7. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 28.05.2015
Abgabe 04.06.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1. (Seed-Generierung)

Auf Seite 56/57 der Vorlesungsmitschrift ist ein Verfahren zur Seed-Generierung unter Windows angegeben. Zeigen Sie, dass die dort genutzten Werte unabhängig voneinander sind. Warum ist dies wichtig?

Aufgabe 2. (Deterministische Zufallszahlengeneratoren)

Zeigen Sie, dass die in der Vorlesung kennen gelernten Pseudozufallszahlengeneratoren basierend

(*a*) auf kryptographischen Hashfunktionen

(*b*) auf Blockchiffren im Counter-Mode

die Sicherheitsforderung Nichtberechenbarkeit von Vorgänger und Nachfolger aus Teilen der Zufallsfolge umsetzen.

Aufgabe 3. (Instanzauthentisierung)

Untersuchen Sie die in der Vorlesung kennengelernten Instanzauthentisierungsverfahren

- Passwortlisten

- Zeitgesteuerte Passwortgeneratoren
- Ereignisgesteuerte Passwortgeneratoren (siehe VL-Mitschrift)
- Challenge Response Passwortgeneratoren

hinsichtlich ihrer Resistenz gegen Phishing, Key-Logging und Replay Attacken.

Aufgabe 4. (Passwörter)

Überlegen Sie sich Verfahren für die Authentisierung basierend auf Passwörtern, die

- resistent gegenüber passiven Angriffen (Abhören der Kommunikationsverbindung)
- resistent gegenüber Man-in-the-Middle-Angriffen

sind.