Open Source, Closed Data

Multi-Level Security in Open Source Desktops

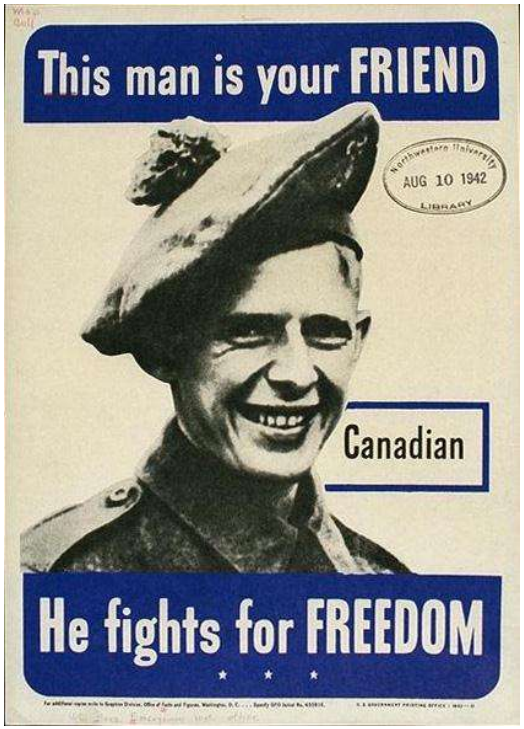
Alan Coopersmith

Sun X11 Engineering Group

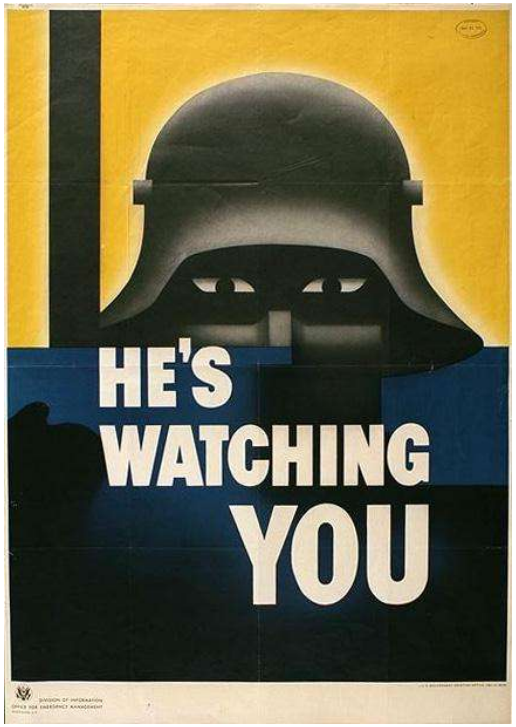
Desktop Developer's Conference 2006

Why multiple levels?

- Data/access shared with selected others



- Data/access kept secret from others



WWII US Government Propoganda Posters from

http://www.library.northwestern.edu/govpub/collections/wwii-posters/

Who uses these?

- Government agencies
  - Top Secret, Classified, Shared with Allies, Shared with other Agencies, etc.
- Companies
  - Customer Privacy Protected, Subject to Insider Trading Rules, Corporate Secret, Shared with Partners, etc.
- Consultants
  - Public, Client A, Client B, etc.
- Open Source Developers?
  - GPL vs MIT, Open Source vs. NDA/Proprietary

Common Restrictions

- Transferring information between apps
  - Copy-and-paste, drag-and-drop, properties
- Grabbing images of other apps
- Intercepting input for other apps
- Closing windows of other apps

3 Extensions add Security Labels to X

- Security (aka XC-Security)
  - Added to X11R6.3 by X Consortium
  - Included in all XFree86 & X.Org releases since
- X-SELinux
  - Created by Eamon Walsh at NSA
  - Source available in branch of X.Org monolithic CVS
- XTSol
  - Originally from Trusted Solaris, now being incorporated into Solaris & Solaris Trusted Extensions.
  - Source available under X11 license from opensolaris.org.

One more extension to hook them up

- X-ACE puts a common set of hooks into core X server for security extensions to apply policy checks
  - no actual wire protocol
- Also written by Eamon Walsh for NSA as part of SELinux X work
- Security & AppGroup extensions modified to use it
- Can be found in branch off X.Org 6.7 monolithic CVS and branch off current git modular tree
- Working to integrate for X.Org 7.2 modular release

XC-Security

- Two fixed labels: Trusted & Untrusted
- Not widely used until OpenSSH started using it
  - ssh -X : Untrusted
  - ssh -Y : Trusted
- Trusted clients have full access to X server
- Untrusted clients restricted
  - Can't steal data from Trusted clients or manipulate them

XC-Security: Restrictions on Untrusted clients

- Can only use resource ids of resources belonging to Untrusted clients (except for in a few requests)
- Can only call extensions registered as secure
- Can't query, remap, or grab keyboard
- Can't set window background to None
- Can't change access control
- Can only read/write window properties according to permissions listed in SecurityPolicy
  - `$(libdir)/xserver/SecurityPolicy` in X11R7.x

For the full list & details, see the Security Extension Spec in xorg/doc/xorg-docs/hardcopy/Xext/security.PS.gz

SE-Linux & XTSol

- Much in common since both originate from similar requirements from US Government specs
- Allow for multiple site configurable security labels or domains to separate information
- Provides a “Trusted Path” for applications with highest level security requirements
-

Trusted Path

- Guaranteed that entire path from input device, through kernel, then X server and all the way to client is only going through trusted programs and secure from snooping by untrusted programs.
- Used when inputting passwords and other sensitive data
- Specially labeled so user knows it's safe to enter password

SE-Linux

- Policies determine which actions are allowed for clients based on their client id & SELinux Security Identifier (SID)
- Policy decisions use same framework as SELinux kernel

Original announcement: "SE-X available"
http://www.nsa.gov/selinux/list-archive/0405/7030.cfm
More detailed technical report:
http://www.nsa.gov/selinux/papers/x11-abs.cfm

XTSol

- Part of Solaris Trusted Extensions™
  - Formerly separate Trusted Solaris fork of the OS
  - Now add-on extensions to Solaris 10 and beyond
  - Extension provided for both Xsun & Xorg
  - Support in both GNOME (JDS) & CDE desktops
- Every window displays security label
- All actions passed to system auditing for potential logging based on system audit policy

See OpenSolaris Security Community for more info:
http://www.opensolaris.org/os/community/security/projects/tx/

Challenges for Recent Extensions

- Composite
  - To be effective, composite manager has to be part of Trusted Path
  - Cannot interfere with window labeling
  - When applying effects like transparency, must preserve restrictions on access to contents of other windows
- XEvIE
  - Also has to be part of Trusted Path to maintain security of input devices
- X-Resource
  - What information should it expose about other labels?

What do app authors need to do?

- Be prepared for some requests to be ignored, delayed, or rejected when running in a secure environment
- Test with ssh forwarding as Untrusted client
  - If access to properties is rejected that shouldn't be, file bugs in Xorg bugzilla to get SecurityPolicy updated

Alan Coopersmith
alan.coopersmith@sun.com
http://blogs.sun.com/alanc/
http://people.freedesktop.org/~alanc/