MAST

MOBILE APPLICATION SECURITY TOOLKIT

CAN YOUR APP DEFEND ITSELF IN THE WILD?

You have to launch your app 'yesterday,' even though you need to spend more time securing it.

Left unprotected, your app's data can be read like an open book. Proprietary algorithms. Copyrighted content. Crypto keys. It's all there for prying eyes.

Let's be honest: your app's data is exposed. Those hastily installed off-the-shelf protections? They can be removed just as quickly with off-the-shelf tools. Your employees' personal devices? You have to assume they host malware waiting to slip into your app's code. With enough time, competitors bent on reverse engineering your app will break through.

YOUR APP NEEDS MAST.

The result of research funded by the Defense Advanced Research Projects Agency (DARPA), Mast protects your app from hackers, reverse engineers, software pirates, and competitors. It seamlessly integrates with your development and requires no changes to your source code, allowing you to launch sooner and have confidence in your security.

THWART ALL KNOWN REVERSING AND ANALYSIS TOOLS.

Resist reverse engineering - By diffusing and encrypting sensitive code, and adding myriad 'dead ends,' Mast makes static analysis a months-long task.

Evade runtime tampering - Mast embeds checks that set off alarms when tripped, and prevents attackers from modifying your code.

Deny jailbroken devices - Since your app can't trust this environment, Mast helps it know when to turn off and stay off.

KEEP AHEAD OF THE LATEST ATTACKS.

New reverse engineering techniques emerge every day. We know, because we monitor for new threats continuously. Every time we update Mast, it will break attacker's newest tools immediately, setting them back to zero.

THREE-STEP INSTALLATION

ONE

Run the included installer on a developer workstation

TWO

Launch Xcode

THREE

Select desired protections in "Build Settngs" and build your app

That's it. Your app is now protected!

MAST

DEAD SERIOUS PROTECTION. DEAD SIMPLE INSTALLATION.

Mast ensures that your application acts as a black box: data goes in and comes out, but no one can see how it works. Without modifying your source code or requiring expertise in state-of-the-art security, Mast bakes in dozens of novel software protection techniques through the Xcode compiler, including:

STATIC ANTI-REVERSING

- Code diffusion
- Selector encryption
- Instruction entropy

DYNAMIC ANTI-DEBUGGING

- Deny debugging attempts
- Deny library interposing

ANTI-JAILBREAK

- Detect degraded security and apps from jailbroken or compromised phones
- Recognize common tools

PRE-LAUNCH REVIEW

While Mast compiles your iOS app, it searches for common security oversights such as protecting user data in the iOS "keychain," proper use of TLS, and keeping user data out of the pasteboard and screenshots. The list of checks grows over time, just like the reversing protections.

DISTRESS SIGNAL

If it detects reverse engineering attempts, the system can be configured to alert you and existing fraud systems.

ABOUT TRAIL OF BITS

We hold a unique leadership role in the high-end security research industry. Our team has a track record of discovering critical Internet vulnerabilities in targets hardened by dedicated security teams, including major shipping software products and even the Internet Public Key Infrastructure. Our clients call on our deep expertise in reverse engineering the iOS and Android security models, cryptography, virtualization, malware behavior and software exploits. We have presented on these topics in major security conferences, such as Blackhat, CanSecWest, and REcon.

WHY SECURITY TEAMS LOVE MAST

NO SECURITY EXPERTISE REQUIRED

NO SOURCE CODE CHANGES

INTEGRATES WITH XCODE

TUNABLE SECURITY FEATURES

CUSTOM CALLBACKS TO NOTIFY YOU

APPSTORE COMPATIBLE AND COMPLIANT

REQUIREMENTS

Mast requires an up-to-date Xcode. Support for Android is upcoming.