DSC 1766

Australian Government
Department of Defence
Science and Technology

Cross Domain Desktop Compositor

A secure multi-level terminal

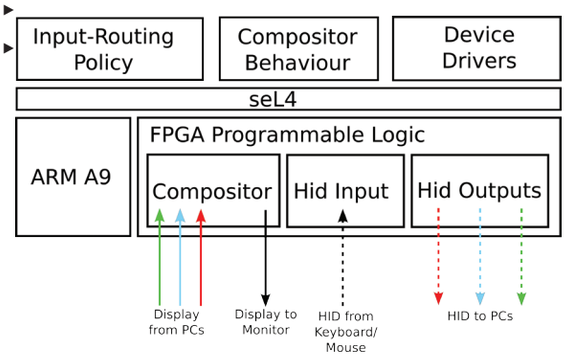
The Cross Domain Desktop Compositor (CDDC) is a cross domain access solution. The CDDC takes digital display outputs from desktop computers and creates a composited cross domain desktop experience while preserving strong isolation guarantees.

Problem

- People deal with information spanning multiple security domains or different levels of safety criticality that must remain isolated.
- A common solution is to use multiple air-gapped computers, one for each domain or criticality. Existing converged solutions are very complex, and thus untrustworthy or difficult to evaluate.
- This leads to duplication of user-facing parts of computers (e.g. monitors and keyboards), reduces usability, and complicates authorised information transfer between domains.

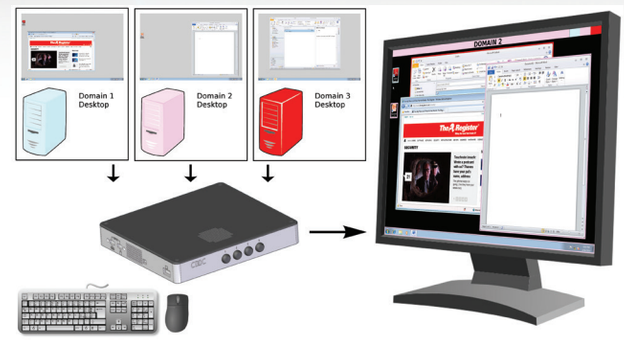
Solution

- PCs are connected to CDDC via HDMI/keyboard/mouse only!
- CDDC composes windows from each computer onto a single display.
- A single keyboard and mouse are connected to the CDDC, which forwards input to the appropriate PC.
- Isolation of PCs is enforced by hardware, and trusted software running on top of seL4.



Next Steps

- Feasibility study into formal verification that the application code that enforces security policy (running on the formally verified seL4 microkernel).
- Trusted on-screen review (and security policy enforcement) of authorised information transfer between domains.
- Non-bypassable auditing of authorised information transfer.
- Applications spanning multiple domains.



How it works

Compositor

- A display cable connects the CDDC to each PC. Each PC treats the CDDC as a monitor. The use of a display cable enforces one-way communication from the PCs to the CDDC.
- Software running on each PC encodes the position and size of each window in the video stream.
- The CDDC decodes window geometry from each PC, and draws the windows (and only the windows) of each PC to a connected monitor.
- Each window is drawn with an unspoofable border, with different colours used to distinguish windows from different domains.

Input Routing

- A USB cable connects the CDDC to each PC. Each PC treats the CDDC as a keyboard and mouse.
- Trustworthy software running on seL4 inside the CDDC reads input events from the connected keyboard and mouse and forwards them to PCs.
- The routing of input events to PCs is based on a configurable policy.