection and prevention approach that extends out to mobile apps. This goes beyond traditional Mobile Runtime App Self Protection (RASP) technologies and is a new category of cybersecurity that the leaders in this space are only starting to explore – Extended Threat Defense.

Extended threat defense platforms prevent, detect, respond and predict cyberthreats and fraud signals for Android and iOS apps, keeping Financial Service Providers safe from zero day attacks.

Released in early 2022, Verimatrix XTD (Extended Threat Defense) is the mobile industry's first extended threat defense platform that deploys agentless, zero-code app protection and telemetry which transforms any unmanaged device into a pseudo-managed device, allowing customers to effortlessly protect the valuable connections between a Financial Services Institution and its customers.

Verimatrix XTD (Extended Threat Defense) is the mobile industry's first extended threat defense platform that **deploys agentless, zero code app protection and telemetry** which transforms any unmanaged device into a pseudo-managed device

Adhere to Secure Standards and Best Practices

To achieve a secure mobile app environment, Financial Services Providers need to also focus on the four key areas: design, development, testing, and release. Understanding the threat landscape ensures that app security design is updated to include appropriate countermeasures against potential attacks. Use of secure coding standards and security best practices ensures that countermeasures are added appropriately to the app. Testing is used to validate the correct implementation and detect defects, while appropriate PEN Testing is essential to ensure that the security environment has been properly designed and implemented. Monitoring the use of the app and looking for patterns of attacks after release helps feed the assessment of security threats for the next cycle.

Conclusion

In the digital age, the challenge for Chief Security Officers and Chief Information Officers is to provide access to core services while ensuring the security of their systems and apps. As mobile phones have become the preferred way to access digital services, and millions of unmanaged devices connect to enterprise systems, the need for effective mobile app security has never been greater.

In this cybersecurity white paper, we've examined the evolving mobile app security landscape and the importance of in-app security measures in the face of emerging threats. We've seen that securing mobile apps is a complex and ongoing process, requiring a proactive and adaptive approach that goes beyond traditional Mobile Runtime App Self Protection technologies. To truly secure our digital systems and apps, we must think like hackers and build better security, leveraging external expertise and extending threat defense out to mobile apps. By doing so, we can stay one step ahead of cybercriminals and protect the integrity of our digital lives.

Acknowledgements

This white paper is based on the 2022 paper, "The Value of Designed In Security," a collaboration between Consult Hyperion and Verimatrix.

consult hyperion
securing tomorrow's transactions

Consult Hyperion is an independent strategic advisory and technical consultancy, based in the UK and US, specialising in secure electronic transactions in the areas of Payments, Identity and Future Mobility. With over 30 years' experience, we help organisations across the globe exploit opportunities presented by new technologies, regulatory changes and consumer expectations. We design systems that support mass scale secure electronic payments, fare collection and identity transaction services. We deliver value to our clients by supporting them in delivering on their strategy through digital innovation and unblocking technical challenges. Hyperlab, our inhouse software development and testing team, rapidly prototypes new concepts, delivers security critical software for mass deployment, and thoroughly tests the functionality and security of third-party products on behalf of clients.

For more information contact pressoffice@chyp.com

verimatrix

For 28 years, Verimatrix (Euronext Paris: VMX) has empowered a connected world with people-centered cybersecurity, video protection and anti-piracy solutions. The world's leading brands turn to Verimatrix to predict, prevent, detect and defend their mobile apps, APIs, content and devices from cyberthreats and piracy. From streaming media and banking, to e-commerce and healthcare, gaming and automotive -- we safeguard the valuable connections between companies and their customers. Verimatrix helps partners get to market faster, scale with ease, and protect valuable assets and revenue streams.

To learn more visit VerimatrixCybersecurity.com