Securing X

Keith Packard
Hewlett Packard Enterprise
keithp@keithp.com

Hewlett Packard
Enterprise

Attack Surface

- Input
  - Monitoring input events
  - Synthesizing input events
- Output
  - Spoofing output
  - Screen capture
- Cut & Paste
  - Capturing cut buffer data
  - Replacing cut buffer data

Hewlett Packard
Enterprise

Simple Security Fixes

- Input Monitoring
  - Per-client keystate tracking
  - Deliver events only to window owner
- Input Synthesis
  - Disable all testing extensions by default
    - Breaks accessibility

Hewlett Packard Enterprise

Multi-level Security

- Start from X Security Extension
  - 'trusted' vs 'untrusted' clients
  - Most clients are trusted
- Make most clients 'untrusted'
- Labeling options
  - Different X authentication data
  - Special POSIX user/group for clients
  - SELinux labels on client process

Hewlett Packard Enterprise

Privileged Operations

- Key grabbing on root
- Selecting for events on other client resources
- GetImage on other client drawables
  - also on areas of your window covered by other client drawables when not composited
- Testing extensions
  - makes accessibility work again
- Relevant Composite extension bits
- Window management on root
- other stuff ...

Hewlett Packard Enterprise