Flask/TE Support for X

Eamon F. Walsh
ewalsh@tycho.nsa.gov
National Security Agency
National Information Assurance Research Laboratory
(NIARL)

X Server History

- Late 2007: xserver 1.4
  - XACE 1.0
- In release candidacy: xserver 1.5
  - XACE 2.0
  - X/Flask extension
- Some distros are shipping a 1.5 release candidate at the present time.

Documentation!

- "X Flask Extension Specification."
  - How to enable the extension.
  - How the Flask extension labels objects, and what objects and permissions are enforced by it.
  - API available through the extension.
- "A Crash Course in X for Flask Developers."
  - Tries to explain internals of X from a security perspective.

My Tasks

- Develop XACE and X/Flask extension.
  - Work on the X server is not finished yet.
- Develop library support for X/Flask.
  - XCB Python and C bindings.
- Some desktop infrastructure work.
  - gdm, PAM, window manager.
- Assist with policy writing and desktop integration.

X Server Task

- Fallout from initial merge
  - Sporadic bug reports.
  - Performance issues.
- Future work
  - Refine X/Flask controls as needed.
  - Secure Direct Rendering/OpenGL interfaces.
  - Respond to new X features and extensions.

New X Technologies

- "Hotplugging" of monitors and devices.
  - RandR extension.
  - DBUS/HAL integration.
- Kernel modesetting.
  - Trend of moving X facilities into the kernel.
  - Reduced flickering on VT switch.
  - Allow kernel oops messages to appear.
  - Crashed X server won't lock up the terminal.

New X Technologies (2)

- Multi-Pointer X
  - Multiple, independent mouse pointers.
  - Dynamically configurable.
  - Merged to trunk; targeted for xserver 1.6.
  - Potential security applications.
- XCB
  - Lightweight, auto-generated client-side library.
  - Supports multiple language bindings.

Here at OLS 2008

- Get a handle on the policy work.
  - MLS constraints.
  - Interfaces for domain interaction.
- Distribute documentation.
- Collect user feedback.

GDM

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Solving the server labeling problem
  - bring down the X server and launch a new one.
  - launch the user server on a different virtual terminal.
  - dyntrans the X server or relabel server objects.
  - work around the problem in policy.
- Accomplishments to date
  - Have patches in gdm supporting relabel/dyntrans.
  - Worked on a prototype that relaunches the server.

Window Manager

- Labeling
  - Compositing-based secure labels.
  - Better solution for mapping contexts to colors.
- Object Management
  - Create windows, properties and other objects under a different context depending on the client?

Policy

- Desktop applications launched from nautilus, gnome-panel, etc.
  - Transition all desktop applications.
  - Modify nautilus, gnome-panel, etc. to set exec contexts.
- Interactions between derived types.
  - Need better refpolicy interfaces.
  - RBACsep could help here.

Desktop Community

- Engage GNOME, KDE community representatives.
- Lobby for security improvements, incorporation of security features.
  - Background None windows.
  - MPX and input security.
  - Don't unnecessarily use X server extensions.
  - Cut & Paste.