Redefining Personal Computing with Virtualization

Monica S. Lam
Stanford University
MokaFive, Inc.
Trends

Personal Computing: Shake up after 25 years of PC dominance
Opportunity for a Clean-Slate Approach

10x cheaper, 10x more users
Triple Play: Internet Access, TV, Telephone

Media

Communication

Games

Computation
Emerging Computing Models

- In your pocket
- Always on

- Rich legacy apps
- Locality of reference
- Offline execution

- Device independent
- Central management
Emerging Computing Models

- In your pocket
  - Always on

- TV out

- Mobile

- Cloud
  - Device independent
  - Central management

- PC
  - VDI
  - Google Gears
  - Native client

- Rich legacy apps
- Locality of reference
- Offline execution
Tian Di Ren (天地人) 3-Tier Architecture

My key, cache, window into my digital cloud: ID, personality, assets, and the internet

Personalize the generic PC, borrow the power, display, keyboard, memory, etc

PC, TV at home, on the road, in hotels, on the plane
How Do We Get There?
Laptops Today

Ongoing Issues
• Security
  – Zero-day root-kit vulnerability
  – Data center security
  – Data leakage
• Business continuity
• Management cost

Emerging trends
• Going green
  – Working from home
• BYOPC
• Mac vs Windows
• Cell phones vs. PCs
Convergence of Personal & Corporate

Dilemma:
How to empower individuals and provide security?

78% use personal computers for work
43% use work computers for personal use

% of workers altering security settings 25%
% of workers downloading personal applications 31%
% of workers downloading personal pictures & videos 43%
Laptops Today

Monolithic system
→ every PC is different
→ hard to manage by IT/users

System Stack: HW, OS, apps
Principals: HW owner, IT, user
Security vs Choice
Separation of Concerns

Characteristic of all intelligent thinking

- Focus on one, knowing that we are only occupying ourselves with one aspect
- It is being one- and multiple-track minded simultaneously
- The only available technique for effective ordering of one's thoughts.

3 Sets of Concerns

- User
- IT
- Ubiquity
Virtualization

**Separation of Concerns** achieved through
- Modularity
- Encapsulation
- Abstraction

**x86 virtualization** separates
- Hardware instance: Dynamic binding of VM
- Hardware and OS: Multiple OSes
- Hardware config: Virtual device drivers
- Different user roles: Different VMs
Tian Di Ren (天地人) 3-Tier Architecture

- **天 (Heaven)**: servers
- **地 (Earth)**: data
- **人 (Man)**: My key, cache, window into my digital ID, digital personality, digital assets, and the internet
  - **Personalize the generic PC, borrow the power, display, keyboard, memory, etc**
- **PC, TV**
  - at home, on the road, in hotels, on the plane
1st Approx: Desktop As a Service (DaaS)

- Stanford Collective project, MokaFive
- LivePCs: managed virtual machines in the cloud
- PCs: generic computing platform
- Phone: mobile access, write-through cache, network accelerator
System Design and Implementation
3 Sets of Concerns

User:
- Data
- Personal Apps

IT:
- AAA
- Guest OS, AV
- Corporate Apps

Ubiquity:
- PCs, devices
- Host OSes
- Environment: printers, network
- Mobility, portability
System Anatomy
System Anatomy

- User Data
- User Apps
- IT: Managed Apps
- Guest Manager
- IT: Guest OS + Anti-virus
- Virtual Machine Monitor
- LivePC Manager
- Flash Manager
- Host Manager
- Baremetal
- Windows
- Mac
- Linux
- Client PC + Devices

Cross-platform:
- Windows, Mac, Linux
- 3D graphics
- Printer
System Anatomy

- User Data
- User Apps
- IT: Managed Apps
- Guest Manager
- IT: Guest OS + Anti-virus
- Virtual Machine Monitor
- LivePC Manager
- Flash Manager
- Host Manager
- Baremetal
- Windows
- Mac
- Linux
- Client PC + Devices

Dynamic install
Flash performance opt.
Document access on mobile phones
## System Anatomy

<table>
<thead>
<tr>
<th>Baremetal</th>
<th>Windows</th>
<th>Mac</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client PC + Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User Data
- User Apps
- IT: Managed Apps
- Guest Manager
- IT: Guest OS + Anti-virus
- Virtual Machine Monitor
- LivePC Manager
- Flash Manager
- Host Manager

### Authentication
- LDAP

### Authorization
- revocation, offline access

### Accounting
- logging, dlp

### Role-based customization

### Encryption
- role-based customization

### System Virtualization
- LUNs
- Storage
- system update, caching, prefetching, demand paging

### Multi-tenancy
System Anatomy

- User Data
- User Apps
- IT: Managed Apps
- Guest Manager
- IT: Guest OS + Anti-virus
- Virtual Machine Monitor
- LivePC Manager
- Flash Manager
- Host Manager
- Baremetal
- Windows
- Mac
- Linux
- Client PC + Devices

VMware player
Virtualbox
System Anatomy

Single sign on
VPN integration
Uniquification:
  Domain join, SID
User-installed apps
Separation of
  system & user data
Data & app backup
Design Principles

Separation of Concerns

90-10 rule: 90% of the code handles exceptions
• “Re-install the OS”
• Outside-the-box management
  – Only solution to zero-day rootkit attacks

Bootstrapping from a small trusted code base
• Baremetal
• LivePC Player
• IT-managed base image: Windows + AV
• User apps & data
Desktop as a Service (DaaS)

- In your pocket
- Always on
- Device independence
- Central management

- Rich, legacy apps
- Locality of reference
- Offline execution

LivePCs
Current Research

Tian Di Ren (天地人) application infrastructure
- Users maintain ownership of personal data
- Distributed social networking applications

Part of Stanford POMI 2020
(Programmable Open Mobile Internet)
- An NSF Expedition, 2008