The value of designed in security

October 2022

In partnership with
Verimatrix

verimatrix

consult hyperion
securing tomorrow's transactions

The value of designed in security

Introduction

The way we interact with financial institutions, merchants, entertainment, government, etc has changed dramatically over time.

Today's marketplace is increasingly digital, and the mobile phone is now the preferred way to access the digital services on offer.

In the past, access to financial systems was limited to trained and vetted staff, through firewalls from security hardened devices. In the digital age, that access is now via mobile apps and APIs, operating on insecure and complex devices. From an IT perspective, we now have millions of unmanaged devices connecting to our enterprise.

The question CSO's & CIO's now need to ask is are their systems secure? How do they secure the systems and apps they deploy in order to provide access to their core services?

This paper examines the mobile app security landscape, how the threats are evolving, and how designed in security is essential in the face of these threats.

Evolution of the consumer

Historically humans have lived in our "tribes" with everyone we know and trust within constant and instant communication. As society has become "more connected", we've broken down the link with our immediate "tribe", friends and family are now spread around the global. Psychologists believe that one of the appeals of mobile is that it puts us back into constant and instant communication with our tribe.

Today Gen Z and millennials are becoming an increasingly important group for merchants and Financial Institutions (FIs) to attract, but they are notoriously less loyal than previous generations and they are mobile first. They use their mobile 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, FIs and merchants are developing and deploying mobile apps to engage the new breed of consumer. It is essential to the operation of these apps to have access to backend systems through apps and to capture sensitive data.

For Gen Z and millennials will loyalty be based on brands inserting themselves into their mobile tribes? If so, they don't just need to offer a good mobile experience, they need to offer a trusted one.

For the consumer, the mobile is becoming the primary means to access commerce and financial services

Evolution of security

This shift to mobile and app based service provision represents quite a challenge to FIs.

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 centres were secure buildings with cameras, restricted access, security guards, firewalls and APIs to allow good traffic through and block bad traffic.

However perimeter defenses alone are no longer sufficient to secure the ecosystem that an FI'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, in effect it is an unmanaged device, FI's must find another way of securely providing their services. Protecting APIs is not enough, it leaves FIs blind to the mobile device.

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 in order to provide a secure trusted service.

An FI must adopt a risk based approach to security, move from a world of trust to one where they "don't trust, always verify".

Today's extended threat surfaces require a different approach to security

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 data it uses.

Whilst some mobile devices provide hardware backed security, such as a 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.

FIs face the challenge of ensuring their apps deploy a sufficient set of controls such that an unmanaged device exhibits similar security characteristics of a managed device, in effect the device becomes pseudo-managed through control points built into the app.

In order to design in the security required to provide a sufficient level of assurance, an FI must understand the threats and vulnerabilities of the ecosystem their app will operate in.

With the threats and vulnerabilities understood, the FI can then determine which control points and countermeasures are required to secure their service.

Defining device Security:	
Managed	Personal computers, laptops, mobile devices, virtual machines, and infrastructure components with agents that allow information technology staff to discover, maintain, and control them.*
Unmanaged	A consumer, employee or enterprise owned device onto which it is not possible to install a security agent.
Pseudo-managed	Using the service provider’s app as the control point to bring Managed Device like controls to Unmanaged devices.

*https://csrc.nist.gov/glossary/term/managed_devices

Understanding the threats

A mobile app processes, stores and transmits sensitive data, this data must be protected such that external actors cannot access and misuse it.

There are various actors who could look to compromise an app's security, or lack of, with differing motivations for doing so:

- Kids for kicks, or kudos, with their peers
- Academics who research mobile security with a goal of improving data protection and security
- Criminals
  - Small scale, seeking moderate gains
  - Industrial scale, capable of exploiting weaknesses on a significant scale

By understanding how these actors operate we can begin to see the whole picture and gain knowledge of the threat surface. With this understanding of how the attackers operate, developers can build the security architectures within which they can apply appropriate countermeasures to ensure their apps are secure.

There are many techniques used by attackers to exploit security weaknesses in mobile apps, including:

- Running the app on a rooted device or an emulator
- Tampering with the app to modify it's behaviour
- Cloning the app
- Snooping the communications to / from the app

The techniques employed are continually evolving, constantly changing the threat surface.

Methods of mobile app attack

- **Tampering / Reverse Engineering**
- **Malware Captures Credentials / Assets**
- **Cloning**
- **Snooping**
- **Identity Theft**

Understanding the security vulnerabilities

There are many blogs and web sites dedicated to mobile app security. The Open Web App Security Project (OWASP*) is a non-profit foundation that works to improve the security of software by providing education, training, tools and resources to help developers.

The OWASP periodically produces a list of the Top 10 critical security concerns for both web and mobile apps. Over time the names can change and categories merge, but despite being known as weaknesses for several years, many of the vulnerabilities remain in the top 10.

These vulnerabilities highlight the need for designed in security and are on the checklist of many PEN test teams as obvious / known sources of security vulnerability.

The OWASP also produce a Mobile Application Security Verification Standard, which provides a good starting point for developers looking to understand the controls and countermeasures they need to build into their mobile apps.

Web App Security Risks 2021	
Broken access control	Vulnerable components
Sensitive Data Exposure	Broken Authentication
Injection	Software and Data Integrity Failures
Insecure design	Security logging and monitoring failures
Security misconfiguration	Server side request failures

Vulnerabilities such as Insecure Data Storage, Communication, Cryptography, Code Quality are all symptoms of a lack of designed in security

Web App Security Risks 2021	
Broken access control	Vulnerable components
Sensitive Data Exposure	Broken Authentication
Injection	Software and Data Integrity Failures
Insecure design	Security logging and monitoring failures
Security misconfiguration	Server side request failures

*https://owasp.org/

** https://owasp.org/www-project-top-ten/ *https://owasp.org/www-project-mobile-top-10/2016-risks/*

Securing against the threats

The complexity of the threats to mobile apps requires a layered approach to security. A core design approach of “trust nothing, verify everything” is essential to ensure security of app data.

Where persistent storage of “secure or sensitive” data is required, the security design will need to consider the appropriate use and protection of:

- Encryption keys
- Secure cryptography functions
- Use of Whitebox / SE / TEE

Securing against the threats

Mobile apps rely on their host environment. The mobile devices are unmanaged and untrusted, FIs need to take this into account when designing their security and turn the app itself into their security agent on the device, with sufficient control points to allow the system to make informed decisions as to when to allow and not allow traffic from the mobile app.

Adding security to an existing app is difficult. Some countermeasures such as code obfuscation can be applied as a security wrapper, but this is only one layer of the protections needed. Adding data encryption and secure comms is complex. Only by designing in security with a holistic view can an FI hope to build appropriate defenses.

App lifecycles and an FI’s back end system plays a critical role in assessing and enforcing the security. As the threats evolve so to must the app defenses.

Security Countermeasures

- Secure Design
- PEN Testing
- TEE / Whitebox
- Data encryption / Code obfuscation
- Certificate Pinning
- Device Fingerprinting
- Attestation
- Anti-tamper
- Multi Factor Authentication

Trusting an untrusted device

In order to provide access to it's services, an FI needs to ensure that the device and app are secure and operating as intended. The app designers need to ensure:

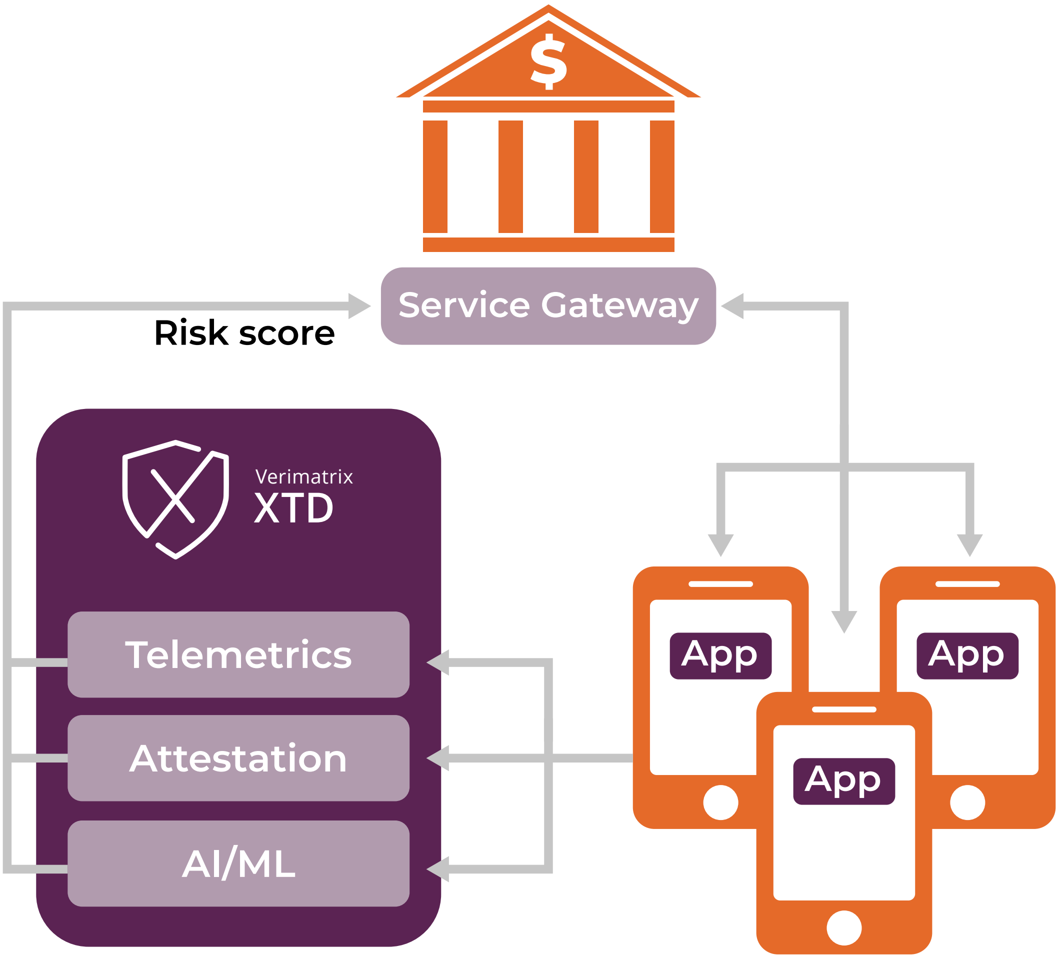
- the app is running in a trustworthy environment
- the mobile has not been subject to jailbreaking / rooting, or running in emulation
- the app is as distributed, no code injection or hooking is present

Whilst the app itself will contain tamper detection and countermeasures, it also needs external monitoring to extend the threat defense.

Data feeds to attestation and telemetric service enhance the threat defense.

Whilst isolated analysis of individual data points can be part of the solution, a more complete system considers how those data points combine together to reveal a story about the threat landscape of each individual app and device in an installed base. This allows a more accurate analysis and more attacks can be detected, meaning more risks mitigated and less false-positives, i.e. end-users denied access to the service unnecessarily.

The FI's service gateway takes input from the attestation and telemetrics service to determine if access to its services is to be allowed. There are no absolutes here, consideration is given to degrees of security and levels of acceptable risk.



Where to source expertise

Expertise in security systems and mobile app security technologies may or may not be wholly within an FI's core competencies. Fortunately there is a whole software security industry who can provide tools and services to help FIs develop and maintain secure apps and services.

The players in the software security industry are constantly monitoring the threats and techniques which are used to attack mobile apps and platforms. They develop best practices, tools and services to counter known threats and evolve as the threat landscape evolves.

Software security companies can provide expertise in design; packaged countermeasures; attestation services; PEN testing. An FI needs to determine to whether to engage with these companies and to which level. This will depend on the in-house expertise and capabilities and to the amount of control an FI wishes to have.

An important part of this decision is whether to source technology "tools" or whether to engage with an enterprise-grade cybersecurity solution for protecting mobiles and mobile apps.

Once an FI has determined the appropriate level of security for its services, which may be in the form of regulatory requirements, consumer demand or corporate mindset, 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 in the appropriate level of security.

The defenses and tools used require regular review, as fraudster capabilities and target markets evolve the threats evolve and move across verticals.

Enterprise-grade security:

- **Proven to identify and mitigate threats.**
- **Technology backed-up by human expertise.**
- **Proved by a mature and stable company.**
- **Delivered to ISO audited processes.**

Coping with an evolving threat landscape

Designed in security produces solutions suitable for a point in time, however FIs need to be cognisant that the threat landscape will continue to evolve once their app has been deployed.

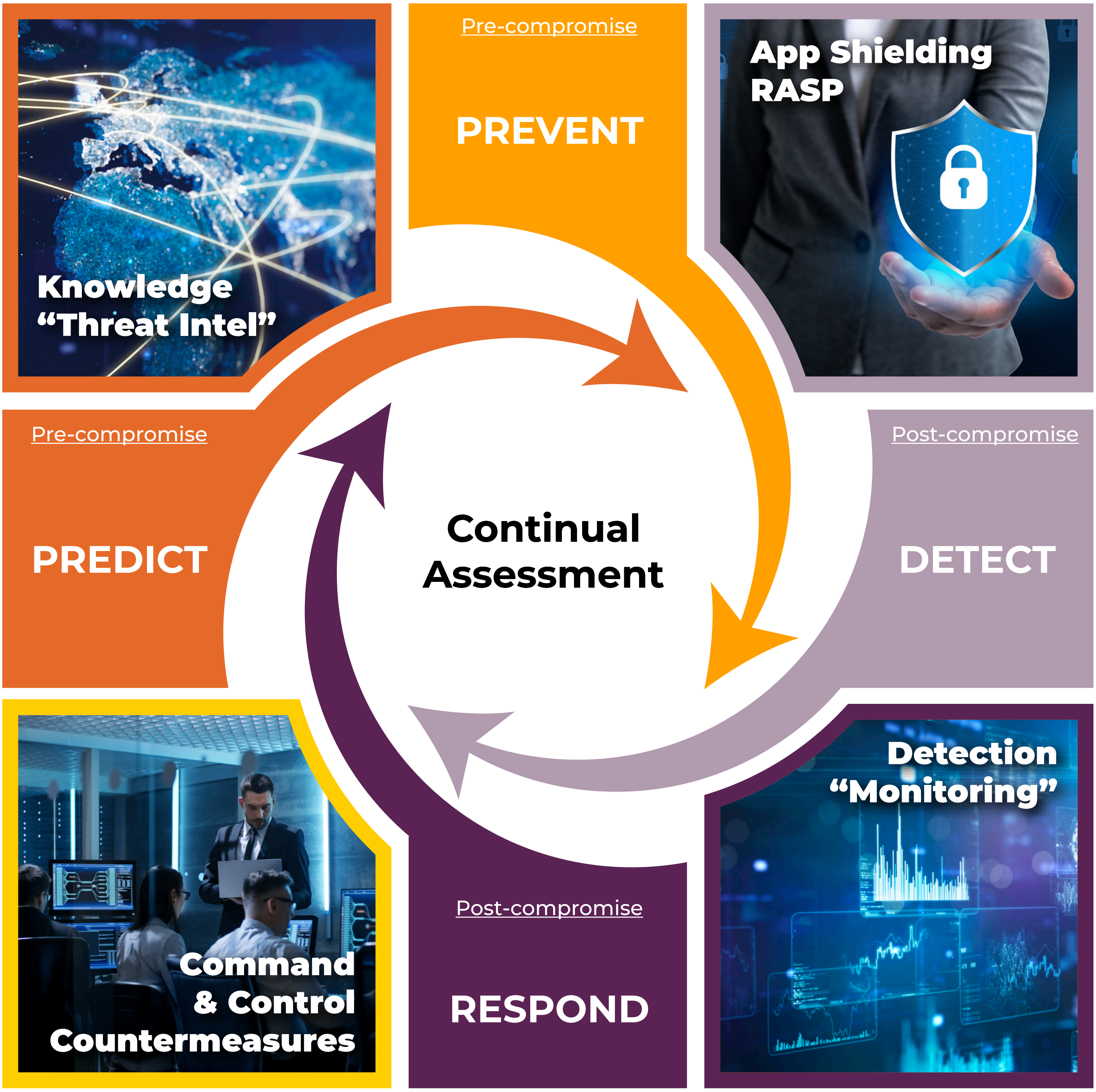
The best place to be when an attack occurs is somewhere else. By adopting best practice mobile app security, continually evolving their security, an FI can prevent compromise rather than react and respond to compromise.

The Gartner Adaptive Security Architecture provides a basis for developing an evolving security architecture. Just as physical security assess the threats and builds fences against the known threats, deploys monitoring equipment to detect and react to any compromise, whilst assessing future threats and upgrading physical security and monitoring in a constant cycle, so to must an FI approach it's digital security.

Continual Assessment

Applying an Adaptive Security Architecture, understanding the potential attacks and the security baseline required, enables FIs to predict future attacks and deploy the appropriate countermeasures required to prevent them. Producing secure apps and systems that are adequately hardened to prevent known and theoretical attacks. These apps and systems monitor their perimeters in order to detect and contain incidents, responding with appropriate measures, changes in the security design, protection mechanisms deployed.

This results in a virtuous cycle of security, with continual monitoring, attestation and analysis at its core.



Application security lifecycle

The continual analysis of security threats feeds the app development lifecycle, producing updates in the app design, device monitoring and attestation systems alongside the FIs feature set.

Design

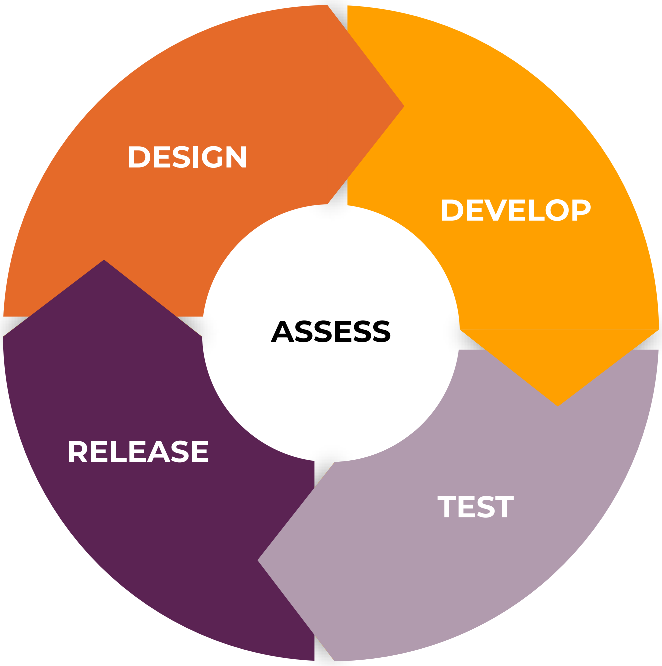
Understanding the threat landscape ensure the app security design is updated to include appropriate countermeasures are deployed against the threats.

Develop

Use of secure coding standards, and security best practice ensure the countermeasures are added appropriately to the app.

Test

Testing is used to validate the correct implementation, and detect defects, whilst appropriate PEN Testing is essential to ensure that the security environment has been properly designed and implemented. Black box PEN testing is not sufficient, the PEN test needs to go under the hood to ensure the app is secure.



Release

Once the app has been released, monitoring its use, looking for patterns of attacks, which helps feed the assessment of the security threats for the next cycle.

Conclusion

The complex threat environment that mobile apps are deployed in require a holistic approach to security. The app should not be seen in isolation, but as part of the FI's system.

System security design needs to 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.

Securing mobile apps is complex and evolving, there are advantages of building in house capabilities, but the levels of expertise available externally should indicate that a degree of bought in expertise is necessary to maintain a secure service which constantly evolves and updates.

Gartner's Adaptive Security model tells us that to truly secure an unmanaged device and the apps running on it, we need to take an enterprise threat detection and prevention approach that extends out to the mobile app. This goes beyond traditional Mobile Runtime App Self Protection (RASP) technologies and is a new category of cyber security that the leaders in this space are only just starting to look at.

consult hyperion
securing tomorrow's transactions

About Consult Hyperion

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™

About Verimatrix

Verimatrix (Euronext Paris: VMX) creates security solutions for the most vulnerable and unprotected aspects of our digital world. Our enterprise threat defense and anti- piracy solutions secure content, apps, and devices with intuitive, people-centred and frictionless security across a diverse range of global industries from streaming media, broadcast and sports, to automotive, financial services and healthcare. Verimatrix enables the trusted connections our customers depend on to deliver safe, compelling experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

To learn more visit www.verimatrix.com