WEF - Web Exploit Finder

Benjamin Mack – Thomas Müller – Mehmet Arziman
Hochschule der Medien, Stuttgart

June 2006

Agenda

1. Motivation
2. System Overview
3. Browser Control
4. VMware Control
5. Management Console
6. Windows Rootkit

The Problem

- All Web-Browsers have vulnerabilities
- They allow to infect the OS without user interaction (Drive-By-Downloads)
- Users don't install security updates
- Even fully patched systems are vulnerable to zero-day exploits
- Unkown amount of malicious sites on the web

Detect Malicious Sites

- Malicious sites have to alter the windows operating system
  - download additional files to the hard drive
  - add or modify registry entries
  - start new processes
- Two different approaches
  - Check for new and altered files and keys after visiting a page (Honey-Client)
  - Monitor all suspicious actions in real time

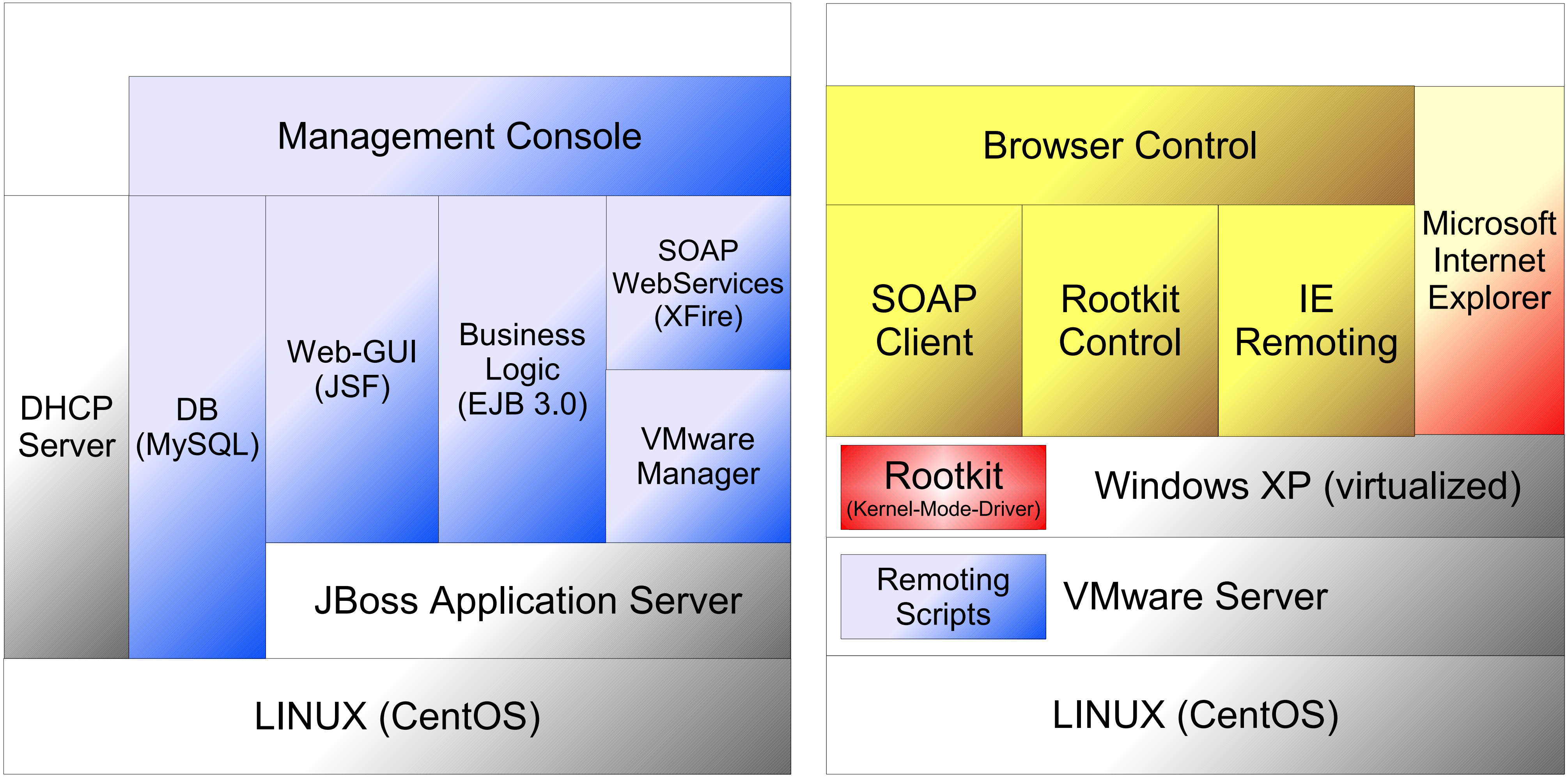
Project Goals

- Build a Distributed System to identify malicious sites

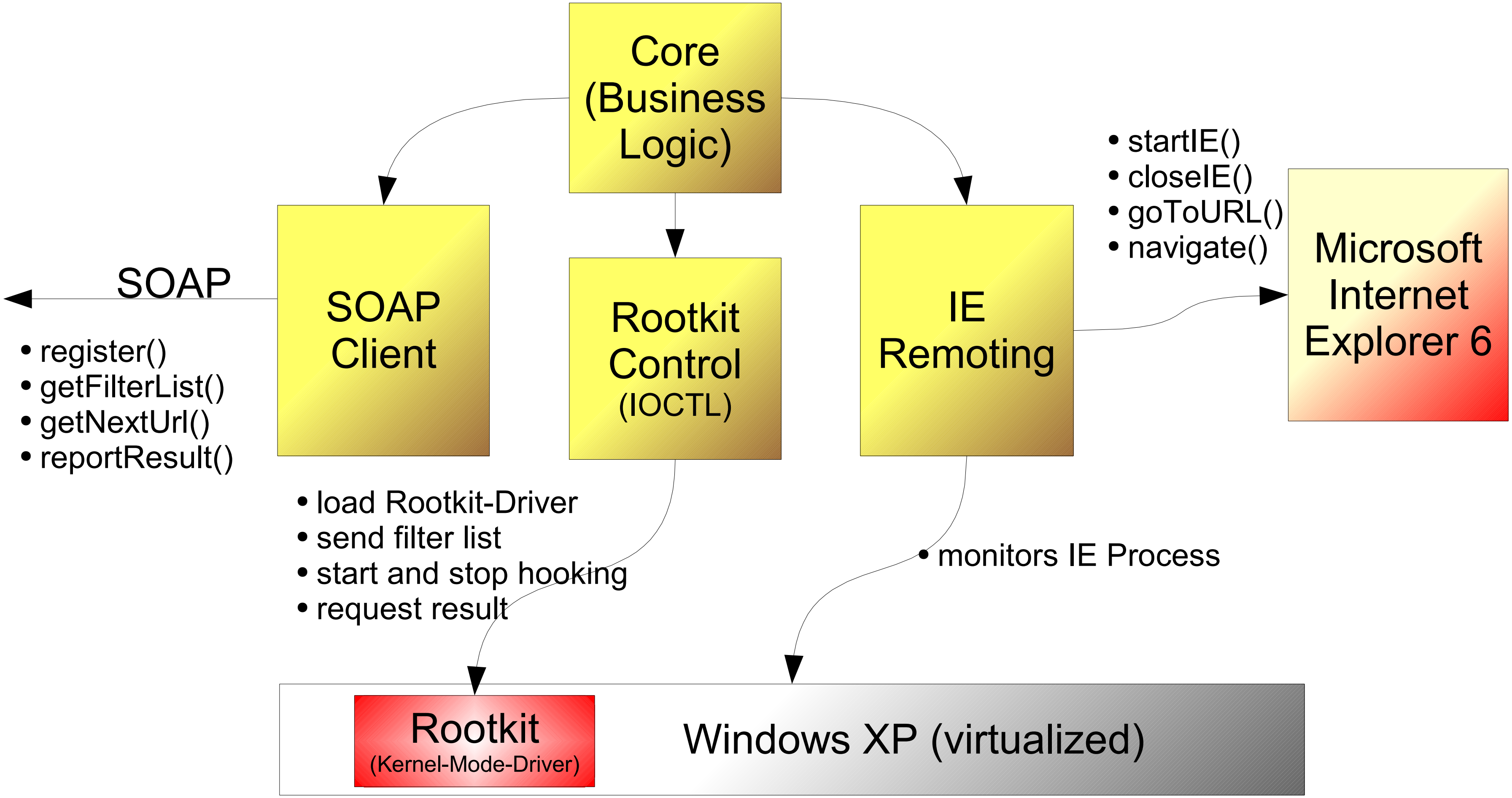
  We need to...

  - Modify the windows kernel to monitor suspicious system calls
  - Remote control Microsoft's Internet Explorer
  - Technology to protect ourselves
  - Component to easily control the whole system

System Overview



Browser Control



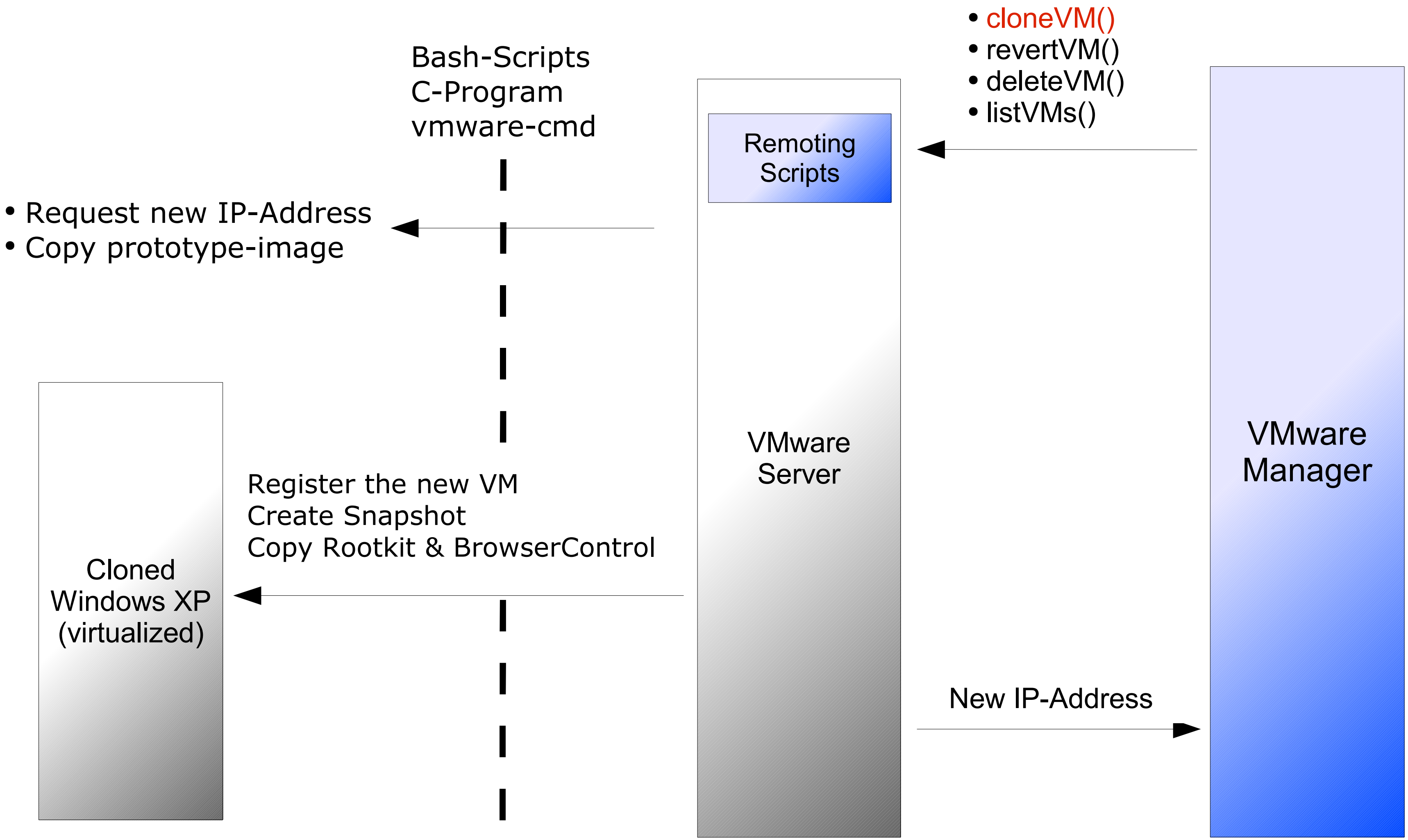
- startIE()
- closeIE()
- goToURL()
- navigate()

- register()
- getFilterList()
- getNextUrl()
- reportResult()

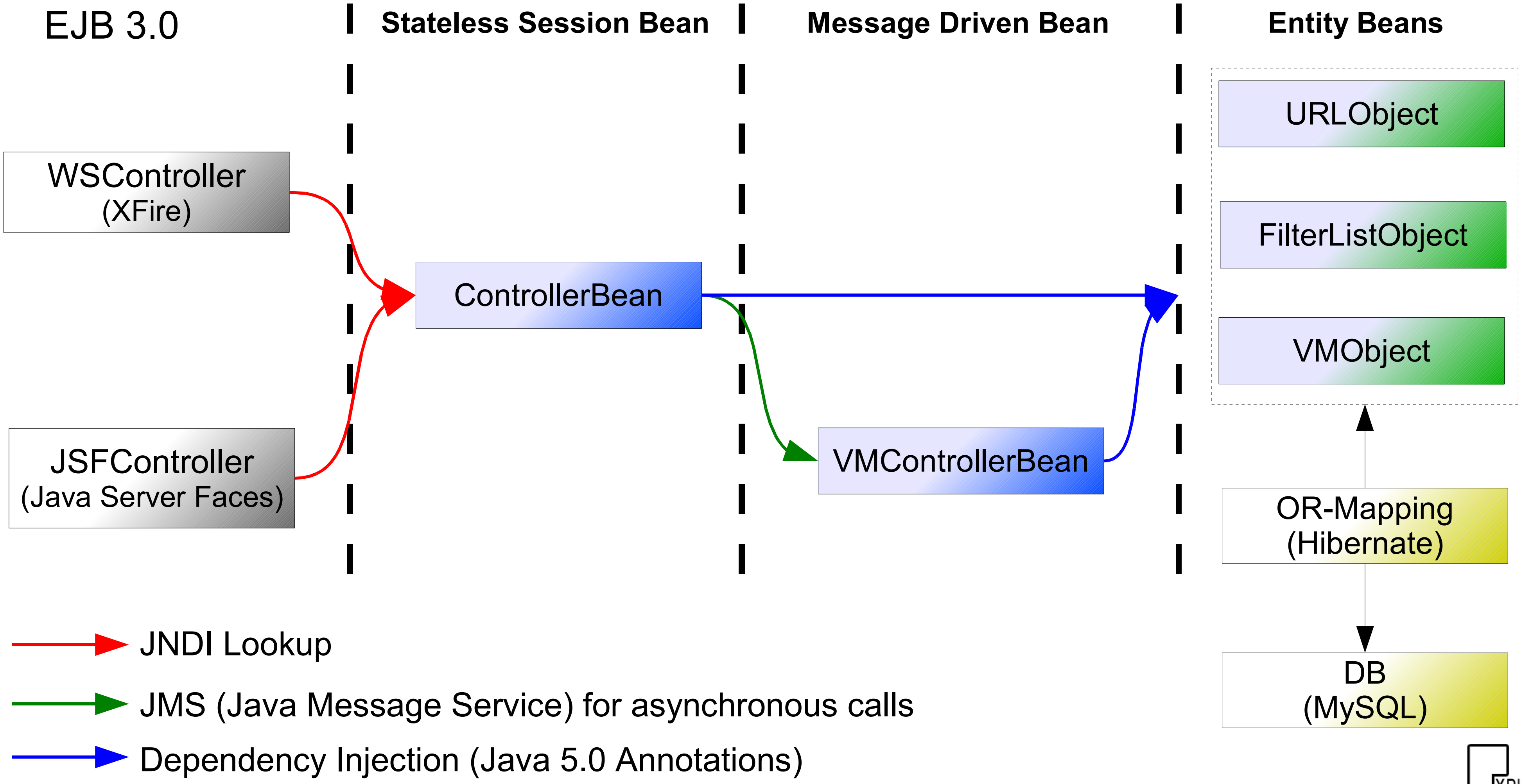
- load Rootkit-Driver
- send filter list
- start and stop hooking
- request result

- monitors IE Process

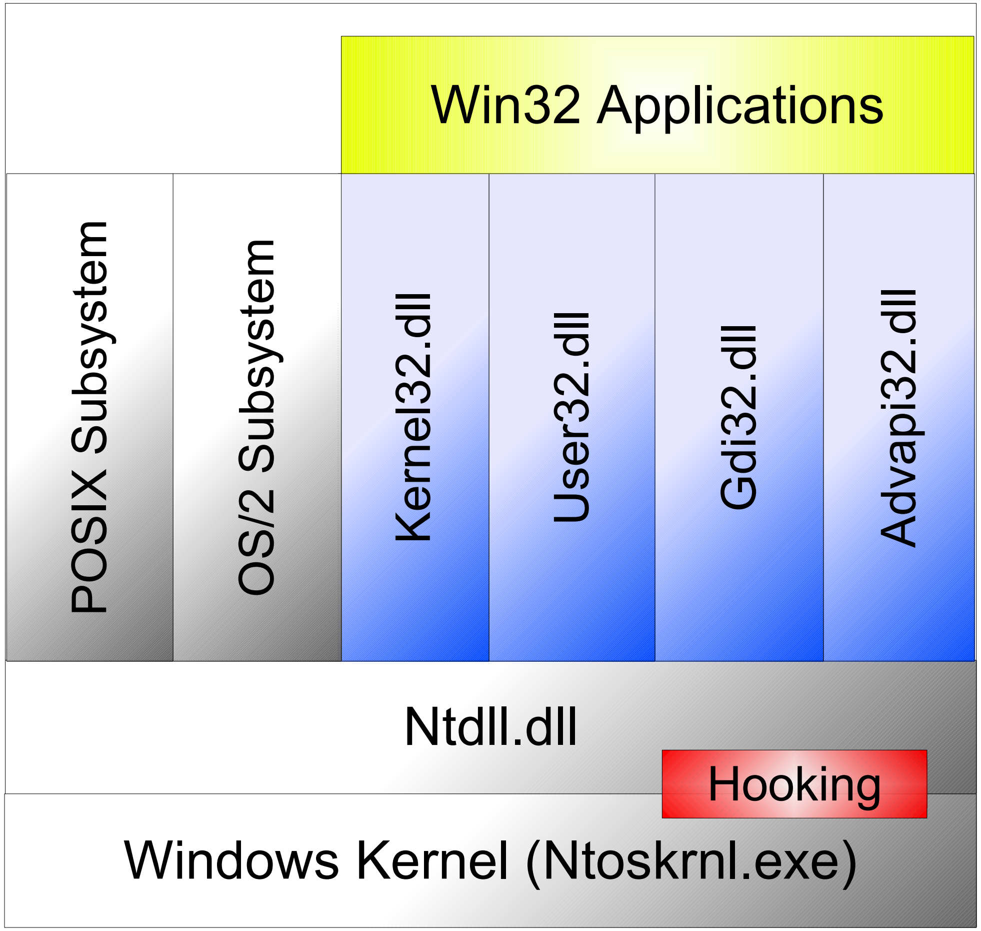
VMware Control



Management Console



The Windows API



Win32 Applications

POSIX Subsystem

OS/2 Subsystem

Kernel32.dll

User32.dll

Gdi32.dll

Advapi32.dll

Ntdll.dll

Hooking

Windows Kernel (Ntoskrnl.exe)

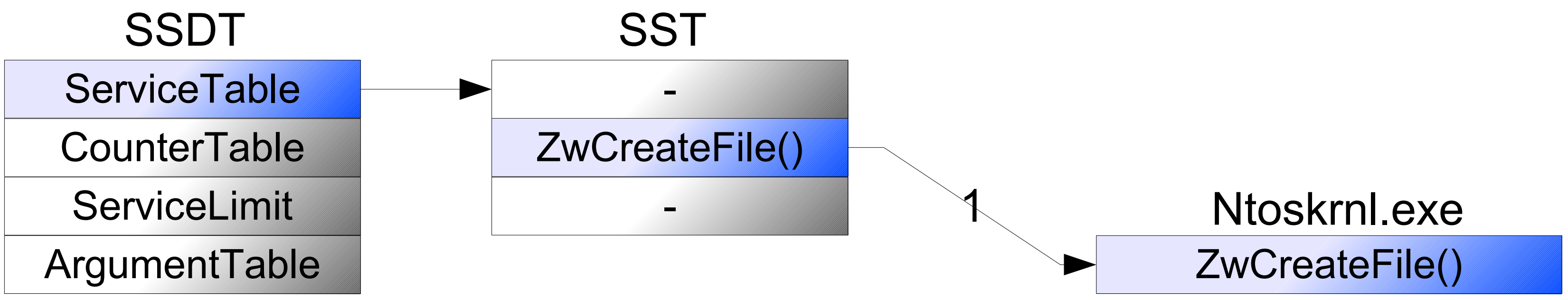
Application call CreateFile()

Dispatcher-Stubs **Nt**CreateFile() Method

Real Implementation **Zw**CreateFile() Method

Windows Kernel Rootkit

Before:



SSDT

ServiceTable

CounterTable

ServiceLimit

ArgumentTable

SST

-

ZwCreateFile()

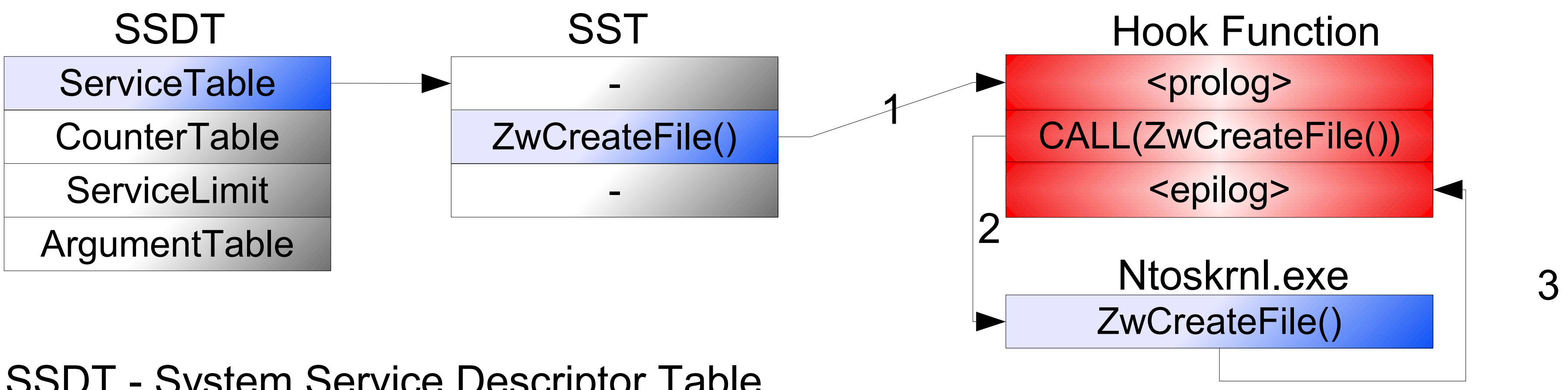
-

1

Ntoskrnl.exe

ZwCreateFile()

After:



SSDT

ServiceTable

CounterTable

ServiceLimit

ArgumentTable

SST

-

ZwCreateFile()

-

1

Hook Function

<prolog>

CALL(ZwCreateFile())

<epilog>

2

Ntoskrnl.exe

ZwCreateFile()

3

SSDT - System Service Descriptor Table

SST – System Service Table

Open Tasks

- Use Web-Crawler to find more URLs
- Monitor more system calls
- Add Regular Expressions functionality
- Support for Firefox and Opera
- Let web-users enter URLs
- Send malicuous URLs to Blacklists

Questions ?