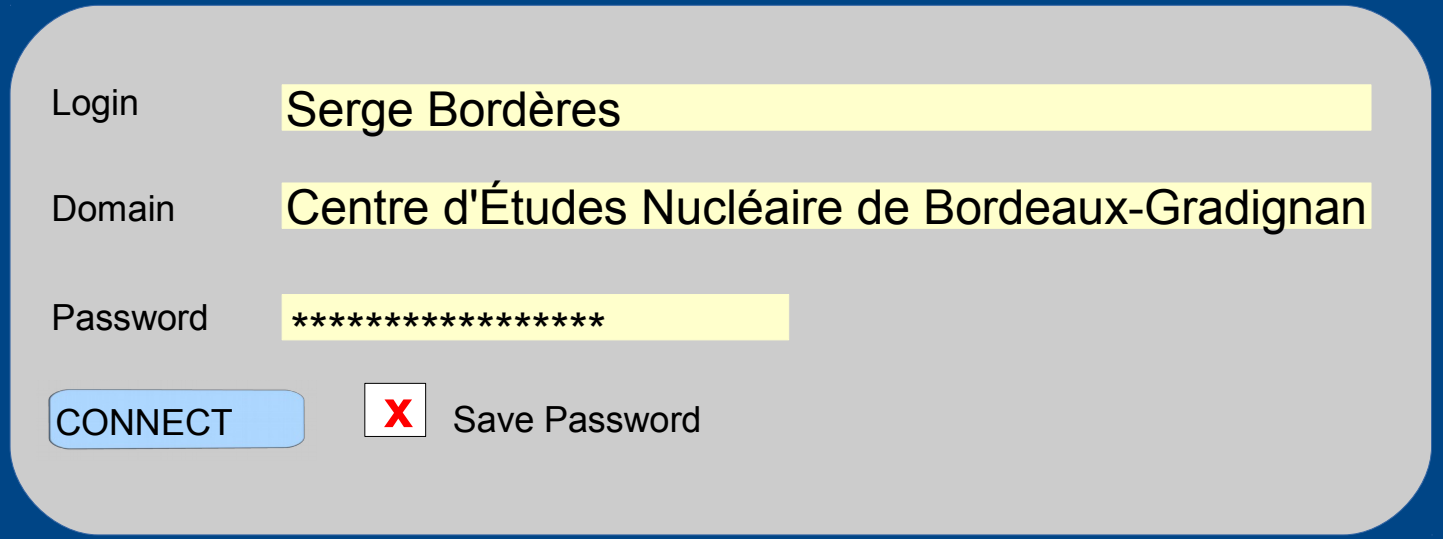
jres Montpellier 2015

Du smartphone au frigo : la grande évasion du mot de passe



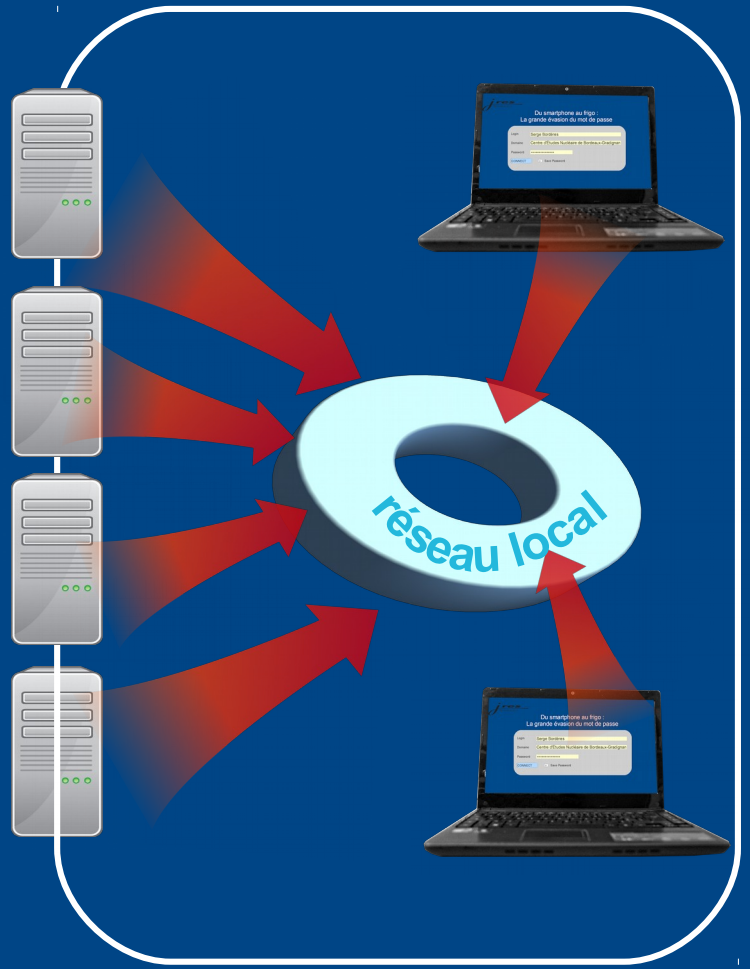
cnrs dépasser les frontières

9 novembre 2015

université de BORDEAUX

L'ancien temps

- « Avant », on savait ce qu'il y avait dans le système d'information.
- Il existait une ligne de front claire.



La sphère personnelle connectée

L'attaque des objets

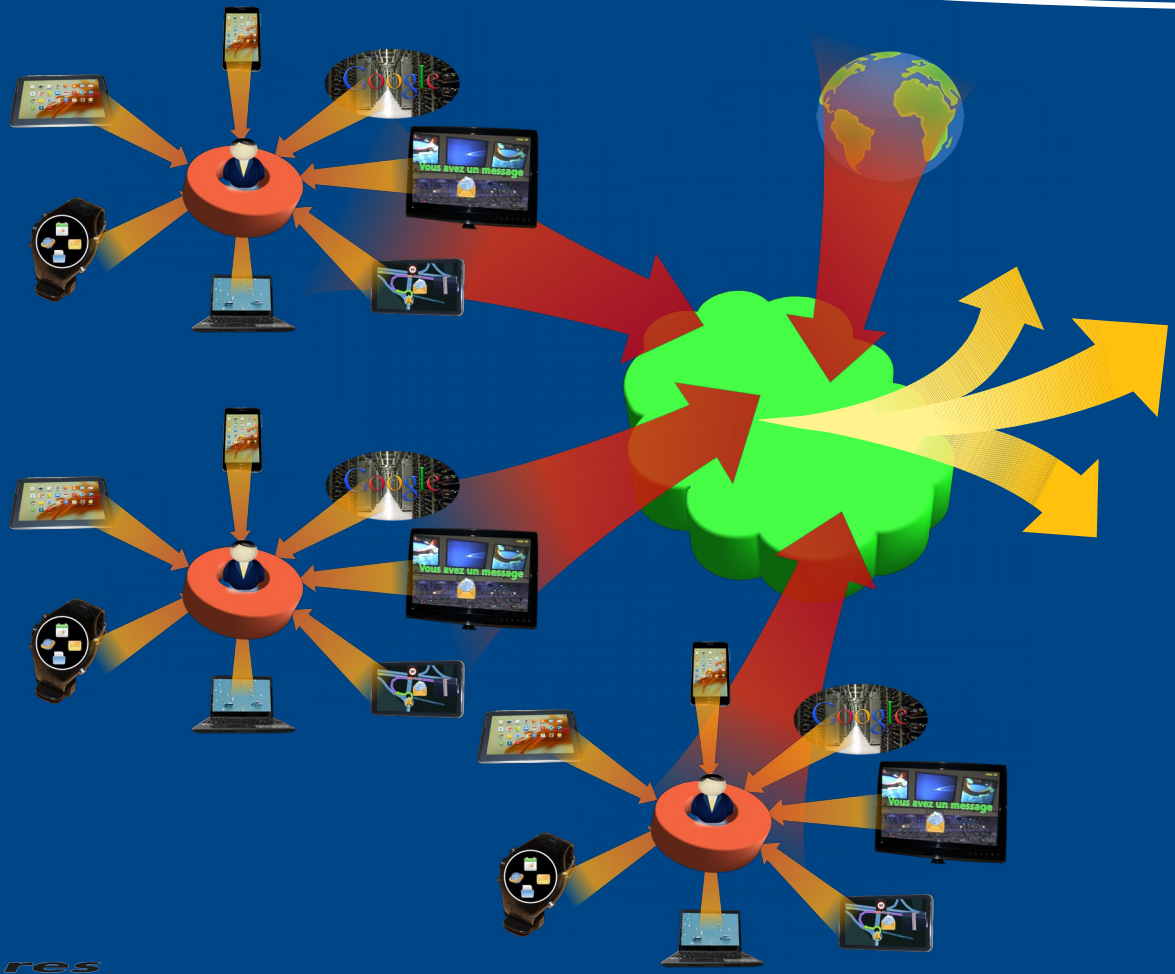
- D'après la société Proofpoint, fin décembre 2013/début 2014, une vague d'attaques par mail a été détectée. Au moins 25 % de ce trafic provenait de divers objets tels que des box Internet, des télévisions et au moins un réfrigérateur

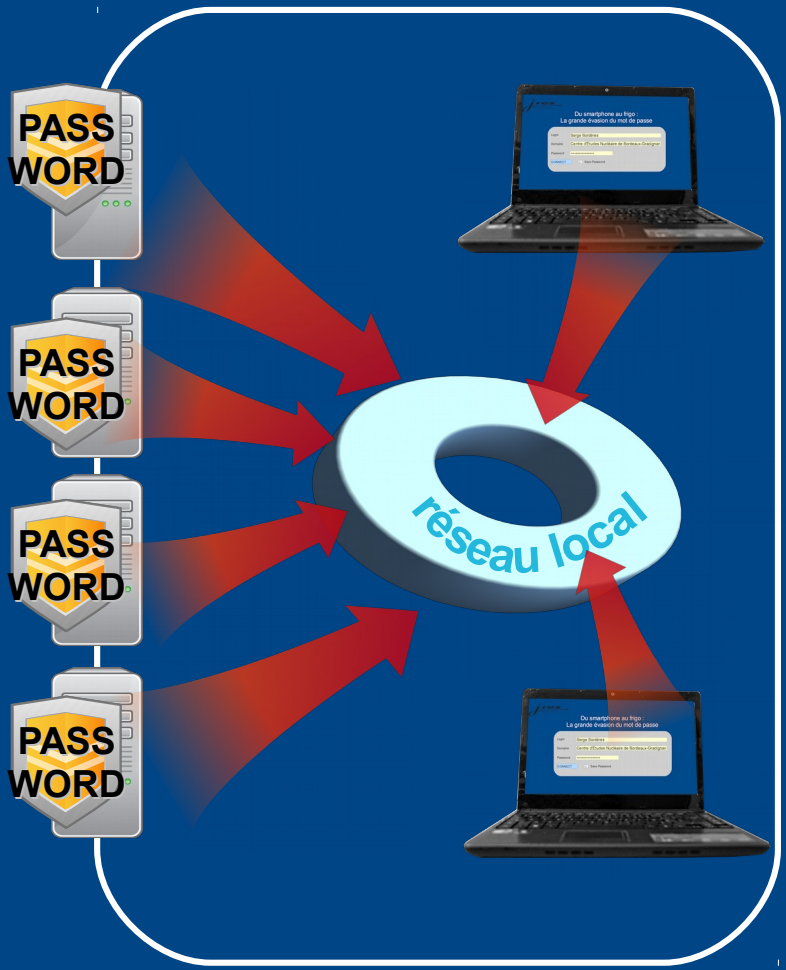
- La société Pentester a annoncé en août 2015 avoir découvert une faille d'implémentation SSL dans un réfrigérateur qui permet une attaque man-in-the-middle

Password Inside

- Quasiment toutes les applications clientes imposent l'enregistrement des mots de passe
- Dans des conditions souvent inconnues et en tout cas très hétérogènes
- Les mots de passe se diffusent dans une multitude d'appareils ou prestataires
- Attaquer un matériel connecté (du smartphone au frigo en passant par le PC classique) c'est la certitude d'y trouver des identifiants, y compris professionnels !

Fin de la ligne de front





Fin de la ligne de front

- Un système d'information qui met en œuvre des services accessibles par de simples mots de passe favorise l'usage de matériels personnels.
- La ligne de front disparaît puisque n'importe quel terminal peut se connecter. Les matériels n'apparaissent plus sur notre radar.
- Le périmètre du système d'information devient (très) flou.
- Le BYOD (Bring Your Own Device) c'est dépassé.
  Nous sommes au IUMOD (I Use My Own Device).

Oui, mais c'est interdit !

- *EXP-MAIT-MAT : maîtrise des matériels. Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité.* ***La connexion d'équipements non maîtrisés****, non administrés ou non mis à jour par l'entité (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles)* ***sur des équipements et des réseaux professionnels est interdite****.*

- *EXP-CONF-AUTH : confidentialité des informations d'authentification. Les informations d'authentification (****mots de passe*** *d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des* ***données sensibles****.*

Oui, mais le monde change

- Les nouvelles technologies sont introduites dans la sphère privée avant la sphère professionnelle. La société a désormais une très grande influence sur les comportements numériques.

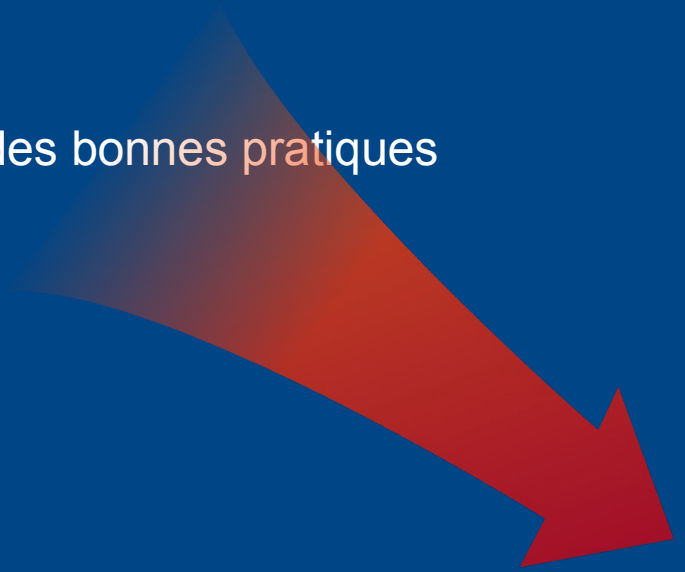
- Le foisonnement de systèmes, d'applications, de technologies complexifie l'environnement de l'utilisateur tout en lui donnant de nouvelles possibilités d'interagir avec son environnement professionnel.

- La voix des ASR porte de moins en moins

Où est-ce que ça fuit ?

De partout

Du non respect des bonnes pratiques



A des attaques très techniques

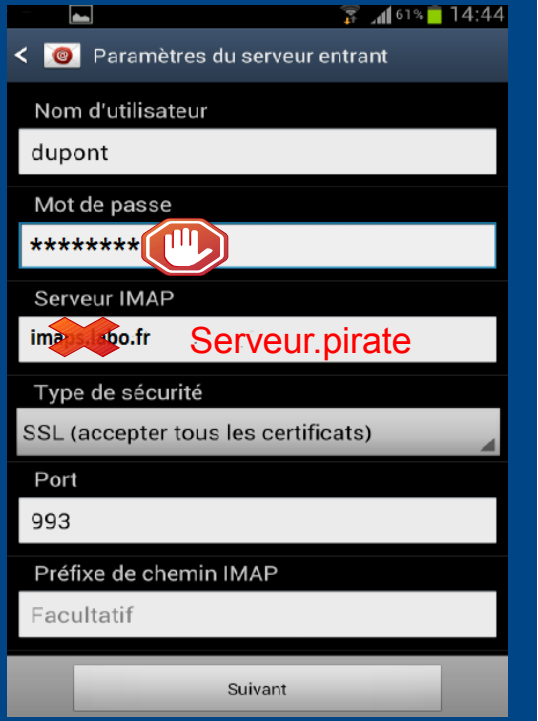
Où est-ce que ça fuit ?

Recette pour voler un mot de passe sans rien connaître à Android ou iOS

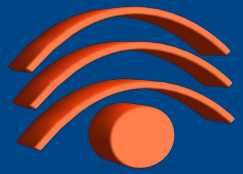
1. Procurez-vous un mobile Android ou iOS sans code de verrouillage d'écran.

2. Dans les paramétrages du client de mail, sans toucher au champ mot de passe, faites pointer le serveur de mail vers votre serveur pirate.

3. Dans le système d'authentification de votre serveur pirate (PAM par exemple) tracez le mot de passe qui passe en clair (Pam_exec)



Où est-ce que ça fuit ?



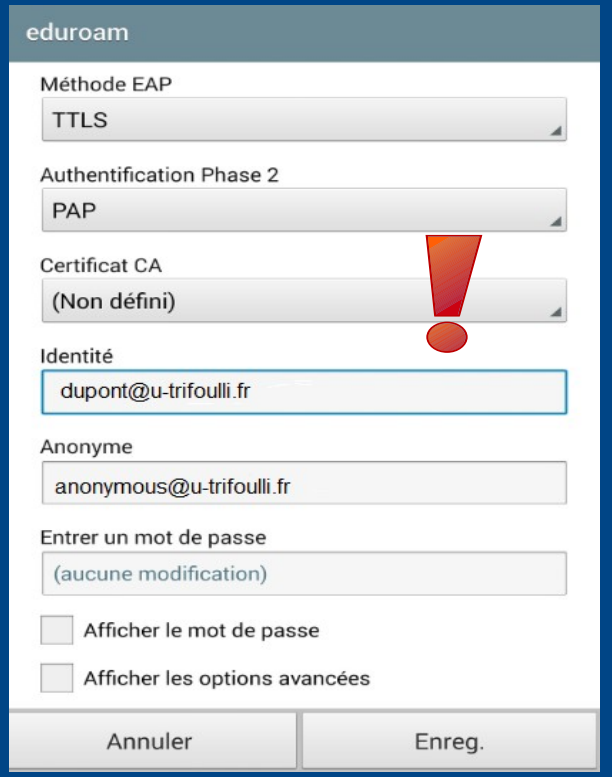
Recette pour voler un mot de passe sans toucher aucun appareil

1. Installez-vous dans un endroit passant, placer une borne Wifi et diffusez le SSID Eduroam.
2. Adossez le SSID à votre propre serveur Radius.
3. Lancez le serveur Radius en mode debug.
4. Attendez …..
5. Dès que quelqu'un tentera de se connecter à Eduroam vous avez de grandes chances de lui voler son mot de passe.

Où est-ce que ça fuit ?

Recette pour voler un mot de passe sans toucher aucun appareil

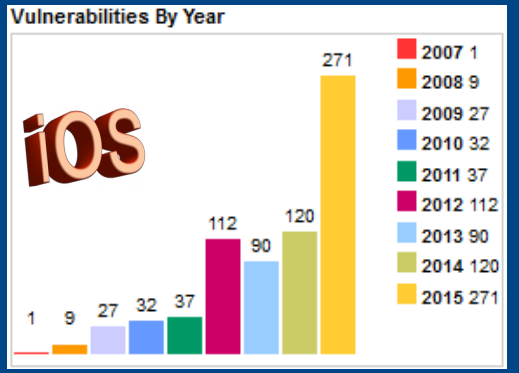
- Souvent le SSID Eduroam est mal configuré.
- Les aides en ligne ne donnent pas toujours la bonne procédure.
- Les mauvaises pratiques se propagent d'utilisateurs à utilisateurs.

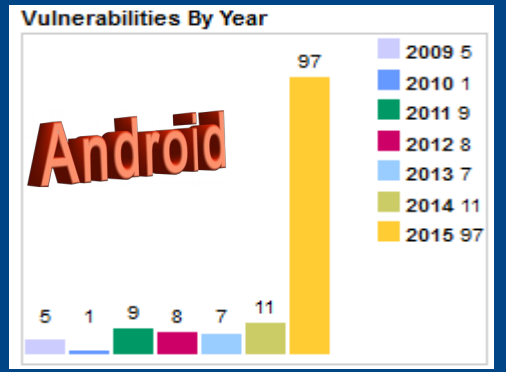


Où est-ce que ça fuit ?

Par les vulnérabilités des terminaux, mobiles, objets….

- Tous les systèmes d'exploitation contiennent des vulnérabilités utilisables pour voler des informations à distance.
- Les mobiles n'y échappent pas, les objets connectés encore moins.
- L' « objetisation » minimise la notion de sécurité au nom de la simplicité, de la fonctionnalité ou de la modernité.





Où est-ce que ça fuit ?

Dans une sphère privée qui a accès au mot de passe ou à ce qu'il autorise ?

- La famille ?
- Les personnels des centres de recyclage ? Les réparateurs ?

Enquête Symantec sur la mobilité - 2015

- A l'insu du propriétaire seriez-vous prêt à vous servir de son smartphone → oui= 52 %
- Je suis la seule personne à utiliser mon smartphone → oui = 77 %
- Je suis la seule personne à utiliser ma tablette → oui= 29 %

http://www.youscribe.com/catalogue/tous/etude-de-symantec-norton-sur-la-mobilite-2015-2583578

Accentuer la sensibilisation ?

- Les règles et sensibilisations ne pourront pas enrayer à elles seules l'évasion des mots de passe.

- Parce que les utilisateurs sont déjà assommés de consignes et doivent acquérir un niveau de compétence, multi-systèmes, élevé qui pousse au relâchement des bonnes pratiques.

(re-)créer une ligne de front

Durcir les terminaux ? (MDM, conteneurs...)

- Cela n'aura pas beaucoup d'effet tant qu'il restera possible de se connecter avec n'importe quoi (durcir une TV ?).

Authentifier qui se connecte, avec quoi et comment.

- Mettre en œuvre des méthodes et protocoles permet de fortement minimiser les risques de dispersion des terminaux et des mots de passe.

Dispositif pour les nomades au CENBG

Quelques mots sur le Centre d'Études Nucléaire de Bordeaux-Gradignan

- Laboratoire mixte CNRS-IN2P3/Université de Bordeaux.
- Environ 120 personnes / 9 groupes de recherches.
- Recherches fondamentales et expérimentales sur la structure du noyau, astroparticules, neutrinos.
- Recherches interdisciplinaires, traitement des déchets, actions des rayonnements, métaux et nanoparticules sur le vivant, excitation nucléaires par laser.
- 3 plate-formes expérimentales dont un accélérateur de particules.
- Population historiquement très mobile.

Dispositif pour les nomades au CENBG

Contexte technique

Connexion au réseau local

- Toute machine présente sur le réseau local est authentifiée.
- Sur le réseau filaire avec adresse MAC (802.1X possible).
- WIFI : WPA2 Enterprise avec EAP/TLS (certificat).
- Environ 40 Vlans.

Connexion depuis Internet

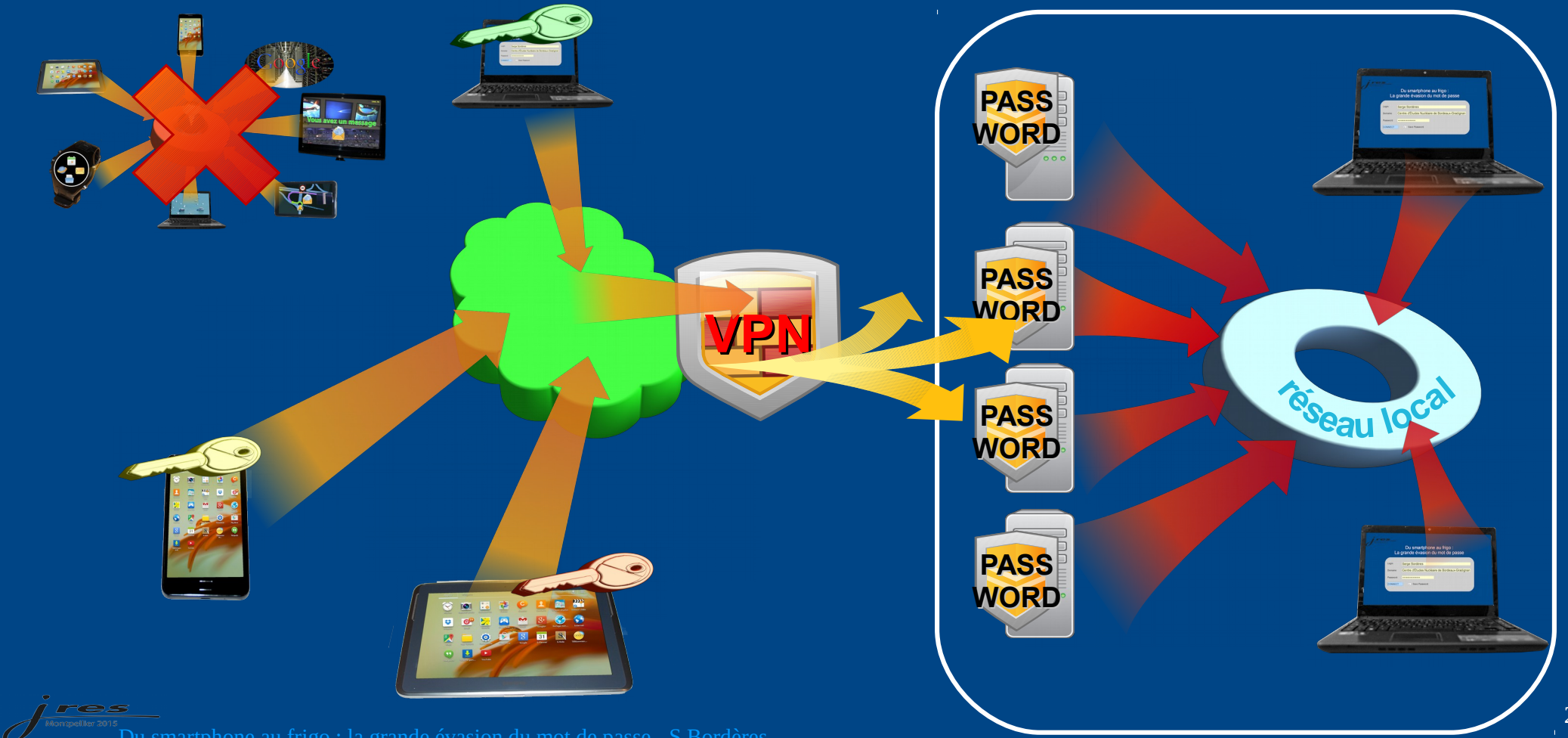
- De plus en plus par VPN (OpenVpn). ~1800 connexions/mois.
- Authentification à double facteur (certificat + mot de passe indépendant).
- Peu de choses directement accessibles. Par exemple, IMAP accessible uniquement par VPN.

Dispositif pour les nomades au CENBG

Le projet

- Comment intégrer les mobiles ? (Android et iOS). Comment profiter des nouvelles technologies, se connecter de partout mais pas avec n'importe quoi ?
- Sans affaiblir la sécurité :
  - Garder la connaissance et la maîtrise du parc.
  - Réduire les risques d 'évasion des mots de passe.
- Le plus simple possible pour l'utilisateur.
- Pas d'investissement matériel ou logiciel.
  Utilisation des moyens déjà existants.
  - OPENVPN
  - FREERADIUS
  - IGC Local

Dispositif pour les nomades au CENBG



Dispositif pour les nomades au CENBG

Authentification VPN à double facteur

1er facteur : Un certificat issue d'une IGC local spécifique.

- Chaque machine a un certificat spécifique, installé par le service informatique.
- Dans le magasin du système d'exploitation (pas dans les applications).
- Pas exportable.
- Dans Android et iOS, l'import du certificat impose le positionnement d'un code de verrouillage d'écran.

Dispositif pour les nomades au CENBG

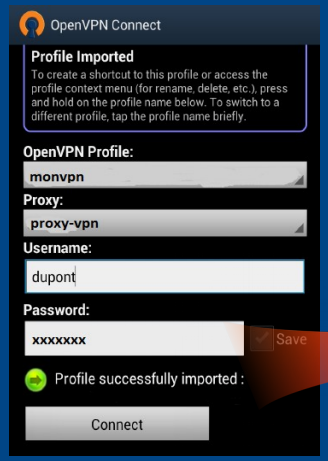
Authentification VPN à double facteur

2ème facteur : Un mot de passe qui ne doit PAS être enregistré.

- Le principe : l'enregistrement du mot de passe doit être plus compliqué que le contraire.
- Ce mot de passe ne peut pas être compliqué compte tenu de l'ergonomie des mobiles.
- La méthode : un mot de passe variable.
  - Formé d'une partie secrète (un code pin de 4 chiffres par exemple).
  - Suivi de caractères aléatoires, différents entre 2 connexions.
- La seule chose que devra taper l'utilisateur pour être connecté sur l'application.

Dispositif pour les nomades au CENBG

Principe du mot de passe variable



ABCDXY

VPN

XY

Idem précédente Connexion ?

OUI

NON

RADIUS

ABCD

Secret valide ?

OUI

NON

Dispositif pour les nomades au CENBG

Configuration d'une application avec un mot de passe aléatoire

- La méthode consiste à retourner le problème de l'enregistrement du mot de passe en un avantage.
- Le mot de passe fourni à l'application est un mot de passe aléatoire (Token), que l'utilisateur n'a même pas besoin de connaître.
- Ce Token devient le mot de passe de l'utilisateur pour cette application, sur ce terminal.
- Dispositif proche du protocole Oauth utilisé par Google. Mais les applications ne sont pas compatibles.

Dispositif pour les nomades au CENBG

Configuration d'une application : mail

- La première fois l'utilisateur ouvre sa connexion VPN.
- Il entre un mot de passe en tapant aléatoirement sur le clavier.
- Ce mot de passe devient son mot de passe pour la messagerie sur cet appareil.
- Ce mot de passe est enregistré.
  - Il ne le connaît pas.
  - Il n'est utilisable qu'à travers la connexion VPN.

Dispositif pour les nomades au CENBG

Techniquement, par rapport à l'existant

- La gestion du mot de passe variable pour le VPN représente ~30 lignes de Bash.
- La gestion du mot de passe aléatoire ~90 lignes de Bash.
- Deux lignes supplémentaires dans la configuration PAM du serveur.
  Associé à un script Bash d'interrogation du serveur Radius (entre 30 et 50 lignes suivant ce qu'on veut faire).

Dispositif pour les nomades au CENBG

Bénéfices

- L'ensemble des terminaux utilisables est connu.
- Tous les systèmes utilisent le même procédé.
- Possibilité de révocation des certificats ou des autorisations (Radius) par machine.
- Dates d'expiration des certificats ou autorisations pour sortir les machines inutilisées.
- L'utilisateur reçoit une notification à l'approche de l'expiration de ses autorisations ou certificats.
- L'administrateur dispose d'un rapport hebdomadaire des futures expirations.

Dispositif pour les nomades au CENBG

Bénéfices

- Si le mot de passe applicatif (token) est compromis, il n'est pas utilisable sans la connexion VPN.

- Applications testées
  - Mail (à priori avec n'importe quel client).
  - Synchronisation d'agenda Owncloud.
  - Synchronisation de fichiers Owncloud.

Dispositif pour les nomades au CENBG

Inconvénients

- Sur le serveur applicatif l'authentification doit passer par PAM.
- Le mot de passe aléatoire doit être tapé...parce que les applications ne prévoient pas de générer un mot de passe aléatoire.

Dispositif pour les nomades au CENBG

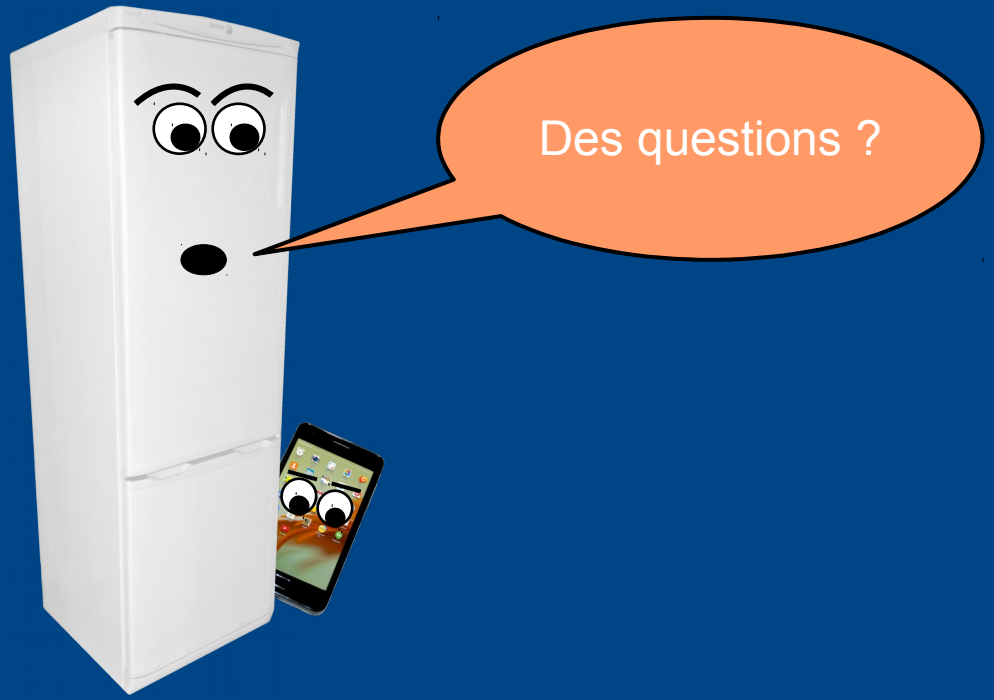
Retour d'expérience

- Environ 80 utilisateurs VPN (tous systèmes confondus)
- Pour les mobiles (avec mot de passe aléatoire pour les applications)
  - Pas de recherche de diffusion massive.
  - Plutôt associer quelques utilisateurs pour éprouver la solution.
  - Élargissement possible avec confiance dans le procédé.
  - Aujourd'hui 10 utilisateurs avec mobiles / 12 smartphones ou tablettes.
  - Principalement Android. Un iOS.

Dispositif pour les nomades au CENBG

Futur ?

- Comment utiliser des protocoles tels que Oauth ou du type Google Auth ?
  - → Mais il faut que les applications clientes soient compatibles.
- Généraliser le principe des tokens sur tous les types de système.


Des questions ?