Aufgabe 1.1

Gruppe:  
Dennis Röllke 108 012 233 235  
Jan Kaiser 108 012 211 505  
Phillip Müller 108 012 236 929  
  
Typische Race Condition Attacken nutzen die Time-of-Check, Time-of-Use Lücke aus. Um Zugriff auf eine Datei zu erhalten sind zwei Schritte notwendig. Zunächst werden die Rechte überprüft (TOC), dann wir die Datei ausgeführt (TOU). Aufgrund der zugrundeliegenden Prozessorarchitektur ist es möglich die Taktzyklen abzupassen und einen Eigenen Befehl (Time-of-Attack) nach der Rechte Abfrage (TOC), aber vor der eigentlichen Programmausführung (TOU) einzuschleusen. Besonders Programme mit gesetztem s-Bit sind für diese Angriffe interessant, da sie unabhängig von der realen UID mit superUserID ausgeführt werden.