



33 SELinux-erweitertes XWindow

SELinux bietet über Flask auch die Möglichkeit, externe Object-Manager anzubinden, die für die Entscheidung, ob der Zugriff erlaubt ist, den Security-Server im Linux-Kernel fragen (siehe Kapitel 11.2).

Eine Applikation, die das nutzen könnte, ist der X-Server. Es gab in der Vergangenheit bereits mehrere Versuche, den X-Server in die Lage zu versetzen, diese Anfragen an den Security-Server weiterzuleiten. Dies hat mehrere Gründe. Im Moment bietet der X-Server wenig Möglichkeiten, die Sicherheit der verschiedenen X-Clients zu garantieren.

- **Vertraulichkeit**
Viele Applikationen nutzen als X-Client gleichzeitig einen X-Server. Es ist für eine Applikation sehr leicht, die Vertraulichkeit der weiteren gleichzeitig laufenden Applikationen zu brechen. Ein Screenshot ist sicherlich die am einfachsten nachzuvollziehende Methode, um die Ausgaben eines weiteren X-Clients zu stehlen. Auch die Zwischenablage hat auf die Daten aller Applikationen Zugriff und kann genutzt werden, um Daten einer Applikation einer weiteren Applikation zur Verfügung zu stellen. Bösertige Applikationen können diese Funktionen für sich nutzen.
- **Integrität**
Der X-Server schützt nicht die Datenintegrität. Ein X-Client kann die Ausgabe eines weiteren X-Clients direkt verändern. Bösertige Clients können auch die Eingaben weiterer X-Clients verändern und zusätzliche Daten injizieren.
- **Verfügbarkeit**
Der X-Server schützt auch seine eigene Verfügbarkeit unzureichend. Einzelne X-Clients können die Fenster weiterer X-Clients schließen und die Zeichensätze und die Zugriffskontrolllisten des X-Servers manipulieren (`xhost(1x)`).

Bereits 2003 wurden diese Probleme von Doug Kilpatrick et al. [17] erkannt und wurden erste Modifikationen an dem X-Server und SELinux vorgenommen. Diese Modifikationen waren aber lange Zeit nur als Patch verfügbar und wurden von den Distributionen nicht genutzt.

Mit dem X.org X-Server X11R7 wurde im Februar 2007 erstmalig das XACE-Framework (X Access Control Extension) aufgenommen. Dies wurde von Eamon Walsh auf dem SELinux Symposium (siehe Kapitel 34) vorgestellt [18].

XACE ist ein Satz von »hooks«, der von anderen X-Erweiterungen genutzt werden kann, um über den Zugriff zu entscheiden. Das Ziel von XACE ist der geordnete Zugriff auf die Funktionen und ähnelt damit dem LSM-Ansatz des Linux-Kernels.

XACE stellt damit eine Verallgemeinerung der bereits existenten Security-Erweiterung dar, die bisher nur ein sehr einfaches Modell unterstützte: X-Clients konnten vertrauenswürdig sein oder nicht. Nicht vertrauenswürdige X-Clients wurden in bestimmten Bereichen beschränkt. Die einzige Applikation, die diese bisher vorhandene Funktion tatsächlich genutzt hat, ist die Secure-Shell, die zwei verschiedene Arten des X-Forwarding kennt (-X und -Y). XACE ersetzt zum größten Teil die vorhandenen sicherheitsspezifischen Prüfungen mit Callback-Funktionen. Diese können dann von zusätzlichen Modulen genutzt werden. Hierzu gehört dann auch SELinux.

Auf der Roadmap für die Version X11R7.3 des X.org X-Servers ist die Unterstützung von SELinux aufgeführt. Diese Version wurde im August 2007 erwartet und wurde bisher noch nicht veröffentlicht.