

Sichere Ausführung von Untrusted Code

Evaluation verschiedener Ansätze und Einsatz an vier Fallbeispielen

Material verfügbar unter: <http://myhpi.de/~nicolai/>

Gliederung

1. Statische vs. dynamische Analyse
2. Erfolgskriterien für statische Quellcodeanalyse
3. Übertragung auf C / C++
4. Erfolgskriterien für dynamische Analyse
5. Klassifikation / Evaluation dynamischer Ansätze
6. Sichere faire Ausführung für RealTimeBattle
7. Sicheres und faires Benchmark in Asparagus
8. DCL
9. Übungsbetrieb BSA

Kriterien für den Erfolg statischer Analyse

1. Verfügbarkeit des Quellcodes
2. Unterstützung der Programmiersprache
3. Unterstützung von “echten” Programmen (COTS)
4. Bewältigung der auftretenden Komplexität
5. Schutz vor bösartiger Speicheranipulation
6. Garantie für die Prozessumgebung

Kriterien für den Erfolg dynamischer Analyse

1. Änderbarkeit / Verfügbarkeit des Binär-codes
2. Unterstützung der Plattform / Hardwarearchitektur
3. Unterstützung von "echten" Programmen (COTS)
4. Übersicht über den Betriebssystemzustand
5. Schutz vor bösartiger Speicher-manipulation
6. Garantie für die Prozessumgebung

Auswertung dynamischer Ansätze

<i>Methoden/ Kriterium</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>
Quellcode-Substitution	notwendig	nicht relevant	erfüllt	nicht erfüllt	erfüllt	nicht erfüllt
Binär-code-Modifikation	nicht relevant	notwendig	erfüllt	kaum erfüllt	erfüllt	nicht erfüllt
Maschinen-code-Interpreter	nicht relevant	notwendig	erfüllt	schwer zu erfüllen	erfüllt	nicht erfüllt
IDS-Systeme	nicht relevant	nicht relevant	nicht relevant	nicht erfüllt	nicht erfüllt	nicht erfüllt
Härtungs-Mechanismen	nicht relevant	notwendig	erfüllt	nicht erfüllt	erfüllt	nicht erfüllt
Interpreter-Sprachen	nicht relevant	nicht relevant	teilweise erfüllt	kann erfüllt sein	erfüllt	nicht erfüllt
System Call-Interposition	nicht notwendig	notwendig	erfüllt	erfüllt	nicht notwendig	erfüllt
herkömmliche Betriebssystemmittel	nicht notwendig	notwendig	erfüllt	erfüllt	nicht notwendig	teilweise erfüllt
DTE / MACL-Systeme	nicht notwendig	notwendig	erfüllt	erfüllt	nicht notwendig	erfüllt