Sandboxes, Emulators, and Virtualization
Isolation...

Brian Gaines

April 8, 2013
Who is this guy?

- Name is Brian Gaines
- I taught Computer Organization last semester...
  - (yup, it is okay to still hate me)
- I know your professor and he wanted someone to fill in for his normally scheduled class...
- I once programmed OSes in my spare time
Overview

- Sandboxes
- Emulators
- Virtual Machines
- What are they and why you should care...?
Sandboxes

- Loose definition: security mechanism that provides access to resources within a constrained environment
- Process sandboxing
Process Sandboxing

- Limited set of API calls
- Reduced communications functionality
- Reduced storage functionality
- Monitoring access
- Reduced code access
Examples of Sandboxes

- iOS App sandboxes
- BSD Jails
- Sandboxie
- Google Native client
- Many many others...
Google Native Client

- Native x86/x86-64 code within a browser environment
- Browser plugin
- Inner and outer sandbox
- How?
Inner sandbox

- Binary validation
  - Static analysis
  - Detects security defects
- No allowance for self-modifying code or overlapping instructions
- Use of segmented memory
- Trusted service runtime co-exists with untrusted application
  - Mechanism for transitioning between
Outer sandbox

- System-call interception
- limited details...
Emulators

- Loose definition: system that attempts to duplicate functionality of another system, may include software and hardware
- DOS emulator
- System emulators
- A type of sandbox
- Examples: DOS Box, Wine, BOCHS, QEMU, etc.
Virtual Machines

- History
- Language virtual machines
- System virtual machines
- other
History

- Popek & Goldberg
- Sufficient conditions for supporting virtualization
- Virtual Machine Properties
  - Efficiency
  - Resource control
  - Equivalence
- Patents
Virtualization

- Patents expired/expiring
- (IBM) Execution unit shared by plurality of arrays of virtual processors, 1969
- (DEC) Computer program protection means, 1972
- (Fujitsu) Virtual machine system, 1980
- (Honeywell) Hardware virtualizer for supporting recursive virtual computer systems on a host computer system, 1981
Language virtual machines

- Platform independent environment
- JavaVM, Squeak, etc..
System virtual machines

- Methods
- Virtual devices
- Paravirtualization
- Security of virtual machines
Methods

- Trap and emulate? (Separate from methods?)
- Binary translation
- Hardware assisted
- Device virtualization
Why do you care?

- David (may) choose to test you on these concepts...
- These concepts are used pervasively in industry...
- If you want to understand current security trends, these concepts are either used to implement or analyze...