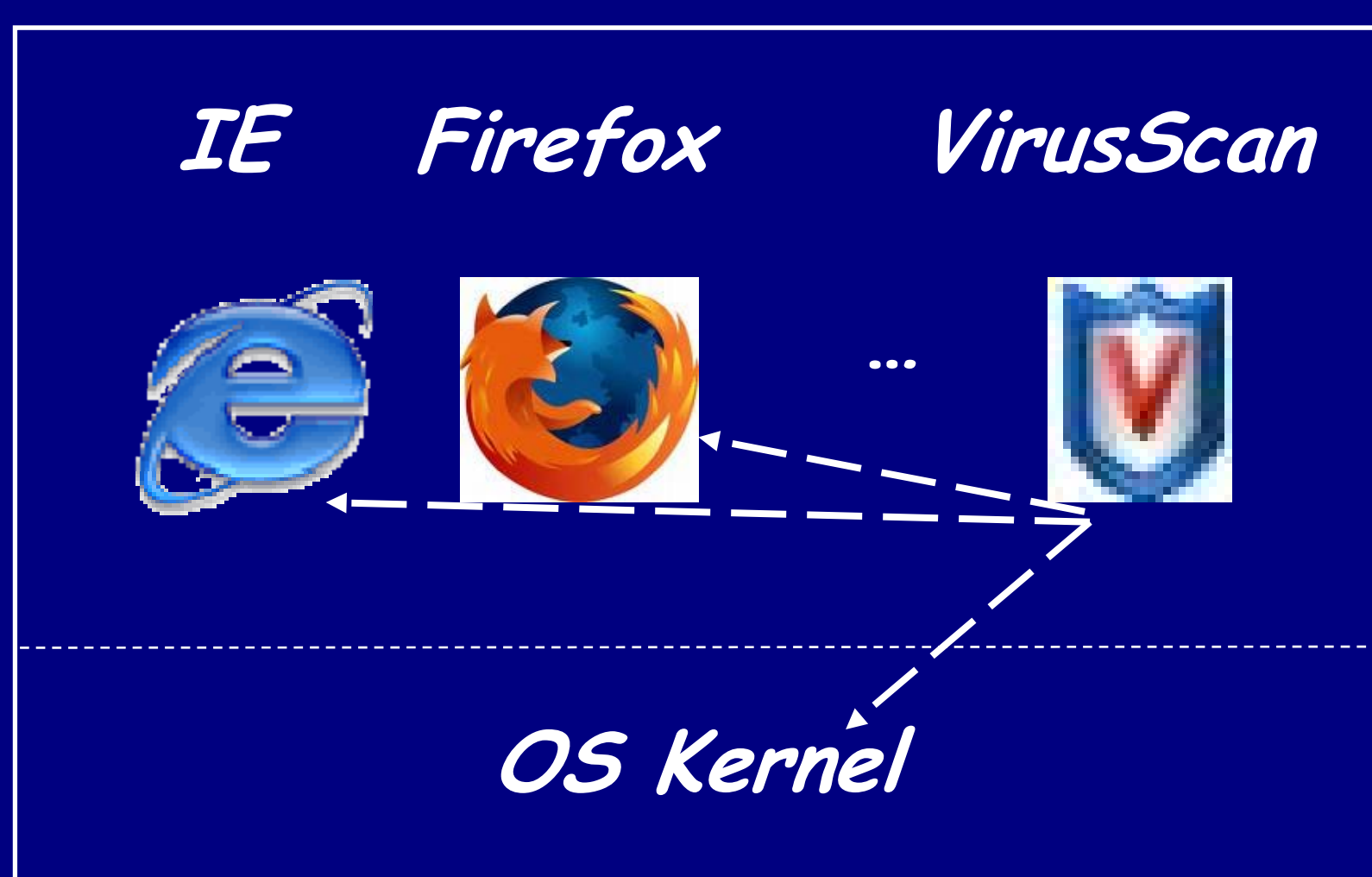




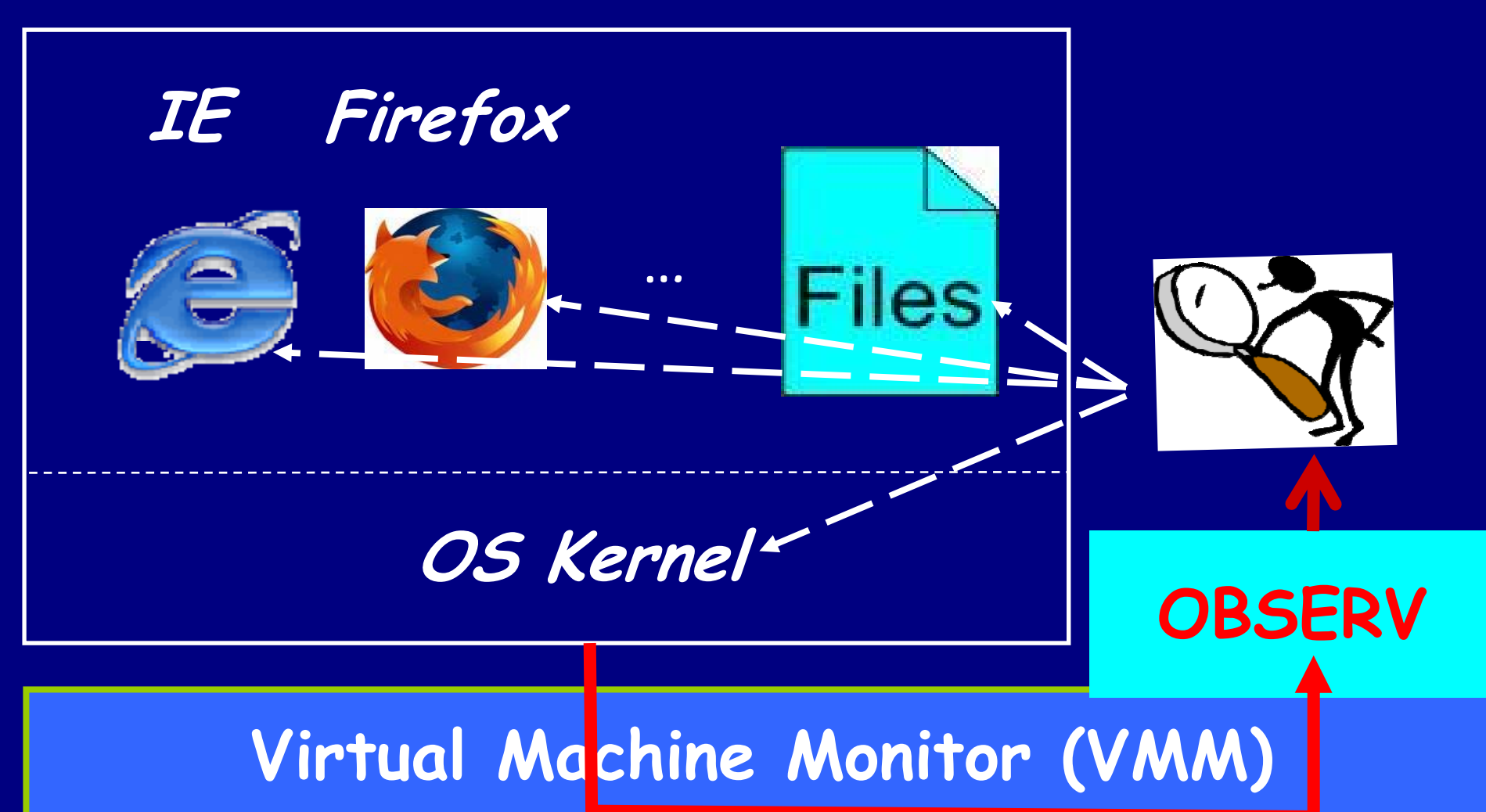
1. Problem

Elusive malware such as rootkits and bots are increasingly capable of detecting, evading, or subverting malware detection facilities in the victim. Current malware detection practice is fundamentally flawed in that host-based anti-malware systems run inside the very hosts they are protecting, making them vulnerable to malware's counter-detection and subversion.

2. "Out of the Box" Malware Defense



(a) Traditional "in the box" approach



(b) Proposed "out of the box" approach

3. Challenges and Enabling Techniques

- Challenge I: *semantic gap* between the "out of the box" view and the "in the box" view → • **Guest view casting**: based on the insight that the guest OS provides all semantic "templates" of data structures and functions to reconstruct a VM's semantic view
- Challenge II: *elusive nature* of malware (e.g., rootkits) → • **Cross-view analysis**: attacking the self-hiding nature of malware

4. New Capabilities

- Non-intrusive VM monitoring
- View comparison-based stealth malware detection
- "Out of the box" deployment of commodity anti-malware software

5. Applications

- Protecting virtual data centers and cyberinfrastructures
- Running untrusted client apps
- Next-gen anti-malware software
- Computer forensics
- Cyber security education