Internet is dangerous
worms, viruses, spyware, adware
don't execute malicious code

Overview
- Virtualization
  - fast
  - minimal interposition
- Emulation

Overview
- Virtualization
- Emulation
  - greater control
  - slower

Overview
- Full-time protection

Overview
- Virtualization
  - Emulation
  - Full-time protection
  - Don't execute code from the Internet

Tainting
Tainting
- Why
  - Stack smashing attacks
  - Heap corruptions
  - Root toolkits
- What
- How

Tainting
- Why
- What
- Divide processor's registers into two classes: data & system
- Untrusted I/O considered tainted
- Prohibit system registers from referencing tainted data
- How

Virtualization
- VM (Virtualized)
- Virtual Machine Monitor
- Physical Hardware

Virtualization & Emulation
- VM (Virtualized)
- Virtual Machine Monitor
- Processor emulator
- Physical Hardware

Architecture
Virtualization & Emulation

Control VM
VM (Virtualized)
Virtual Machine Monitor
Physical Hardware

Packet Arrives

Packet Arrives

Protected VM accesses tainted data

Protected VM accesses tainted data

VM attempts to execute tainted data

VM attempts to execute tainted data

Disk I/O

Disk I/O

Normal execution resumes

Normal execution resumes
When do we revert to virtualization?

- After each instruction
- When entering the virtual machine monitor
When do we revert to virtualization?
- After each instruction
- When entering the virtual machine monitor
- At the end of each translation block chain

Performance
- Micro benchmarks
  - lmbench2 (1.1x - 3.7x)
  - fork (3.7x) (259 µsec)
  - fork + /bin/sh (1.2x) (6,724 µsec)
- Macro benchmark

Lessons
- V2E & E2V transition cost
- False tainting
  - Page granularity
  - ECC memory
  - Application awareness

Summary
- Comprehensive & high performance
- Full-time protection
- V2E & E2V