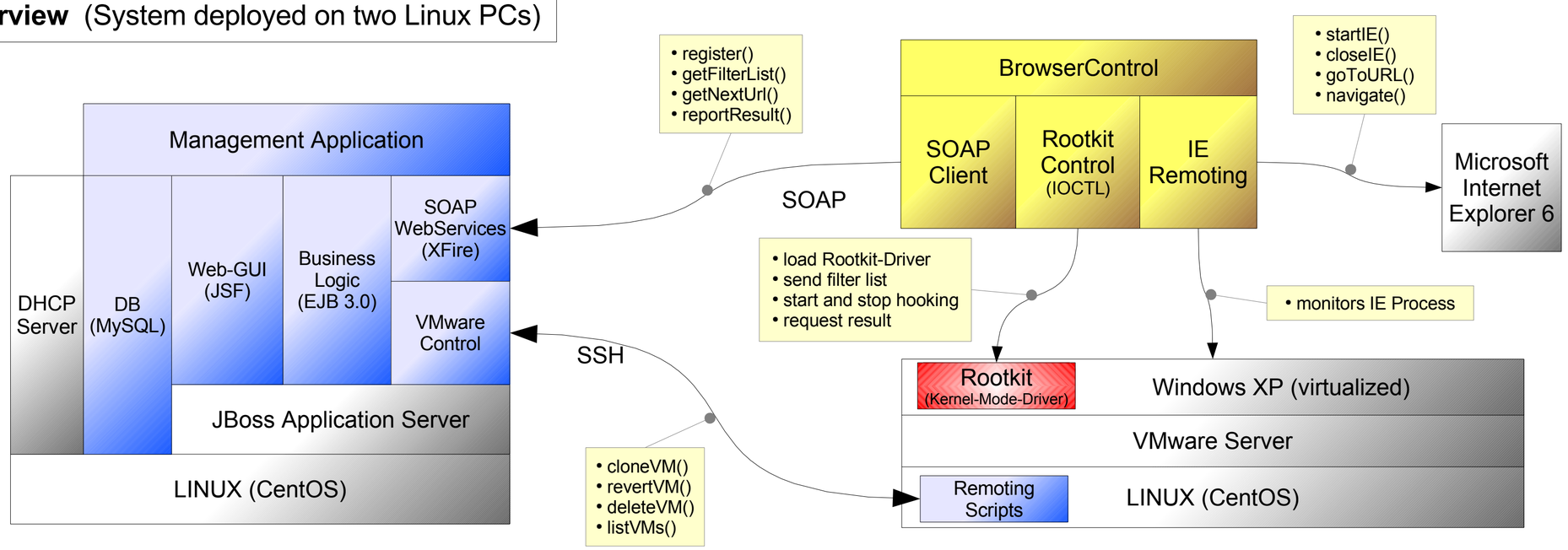
WEF – Web Exploit Finder

Detecting Drive-By-Downloads using VMware and Rootkit-Technologies

Thomas Müller, Benjamin Mack, Mehmet Arziman - Hochschule der Medien (HdM), Stuttgart

Rootkit
Management
BrowserControl

Architecture Overview (System deployed on two Linux PCs)



Abstract

- All Web-Browsers have vulnerabilities and allow to infect the OS without user interaction (Drive-By-Downloads)
- Even full patched systems are vulnerable to zero-day exploits
- There is an unkown amount of malicious sites on the web
- We need to build a Distributed System to identify malicious sites:
  - Modify the windows kernel to monitor suspicious system calls
  - Remote control Microsoft's Internet Explorer
  - A technology to protect ourselves
  - A component to easily control the whole system

For more information see **http://labs.xnos.org**

Rootkit (SST-Hooking)