Chapter 8
Conclusion

Abstract In this chapter, we conclude our work and summarize this book.

To battle various security threats in Android applications, we propose a semantics and context-aware approach. We argue that such an approach improves the effectiveness Android malware detection and privacy preservation, ameliorates the usability of security-related app descriptions and can solve complex software vulnerabilities in mobile apps. Our argument has been validated via the design, implementation and evaluation of a series of security enhancement techniques.

DroidSIFT demonstrated that semantics-aware Android malware classification not only achieves high detection rate and low false positive and negative rates, but also defeats polymorphic and zero-day malware. Moreover, it is resilient to bytecode-level transformation attacks and outperforms all the existing antivirus detectors with respect to the detection of obfuscated malware.

AppSealer showed that with the analysis of program semantics in advance, the patch of complex application vulnerabilities can be automatically generated. In addition, static program analysis facilitates a selective patch code instrumentation and therefore improves the runtime performance of patched programs.

Capper illustrated that a context-aware privacy policy can effectively differentiate legitimate use of private user data from real privacy leakage, because program context can faithfully reflect the true intention of critical operations.

DESCRIBEME showed that natural language app descriptions, of better readability and higher security sensitivity, are created via program analysis and comprehension of application semantics. Automatically produced descriptions can help users avoid malware and privacy-breaching apps.

M. Zhang, H. Yin, *Android Application Security*, SpringerBriefs in Computer Science, DOI 10.1007/978-3-319-47812-8_8