MALWARE MITIGATION THROUGH CENTRALIZED COMPUTATION AND VIRTUALIZATION
Gary Brown
CS 615
4/21/10
1960s-70s

- Computers
  - Large
  - Expensive
  - Managed

- Terminals
  - Desktop form factor
  - “dumb”
    - Cathode ray tube/input device
INTEGER*4 TYPPAR, TYPANT, SNOLGE(9), SORDEN(9), NSNGL,
THE MICROPROCESSOR

- Introduced in 1970s
- Revolutionary
  - Decreased size
    - Smaller manufacturing architectures
  - Decreased price
    - Fewer materials
    - Efficient practices
  - Increased capability
- Practical
  - Entertainment systems
  - Personal computers
NETWORKS AND CONNECTIVITY

ARPANET
→ Educational Institutions
  → Residential ISPs
    → Wireless Providers
**STATE OF THE ART**

- **Ubiquitous Computational Capabilities**
  - Computers in every home, business
    - 2-4 core
    - 2-3GHz
  - Elaborate gaming systems
    - PS3 Cell processor
    - Parallel-processing GPUs
  - Smartphones in every pocket
    - 1GHz Qualcomm Snapdragon CPU

- **Inescapable Connectivity**
  - WiFi
  - 3/4G
  - Satellite
2009 Statistics

- WiseCrunch et al\(^1\)
  - 1.73 billion Internet users
  - 2.6 million malicious code threats, 1/2009
  - 3.5 million malicious code threats, 12/2009
  - Increase of over 900,000 discrete signatures
  - 148000 computers made zombies per day
EFFECTS

- Decreased Performance
- Information Theft
  - 1.1 million victims in 2008\(^2\)
- SPAM
  - 200 billion per day\(^1\)
- Distributed Denial of Service
Solutions

- Licenses to Compute
- Centralized Computing
- Virtualization
- Combination
CENTRALIZED COMPUTING

- Desktop and mobile terminals
  - I/O devices
  - Connectivity modules

- Backend Computation
  - Scalable resources
  - Professional administration
BENEFITS

○ Feasible
  • Increasing connectivity speeds
  • Prevalence of web services

○ Available
  • guaranteed with connectivity
  • No “disk” failures
  • No extensive hardware replacements/upgrades

○ Cost-effective
  • “Pay as you go”
  • Reduced hardware cost
  • Reduced energy cost

○ Secure from Loss/Theft
  • Centralized
  • No need for remote device wipes
    ○ Simply blacklist missing device
VIRTUALIZATION

- Administrator-controlled environment
  - Controls bare metal host
  - Manages image augmentation

- Static boot images
  - All changes/contamination eliminated with reboot

- Separate file storage
  - Contains items users wish to keep
**Benefits**

- **Integrity**
  - Users cannot alter image
  - Contamination easily corrected

- **Administrative Ease**
  - Image tailoring per user request
  - Mass distribution
Centralized Virtualization

- Primitive example
  - Amazon EC2

- Administrative benefits of centralized computing

- Made easier with “clean slate” reboots
Questions?
SOURCES