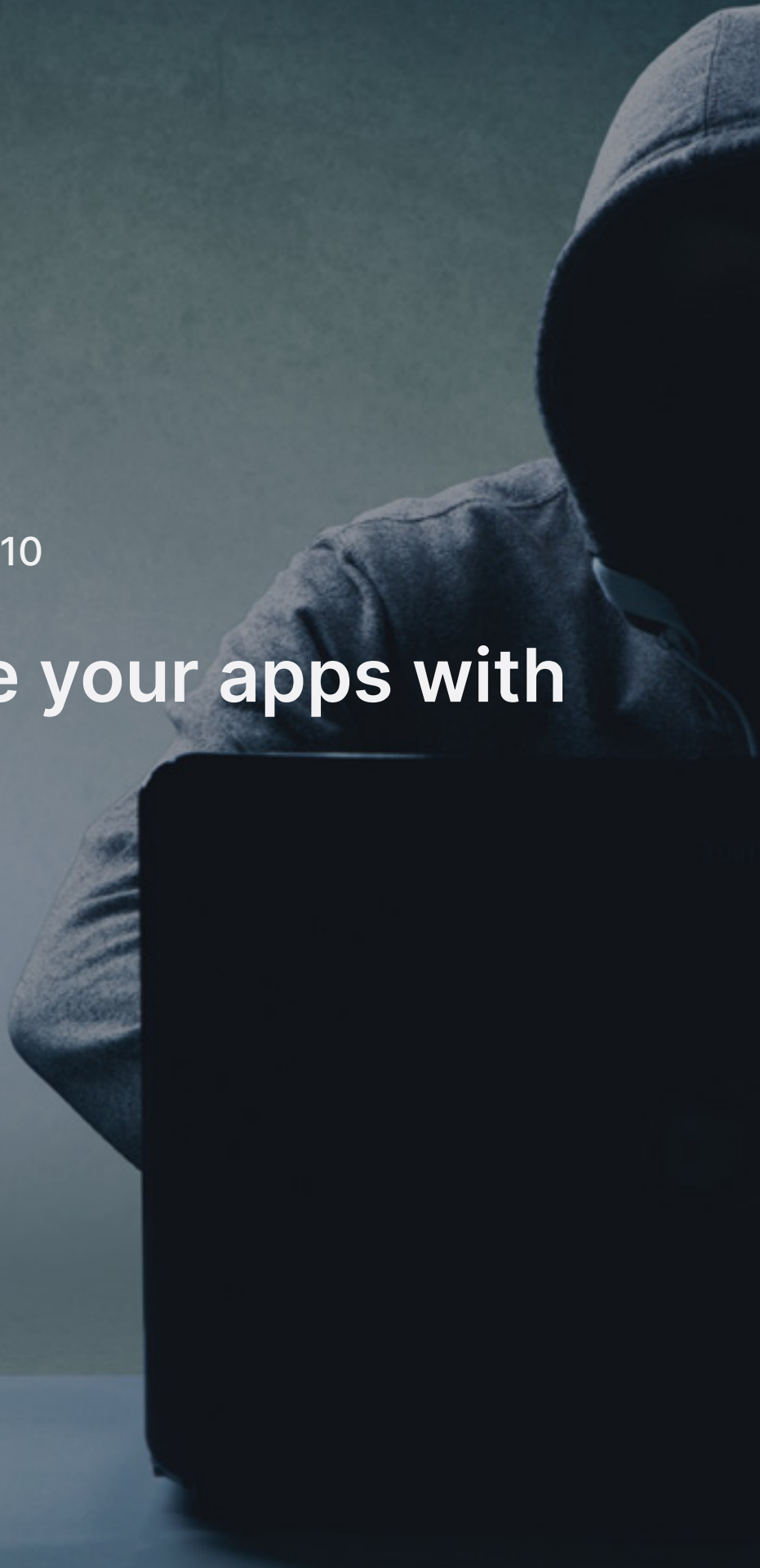


PROMON

 OWASP MOBILE TOP 10

How to secure your apps with App Shielding



Executive summary

Mobile application developers should be familiar with possible security risks that a mobile application might face. Knowing possible risks makes it easier to avoid possible pitfalls and develop secure applications.

The [Open Web Application Security Project](#) (OWASP) is a non-profit foundation that works to improve the security of software. OWASP has created freely available learning materials and tools to help build secure web and mobile applications, including a list of the top ten most common threats to mobile applications ([The OWASP Top 10](#)).

In addition to the OWASP Top 10, the OWASP Mobile Project has produced comprehensive standards documentation and test procedures for [Mobile Application Security Verification Standards](#) (MASVS), which in turn can be linked to the OWASP Top 10. The MASVS is a living document available on [GitHub](#). Although the OWASP Top 10 and the MASVS are good assets for all applications, they are more applicable to financial, payment and banking applications – as well as other apps handling sensitive personal data. This document outlines how App Shielding can assist you in addressing the OWASP Top 10.

App Shielding in brief

[Gartner](#) defines App Shielding as a security solution implemented within the application to make it more resistant to attacks. Gartner categorizes App Shielding capabilities into prevention, detection and «other» capabilities including Runtime Application Self-Protection (RASP). App Shielding can assist developers and publishers in addressing some of the challenges identified by OWASP.

OWASP mobile top 10

- M1 Improper platform usage
- M2 Insecure data storage
- M3 Insecure communication
- M4 Insecure authentication
- M5 Insufficient cryptography
- M6 Insecure authorization
- M7 Client code quality
- M8 Code tampering
- M9 Reverse engineering
- M10 Extraneous functionality



M1 Improper platform usage

This risk category covers the misuse of a platform feature, or failure to use platform security controls. This may include:

- Correct usage of platform permissions
- Detection of custom keyboards
- Misuse of the keychain
- Android intents



App Shielding detects the state of the device (root/jailbreak detection), blocks emulators, and identifies permissions enabled on the device.

M2 Insecure data storage

This risk category covers insecure data storage and unintended data leakage, both from disk and during runtime and user interaction. This may include:

- Compromised file systems
- Incorrect storage of data
- Incorrect usage of keyboard cache
- Screen readers



App Shielding addresses this category by blocking screen readers and key loggers, as well as offering a secure local storage mechanism with device binding (blocking the copying of data to another device).

M3 Insecure communication

This risk category covers failure in securing the integrity of data in transit, such as poor handshakes or lack of network encryption. This may include:

- HTTP instead of HTTPS
- Incorrect SSL versions
- Poor handshaking/weak negotiation (e.g. lack of certificate pinning)

Although App Shielding itself does not offer network security, it adds security to the implementation by protecting the application both at rest and at runtime.

M4 Insecure authentication

This risk category covers server authentication of the end user or bad session management. This may include:

- Failure to identify the user at all
- Failure to maintain the user's identity
- Weaknesses in session management

This could be due to:

- Insecure authentication input
- Poor two-factor implementation
- Insecure user credentials

Although App Shielding itself does not offer authentication mechanisms, it adds integrity to the process by ensuring that the app is not tampered with. It also enables device binding and secure storage of tokens through secure local storage mechanisms.

M5 Insufficient cryptography

This risk category covers lack of (or insufficient usage of) appropriate cryptography. Cryptography is an essential ingredient for protecting data stored on mobile devices, and is a risk category where things can potentially go horribly wrong. Failure to address this category may result in:

- Stolen app and user data
- Access to encrypted files

Failures are commonly caused by:

- Old or misconfigured cryptography
- Use of non-proven cryptographic libraries



App Shielding ensures that the security mechanisms cannot be removed from an app, protects apps against repackaging, and ensures that local data is non-copiable and properly encrypted.

M6 Insecure authorization

This risk category comprises risks related to an adversary using a client to login as a legitimate user. Areas covered include:

- Password enforcement
- Token management in the client
- Session management in the client



App shielding ensures the legitimacy of an application, and that it has not been tampered with. Code Injection in an unprotected local client can bypass authentication if the application is already authorized. Furthermore, tokens and other sensitive elements can be stored or deleted on the device securely through secure local storage mechanisms.

M7 Client code quality

This risk category comprises basic security coding practices in application development, and is an umbrella category for code-level implementation in the mobile application. Areas covered include:

- App signing
- Debugging information or access in a public application
- Exceptions management in the application
- Error handling in security controls



App Shielding has self-contained functionality to protect against repackaging and verification of the application signature. Furthermore, it will remove debug information from the application code, and block debugger and emulator access. Security controls and device anomalies are managed and can be reported to the application code for specific handling.

M8 Code tampering

This risk category covers an application's resilience against reverse engineering, as well as specific client-side attacks. It covers unauthorized modification of an application, either as downloaded from the application store or during runtime. Areas covered include:

- Detecting whether the device is jailbroken or rooted
- The presence of debuggers
- Tampering of the executable
- Device binding
- Malware



App Shielding is designed to make an application self-defending and is able to detect and react to all threats defined in M8. The reaction may be handled by the application after an anomaly is detected. The technology also supports device binding through secure local storage mechanisms.

M9 Reverse engineering

This risk category is closely linked with M8, but more focused on application analysis and code patterns, and code stealing and IPR theft risks. Areas covered include:

- Code obfuscation
- The presence of reverse engineering tools and frameworks
- Detection of being run in an emulator
- The presence of debuggers
- Removal of (or bypass of) application security measures



App Shielding is designed to make the application self-defending, and is able to detect and react to all of these threats. The technology is designed not to leave evidence of its findings before reaction, and to ensure that an application is not usable in any way if attempted removed.

M10 Extraneous functionality

This risk is about code control and the prevention of actions including the exportation of debug information or logs. It also includes hidden backdoor functionality risks.








Although IApp Shielding itself cannot protect against bad code or hidden backdoors in an application, the technology is designed not to leak security related information or send out any data from the application.



”

Promon SHIELD™ can assist
app developers and publishers
in addressing OWASP 10 risks

Promon SHIELD™

M1	Improper platform usage	
M2	Insecure data storage	
M3	Insecure communication	
M4	Insecure authentication	
M5	Insufficient cryptography	
M6	Insecure authorization	
M7	Client code quality	
M8	Code tampering	
M9	Reverse engineering	
M10	Extraneous functionality	

PROMON



www.promon.co
info@promon.no
+47 22 02 11 30