Analysis and Retrofitting of Security Properties for Proprietary Software Systems

Autor: Ralf Hund

Die vorliegende Dissertation befasst sich mit der Entwicklung neuer Methoden zur Analyse und nachträglichen Erweiterung von Sicherheitseigenschaften von Softwaresystemen. Die Arbeit konzentriert sich dabei auf *proprietäre* Softwareumgebungen in denen kein Quellcode für die relevanten Softwarekomponenten verfügbar ist. Sowohl die Analyse als auch Erweiterung proprietärer Software erfordert die Entwicklung und den Einsatz speziell angepasster und neuartiger Techniken und Werkzeuge. Die Dissertation unterteilt sich in vier Themenbereiche, in denen jeweils unabhängig voneinander die Analyse und/oder Erweiterung bestimmter Softwaresysteme präsentiert wird.

Der erste Themenkomplex umfasst das Reverse Engineering der unbekannten Verschlüsselung des proprietären Satellitentelephonie-Standards GMR-1. Es wird ein generischer Ansatz zur Identifizierung und Extrahierung unbekannter kryptographischer Algorithmen in mobilen Firmware-Images vorgestellt. Anhand der umfassenden Analyse einer konkreten Firmware wird der GMR-A5-1 Verschlüsselungsalgorithmus rekonstruiert. Dieser weist große Ähnlichkeiten zur bekanntermaßen angreifbaren GSM-A5/2 Verschlüsselung auf.

Ein weiterer Beitrag ist die Entwicklung neuartiger timingbasierter Seitenkanalangriffe auf Kernelspace ASLR Implementierungen. Hierfür wurde die proprietäre Implementierung von Windows Betriebssystemen rekonstruiert und es wurden darauf aufbauend drei verschiedene timingbasierte Angriffe entwickelt. Diese erlauben es einem lokalen Angreifer, große Teile des privilegierten Kernelspace Adressraums zu rekonstruieren. Dadurch können ASLR Sicherheitsmechanismen vollständig umgangen werden. Es wird außerdem eine Betriebssystemerweiterung präsentiert, welche die diskutierten Angriffe effektiv verhindert.

Als drittes Thema befasst sich die Arbeit mit dem Entwurf und der Implementierung der Laufzeitkomponenten des Kontrollflussintegrität-Frameworks MoCFI. MoCFI kann beliebige binäre iOS Applikationen gegen Angreifer schützen indem die Ausnutzung von Softwareschwachstellen verhindert wird. Zu diesem Zweck wurden neue Techniken entwickelt um binäre Anwendungen zur Laufzeit effizient und fehlerfrei zu überwachen. Die Evaluation des Frameworks zeigt, dass MoCFI in der Lage ist diverse weitverbreitete iOS Applikationen mit akzeptablen Geschwindigkeitseinbußen zu schützen.

Im letzten Teil der Arbeit wird ein neuer Ansatz zur Identifizierung von bösartigen Command and Control (C&C) Bot-Netzwerkverbindungen vorgestellt. Durch die Kombination von Netzwerk- mit Host-basierten Informationen werden Verhaltensgraphen erzeugt. Diese verbinden die Systemaktivität eines Bots mit generierten Netzwerkpaketen indem die proprietäre, native Windows-API überwacht wird. In der Evaluation kann gezeigt werden, dass dieser neuartige Ansatz eine effektive Unterscheidung zwischen bösartigen C&C und gutartigen Verbindungen ermöglicht.