Contact details for orders and requests:
Telephone number: +380966852884
E-mail: sales@pakurity.com
Website: https://pakurity.com/

Training course "Secure software development for Android and iOS technology stacks"

Version: 2021-07-06
Author: Glib Pakharenko
Duration: 2 days

The "Secure software development for Android and iOS technology stacks" training allows participants to gain a wide set of knowledge on secure development best practices in general and, in particular, best practices for iOS and Android platforms. They will learn how to identify and examine security bugs for both platforms, the ways of their avoidance. They will gain all required skills to face the most difficult problems, which include:

- enhancement of applications security
- detection and mitigation of security bugs
- implementation and/or improvement of secure development process.

The training course includes practical individual and group studies that will allow the participants to apply the acquired knowledge immediately. The training is adapted for an audience with various levels of initial knowledge. The obtained experience will increase the maturity of secure development process, improve the quality of the products' development from the point of their security.

The training course is designed for:

- software architects
- software developers
- software testers.

Course syllabus: "Secure software development for Android and iOS technology stacks"

1. **General topics**
   - 1.1. Rooting danger (iOS and Android)
   - 1.2. Obfuscation
   - 1.3. Social engineering
   - 1.4. Privacy
   - 1.5. Unofficial markets
2. **Classic memory corruption and cryptography vulnerabilities**
   - 2.1. Architecture of PC and mobile devices. x86, x64 and ARM
   - 2.2. Buffer overflow
   - 2.3. Format string attacks
   - 2.4. Integer overflows
   - 2.5. Heap overflow
   - 2.6. Return oriented programming
   - 2.7. Defences: stack canaries, DEP, ASLR
   - 2.8. Unsafe deserialization CVE-2008-5353
   - 2.9. Unsafe reflection CVE-2004-2331
   - 2.10. Unsafe inner classes
   - 2.11. Thread safety and race conditions
   - 2.12. Insecure cryptography
   - 2.13. Password security
   - 2.14. Certificate PINNING
   - 2.15. Improper error handling
   - 2.16. Insecure components
   - 2.17. Metadata leak
   - 2.18. Backup files
3. **Android specifics**
   - 3.1. Android security architecture

This syllabus can be modified according to the needs of the company/organisation.

3.2. SELinux
3.3. Android permissions
3.4. Unix security (process, user, filesystem)
3.5. Dalvik
3.6. ART
3.7. Dex file format
3.8. SQL injection for content providers
3.9. Activity hijacking
3.10. Broadcast Theft
3.11. Service hijacking
3.12. Broadcast injection
3.13. Insecure pending intents
3.14. Dos null check
3.15. Intent injection
3.16. Log injection
3.17. Weak randomness generators
3.18. OWASP TOP10 mobile risks for Android

4. iOS specifics

4.1. iOS security architecture
4.2. IOS Secure Coding guide
4.3. iOS sandbox
4.4. iOS permissions
4.5. iOS DRM
4.6. UIWebView risks
4.7. Mach file format
4.8. Keyboard caching
4.9. Insecure URL handlers
4.10. SQL injections
4.11. Keychain
4.12. UDID leaks
4.13. OWASP top 10 mobile risks for iOS.