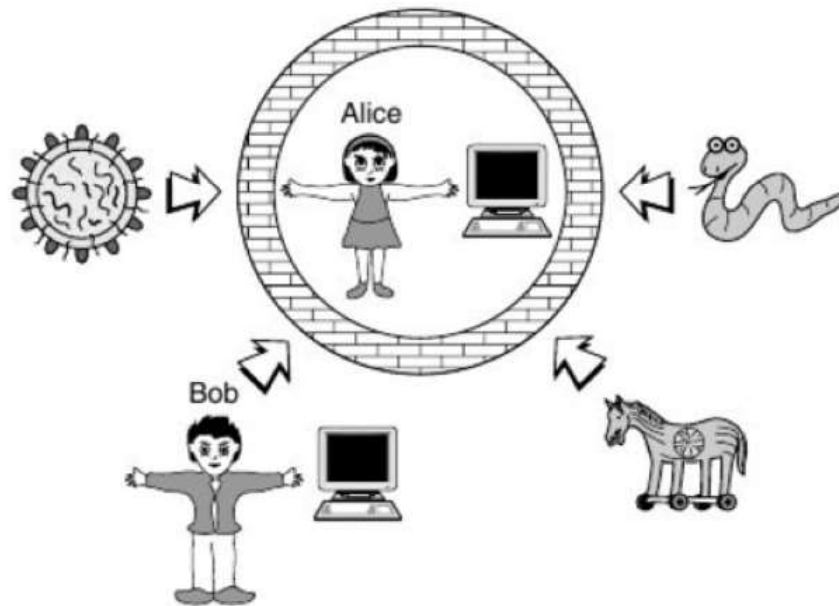


CD-Labor AsTra – Schutz von Software in kritischen Systemen

Dr. Sebastian Schrittwieser

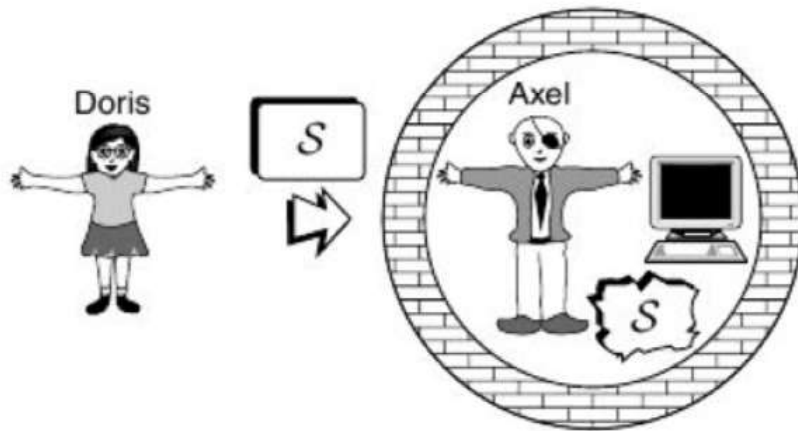


Was ist Softwareschutz?



Quelle: Surreptitious Software, J. Nagra und C. Collberg

Was ist Softwareschutz?



Quelle: Surreptitious Software, J. Nagra und C. Collberg

Relevanz

- Software begleitet uns in nahezu allen Aspekten unseres Alltags
 - Korrektheit von Software ist entscheidend für den unterbrechungsfreien Ablauf von Prozessen des täglichen Lebens
 - Zunehmend starke Safety-Relevanz (z.B. selbstfahrende Autos)
- Softwareschutz
 - Softwarehersteller sind am Schutz ihrer Software vor Analyse und unsachgemäßer Nutzung interessiert
 - Böartige Codemodifikationen müssen wirkungsvoll unterbunden werden
 - Hohe Relevanz für kritische Systeme

Softwareschutz

Analyse

Code Obfuscation

Absichtliche Erhöhung der Komplexität von Programmcode

Modifikation

Software Tamperproofing

Hinzufügen von Programmlogik, welche Code-Modifikationen erkennt

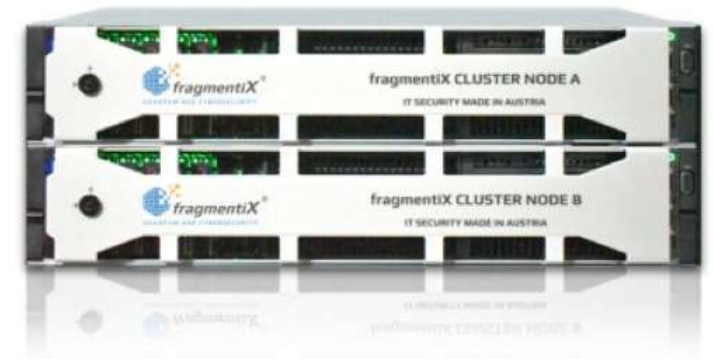
Unerwünschte Nutzung

Hardware-Software Binding

Kopplung der Ausführbarkeit eines Programms an eine bestimmte Hardwareinstanz

Christian Doppler Labor AsTra

- Sicherheit und Transparenz im Softwareschutz
- Softwareschutz verändert den Programmcode auf syntaktischer Ebene
 - Softwareschutz darf keine unbeabsichtigten semantischen Veränderungen bewirken
- Laufzeit: 2024 – 2031
- Firmenpartner
 - fragmentiX Storage Solutions GmbH



Schutztechnik
Neuanordnung

P

```
1 define i32 @src(i32) {  
2   %a = add i32 5, 0  
3   %b = add i32 3, 0  
4  
5   %result = mul i32 %a, %b  
6  
7   ret i32 %result  
8 }
```



P'

```
1 define i32 @tgt(i32) {  
2   %b = add i32 3, 0  
3   %a = add i32 5, 0  
4  
5   %result = mul i32 %b, %a  
6  
7   ret i32 %result  
8 }
```

Translation validation

(Pnueli et al. "Translation validation." Proceedings of the 4th TACAS 1998)

P' ist ein *refinement* von P

Vielen Dank für Ihre Aufmerksamkeit!

sebastian.schrittwieser@univie.ac.at · <https://cdl-astra.at>
