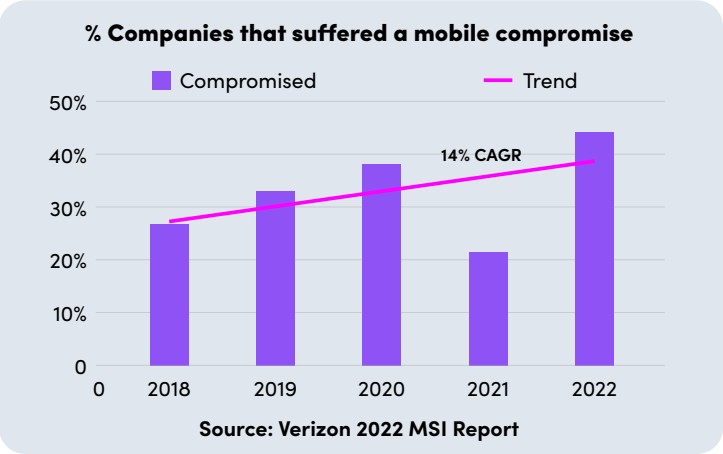
verimatrix
cybersecurity

OWASP Mobile Top 10:

The developer's guide to securing,
detecting & responding to threats to mobile apps

Introduction

There are somewhere around 7 billion mobile devices in use. Most of these devices are connected to the internet and run multiple applications. That number will likely keep increasing, and the risk of mobile cyberattacks will grow right along with it. Threats to mobile devices (and the apps that power them) are accelerating. In fact, according to Verizon's Mobile Security Index, the number of companies experiencing a mobile compromise grew at a 14% CAGR from 2018 to 2022[1].



The Open Worldwide Application Security Project (OWASP) is working to protect the apps on which we all now depend. OWASP is a not-for-profit foundation that aims to strengthen application software security by engaging security professionals worldwide to develop, improve, and maintain safer software. A de facto industry standard, OWASP provides well-thought and well-vetted guidance for developers, including those designing and building mobile apps.

Helping developers understand the potential risks to mobile apps makes it easier for them to avoid pitfalls and protect users and data. To that end, the OWASP Mobile Security Project defines a model and lists requirements for the qualities of secure mobile apps.

The OWASP Mobile Top 10 describes the highest security vulnerabilities mobile applications face. Because the use of and threats to mobile apps keep dramatically changing, in 2023, OWASP updated its previous 2016 Top 10 list to reflect the most current risks and pressing concerns for app developers to address.

Verimatrix XTD (Extended Threat Defense): #1 In Mobile App Security

Verimatrix is a French public company and a proud OWASP member. Our award-winning app security is trusted by leading brands worldwide. When it comes to mobile app defense for iOS, Android, embedded/desktop, and web applications, Verimatrix XTD does it all. Unlike some security vendors, who only offer one-off solutions, Verimatrix provides a wide family of products that include app shielding, runtime application self-protection (RASP), cryptographic key solutions, and multi-layered in-app protection solutions to provide all-encompassing cybersecurity for mobile apps. This includes advanced threat detection and response techniques only available from Verimatrix.

Verimatrix XTD's comprehensive security umbrella will protect against a wide range of cyber threats, helping CISOs, SOC teams, application engineers, and mobile app developers predict, prevent, detect, and respond to cyberattacks from mobile threats coming from apps running on unmanaged devices.

Let's explore the Mobile Top 10 and how Verimatrix XTD can help you address OWASP's most up-to-date list of mobile app vulnerabilities.

[1] *Verizon Mobile Security Index 2022 (verizon.com)*

How Verimatrix Addresses the OWASP Mobile Top 10

OWASP Mobile Top 10 Vulnerability	Verimatrix XTD Capabilities
M1: Improper Credential Usage	Verimatrix Overlay Detector™ identifies and prevents unauthorized screen overlays that can capture sensitive user inputs like credentials, ensuring that they are only used in the intended, secure context of the app.
M2: Inadequate Supply Chain Security	Verimatrix Supply Chain Defender™ monitors app instances for backdoors, whitelists outgoing connections to detect and prevent unauthorized communications, and helps mitigate API risks in compromised mobile applications.
M3: Insecure Authentication/Authorization	Verimatrix Man-in-the-Middle Interceptor™ to detect attacks on certificate pinning.
M4: Insufficient Input/Output Validation	Verimatrix Anti-Tampering™ uses thousands of micro-checks within your app's code to prevent unauthorized mods and allows customizable security settings to address Insufficient I/O Validation by ensuring the app operates as designed.
M5: Insecure Communication	Verimatrix Man-in-the-Middle Interceptor™ detects and prevents man-in-the-middle attacks, where an attacker intercepts and potentially modifies communication between a mobile app and server.
M6: Inadequate Privacy Controls	Verimatrix Anti-debugging™, Verimatrix Anti-hooking™, Verimatrix Anti-tampering™ hardens applications against attacks trying to extract private data.
M7: Insufficient Binary Protections	Verimatrix Anti-Debugger™, Verimatrix Anti-Hooking™, Verimatrix Anti-Tampering™.
M8: Security Misconfiguration	Verimatrix Anti-Debugger™ ensures applications are not debuggable once deployed, preventing alterations to the app's runtime environment, which helps to safeguard sensitive data or functionality due to misconfigurations, but is only a partial solution to this issue.
M9: Insecure Data Storage	Verimatrix Anti-Tampering™ and Verimatrix Rooting Detector™.
M10: Insufficient Cryptography	Verimatrix Whitebox Cryptography secures cryptographic keys by embedding them directly into the app code, making the keys invisible. Secondary detections can be triggered via Verimatrix Anti-Tampering™ or Verimatrix Man-in-the-Middle Interceptor™ if exploited.

**This list and other content regarding what each of the Mobile Top 10 involves and the associated technical and business impacts are collected from the OWASP Foundation.*

M1: Improper Credential Usage

What's Involved?

The risk of improper credential usage is new to the 2023 OWASP Mobile Top 10 and has become so important that it warrants being number one on the list. Insecure credential management can occur when mobile apps use hard-coded credentials or when credentials are misused.

Hardcoding credentials is an unsafe and rather outdated practice that is best avoided. However, if a mobile app contains hard-coded credentials in its source code or configuration files, it is definitely vulnerable. Risk is also increased if credentials are transmitted without encryption or through insecure channels, if a mobile app stores user credentials on the device in an insecure manner, or if user authentication relies on weak protocols that allow for easy bypassing.

Application-specific threat agents that exploit hard-coded credentials and improper credential usage in mobile applications can include automated attacks using publicly available or custom-built tools. These agents could potentially exploit weaknesses from improper credential usage—for instance, by gaining access through improperly validated or stored credentials, bypassing the need for legitimate access.

Technical and Business Impacts

Poor credential management can lead to severe technical impacts. Unauthorized users might gain access to sensitive information or functionality within the mobile app or its backend systems. That can lead to data breaches, loss of user privacy, fraudulent activity, and potential access to administrative functionality.

The business impacts of poor credential management can be substantial, including reputation damage, IP or information theft, fraud, and unauthorized data access.

Verimatrix XTD Helps Overcome Improper Credential Usage

OWASP recommends that security testers attempt to identify hard-coded credentials within a mobile app's source code or any configuration files in order to pinpoint potential security weaknesses. Given its difficult-to-change nature, hard-coding is generally considered to be a poor implementation method for credential management; it's best if it isn't used in the first place.

However, when hard-coded credentials are used, Verimatrix XTD's code and advanced string obfuscation capabilities can help make sure they do not present additional risk. Verimatrix tools scan your source code and/or binary for exposed strings and encrypt or obfuscate them. This ensures that hard-coded credentials are never in the clear when the application is at rest, and encrypted credentials are decrypted only while the application is running. It also thwarts static analysis attempts to get to such hard-coded credentials.

Additional safeguards by Verimatrix XTD also ensure the runtime integrity of the app, preventing it from being dynamically analyzed. Verimatrix protects against overlays used for stealing user credentials and detecting man-in-the-middle (MitM) attacks, preventing a cyberattacker from impersonating a browser or a server. Additionally, apps may be designed at an early stage defined with whitelisted IP addresses to safely connect to. Verimatrix XTD can trigger alerts if attempts are made by the app to connect to unknown or unauthorized network addresses.

M2: Inadequate Supply Chain Security

What's Involved?

The warning about inadequate supply chain security is also new to the Mobile Top 10 list. Supply chain attacks have grown in number and severity over the past several years, with third-party code being embedded in everything. An attacker can manipulate application functionality by exploiting vulnerabilities in the mobile app supply chain—for example, inserting malicious code into the codebase or modifying code during the build process to introduce backdoors, spyware, or other harmful software, enabling them to steal data, spy on users, or take control of the mobile device. Attackers may also exploit vulnerabilities in third-party software libraries, SDKs, or hard-coded credentials to gain access to a mobile app or the backend servers, leading to unauthorized data access or manipulation, denial-of-service, or complete device takeover.

Multiple avenues can lead to attackers exploiting inadequate supply chain vulnerabilities, such as a lack of security in components or libraries sourced from third parties, malicious insider threats or actions during app development, a lack of developer security awareness, and insecure coding practices, which may stem from inadequate app testing and validation.

Technical and Business Impacts

There are a wide range of technical impacts from exploiting this vulnerability, including data breaches, malware infections, unauthorized access, and even the potential compromise of an entire system.

There may be significant business impacts, depending on the nature of the exploit and the organization's size, industry, and overall security posture. Businesses may suffer financial losses from managing a breach aftermath and lost future business from lack of customer trust, reputational damage to the brand, legal and regulatory consequences, and supply chain disruption that delays product delivery.

Verimatrix XTD Identifies Supply Chain Code Issues Early in the Development Cycle

Verimatrix is constantly improving Verimatrix XTD's capabilities and knowledge base to detect known malware in code libraries. When such libraries are being integrated into the application, events are generated that alert their use. Apart from the development lifecycle, Verimatrix XTD also keeps track of deployment supply chain issues and elevates risk levels if a mobile application is downloaded or sideloaded from sites other than the official Google Playstore® or Apple Appstore®. Additionally, Verimatrix XTD enables supply chain code issues to be identified at a very early stage of development by prompting app developers to whitelist IP addresses that an app can safely connect to and alerting them if the app connects to an unknown or unauthorized address.

M3: Insecure Authentication/Authorization

What's Involved?

Exploiting vulnerabilities in authentication and authorization schemes typically involves automated attacks that use available or custom-built tools. Once an attacker understands the vulnerabilities in either scheme, they might directly submit service requests to the mobile app's backend server by either faking or bypassing the authentication, circumventing any direct interaction with the mobile app. Or, they might log into the application as a legitimate user after successfully passing the authentication control, and then force it to browse to a vulnerable endpoint to execute administrative functionality. Both methods are usually done through mobile malware within the device or botnets owned by the attacker.

With mobile apps, attackers can potentially execute malicious functionality by exploiting an authenticated but lower-privilege user. The risk increases when authorization decisions are made on the mobile device instead of through a remote server. Attackers may also anonymously execute functionality within a mobile app or the backend server it uses, especially if the mobile device is designed to encourage short passwords or 4-digit PINs that are easier to break.

Technical and Business Impacts

The technical impacts of poor authorization and authentication largely depend on the type of over-privileged functionality that is executed. For example, over-privileged execution of remote or local administration functionality may destroy systems or access to sensitive information. With poor authentication, a system is unable to identify the user performing an action request, which can immediately halt logging or auditing of user activity.

The business impacts of poor authentication and authorization include reputation damage, information theft, fraud, and unauthorized access to data.

Verimatrix XTD Protects Against Insecure Authentication/Authorization

Verimatrix XTD helps harden apps by preventing hackers from reverse engineering or modifying/tampering with a protected application's code. Verimatrix code obfuscation involves not just symbol obfuscation that renames functions, packages, methods, and classes but implements sophisticated control flow obfuscation. This changes program readability to a very high degree, making it exponentially more difficult for bots and humans to hook into to circumvent the app's genuine functionality. Secret keys and algorithms used to authenticate are obfuscated and cannot be bypassed or modified, since Verimatrix Anti-Tamper checks whether the app's integrity has been compromised. App execution is allowed only if its integrity has been cryptographically verified to be pristine and unmodified.

M4: Insufficient Input/Output Validation

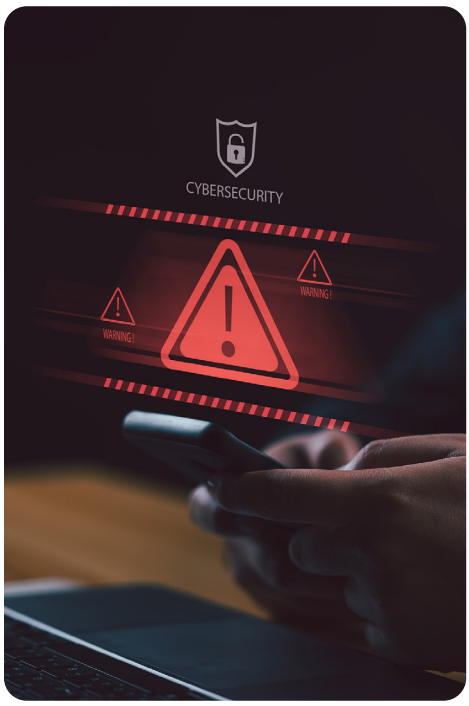
What's Involved?

Another new entry on the Mobile Top 10 is that insufficiently validating app inputs and outputs can increase risk. When user input is not thoroughly checked, attackers can enter unexpected or malicious data that can bypass security measures and lead to code execution vulnerabilities or unauthorized system access. If output data is not properly validated and sanitized, attackers can inject malicious scripts that get executed by users' browsers, leading to cross-site scripting (XSS) attacks, enabling data theft, session hijacking, or manipulation of displayed content.

Failing to consider specific input contexts or expected data formats can result in vulnerabilities like SQL injection or weak format strings. This happens when unvalidated user input is directly incorporated into database queries or improperly handled in format string functions. Without validating data integrity, the app becomes vulnerable to data corruption or incorrect processing. Attackers can then tamper with critical system variables or introduce malformed data that disrupts the app's functionality.

Technical and Business Impacts

This insufficient validation risk can result in unauthorized code being executed, potentially leading to system compromise and unauthorized access. It can allow attackers to manipulate data inputs, resulting in data breaches and unauthorized access to sensitive information. It can also cause application crashes, instability, or data corruption, compromising system reliability and integrity and leading to service disruptions and operational inefficiencies.



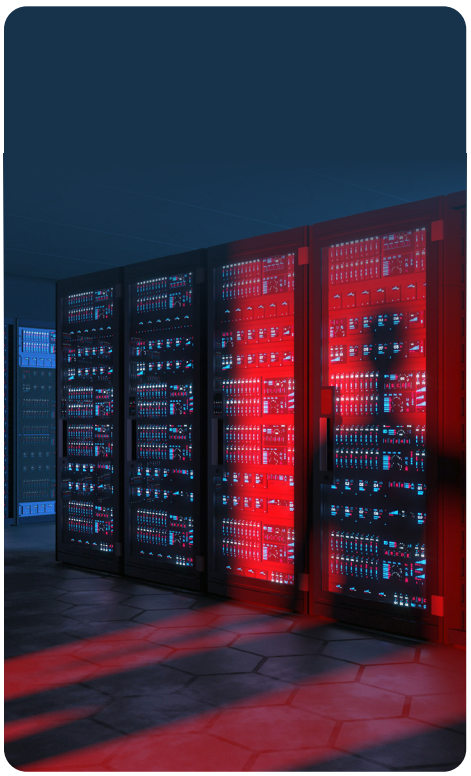
The potential business impacts again include reputational and brand damage resulting from data breaches, system disruptions, and customer distrust. Non-compliance with data protection regulations due to insufficient validation can lead to legal liabilities, regulatory penalties, and potential financial losses. Data breaches or system disruptions caused by this vulnerability may well produce financial losses from incident response expenses, remediation costs, legal fees, and a potential loss of revenue.

Verimatrix XTD Overcomes Insufficient Input/Output Validation

Verimatrix XTD protects the integrity of application code against exploits of inputs or outputs. As with defending against insecure authentication and authorization, the platform prevents modification and overwriting of binary code. For example, not checking validation when the buffer ends enables an attacker to overwrite the end of the buffer into the developer's application. By checking binary integrity at runtime, Verimatrix XTD prevents an attacker from making modifications that could change the app's integrity and behavior.

M5: Insecure Communication

What's Involved?



Most modern mobile apps exchange data with one or more remote servers. Data transmission typically goes through the mobile device's carrier network and the internet. Adversaries that share a local network (i.e., through compromised or monitored Wi-Fi); rogue carriers or network devices like routers, cell towers, or proxies; or even malware on a mobile device can intercept and modify the data that is transmitted in plain text or if it uses a deprecated encryption protocol.

While modern applications do rely on cryptographic protocols such as SSL/TLS, those can be subject to implementation flaws like using deprecated protocols and/or bad configuration settings, accepting bad SSL certificates, or inconsistencies like having SSL/TLS only on select workflows. Inconsistencies in app implementations can lead to vulnerabilities that expose data and session IDs to interception. Observing network traffic on a mobile phone can help identify basic flaws. However, detecting more subtle flaws requires a closer look at the app's design and configuration.

Technical and Business Impacts

Insecure communication can expose user data, which could lead to account takeover, user impersonation, leaks of Personally Identifiable Information (PII), or the interception of user credentials, sessions, or two-factor authentication tokens, which, in turn, can lead to more involved attacks.

From a business perspective, the interception of sensitive data will result in a privacy violation, which has negative compliance impacts. It may also lead to users' identity theft, fraud, or reputational damage to the business.

Verimatrix XTD Keeps Communication Secure

OWASP recommends assuming that the network layer is not secure and is susceptible to eavesdropping. For example, an attacker may insert a proxy between an app and the cloud to listen to all of the traffic going over the network through which the two are communicating. Verimatrix XTD prevents that insecure communication by defending against man-in-the-middle (MitM) attacks, stopping a cyber attacker from impersonating a browser or a server, and detecting overlays, another popular method for stealing user credentials.

Verimatrix XTD ensures that trust anchors, such as certificates that are pinned within a mobile application used for authenticating with a backend service via TLS/HTTPS, cannot be swapped out or modified by an attacker. XTD's anti-resigning and anti-tamper protections preserve the integrity of the protected app just as it was published on the Google Play Store or Apple App Store.

M6: Inadequate Privacy Controls

What's Involved?

Privacy controls are needed to protect Personally Identifiable Information (PII)—sensitive information about users that, if compromised, could enable a cyberattacker to steal a user's identity, misuse their data, or otherwise harm an individual. PII could be leaked (a violation of confidentiality), manipulated (a violation of integrity), or destroyed or blocked (a violation of availability).

Almost all apps process some kind of PII, often collecting and processing more data than is needed for the app's specific purpose. This makes them a very attractive target for cybercriminals. Typical sources for PII are usually well protected via methods like sandboxing, logs, and backups, or through network communication with the server. That means that accessing PII usually requires an attacker to first breach security on another level—like eavesdropping on network communications or using a trojan to access file systems, clipboards, logs, or even a mobile device—then create a backup to analyze separately. An attacker could also access communication and storage media when PII is being processed.

Technical and Business Impacts

There are actually minimal to no technical impacts from privacy violations. It could be that if the PII includes information like authentication data, it can affect certain global security properties like traceability. Or, manipulated user data could render a system unusable for that user. These impacts are relatively uncommon.

However, the business impacts can be very significant. Compromised PII puts businesses at risk of privacy violations. There are a growing number of privacy regulations worldwide, including the very strict European Union General Data Protection Regulation (GDPR). These new laws, combined with growing user anger about the compromise of their data and the very real negative impacts that customers whose data is compromised may experience, make privacy violations a serious concern.

Verimatrix XTD Protects PII

Verimatrix XTD protects PII because any attack on an app could expose private information, risking leaks, improper usage, and loss of customer trust. This is especially important for remaining compliant with the GDPR and other data privacy regulations.

While we never handle PII through our platform, Verimatrix XTD offers those who do process PII robust passive protection and monitoring capabilities, including code obfuscation, anti-debugging, anti-tampering, anti-hooking, emulation detection, and overlay protection to prevent attacks like credential stuffing. In addition, the platform supports safe whitelisting of accessibility services for users with disabilities. This broad array of defenses makes it very difficult for an attacker to access any private data.

M7: Insufficient Binary Protections

What's Involved?

Binary code may hold valuable commercial API keys or other hard-coded cryptographic secrets that an attacker could misuse. This kind of code could also be valuable on its own if it contains critical business logic or pre-trained AI models. Some attackers might also not target the app itself but use it to explore potential weaknesses in the corresponding backend to prepare for an attack.

App binaries can usually be downloaded from app stores or copied from mobile devices, making them easy to set up. They are typically subject to two types of attacks: reverse engineering, in which the app binary is decompiled and scanned for valuable information, like secret keys, algorithms, or vulnerabilities; and code tampering, where the app binary is manipulated, e.g., to remove license checks, circumvent paywalls, or obtain other benefits as a user. All apps are vulnerable to binary attacks, and many will end up the subject of some form of attack at some point. Especially popular apps are likely to be manipulated and redistributed through app stores.

Technical and Business Impacts

If app secrets are leaked, they must be replaced quickly throughout the system. This can be difficult if those are hard-coded into the app; again, this is a practice that should not be used. Information leakage from the binary also has the potential to reveal security vulnerabilities in the backend. There is also a considerable impact on the technical soundness of a system. Through manipulating binaries, attackers can arbitrarily change how apps work, either to their own benefit or to disturb the backends.

Leakage of keys for commercial APIs can impose significant business costs if they are misused on a large scale. The same holds for apps that are tampered with to remove license checks or to publish their functionality with a competing app. Doing this at the individual level for personal use will likely go unnoticed. But at scale, malicious competitors might get a significant advantage because they have significantly lower costs. Theft of intellectual property like algorithms or AI models can also be very costly and harm the application company's business. Perhaps worst of all, popular apps may get redistributed with malicious code, leading to reputational damage even if the original developer is not at fault.

Verimatrix Preserves Binary Code

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach enabled through Verimatrix XTD is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. Verimatrix XTD's polymorphic protection transforms mobile apps into moving targets, making it much harder—even nearly impossible—for hackers to reverse engineer code, exfiltrate data, and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. The platform's additional protection and monitoring capabilities, including anti-debugging, anti-tampering, anti-hooking, emulation detection, and overlay protection, provide extra layers of defense for critical binary code. The protected code itself cannot be

M8: Security Misconfiguration

What's Involved?

Improper configuration of security settings, permissions, and controls can lead to vulnerabilities and unauthorized application access. Attackers may use this weakness to gain access to sensitive data or perform other malicious actions.

Security misconfigurations in mobile apps can be exploited through a range of attack vectors, including

- insecure default settings that may have weak security settings or unnecessary permissions enabled;
- improper or misconfigured access controls that can allow unauthorized users to access sensitive data or perform privileged actions;
- weak encryption or hashing algorithms that can be exploited to gain access to sensitive information;
- lack of secure communication like SSL/TLS protocols that can expose sensitive data to eavesdropping and man-in-the-middle attacks;
- unprotected storage of sensitive data;
- insecure app files with world-readable and/or world-writable permissions;
- and misconfigured session management that can lead to session hijacking with attackers impersonating legitimate users.

Given persistent time constraints, a lack of awareness, or human error during development, security misconfigurations in mobile apps are unfortunately common. They frequently result from simple errors, such as failure to disable debugging features in release builds, allowing insecure communication protocols like HTTP instead of enforcing secure HTTPS, leaving default usernames and passwords unchanged, and having inadequate access controls that allow unauthorized users to perform privileged actions.

Technical and Business Risks

Security misconfigurations can have significant technical impacts on mobile apps. Misconfigurations may result in data breaches by allowing attackers to access sensitive information like user credentials, personal data, or confidential business data. Weak or misconfigured authentication mechanisms can lead to account takeovers or the impersonation of legitimate users. What's more, misconfigurations in a mobile app can provide attackers with a foothold to compromise the backend systems or infrastructure.

There are also several possible business impacts. Breaches resulting from security misconfigurations can lead to financial losses, including legal penalties, regulatory fines, and damage to the organization's reputation. Misconfigurations can result in the loss or theft of sensitive data, leading to legal and financial consequences. Exploitation of security misconfigurations can lead to app downtime, service disruption, or compromised functionality, affecting the user experience and business operations.

Verimatrix Reduces Risks from Misconfigured Security

Verimatrix XTD's breadth of defensive capabilities—code obfuscation, anti-debugging, anti-tampering, anti-hooking, emulation detection, and overlay protection—make it difficult for an attacker to execute an exploit in the event s/he is somehow able to access application code or data. Additionally, Verimatrix XTD can prevent apps from running on jailbroken iPhones or rooted Android devices if our customer wishes to prevent that behavior. Since jailbreaking and rooting may be common for some customers, a given organization can choose to leverage this protection depending on its risk appetite. Apps protected by Verimatrix and running on end-consumer devices have the capability to be monitored for security threats and vulnerabilities. Mitigating steps can be taken immediately or after observing end-user app behavior over a period of time, if needed.

M9: Insecure Data Storage

What's Involved?

Insecure data storage in a mobile app exposes vulnerabilities to various attacks, like unauthorized physical or remote access to a mobile device's file system, exploiting weak encryption, intercepting data transmissions, and leveraging malware or malicious apps installed on the device. Rooted or jailbroken devices enable attackers to bypass security measures and gain direct access to sensitive data. And social engineering techniques can be used to deceive users into providing access to their data or manipulating an app's behavior.

Various security weaknesses can put the confidentiality and integrity of stored information at risk. For instance, weak or nonexistent encryption allows attackers to easily access and decipher sensitive data. Storing data in easily accessible locations within the device's file system exposes it to unauthorized extraction or manipulation. Insufficient access controls and user authentication mechanisms further compound the problem, enabling unauthorized individuals to gain access to sensitive data. The absence of secure data transmission protocols can leave data vulnerable to being intercepted during communication between the mobile app and external servers.

Technical and Business Impacts

Security weaknesses in mobile application data storage create opportunities for multiple harms. Sensitive data is susceptible to unauthorized access and breaches. Attackers can exploit vulnerabilities to extract or manipulate sensitive data, leading to potential privacy violations and the loss of confidential information. User accounts may be compromised if attackers gain access to login credentials or personal information that is insecurely stored. Without proper data protection measures, attackers can modify or tamper with the stored data, leading to challenges with data integrity, inaccurate information, or the injection of malicious content into the app's data stores. And attackers may gain unauthorized access to critical application resources like sensitive files, configuration files, or cryptographic keys stored within the app.

The business risks are just as severe. Data breaches often impose heavy costs associated with breach investigation, notifying affected customers, providing identity theft protection services, potential legal settlements, and loss of business opportunities. Breaches can result in non-compliance with industry regulations and data protection standards, subjecting app developers to penalties or legal action. Data breaches and compromised user accounts can severely damage an organization's reputation and lead to a loss of customer trust and loyalty. All of these significant impacts put app businesses at a competitive disadvantage.

Verimatrix Obscures Insecure Data Storage

Verimatrix XTD makes it very difficult for attackers to exploit data storage practices that may be insufficient for truly protecting the storage location. The platform bolsters a basic secure storage strategy, providing code obfuscation, anti-debugging, anti-tampering, anti-hooking, emulation detection, and overlay protection that frustrate an attacker's attempts to discover where the insecure storage is and dramatically reduce the possibility of exploiting it.

M10: Insufficient cryptography

What's Involved?

While encryption is a strong security technique, there may be vulnerabilities in the cryptographic mechanisms used to protect sensitive information that undermine its effectiveness. These can result from a range of issues, such as using weak encryption algorithms or inadequate key lengths, poor key management practices, improper handling of encryption keys, insecure random number generation, flawed implementation of cryptographic protocols, or vulnerabilities in cryptographic libraries or frameworks.

Attackers may use techniques like brute force, cryptographic, or side-channel attacks to exploit weaknesses in encryption algorithms, key management, or implementation in order to bypass encryption, perform cryptographic attacks, manipulate data, or gain unauthorized access to encrypted information. Insecure hash functions and cryptographic algorithms pose significant security weaknesses in mobile apps. When outdated or weak hash functions are used, attackers can exploit the flaws to reverse-engineer hashed data, revealing the original content.

Technical and Business Impacts

The impacts of insufficient cryptography will be severe. Encryption is used to protect the most sensitive data, and its compromise can result in the unauthorized retrieval and abuse of sensitive information from a mobile device.

Weak or insufficient cryptography can make it easier for adversaries to compromise the confidentiality of sensitive data stored or transmitted by a mobile app, resulting in data breaches and the exposure of sensitive customer data that imposes compliance and other legal consequences. Cryptography weaknesses can jeopardize the protection of proprietary algorithms, trade secrets, or other intellectual property embedded in a mobile app, leading to financial losses for the app developer. If payment transactions or financial data are improperly encrypted, customers may be exposed to fraud and unauthorized access to their funds. Additionally, the costs associated with investigating and remediating security breaches, compensating affected customers, and addressing legal ramifications can be substantial for the app development organization.

Verimatrix Overcomes Insufficient Cryptography Shortcomings

Insufficient cryptography is used to hide secrets in the code or data. For improperly crafted or designed connectivity, Verimatrix provides man-in-the-middle detection to prevent a cyberattacker from impersonating a browser or a server. But even if a man-in-the-middle attack is detected, there is still a certain level of risk associated with improperly implementing cryptography. For instance, exposed cryptographic keys are a known vulnerability in app code. Verimatrix Whitebox Cryptography effectively dissolves keys into the code itself and obscures algorithms to keep critical applications and data safe, even if a hacker has complete access to the device on which the algorithms are executing.

About Verimatrix XTD

Verimatrix Extended Threat Defense (XTD) is a cybersecurity suite engineered to shield mobile and web applications from today's modern cyber threats. It addresses the critical problem of overlooked vulnerabilities in mobile apps, and from connected unmanaged consumer devices, which often go unnoticed in current security setups.

Key Differentiators

Comprehensive Protection: XTD offers a comprehensive set of application shielding and threat detection capabilities, making it a one-stop solution for application protection needs.

Real-time Threat Intelligence: Leveraging AI and ML technologies, XTD provides real-time, continuous threat intelligence, enabling organizations to detect and respond to new threats effectively.

Seamless Integration: XTD seamlessly integrates into existing CI/CD processes without causing disruption, ensuring smooth deployment and operation.

Expertise and Support: Verimatrix offers security and development expertise, assisting organizations in quickly protecting their applications whether it be through zero-code deployments, on-premise toolkits, or white glove, curated implementations.

Compatibility and Flexibility: XTD is compatible with Android, iOS, desktop/embedded, and web applications, offering advanced obfuscation techniques and multi-layered security solutions across various platforms, browsers, JavaScript, frameworks, and libraries.

Why Choose Verimatrix XTD

By investing in Verimatrix XTD, organizations can:

- Fortify their defenses against cyber threats targeting mobile and web applications.
- Ensure the security and availability of their digital assets, protecting their reputation and maintaining customer trust.
- Benefit from a comprehensive and easy-to-use solution that seamlessly integrates into existing workflows.
- Stay ahead of evolving threats with real-time threat intelligence and expert support from Verimatrix.

Verimatrix XTD protects the applications that drive the digital economy, giving you peace of mind.

Get a free demo of Verimatrix XTD

Talk to us

verimatrix
DRIVING TRUST

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and 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**