

# Preface

This book is an introduction to the cutting-edge technologies for discovery, diagnosis, and defense of emerging security problems in modern Android applications.

With great power comes great threat. Recently, due to the popularity of Android smartphones, Android apps have attracted varieties of cyber attacks: some involve advanced anti-detection techniques; some exploit “genetic” defects in Android programs; some cover up identity theft with camouflage; some trick end users to fall into a trap using intriguing but misleading language. To defeat malicious attempts, researchers strike back. Many traditional techniques have been studied and practiced: malware classification, taint analysis, access control, etc. Yet, intrusive techniques also advance, and, unfortunately, existing defenses fall short, fundamentally due to the lack of sufficient interpretation of Android application behaviors.

To address this limitation, we look at the problem from a different angle. Android apps, no matter good, bad, or vulnerable, are in fact software programs. Their functionality is concretized through semantically meaningful code and varies under different circumstances. This reveals two essential factors for understanding Android application, semantics and contexts, which, we believe, are also the key to tackle security problems in Android apps. As a result, we have developed a series of semantics and context-aware techniques to fight against Android security threats. We have applied our idea to four significant areas, namely, malware detection, vulnerability patching, privacy leakage mitigation, and misleading app descriptions. This will be elaborated through the whole book.

## Intended Audience

This book is suitable for security professionals and researchers. It will also be useful for graduate students who are interested in mobile application security.

Android Application Security

A Semantics and Context-Aware Approach

Zhang, M.; Yin, H.

2016, XI, 105 p. 37 illus., 29 illus. in color., Softcover

ISBN: 978-3-319-47811-1