Défi SEC-SI

Systèmes Embarqués et Grandes Infrastructures Défi Sécurité
Année 2008

AGENCE NATIONALE DE LA RECHERCHE
ANR

SAFE-OS

Système d'exploitation sécurisé et cloisonné pour l'internaute
http://safe-os.lri.fr/

Thomas Hérault[1], François Lesueur[1]
Sylvain Peyronnet[1], Ala Rezmerita[1]
Sébastien Tixeuil[2]

[1]LRI, Université Paris-Sud 11, ORSAY
[2]LIP6, UPMC Paris Universitas, Paris

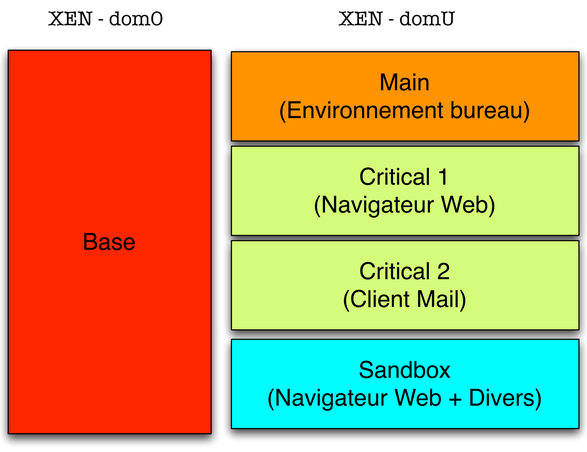
Objectif

Mettre à la disposition des citoyens un système d'exploitation sécurisé permettant d'accéder depuis un ordinateur aux services de banque en ligne, d'e-administration et d'envoi de messages signés.

Utilisabilité *Confidentialité* *Intégrité* *Adaptabilité*

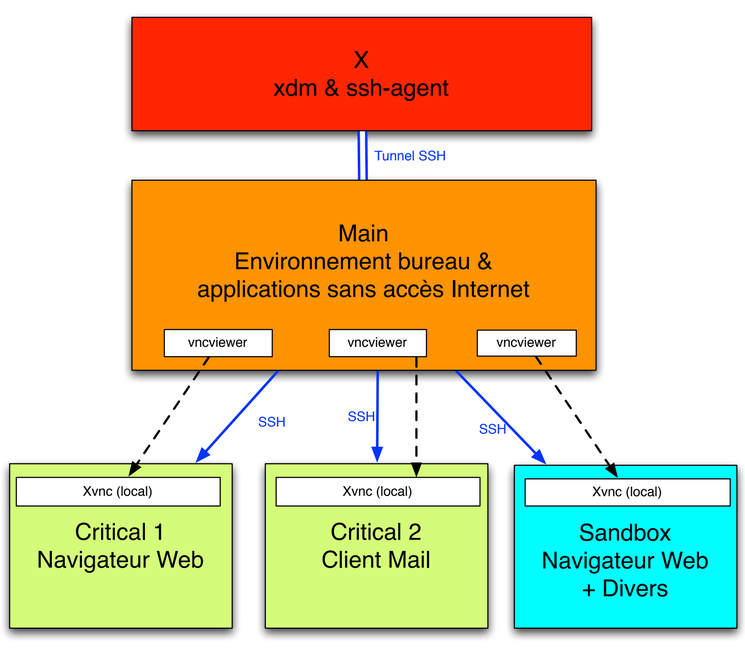
Architecture

Virtualisation XEN

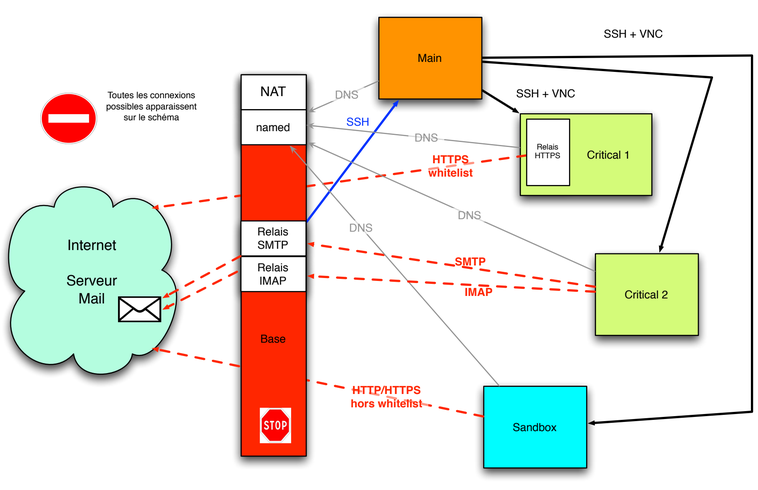


- Nombre variable de machines virtuelles
- Chaque machine virtuelle possède son propre niveau de sécurité et ses applications dédiées

Schéma de communication



Filtrage



- Pare-feu et relais gérés dans le dom0
- Seuls les services nécessaires sont autorisés

Fonctionnalités

Mise à jour automatique

- Nécessité de maintenir les restrictions d'accès Internet pour les VM
- Mise à jour au démarrage de la machine
- Modèle pour chaque VM sur la machine physique
- Mise à jour de ces modèles (*apt-get*)
- Propagation des changements (*rsync*)

→ **Le processus de mise à jour des VM empêche la fuite d'information**

Filtrage de la VM mail

Filtrage des mails sortants (SMTP)
- *Whitelisting* des destinataires
- Gestion interactive des destinataires autorisés
- Le filtre en dom0 force la connexion vers un serveur SMTPS de confiance
- Utilisation d'un filtre *ad hoc* avec *ProxSMTP* (http://memberwebs.com/stef/software/proxsmtp/)

Filtrage des mails entrants (IMAP)
- Le filtre en dom0 force la connexion vers un serveur IMAPS de confiance avec le *login* de l'utilisateur
- Utilisation de *Perdition* (http://www.vergenet.net/linux/perdition/)

Filtrage de la VM web

- Seules les connexions HTTPS sont autorisées
- *Whitelisting* des sites autorisés
- Le relais est exécuté dans la VM web
- La VM web est considérée non corrompue, car limitée aux sites de confiance
- Utilisation de *Tinyproxy* (https://www.banu.com/tinyproxy/)

→ **Le processus de filtrage empêche les connexions vers les sites malveillants**

Perspectives

Migration des données

- Chaque VM a son propre système de fichiers
- La sauvegarde des pièces jointes doit parfois être accessible depuis une autre VM
- Certaines données non critiques devraient pouvoir être envoyées par mail

→ Transfert de données entre VM
→ Application dédiée sur la VM Main (environnement bureau)

Whitelists collaboratives

- Les whitelists sont difficiles à maintenir
- Différents utilisateurs peuvent avoir besoin d'accéder à des sites différents
- Les utilisateurs ont des niveaux d'expertise différents

→ Algorithmes collaboratifs
→ Création de *whitelists* générales
→ Modération des ajouts dans les *whitelists* locales

LABORATOIRE DE RECHERCHE EN INFORMATIQUE
UNIVERSITÉ PARIS-SUD 11
cnrs dépasser les frontières
INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE
INRIA centre de recherche SACLAY - ÎLE-DE-FRANCE
LIP6
UPMC PARIS UNIVERSITAS