Prüfung: Software Reverse Engineering
Datum: 07.10.2015
Prüfer: Tilo Müller
Beisitzer: Johannes Götzfried

Die Atmosphäre ist sehr entspannt, beim Reversen muss man nicht sofort auf das gesamte Ergebnis kommen, sondern wird durch die Fragen Schritt für Schritt zur Lösung geführt.

Ergebnis: sehr fair, 1.0, trotz manchen Kleinigkeiten, auf die ich nicht sofort gekommen bin und einem kurzem Blackout bei den Integer Fehlern.

Teil 1: Reversen
-Welche Parameter, was wird zurückgegeben, 32/64 Bit, Basic Blocks einzeichen, etc
-dazwischen immer wieder Fragen: was ist der Unterschied zwischen den zwei 64 Bit Aufrufkonventionen, woran erkennt man, dass rdi ein Parameter ist, woran erkennt man, ob signed oder unsigned etc
-nach und nach C-Code hinschreiben
-es war ein Primzahlentest (optimiert, da keine globalen Variablen und FPO plus red zone)

Teil 2: Grundlagen
-Unterschied div/idiv, wie funktioniert das allgemein, was macht div mit 2 Parametern
-Wie funktioniert die optimierte Division (sar…)

Teil 3: Speicherverwaltung
-wie funktioniert allgemein Real Mode/Protected Mode/Long Mode
-Was ist das Ring Konzept + typische Ring 0 und Ring 3 Befehle nennen
-Wie funktioniert das Berechnen einer Adresse bei Protected Mode genau (hinzeichnen)
-Was ist bei Pages die 4 MB statt 4K groß sind, anders ? (Offset größer + nur ein Lookup)

Teil 4: Explotation
-Beispiele für Integerfehler (Überläufe, Vorzeichenfehler) aus der Vorlesung erklären