Xsecurity

Contrôle d'accès aux affichages X. X fournis un mécanisme pour implémenter de nombreux systèmes de contrôles d'accès. L'implémentation actuelle inclus 5 mécanismes.

Host Access Simple host-based access control

MIT-MAGIC-COOKIE-1 Shared plain-text "cookies"

XDM-AUTHORIZATION-1 Secure DES based private-keys

SUN-DES-1 Based on Sun's secure rpc system

Server Interpreted Server-dependent methods of access control

Description des systèmes d'accès

Host Access Tout client sur un hôte dans la liste est autorisé à accéder au serveur X.

MIT-MAGIC-COOKIE-1 Le client envoie un coockie 128bits avec les informations d'initialisation de connexion. Si le coockie match celui que le serveur a, l'accès est donné.

XDM-AUTHORIZATION-1 Similaire au précédent mais utilise une clé 56bits DES et une donnée aléatoire 64bits.

SUN-DES-1 SunOS supporte un système RPC à clé public.

Server Interpreted Fournis 2 chaînes au serveur. La première représente le type d'entrée, et le second contient la valeur de l'entrée.

Le fichier d'autorisation

Excepté pour les mécanismes Host Access est Server Interpreted, chaque système utilise des données dans le fichier .Xauthority pour générer les informations d'autorisation à passer au serveur X lors de la connexion. MIT-MAGIC-COOKIE-1 et XDM-AUTHORIZATION-1 stockent des données secrètes dans ce fichier, donc tout ceux qui peuvent lire ce fichier peuvent avoir accès au serveur. Chaque entrée dans le fichier .Xauthority match une famille de connexion (TCP/IP, DECnet ou local) et le nom de l'affichage X (hostname et la numéro d'affichage). Une famille spéciale, FamilyWild (valeur 65535) force une entrée à matcher tout affichage, permettant l'entrée d'être utilisée pour toutes les connexions.

Le serveur X, lorsqu'il fonctionne sur une station de travail, lit les informations depuis le fichier passé sur la ligne de commande avec l'option -auth. Les entrées d'autorisation dans ce fichier sont utilisés pour contrôler les accès au serveur. Dans chaque schéma listé ci-dessous, les données nécessaire au serveur pour initialiser un schéma d'autorisation sont identique aux données nécessaires au client pour générer les informations d'autorisation. Le même fichier peut être utilisé par les 2 processus.

MIT-MAGIC-COOKIE-1 Ce système utilise 128bits de données partagées entre l'utilisateur et le serveur X, Une collection le bits peut être utilisé, Xdm génère ces clés en utilisant un générateur de nombre pseudo-aléatoire, donc la prochaine clé de session ne peut pas être calculée depuis la clé de session courante.

XDM-AUTHORIZATION-1 Ce système utilise 2 informations. 64bits de données aléatoires, et une clé DES 56bits (donnée aléatoire). Xdm génère ces clés en utilisant le même générateur de nombre pseudo-aléatoire que MIT-MAGIC-COOKIE-1.

SUN-DES-1 Ce système nécessite une représentation chaîne du principal qui identifie le serveur X associé. Cette information est utilisée pour chiffrer les informations d'autorisation du client quand elles sont envoyées au serveur. Quand xdm démarre X, il utilise le principal root de la machine sur lequel il tourne (ex : unix.hostname@domain) En plaçant le nom principal correcte dans le fichier .Xauthority, Xlib génère les informations d'autorisation en utilisant la librairie secure RPC.

Types d'accès Server interpreted

IPv6 Une adresse IPv6

hostname Le nom d'hôte

localuser & localgroup Sur les systèmes qui peuvent déterminer les acréditations d'un processus client, ces méthodes fournissent un accès basés sur ces acréditations. Le format des valeurs fournis est spécifique à la plateforme.