



# Dr. James Mickens Direct Examination

## Summary of Conclusions

---

iPhone's security guarantees are predominantly enforced by the iPhone's operating system (iOS)

Evidence suggests that the App Review process does a weak job of enforcing additional security properties that cannot be enforced by the OS alone

iOS, much like macOS, is already capable of installing applications that were not distributed via Apple's App Store

If Apple allowed iPhone users to opt into third-party app distribution channels, those users would not suffer from a meaningfully less-secure experience

# How is Security Enforced on iPhones?

## OFF-DEVICE SECURITY

*app distribution*



Can be  
performed by  
third parties

App Review

Developer Identification

Code Signing

Provides minimal (if any)  
security benefits relative to  
what iOS on-device security  
mechanisms provide

## ON-DEVICE SECURITY

*operating system*



Independent  
of app  
distribution  
method

Digital Signature Validation

Sandboxing

Address Space Layout Randomization (ASLR)

Execute Never (W^X)

Memory Isolation

Kernel Integrity Protection

Page Protection Layer

## ON-DEVICE SECURITY

*hardware*



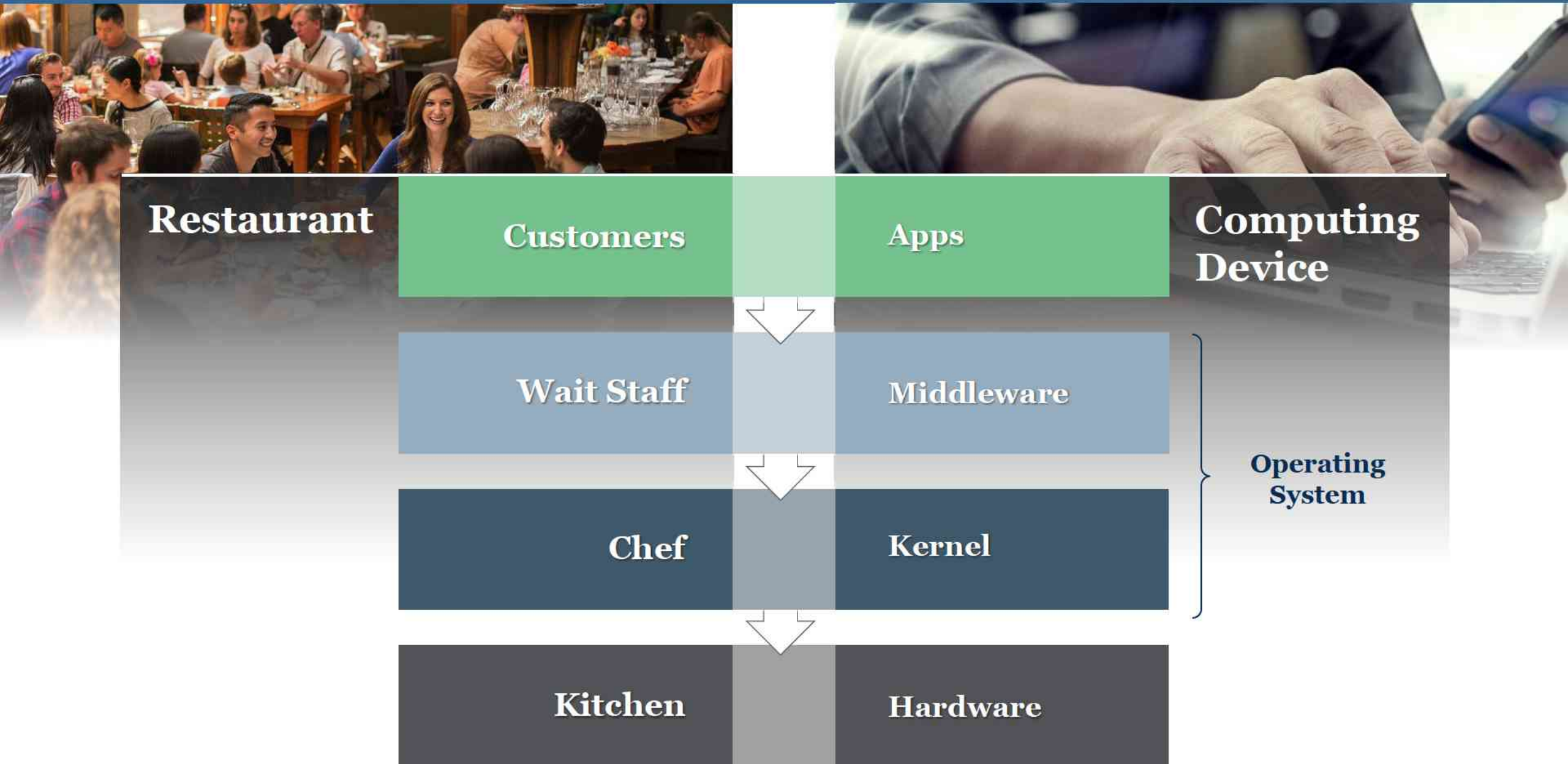
Biometric Authentication

Secure Enclave

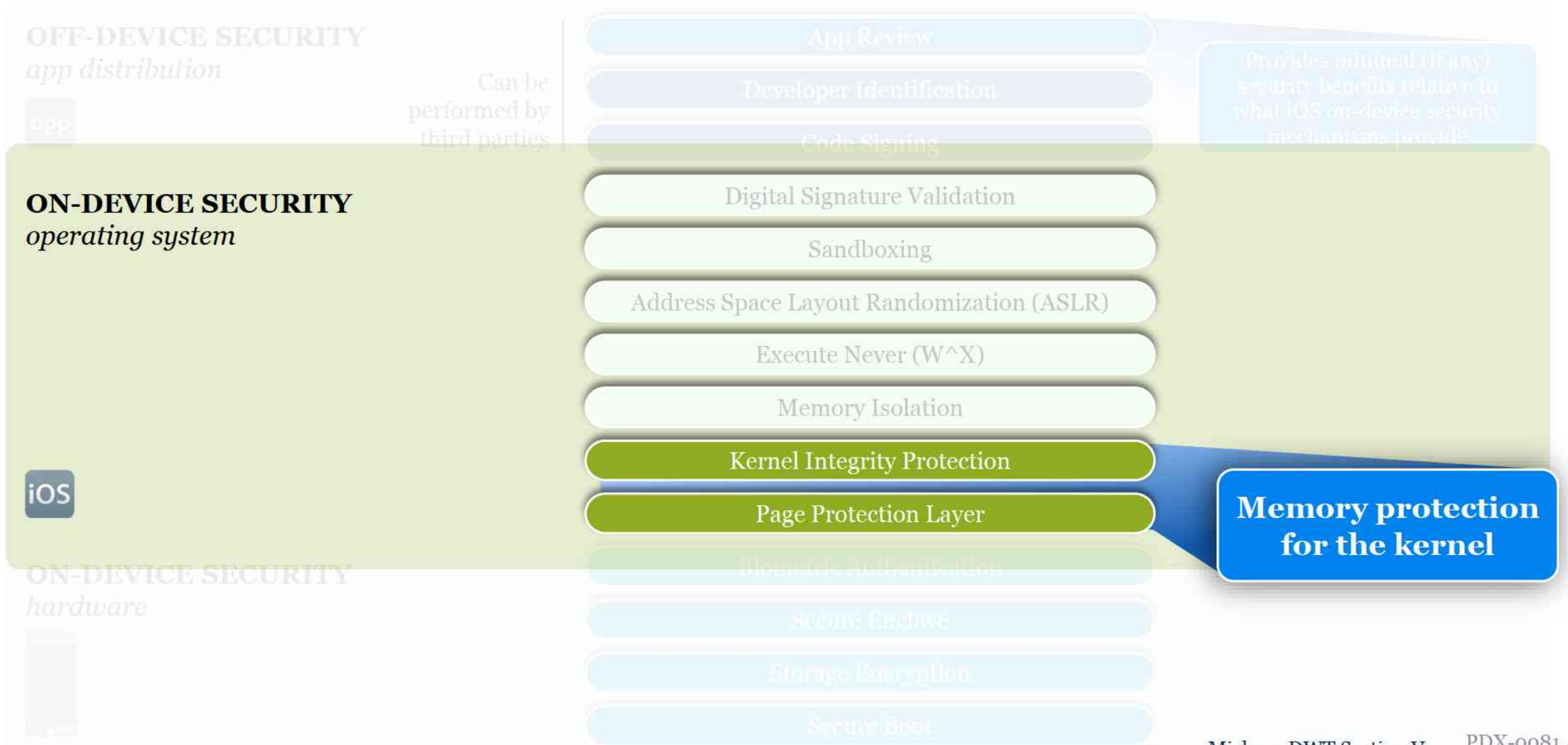
Storage Encryption

Secure Boot

# Operating System Design

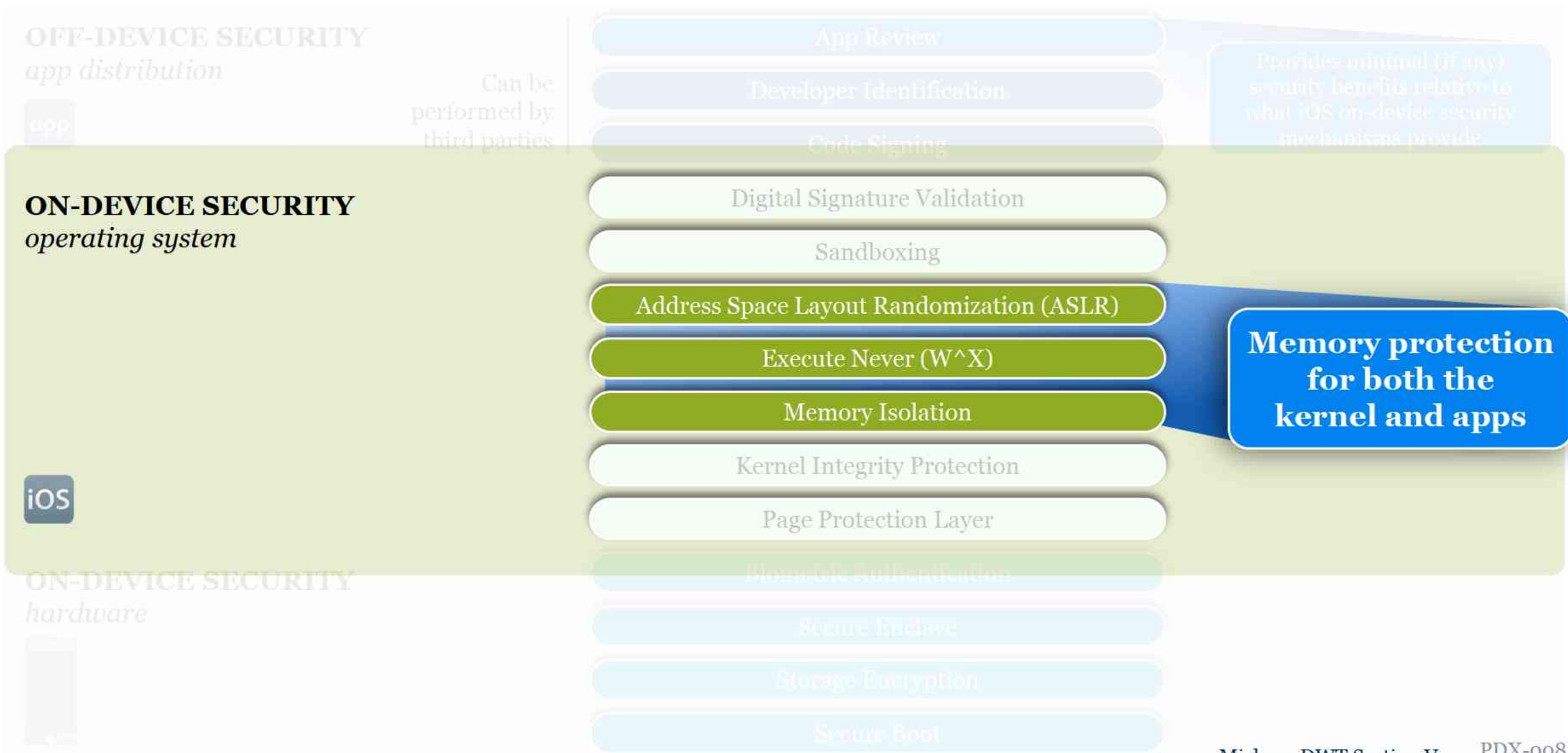


# On-Device Security: Operating System





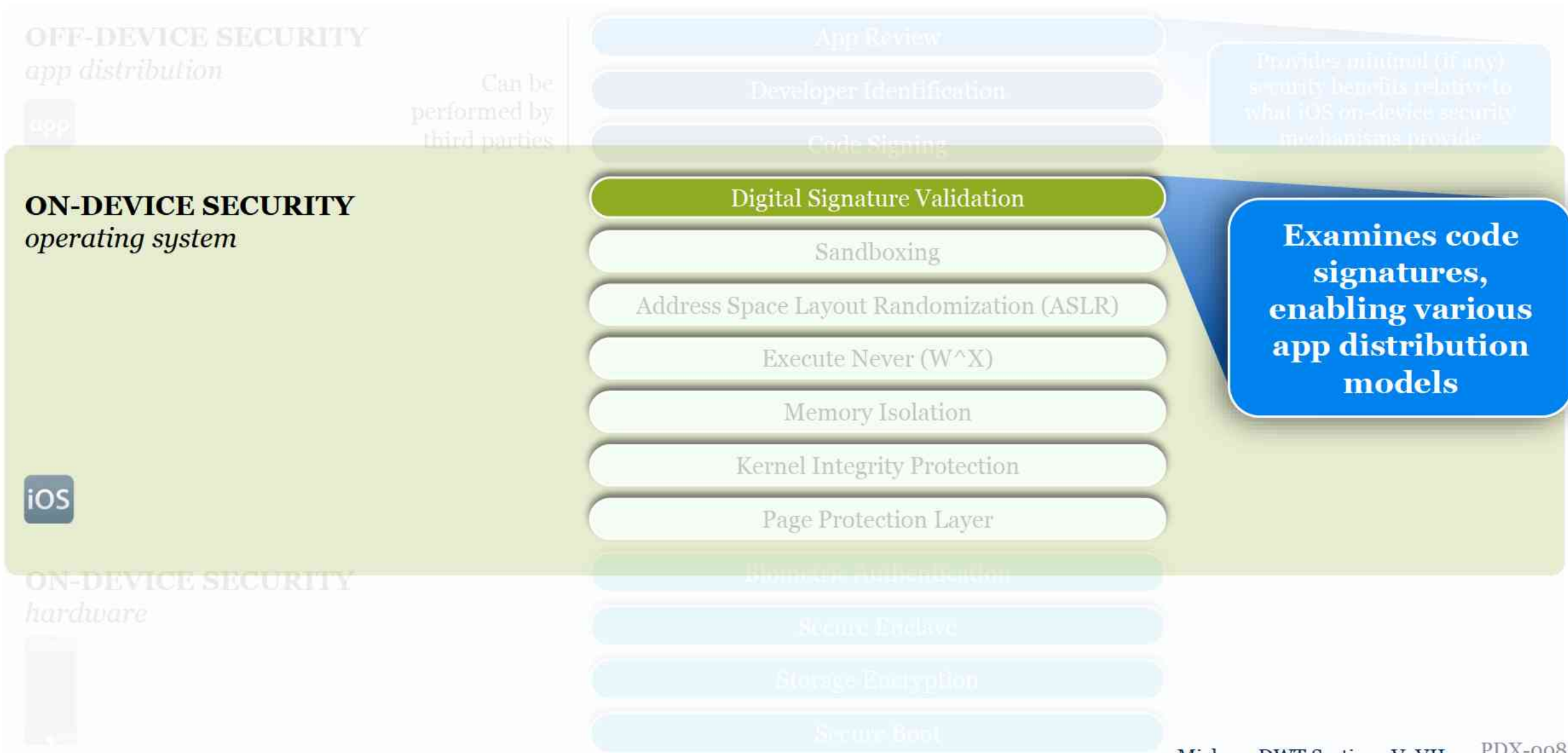
# On-Device Security: Operating System



# On-Device Security: Operating System

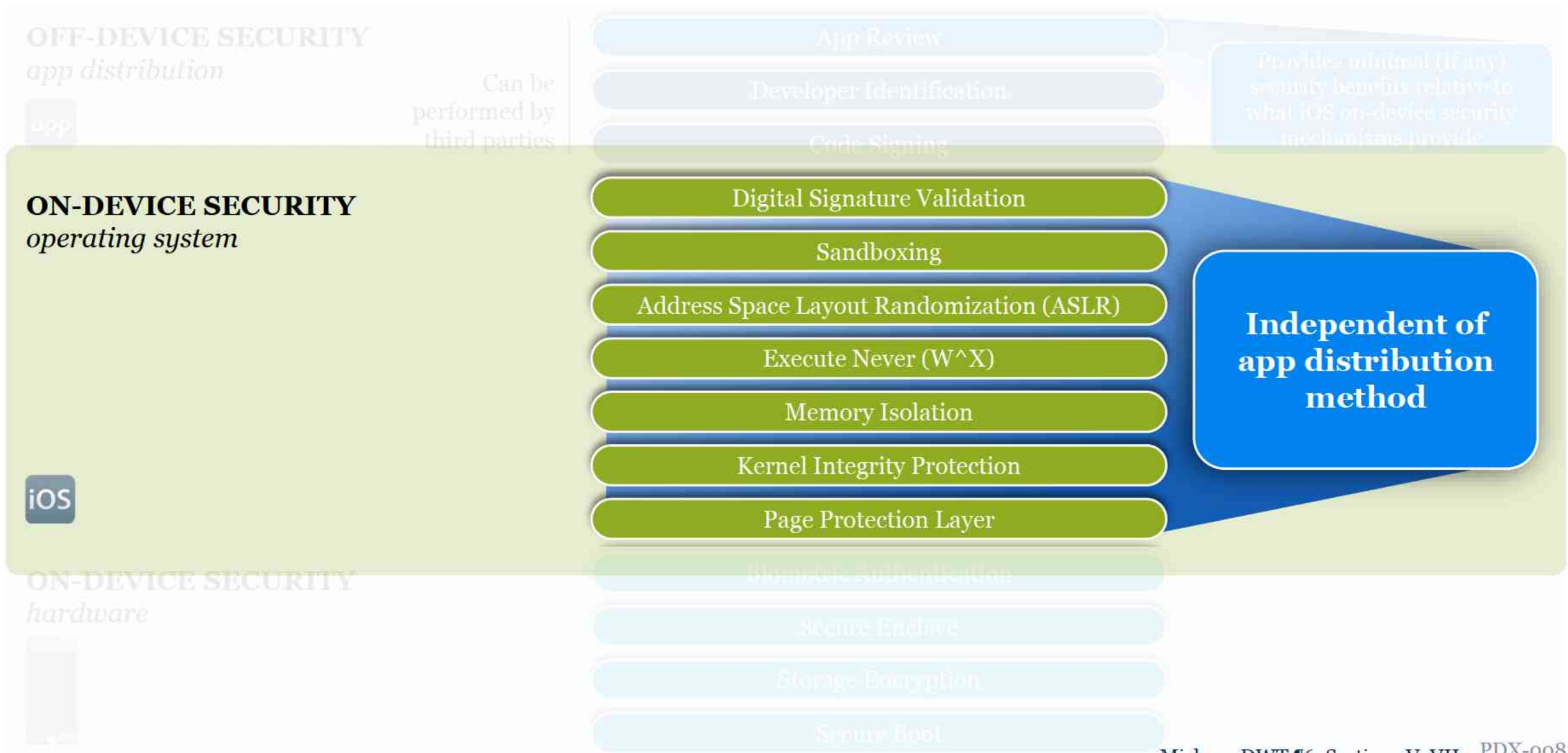


# On-Device Security: Operating System

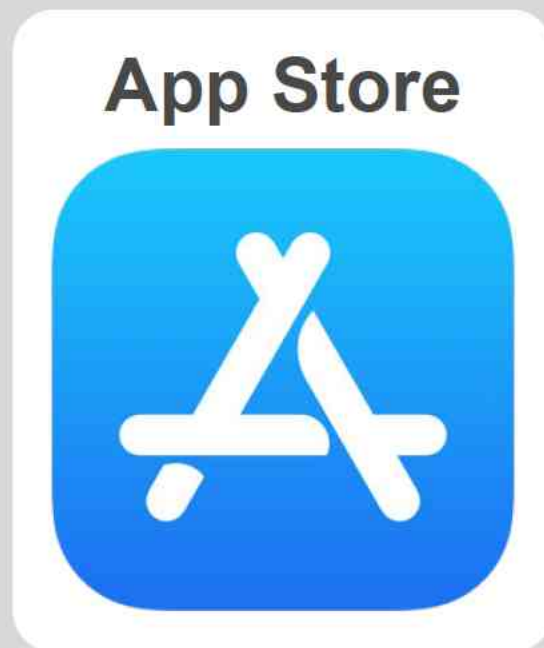




# On-Device Security: Operating System



# iOS: Models of App Distribution



# iOS App Review: Security Properties

## Security Properties

**Sandbox Compliance**

**Exploit Resistance**

**Malware Exclusion**

**User Consent for Private Data**

**Legal Compliance**

# iOS App Review: Security Properties

Security Properties

	App Review	On-Device Security: Operating System
Sandbox Compliance	✓	Sandboxing ✓
Exploit Resistance	✓	ASLR W^X KIP PPL ✓
Malware Exclusion	✓	Anti-malware scanners ✓
User Consent for Private Data	weak, at best ✗	System call monitoring ✓
Legal Compliance	Difficult to ascertain by <b>App Review</b> or the <b>OS</b>	

# iOS: Models of App Distribution

**iOS**

**App Store**






**Apple Developer  
Enterprise Program**



**Internal  
Apple Testing  
Distribution**



# iOS App Distribution Models: Security Features

	<b>ON-DEVICE SECURITY</b> <i>operating system</i>	<b>OFF-DEVICE SECURITY</b> <i>app distribution</i>		
	<ul style="list-style-type: none"> <li>Digital Signature Validation</li> <li>Sandboxing</li> <li>Address Space Layout Randomization (ASLR)</li> <li>Execute Never (W^X)</li> <li>Memory Isolation</li> <li>Kernel Integrity Protection</li> <li>Page Protection Layer</li> </ul>	App Review	Developer Identification	Code Signing
	✓	✓	✓	✓
 Apple Developer Enterprise Program	✓	✗	Partially	Not by Apple
 Internal Apple Testing Distribution	✓	✗	✓	✗

# macOS Operating System



# macOS: Models of App Distribution



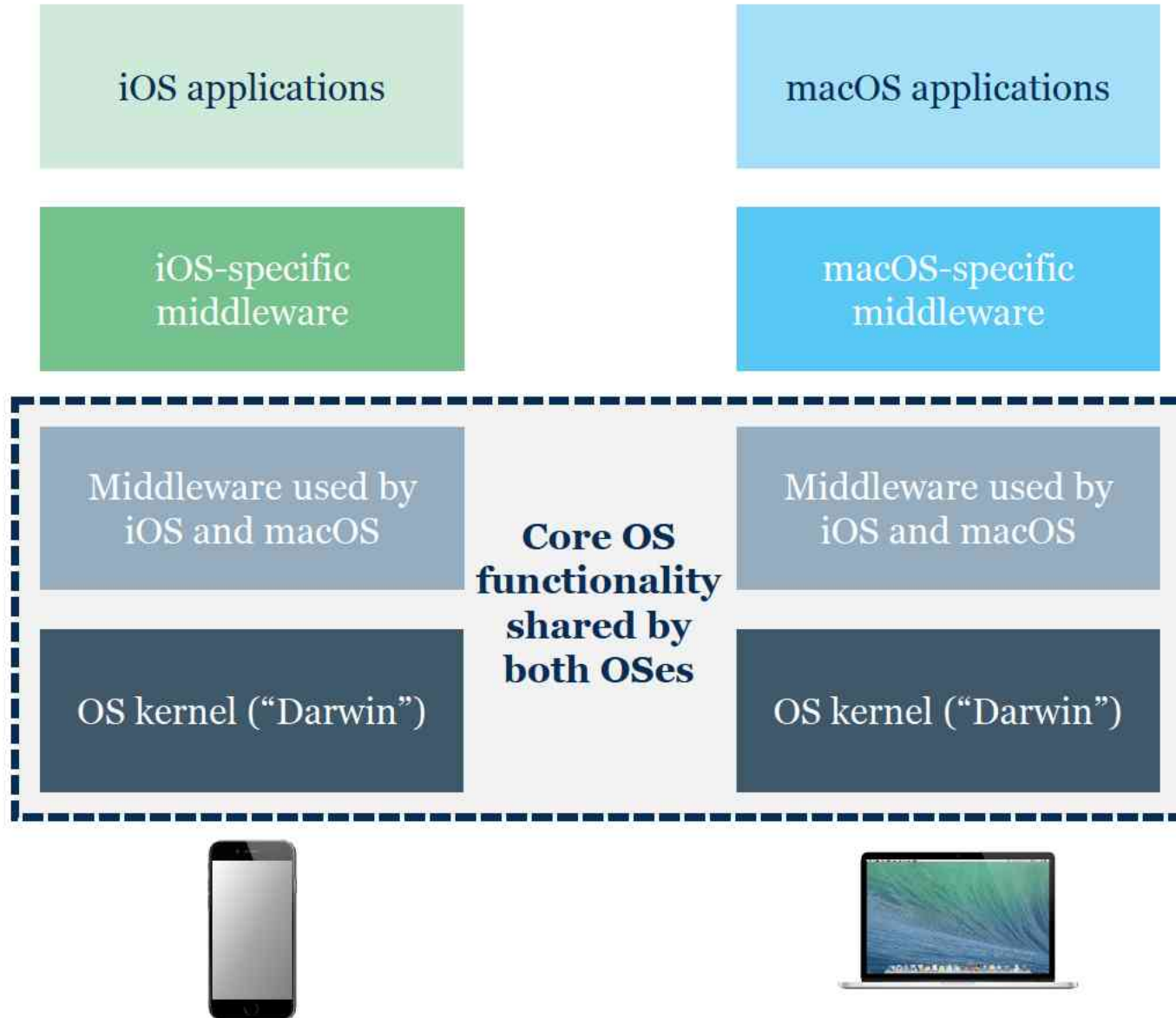
**Mac  
App Store**



**Third Party  
Distribution**  
(Notarization)

**Third Party  
Distribution**  
(unreviewed + unnotarized)

# iOS vs. macOS Software Layers



## Responsible for:

- Providing higher-level "friendlier" mechanisms for users and developers to communicate with hardware
- Customizing core OS-level security features

## Responsible for:

- Implementing the lowest-level (*i.e.*, the most basic) management tasks like resource allocation and application scheduling
- **Enforcing core OS-level security features** (e.g., ASLR, W<sup>X</sup>, etc.) or providing the basic framework for those features (e.g., sandboxing)

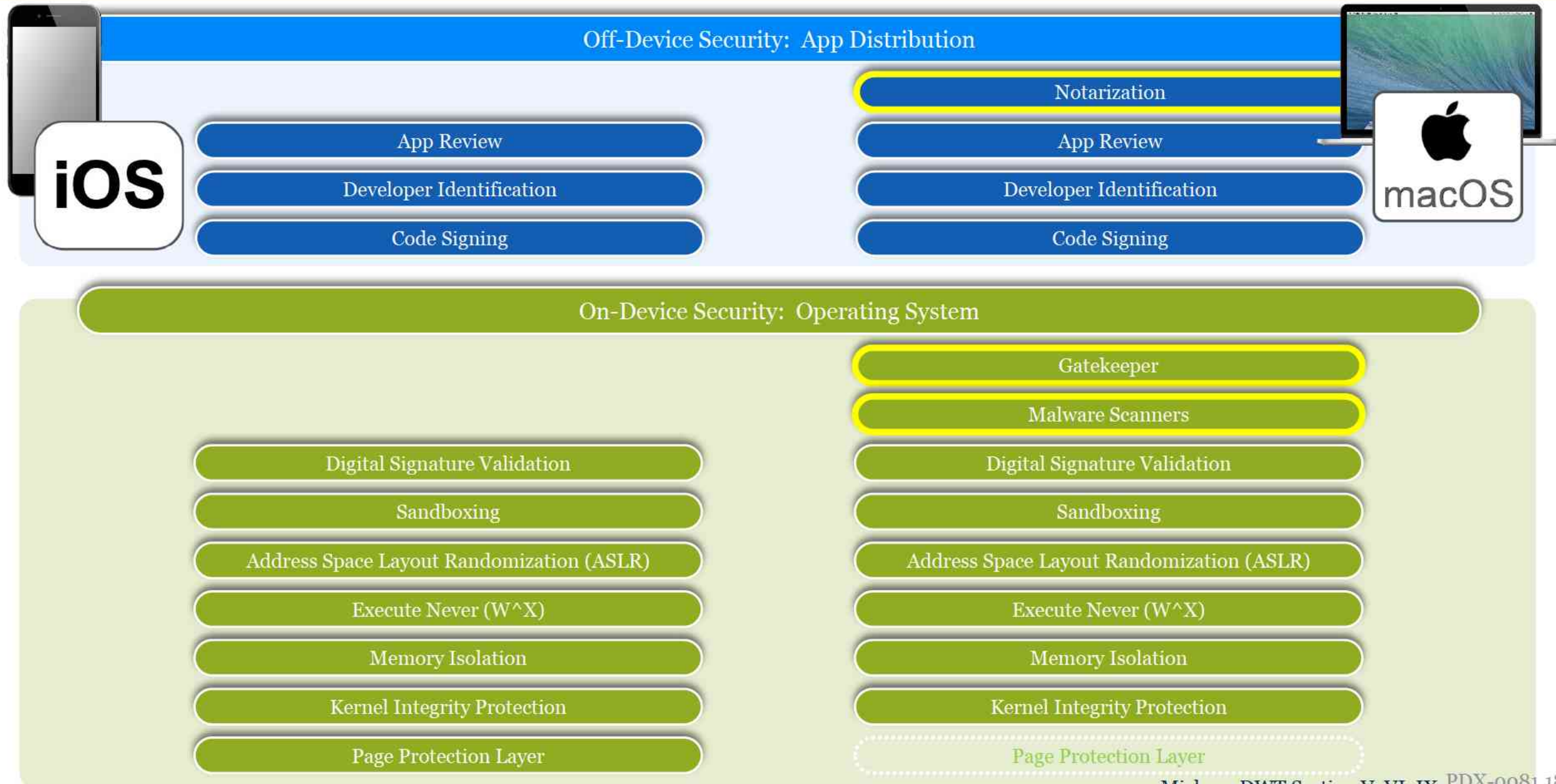


# How is Security Enforced on iOS and macOS?

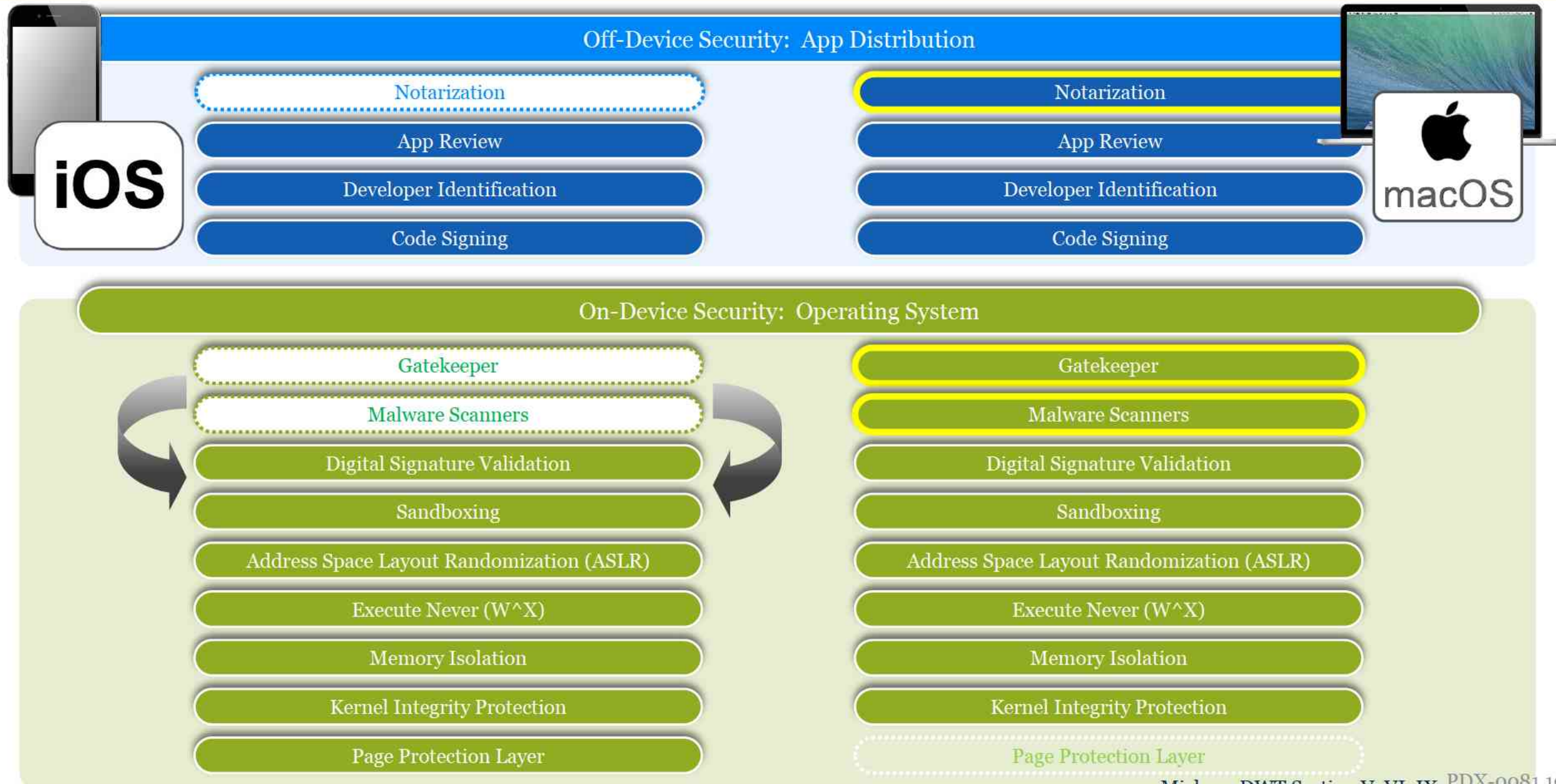






# How is Security Enforced on iOS and macOS?



# How is Security Enforced on iOS and macOS?



# App Distribution: Design Implications

		On-Device OS Security Features	Apps Reviewed by Apple	Apps Signed By:
	App Store	Yes	Yes	Apple
	Developer Enterprise	Yes	No	Enterprise developer
	Internal Apple Testing Distribution	Yes	No	Nobody
	Mac Store	Yes	Yes	Apple
	Notarized	Yes	Yes (malware scan only)	Third-party developer
	Unsigned Third-Party	Yes	No	Third-party developer or nobody