Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer
AISEC

Ausschreibung: HiWi

Hardening Android

Memory errors, such as buffer overflows or use-after-free errors, are vulnerabilities in unsafe programming languages (e.g. C or C++) which are commonly used as starting point for exploiting Android smartphones. Simple code injection on the stack, Return-oriented Programming (ROP) and information leaks are examples of exploits enabled by memory errors.

To secure systems and programs against those attacks, many different defensive strategies have been proposed. Some of those techniques, such as Data Execution Prevention (DEP), Stack Canaries and Address Space Layout Randomization (ASLR), are widely adopted in Android and other OSs. The adoption of other defensive mechanisms, such as memory safety extensions for C and C++, is hindered by their performance penalty.

In this work, different compiler-based security mechanisms should be tested for their applicability in hardening the Android smartphone OS regardless of their perfomance impact.

Requirements

- Ability to work independently and accurately
- Good C programming skills
- Basic knowledge of exploit techniques, ARM assembly and Linux
- Interest in advanced exploit techniques, defensive strategies and ARM architecture
- Interest in compiler development, especially LLVM

Kontakt

Julian Horsch
Telefon: +49 89 322-9986-155
E-Mail: julian.horsch@aisec.fraunhofer.de

Sascha Wessel
Telefon: +49 89 322-9986-118
E-Mail: sascha.wessel@aisec.fraunhofer.de

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)
Lichtenbergstr. 11, 85748 Garching (near Munich), Germany
http://www.aisec.fraunhofer.de