michael.engel [☺] hs-coburg.de

Praktikum zur Vorlesung
Malware-Analyse und Reverse Engineering
Sommersemester 2017

Praktikumsaufgabe 8

Besprechung am Donnerstag, 8. Juni 2017

Hinweise: Praktikumsaufgaben müssen in der vorgegebenen Zeit in den eingeteilten Gruppen bearbeitet werden. Die Lösung der Aufgaben wird bewertet, jedes Gruppenmitglied soll Fragen zu den einzelnen Aufgaben beantworten können. Bei Unklarheiten und Rückfragen wird selbstverständlich eine Hilfestellung gegeben.

8.1 Verhaltensanalyse von Programmen

Schreiben Sie ein Programm, um mit Hilfe des Systemaufrufs `ptrace` das Systemaufruf-Verhalten eines gegebenen Programms zu überwachen. Sie können (und sollten) dazu das in Vorlesung 10 vorgestellte Codegerüst für ptrace verwenden.
Ihr Programm soll nun das folgende Muster von Systemaufrufen erkennen und bei Erkennung das untersuchte Programm abbrechen::

- Öffnen einer beliebigen Datei zum Schreiben und
- die geschriebenen Daten enthalten die (ASCII-)Zeichenkette “VIRUS”

Die entsprechend zu beobachtenden Systemaufrufe sind:

- open
- read

Hinweis 1: Zur Implementierung der Analyse könnte sich hier ein *endlicher Automat* gut eignen.
Hinweis 2: Beim Versuch, den an `open` übergebenen Dateinamen sowie die Puffer von `read` und `write` zu lesen, werden Sie auf ein Problem stoßen. Welches Problem taucht auf und warum?

8.2 Parallele Verhaltensanalyse (optional)

Erweitern Sie Ihr Programm, um die folgenden drei Folgen von Systemaufrufen zu erkennen:

1. Öffnen einer beliebigen Datei zum Schreiben, die geschriebenen Daten enthalten die (ASCII-)Zeichenkette “VIRUS”
2. Öffnen der Datei “/etc/passwd” zum Lesen, lesen daraus und folgendes Öffnen einer Datei zum Schreiben
3. Erzeugen von mehr als 5 Kindprozessen oder von Kindprozessen, die *kein* exec ausführen

Achten Sie bei der Überprüfung darauf, dass die Aktionen aus 1.–3. parallel (also auch miteinander verwoben) stattfinden können!