GOSCON DC

OPEN TECHNOLOGY FORUM

Security Experts on Open Source

redhat. | carahsoft

GOSCON DC

OPEN TECHNOLOGY FORUM

Security Experts on Open Source

Moderator:

Karl MacMillan
Director of Core Technology, Tresys Technology

Panelists:

Daniel Risacher
Associate Director, Enterprise Services and Integration, Department of Defense CIO

Daniel Walsh
Principal Software Engineer, SELinux Technical Lead, Red Hat

John Banghart
SCAP Validation Program Manager, National Institute of Standards and Technology

Steve Battista
Lead Information Security Scientist, MITRE

redhat. | carahsoft

GOSCON DC

OPEN TECHNOLOGY FORUM

Karl MacMillan

Director of Core Technology
Tresys Technology

redhat. | carahsoft

GOSCON DC

OPEN TECHNOLOGY FORUM

Daniel Risacher

Associate Director, Enterprise Services and Integration
Department of Defense CIO

redhat. | carahsoft

GOSCON DC

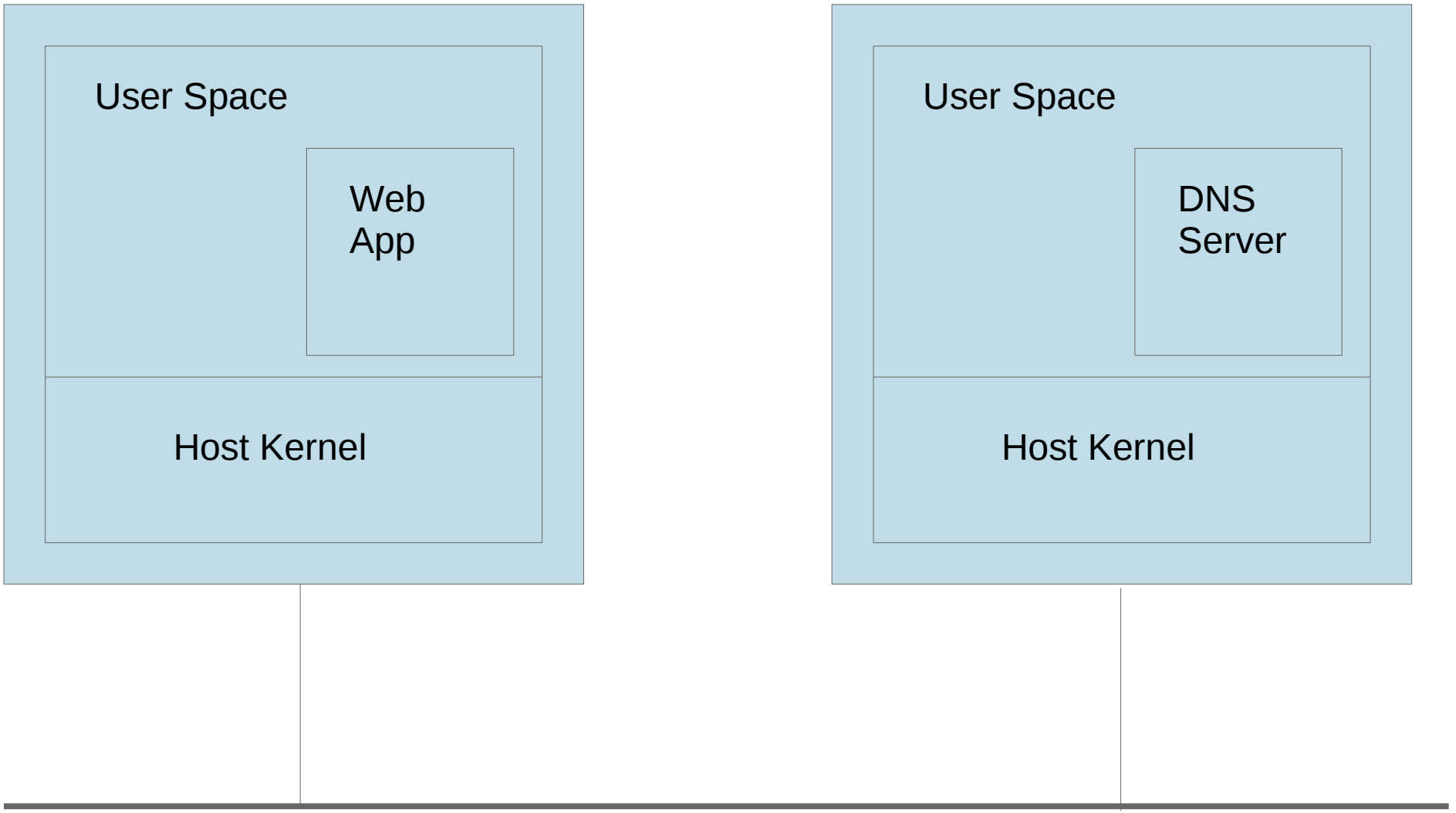
OPEN TECHNOLOGY FORUM

Daniel Walsh

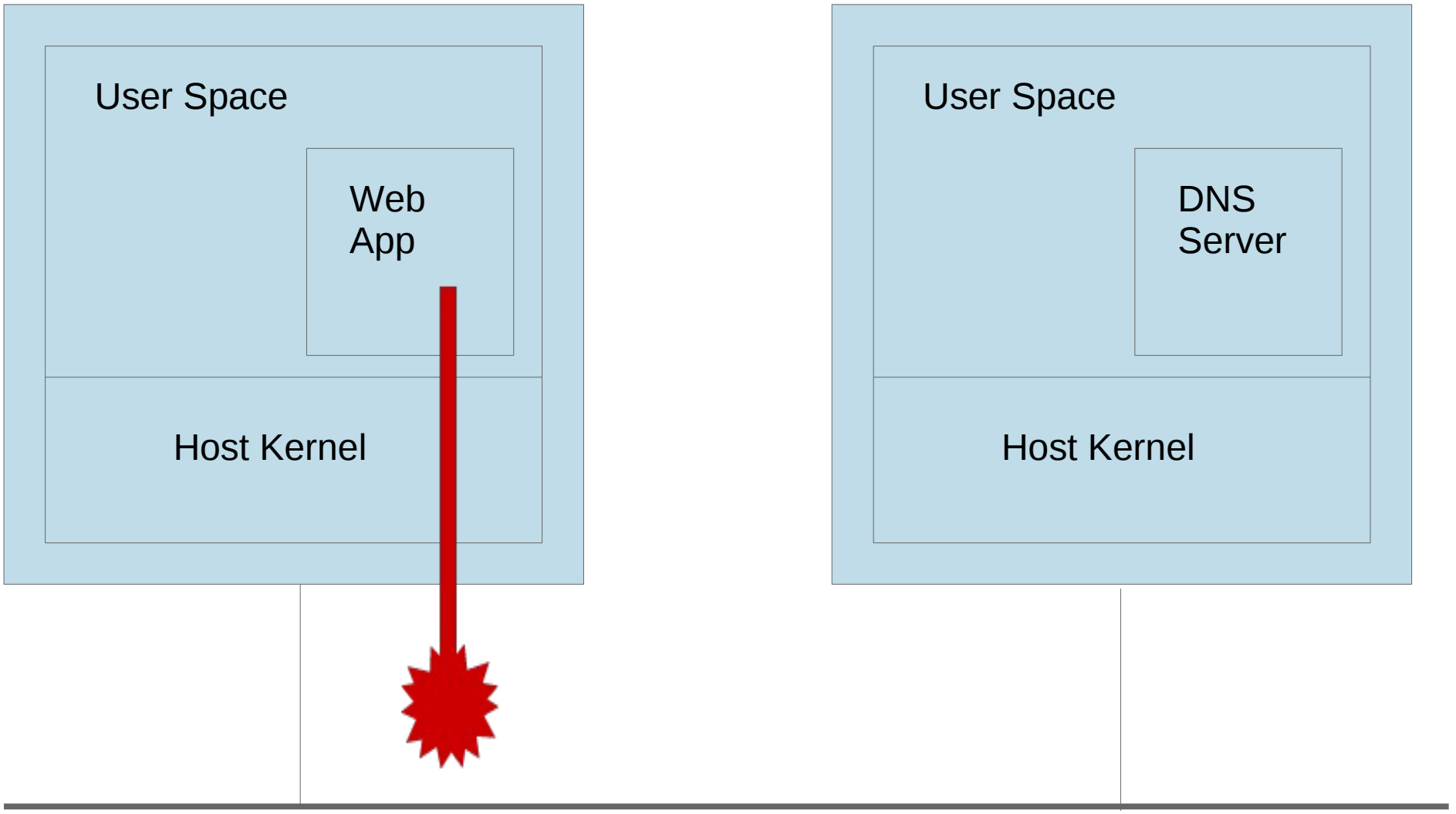
Principal Software Engineer
SELinux Technical Lead
Red Hat

redhat. | carahsoft

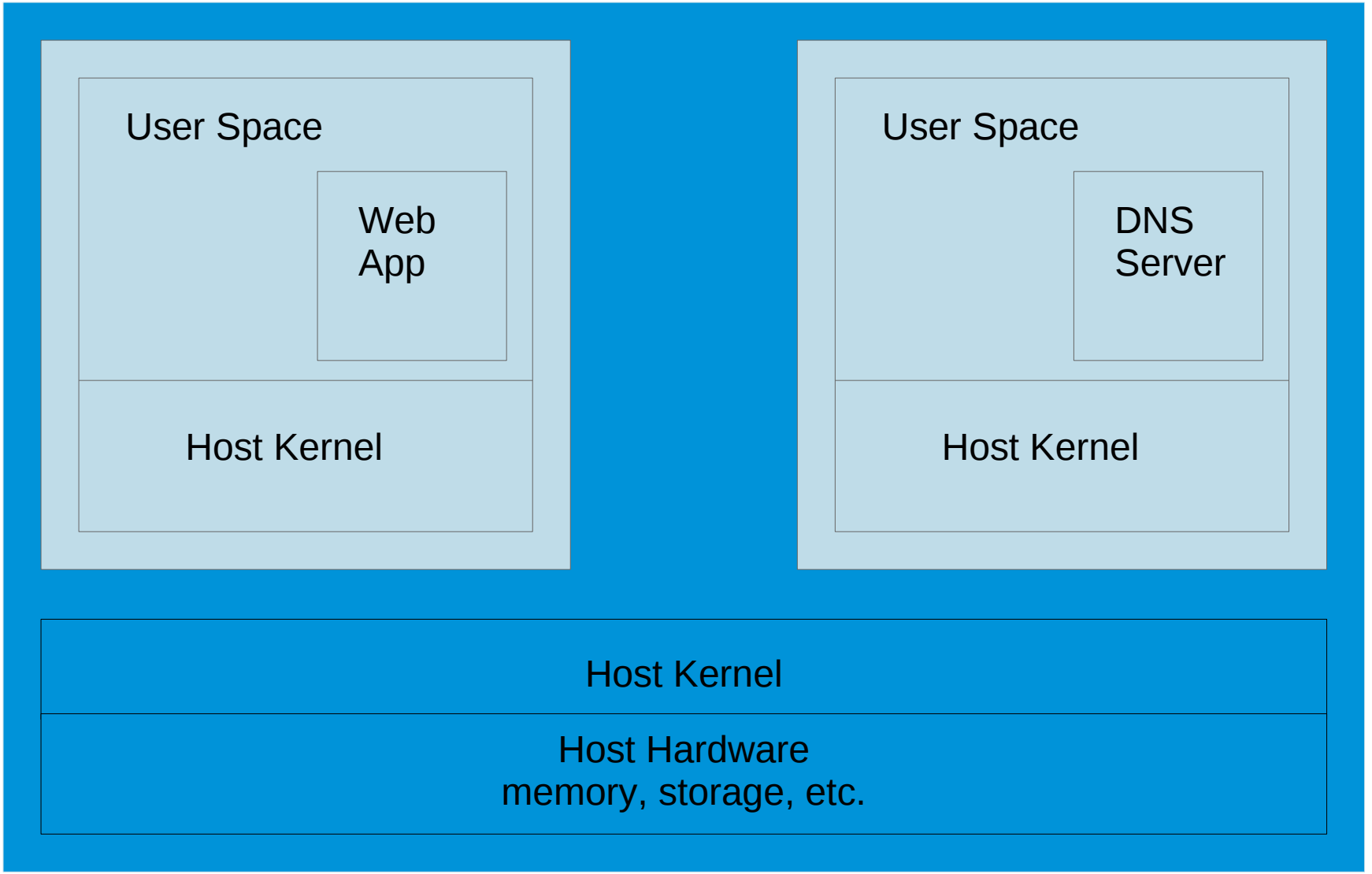
Before Virtualization



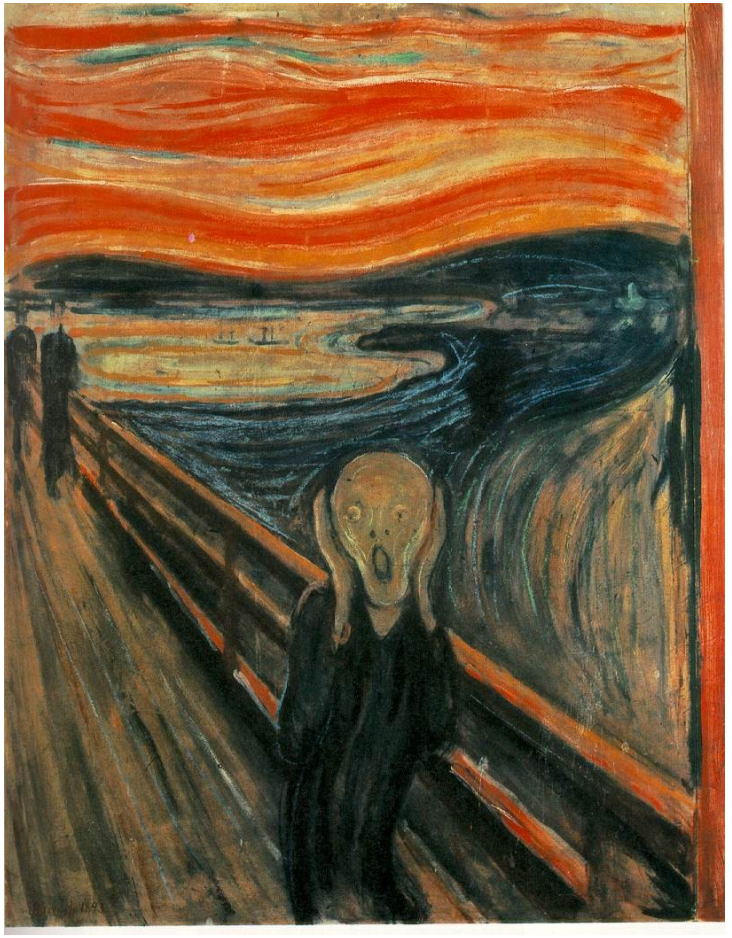
Good tools for detecting network attacks



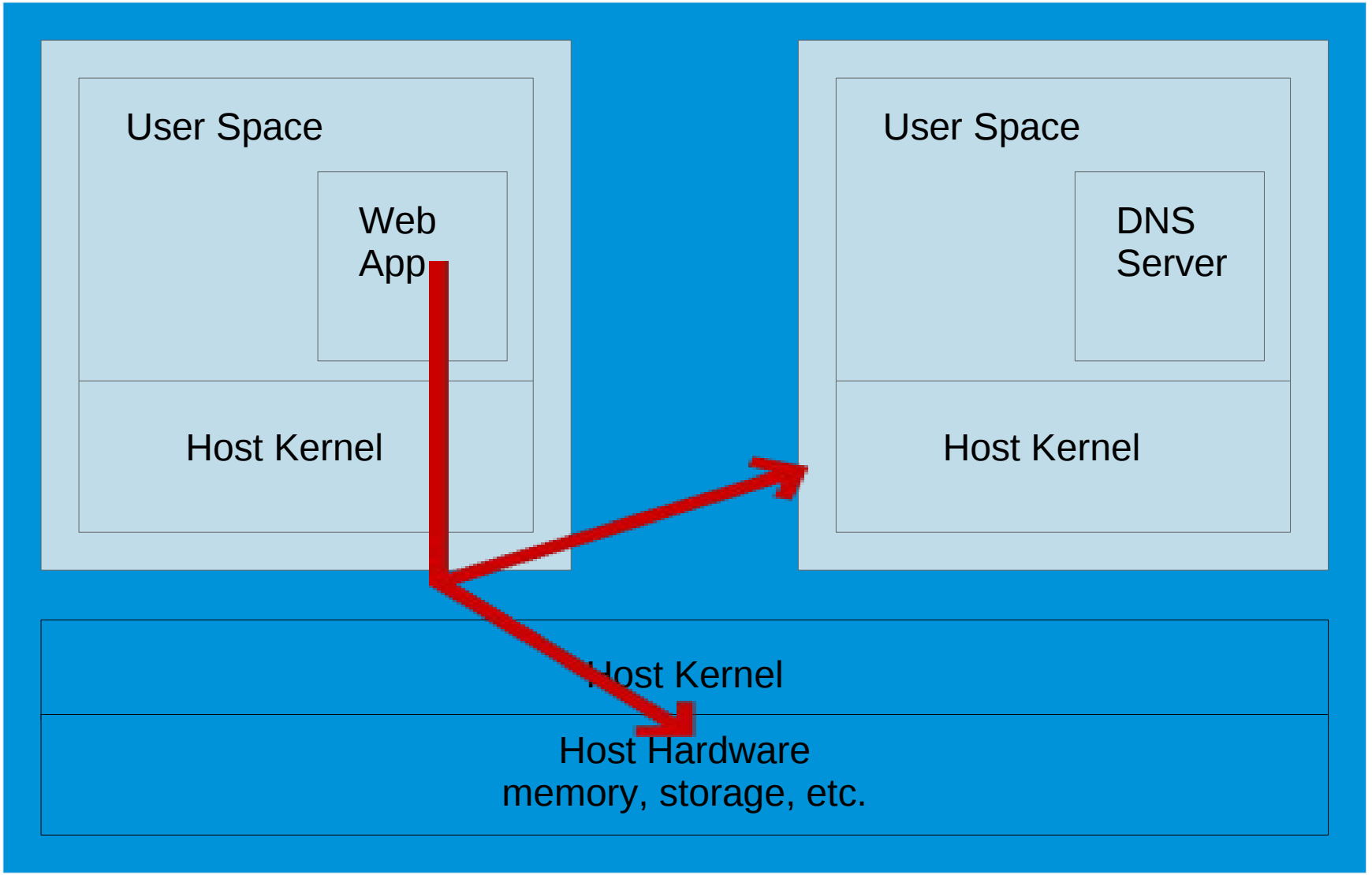
After Virtualization



What could possibly go wrong?



After Virtualization



Hypervisor vulnerabilities

Not theoretical

Evolving field

Potentially huge payoffs

Xen already compromised...

XEN Vulnerability http://www.hacker-soft.net/Soft/Soft_13289.htm

Adventures with a certain Xen vulnerability (in the PVFB backend)

version 1.0

Rafal Wojtczuk
Invisible Things Lab
rafal@invisiblethingslab.com

October 14, 2008

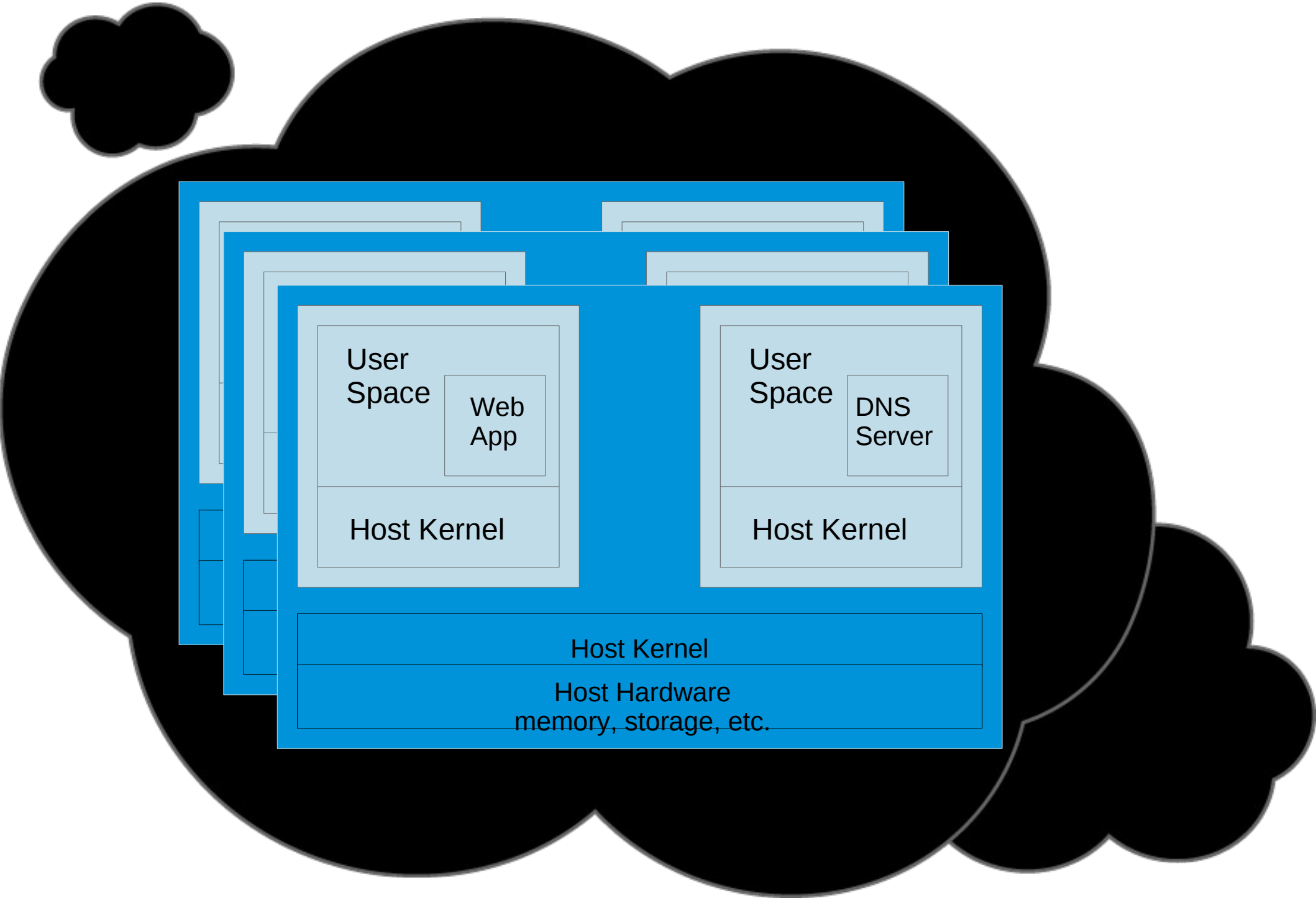
1 Introduction

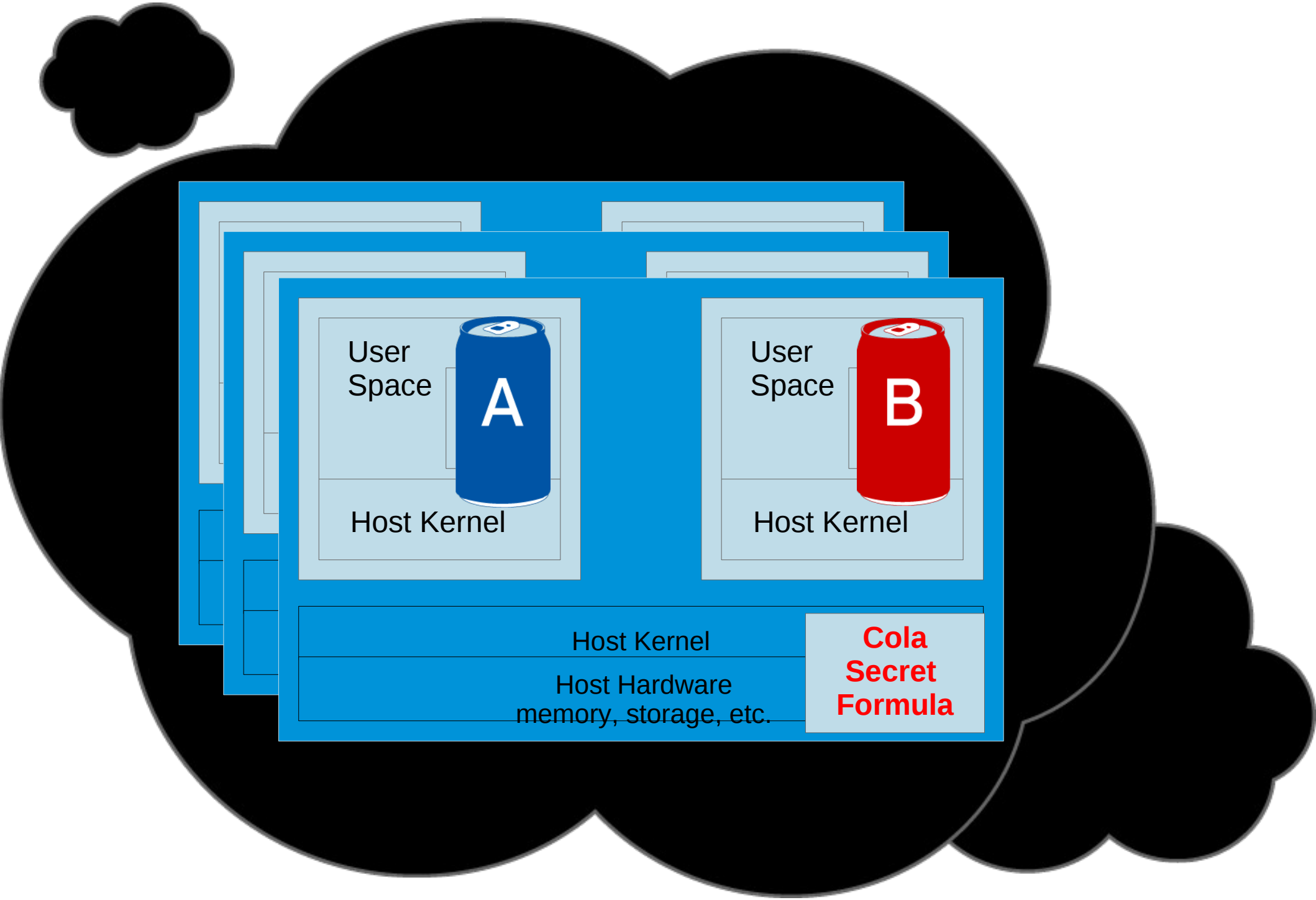
This paper documents the research by the author to understand the nature of and write an exploit for the CVE-2008-1943 vulnerability[1]. In x86_32 architecture case, the exploit can escape from a Xen PV guest to dom0. The challenges posed by SELinux are taken into consideration. Some techniques that failed to succeed with the default configuration (particularly, in x86_64 case) are also documented, because of their potential usefulness in other cases.

The exploits were written for Fedora 8 Linux distribution as dom0; it is the latest release of this popular distribution that comes with a dom0-capable kernel. Additionally, Xen 3.2.0 rpms (retrieved from xen.org site) were installed to the test dom0 machine.

2 The nature of the vulnerability

Who is the weakest link?


User Space
Web App
Host Kernel
User Space
DNS Server
Host Kernel
Host Kernel
Host Hardware
memory, storage, etc.


User
Space
A
Host Kernel
User
Space
B
Host Kernel
Host Kernel
Host Hardware
memory, storage, etc.
Cola
Secret
Formula

Enter SELinux...

SELinux is all about labeling

Processes get labels

Virtual machines are processes!!!

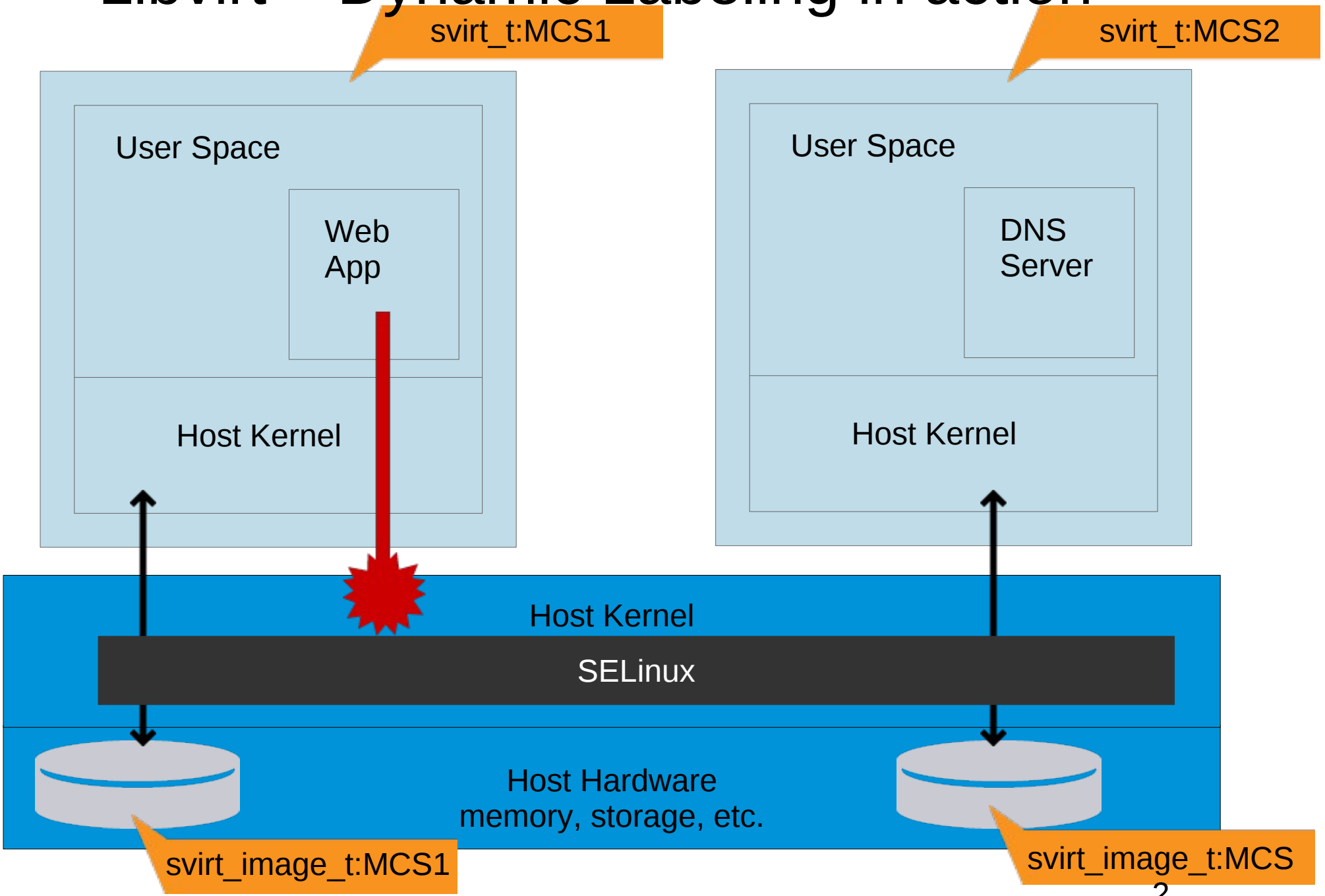
Files/Devices Get Labels

Virtual images are stored on files/devices!!!!

Rules govern how Process Labels Interact with Process/File Labels.

Kernel Enforces these Rules.

Libvirt – Dynamic Labeling in action



GOSCON DC

OPEN TECHNOLOGY FORUM

John Banghart

SCAP Validation Program Manager
National Institute of Standards and Technology

redhat. | carahsoft

References

John Banghart – NIST – john.banghart@nist.gov

SCAP Website – http://scap.nist.gov

National Checklist Program (NCP) – http://checklists.nist.gov

National Vulnerability Database – http://nvd.nist.gov

NIST Documents – http://csrc.nist.gov

- DRAFT SP 800-126: SCAP Specification
- DRAFT IR 7511: SCAP Derived Test Requirements

GOSCON DC

OPEN TECHNOLOGY FORUM

Steve Battista

Lead Information Security Scientist
MITRE

redhat. | carahsoft

GOSCON DC

OPEN TECHNOLOGY FORUM

Panel Discussion

redhat. | carahsoft

GOSCON DC

OPEN TECHNOLOGY FORUM

Questions?

Tell us what you think:
Complete the survey

redhat. | carahsoft