11. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 25.06.2015
Abgabe 02.07.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1. (Rainbow Tables)

Erläutern Sie das Grundprinzip von Rainbow Tables[1]. Beantworten Sie dabei insb. die folgenden beiden Fragen

- Was bedeutet in diesem Zusammenhang Time-Memory-Tradeoff?
- Ab welcher Passwortlänge lohnt sich der Einsatz dieses Verfahrens?

Durch welche Maßnahmen könnte man die Sicherheit auch für kleine Passwörter (z.B. 4-stellige nummerische PINs) deutlich erhöhen?

Aufgabe 2. (Android-Sicherheit)

Welche aktuellen Möglichkeiten existieren, ein Android-Smartphone zu rooten. Geben Sie Verfahren an, die es einem Angreifer erlauben, einen Nutzer unwissentlich dazu zu bringen, sein Android-Smartphone zu rooten.

Aufgabe 3. (Overflow)

Bufferoverflows können verwendet werden, um den Programmfluss illegitim zu beeinflussen. Welche Gegenmaßnahmen muss

[1] `http://kestas.kuliukas.com/RainbowTables/`

(*a*) der Programmierer,

(*b*) ein Compiler (z.B. gcc) und

(*c*) ein modernes Betriebssystem (z.B. Linux)

ergreifen, um das Ausnutzen von Bufferoverflows zu verhinden?

Aufgabe 4. (ROP)

In modernen Betriebssystemen wird das Einschmuggeln von Sourcecode dadurch verhindert, dass *writeable* markierte Speichersegmente niemals als *executeable* markiert werden. Um trotzdem eigene (schädliche) Programmabläufe zu generieren wird *return oriented programming* benutzt. Erläutern Sie diese Angriffsmethode.