## CSci 5271 Introduction to Computer Security Day 8: Defensive programming and design, part 2

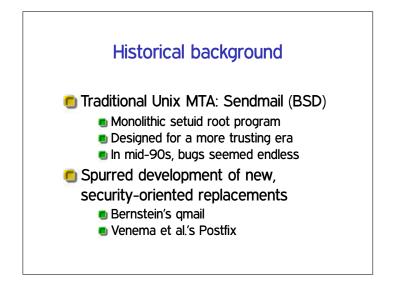
Stephen McCamant University of Minnesota, Computer Science & Engineering

## Outline

Bernstein's perspective

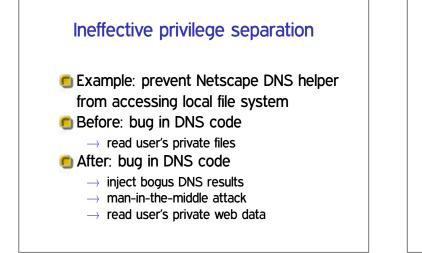
Announcements intermission

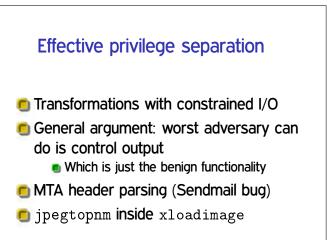
Techniques for privilege separation

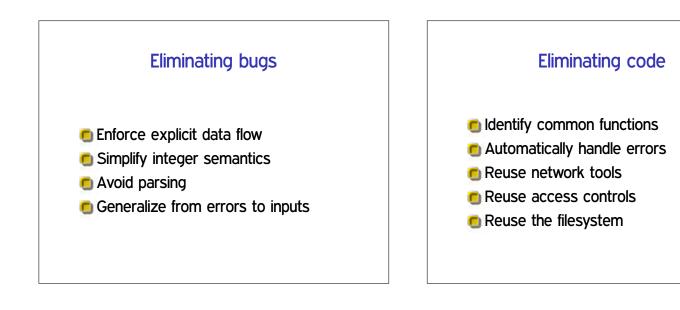


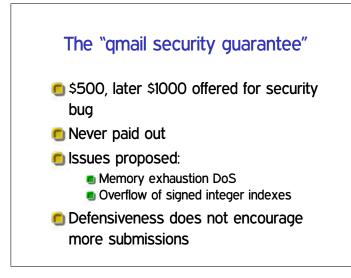
## Distinctive qmail features

- Single, security-oriented developer
- Architecture with separate programs and UIDs
- Replacements for standard libraries
- Deliveries into directories rather than large files











- Originally had terms that prohibited modified redistribution

   Now true public domain
- Latest release from Bernstein: 1998; netqmail: 2007
- Does not have large market share
- All MTAs, even Sendmail, are more secure now





- This is the section of the slides most likely to change in the final version
- If class has already happened, make sure you have the latest slides for announcements

## Outline

Bernstein's perspective

Announcements intermission

Techniques for privilege separation

## **Restricted languages**

- Main application: code provided by untrusted parties
- Packet filters in the kernel
- JavaScript in web browsers
   Also Java, Flash ActionScript, etc.

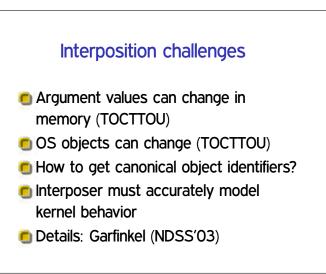
## SFI

- Software-based Fault Isolation
- Instruction-level rewriting like (but predates) CFI
- Limit memory stores and sometimes loads
- Can't jump out except to designated points
- 🖲 E.g., Google Native Client

## Separate processes

- OS (and hardware) isolate one process from another
- Pay overhead for creation and communication
- System call interface allows many possibilities for mischief

# System-call interposition Trusted process examines syscalls made by untrusted Implement via ptrace (like strace, gdb) or via kernel change Easy policy: deny



## Separate users

- Reuse OS facilities for access control
- Unit of trust: program or application
- 🖲 Older example: qmail
- Newer example: Android
- Limitation: lots of things available to any user

## chroot Unix system call to change root directory Restrict/virtualize file system access Only available to root Does not isolate other namespaces

# **OS-enabled** containers (System) virtual machines One kernel, but virtualizes all namespaces FreeBSD jails, Linux LXC, Solaris zones, etc. Quite robust, but the full, fixed, kernel is in the TCB

- Presents hardware-like interface to an untrusted kernel
- Strong isolation, full administrative complexity
- I/O interface looks like a network, etc.

# Virtual machine designs

- (Type 1) hypervisor: 'superkernel' underneath VMs
- Hosted: regular OS underneath VMs
- Paravirtualizaion: modify kernels in VMs for ease of virtualization

## Virtual machine technologies

- Hardware based: fastest, now common
- 🖲 Partial translation: e.g., original VMware
- Full emulation: e.g. QEMU proper Slowest, but can be a different CPU architecture

