

# Rootkits 2008

### Inhalt

- Was ist ein Rootkit?
- Unterschied zwischen Viren, Exploits und Rootkits
- Techniken von Rootkits
- Zukunft von Rootkits

### Was ist ein Rootkit?

Ein Rootkit ist ein Sammlung von Programmen und Code, welche die permanente und unentdeckten Anwesenheit auf einem Computer erlauben (Greg Huglund und James Butler)

Nicht nur für „böartige“ Anwendungen sondern auch für „Nützliche“ (Zweck des Rootkits?):

- Überwachung der Verwendung von Computer
- und der damit verbundenen Durchsetzung von Firmen Policies
- z.B. Kopierschutz (Sony)
- ...

## Unterschied zwischen Viren, Exploits und Rootkits

### Viren

- Nicht kontrollierte, selbständige Verteilung
- Laut und außer Kontrolle

### Exploits

- Softwarefehler nutzen (z.B. Buffer Overflow)

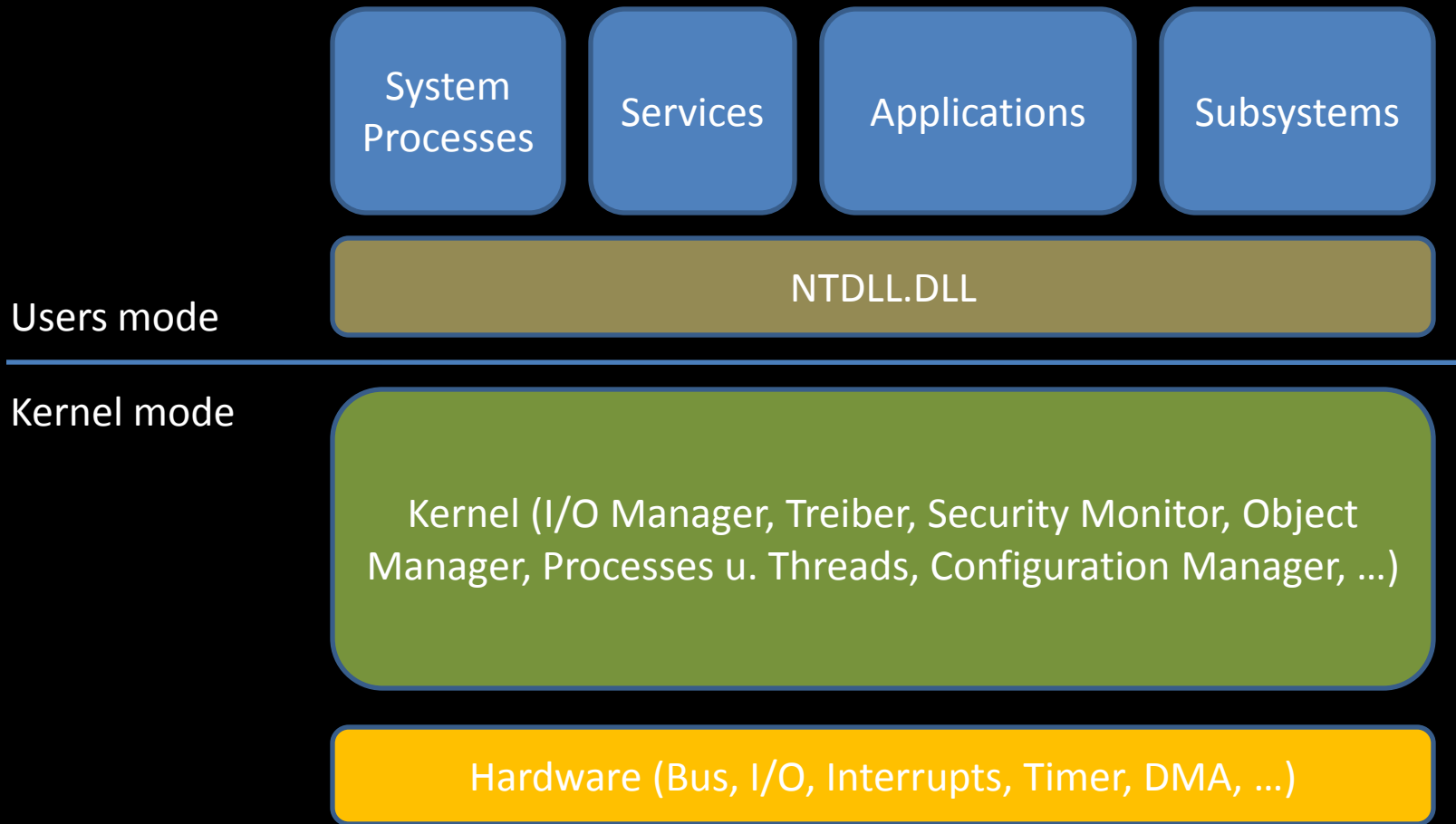
### Rootkits

- Unauffindbar (Stealth)
- Zugriff auf einen bestimmten Computer erhalten
- möglicherweise Nutzung nicht dokumentierter Funktionen und Methoden des OS

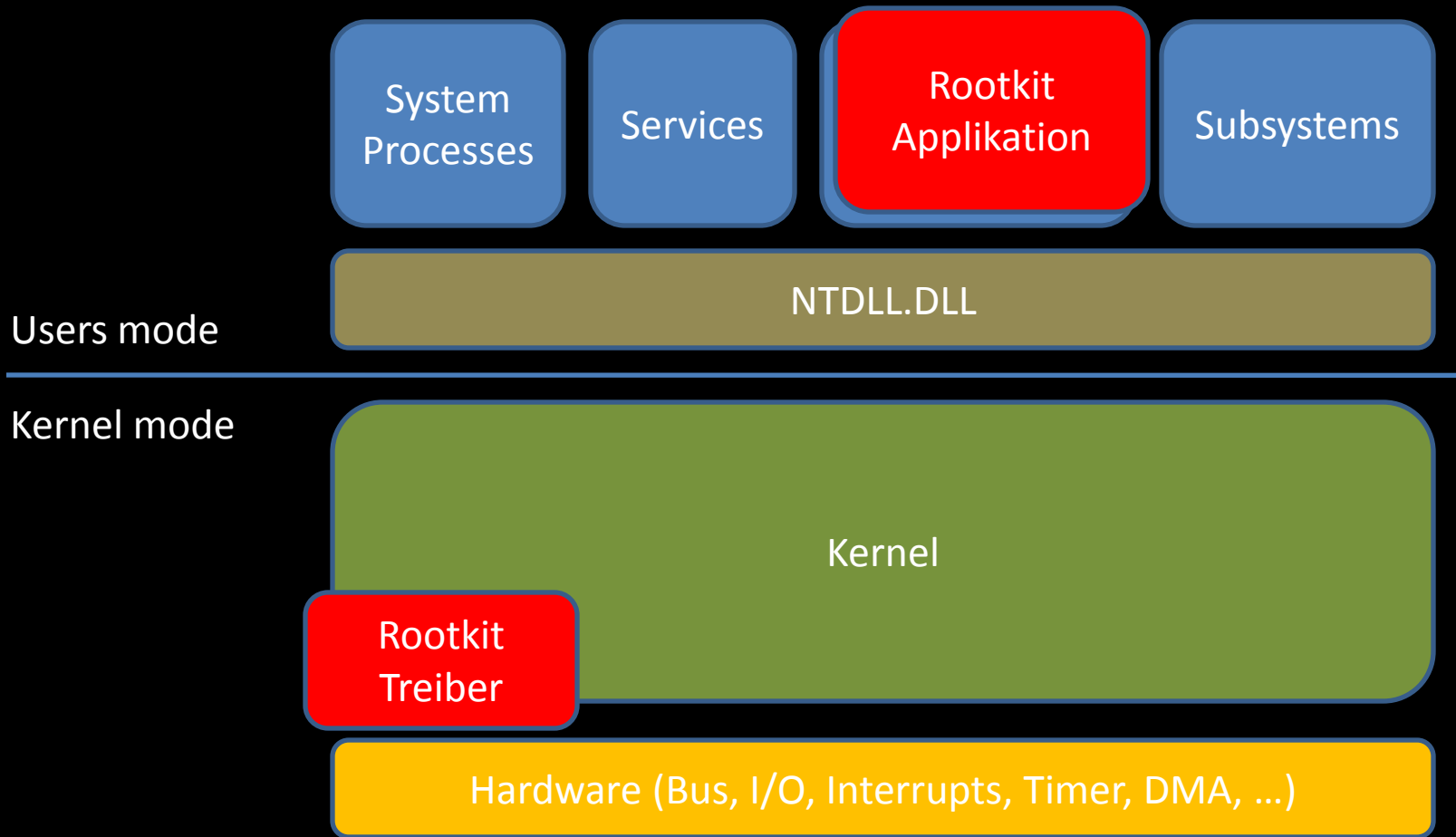
- Techniken von Rootkits

- Ersetzen von Applikationen (Unix: ls, ps, ...; Windows: dir, loader, ...)
- Modifikation von Daten auf der Festplatte (z.B. Pagefile, Programme, ...)
- Modifikation von Daten im Speicher zur Laufzeit (z.B. Kernel Strukturen)
- Modifikation von Hardware Firmware
  
- In modernen OS sind dafür spez. Rechte notwendig (root, Administrator)
- Modifikation oft nur durch Code im Kernel-space möglich → Rootkit muss einen Teil als Treiber laden um nötige Modifikationen durchführen zu können
- In Windows Vista können nur signierte Treiber geladen werden

## • Techniken von Rootkits



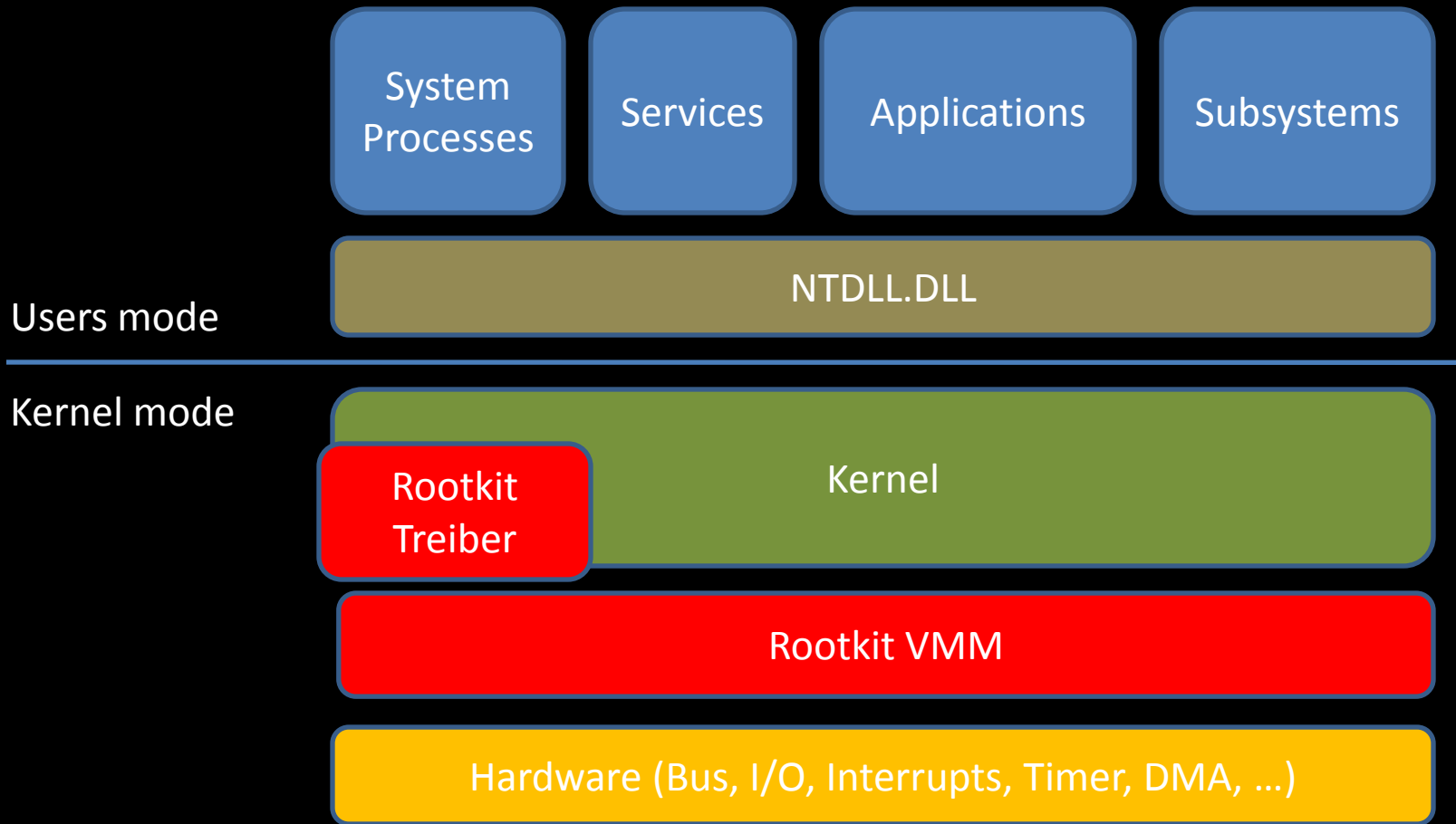
## • Techniken von Rootkits



## Zukunft von Rootkits

- Neue Stealth Techniken ← Reverse Engineering (nicht dokumentierte Funktionen und Strukturen des OS)
- Umgehen neuer OS Sicherheitsfeatures (Windows Vista)
- Virtualisierung

- Virtualisierung



### Referenzen

- Microsoft Windows Internals (4th Edition) - Mark E. Russinovich and David A. Solomon
- Rootkits – Subverting the Windows Kernel - Greg Hoglund and James Butler
- Professional Rootkits - Ric Vieler
- Bluepillproject - <http://bluepillproject.org/> - Joanna Rutkowska and Alexander Tereshkin
- <http://invisiblethings.org> – Joanna Rutkowska
- <http://www.rootkit.com/> - Greg Hoglund