MALFLARE – VEREINIGUNG VON DYNAMISCHER UND STATISCHER CODEANALYSE

Malflare ist ein Plugin für den wohl bekanntesten Disassembler IDA Pro. Mit diesem Plugin wird der Funktionsumfang von IDA mit Daten aus der dynamischen Codeanalyse erweitert. Dabei können neue Zusammenhänge gesehen werden und neue Funktionen realisiert werden. Die gefundene Kombination der Analysetechniken vermag die Nachteile der jeweiligen aufzuheben und die Codeanalyse zu vereinfachen.

Realisierung: Die statische Codeanalyse in IDA wird mit Daten aus der dynamischen Codeanalyse erweitert. Die dynamischen Daten sind dabei Speicher-, Register- und Stack-Werte. Diese werden im Assembly annotiert und mit weiteren Funktionalitäten, die auf die Daten angewendet werden können, ergänzt. Die dynamischen Daten werden dazu in einer abgesicherten VM mit Hilfe des TEMU-Frameworks aufgezeichnet und in Form eines Tracefiles transportiert. Damit kann die Sicherheit gewährleistet werden und das System innert Sekunden auf den Ursprungszustand zurückgesetzt werden.

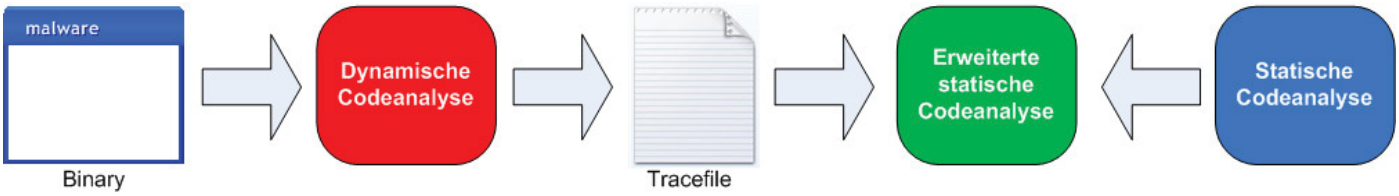

Abbildung 1: Systemübersicht

Dynamische Codeanalyse

Features

- Sichere Umgebung (VM)
- Generisches Tracefile Format
- Speicherabbild aufzeichnen
- Speicheränderungen aufzeichnen
- Initiale Registerwerte aufzeichnen
- Registeränderungen aufzeichnen

Verwendete Komponenten

- TEMU Version 1.00

Entwicklungswerkzeuge

- Eclipse Helios / CDT

Erweiterte statische Codeanalyse

Features

- Pseudo Debugger
- Pfad einfärben
- Registeränderungen annotieren
- Speicher Rekonstruktion
- Call Interpretation
- Loop Detektion

Verwendete Komponenten

- IDA Pro Version 6.1
- IDA Pro SDK Version 6.1

Entwicklungswerkzeuge

- Eclipse Helios / CDT