

# Mobile & Secure End-Point Computing with Managed Virtual Machines

Monica Lam

Stanford University

## **Consumerization of IT: Using home computers**

- Viruses on home computers attacking the data center
  - May test for existence of virus scanners
  - How to test if virus scanners are disabled?
  - How to test for absence of malware?
- Difficulty in managing home computers
- Choice of PCs: Windows, Macs

# Other Pressing Problems

## **Road Warriors: data leakage**

- Stolen laptops with unencrypted data
- Reading email at kiosks and leaving a footprint

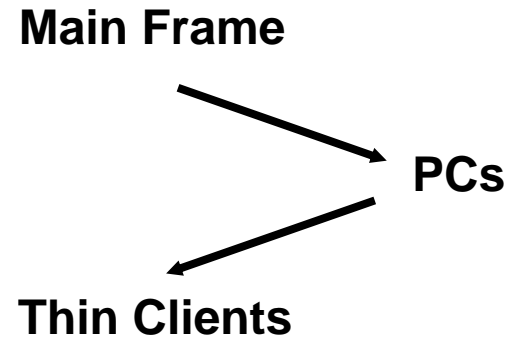
## **Disaster recovery**

- Failed laptops on the road
- New office set ups after man-made/natural disasters

## **Zero-day vulnerabilities**

- Detecting and recovering from rootkit attacks

# Central Management: Sun Rays



- **Stateless protocol: frame buffer protocol+opts**
- **Smart card: instant access to personal state**

[Interactive Performance of SLIM: A Stateless Thin-Client Architecture.  
Schmidt, Lam, Northcutt, SOSP, 99.]

# Sun Ray: Advantages and Disadvantages

- ✓ **Central management**
- ✓ **Mobility: Smart cards enable instant access**
- ✗ **Dependence on the network**
  - ✗ Poor interactive performance over WAN
  - ✗ No offline operation
- ✗ **Does not leverage PCs: TCO, user experience**
  - ✗ Cost of thin clients similar to PCs
  - ✗ Data center: expensive, hard to scale
  - ✗ Single point of failure
  - ✗ Unwillingness to give up on the flexibility of PCs
- ✗ **No peripherals**
- ✗ **Management centralized but not solved**
- ✗ **Solaris → Citrix terminal server, not all Windows apps**

# Virtual Desktop Infrastructure (VDI)

## **Run X86 virtual machines in the data center**

- Windows, Vista, Linux
- VMware virtual machine monitor

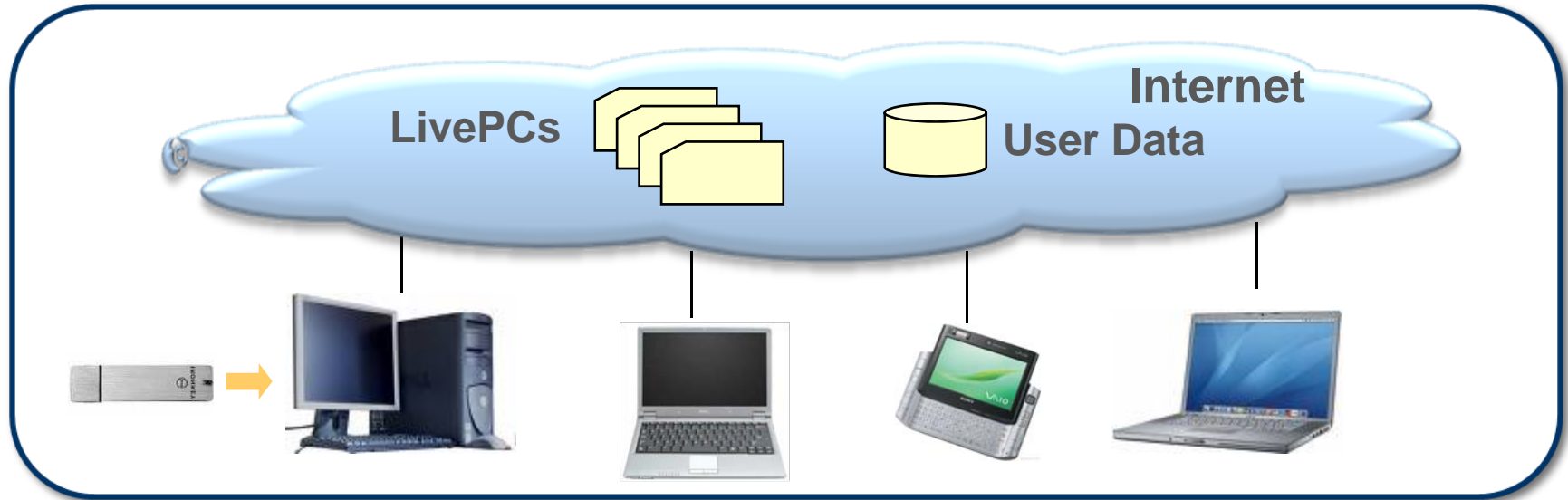
## **Remote display on clients' desks**

[NSF Research Grant #0121481, Lam, Rosenblum, Boneh 2001]

# VDI Advantages and Disadvantages

- ✓ Runs all legacy software
- ✗ Disadvantages of centralized computation
  - ✗ Higher total cost of ownership: 8 users to a server?
  - ✗ Miss out on “killer micro” advantage
  - ✗ Overhead of both virtualization and remote display
  - ✗ Management of many virtual machines

# The Stanford Collective Project → Moka5 LivePCs



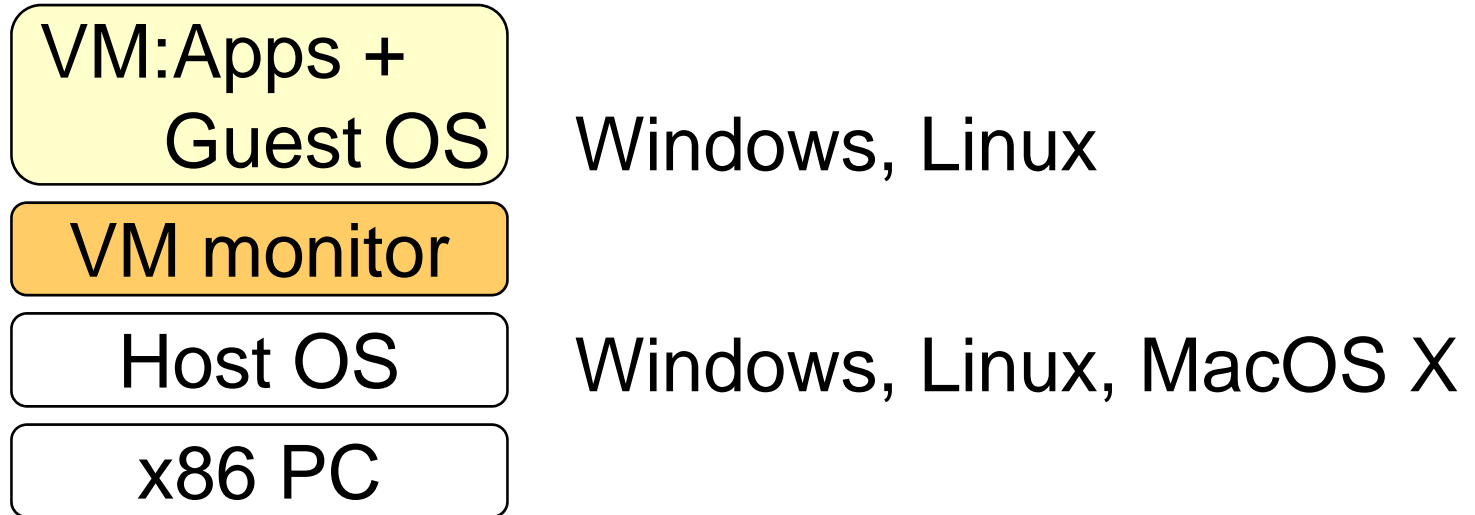
**LivePCs: Managed virtual machines in the cloud**

**PCs (Windows, Linux, Mac PC) become generic platforms**

**Portable flash: personalized cache as a network accelerator**

- Supports disconnected operation

# X86 Machine Virtualization

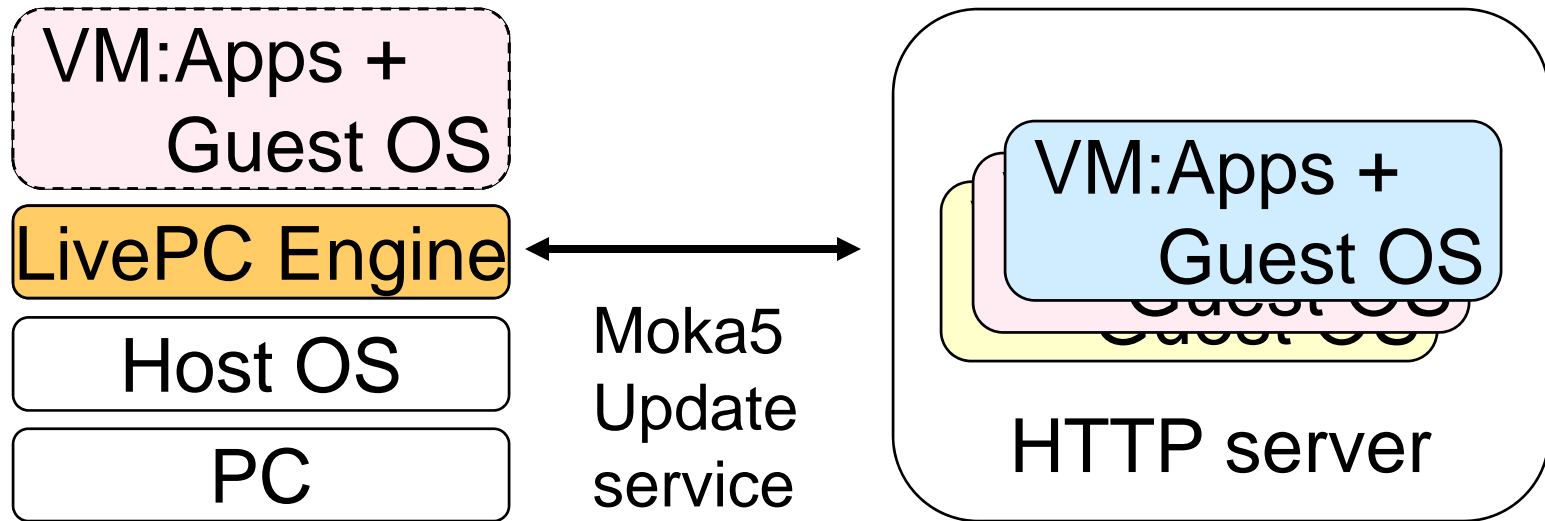


## VM Monitor

**A guest OS can run on a host OS like an app**

**Runs all x86 software w/o modification**

# LivePC Engine



## LivePC: Managed virtual machines

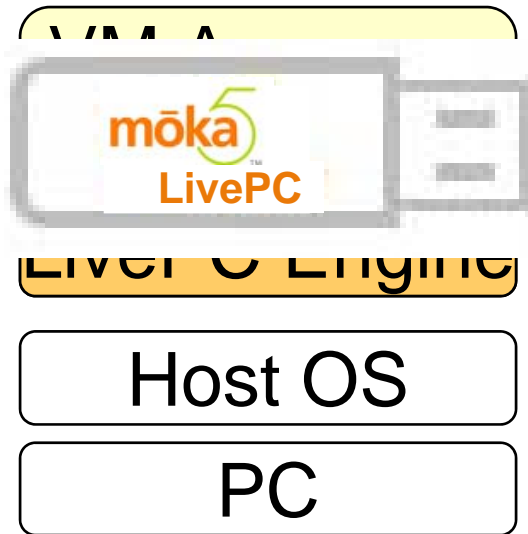
### LivePC Engine:

- Runs latest VM image on local machine
- Streams, caches, prefetches incremental changes on server

**Network connectivity needed just for deployment/updates**

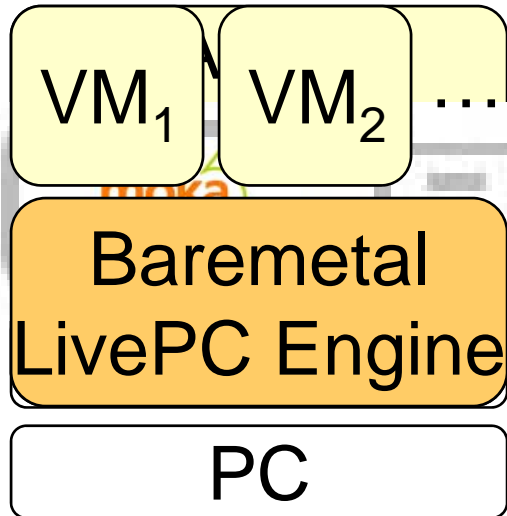
[Optimizing the Migration of Virtual Computers,  
Sapuntzakis, Chandra, Pfaff, Chow, Lam and Rosenblum, OSDI 2002]

# Portable LivePC Engine



Flash memory:  
\$1/GB in 4 years

# Baremetal LivePC Engine (+ Portability)



## Baremetal LivePC Engine

- Closed custom Linux build
- LivePC Engine

**Runs choice of VM on demand**

**Streams LivePCs dynamically**

**Not subjected to keyloggers**

**More secure**

# Demo

# 3 Scenarios

- Remote administration on unmanaged machines
- Mobility with a USB drive
- Managing (distributed) computer facilities

# 1. Unmanaged Machines: Management

## LivePCs: Quick & easy deployment & management

- Imaging
  - Virtual image works across devices (including Macs)
  - One-click publish/subscribe
- Automatic updates
  - Easy to roll out/roll back software and security patches
- Scalable, deterministic: 1000s of users per server
  - Example: SP2 update
- Works on Windows and Macs

[Virtual Appliances in the Collective: A Road to Hassle-Free Computing, Sapuntzakis and Lam, HotOS 2003]

[Virtual Appliances for Deploying and Maintaining Software, Sapuntzakis, Brumley, Chandra, Zeldovich, Chow, Lam, Rosenblum, LISA, 2003]

# 1. Unmanaged Machines: Security

## **Isolation and control**

- Home computer viruses isolated
- Guaranteed configuration
- Baremetal eliminates the possibility of keylogging

## **Rejuvenation: outside-the-box solution**

- Only solution that guarantees to remove all rootkits
- Rejuvenation incurs no additional delay.

## 2. Mobility

### Auto-install on Windows

- Administration privilege needed for first execution
- Same USB works on Windows and Macs (Macs need fusion)



### Data protection

- Leaves no personal data behind
- Takes nothing away
- Hardware-provided security
  - Ironkey: hardware encryption
  - Biometric USB drives



### One-click recovery on a new drive

### Baremetal avoids keyloggers



[The Collective: A Cache-Based System Management Architecture, Chandra, Zeldovich, Sapuntzakis, Lam, NSDI 05]

# 3. Managing Facilities

## **Supports dynamic provisioning across machines**

- Hoteling: training, call centers, classroom labs, conference computers
- Distributed branch offices

## **Isolated user-supplied environments**

- Isolation between user and host platform
- Kiosks, hotel business centers, guest rooms

## **LivePCs: a new platform that supports**

- Management
- Security
- Mobility

**[www.moka5.com](http://www.moka5.com)**:

- A library of community contributed LivePCs

# Computer Revolution

mainframe



mini



workstation



PC



laptop



phone

