Sécurité et Mobilité

Jeudi 7 février 2013

Coordination scientifique :
– ***Luc Boucher*** *(Euriware)*
– ***Guillaume Désveaux*** *(CISCO)*

Amphithéâtre Becquerel, École Polytechnique, Palaiseau

http://www.association-aristote.fr
info@association-aristote.fr

Edition du 1 ventôse an CCXXI (*vulg.* 19 février 2013)

ARISTOTE Association Loi de 1901. Siège social : CEA-DSI CEN Saclay
Bât. 474 91191 Gif-sur-Yvette Cedex.
Secrétariat : Aristote, École Polytechnique, 91128 Palaiseau Cedex.
Tél. : +33(0)1 69 33 99 66 Fax : +33(0)1 69 33 99 67
Courriel : Marie.Tetard@polytechnique.edu
Site internet http://www.association-aristote.fr

Table des matières

Chapitre 1

Programme de la journée

1.1 Introduction

Auparavant, les employeurs fournissaient des ordinateurs de bureau et portables qui étaient généralement les outils les plus avancés auquel un employé a eu accès. L'explosion des appareils grand public, ordinateurs portables, *netbooks*, tablettes, *smartphones*, *e-readers*, et d'autres ont consacré la consumérisation de l'informatique.

Aujourd'hui les employés ont généralement des outils de productivité plus avancés dans leur vie personnelle que ceux proposés par l'entreprise. Rapidement les employés ont demandé à leurs organisations informatiques de pouvoir utiliser ces outils de productivité au travail. De nombreuses organisations informatiques ont d'abord rejeté l'idée, invoquant des raisons de sécurité et l'incapacité de les gérer à l'échelle de l'organisation. Cette réponse a aussi entrainé une attente forte de la part des utilisateurs de disposer d'équipements de productivité fournis par l'informatique interne pour remplir leur mission.

Avec plus de sept milliards d'appareils mobiles prévus pour entrer dans l'entreprise en 2015, les salariés sont de plus en plus mobiles. Dans de nombreux pays, l'adoption des *smartphones* atteint 50%, suivie de près par les tablettes. Cette tendance, combinée à la popularité grandissante de la vidéo et d'autres applications multimédia, met la pression sur les services informatiques pour prendre en compte ces nouveaux équipements.

Aujourd'hui moins de 50% des entreprises françaises autorisent l'utilisation de terminaux mobiles personnels au travail. Aux Etats-Unis en Asie et en Amérique latine, ce pourcentage grimpe allègrement à 80%. En effet 33% des responsables informatiques jugent que la sécurité est le premier obstacle au développement du *Byod*. Toutefois pour 15% d'entre eux les salariés concernés sont plus efficaces, 12% assurent que leur satisfaction s'en ressent, 17% assurent que le *Byod* permet de réduire les coûts en entreprise.

Le matin : nous développerons ces tendances et les contraintes réglementaires et organisationnelles dans laquelle elles s'inscrivent.

L'après-midi : nous aborderons les solutions et les retours d'expériences sur la façon de répondre à ces enjeux de façon efficace :

- se connecter au réseau de votre entreprise où que vous soyez ;
- sécuriser les données des équipements ou qu'ils soient ;
- automatiser l'ajout de nouveaux périphériques au réseau ;
- appliquer des politiques dans tous les dispositifs sur le réseau et gérer les identités ;
- gérer filaire, sans fil, `VPN`, et de l'identité d'une interface utilisateur unique ;
- tracer et contrôler les informations qui entrent et sortent du système d'information.

1.2 Programme

08h45-09h15	*Accueil des participants, café*	
09h15-10h00	**Benjamin Morin** (ANSSI)	BYOD : Maîrise et sécurité
10h00-10h30	**Dominique Mouchet** (Altetia)	La consumérisation du marché de l'informatique et le BYOD
10h30-11h00	**Loup Gronier** (LEXSI)	Retour d'expériences issues des audits
11h00-11h15	*Pause café*	
11h15-11h45	**Sébastien Bombal** (AREVA)	Le problème posé dans un Groupe industriel
11h45-12h15	**Sid Lazizi** (Mobile Iron)	Le MDM, les tendances et évolutions
12h15-12h45	**Patrick Borras** (UCOPIA)	Internet et les obligations légales, la réponse UCOPIA
12h45-14h00	*Déjeuner (salon de marbre)*	
14h00-14h30	**Pascal Michel, Thierry Bôle** (IFPen) **Christophe Corlay** (IFP SChool)	IFP Energies nouvelles et IFP School – deux points de vue sur la mobilité
14h30-15h30	**Yvic Le Scouezec** **Frederic Buisson** (CISCO)	La gestion de la mobilité et des équipes en interne
15h30-15h45	*Pause*	
15h45-16h15	**Laurent Gydé** (Renater)	La mobilité sécurisée par les services RENATER – la fédération d'identité pour la mobilité numérique – eduroam pour l'accès wifi fédéré
16h15-16h45	**Jacques Le Rest** (Ifremer)	Solution d'accès Wifi UCOPIA
16h45-17h15	**Philippe Breider** (Vmware)	VXI
17h15	Conclusions de la journée	

Chapitre 2

Compte-rendu de la journée

Ce compte-rendu a été réalisé par Alice Albessart pour l'agence Umaps-Communication de la recherche et de l'innovation `http://www.umaps.fr`.

Sécurité et Mobilité

Le séminaire est lancé par les organisateurs Luc Boucher (Euriware) et Guillaume Désveaux (Cisco) qui souhaitent que cette journée d'étude soit l'occasion de recouper l'ensemble des problématiques liées aux questions de sécurité et de mobilité exacerbées par l'apparition d'une nouvelle pratique : le `BYOD` (Bring Your Own Device)

Benjamin Morin (ANSSI) BYOD : Maîrise et sécurité

Benjamin Morin a abordé d'emblée les risques liés au BYOD : le vol de données, la prise de contrôle à distance, l'espionnage, mais aussi la perte, l'emprunt, les applications malveillantes, indiscrètes ou vulnérables, les failles du système, la maîtrise limitée des terminaux par l'utilisateur.

Face à ces risques, il nous recommande de prendre des mesures appropriées, par exemple, en optant pour des terminaux sécurisables, en interdisant l'installation d'applications, et en imposant une authentification robuste du porteur. A l'heure actuelle, les propriétaires de smartphones n'ont qu'une maîtrise limitée de leurs terminaux, alors qu'ils devraient être en mesure de les contrôler et de les sécuriser.

Benjamin Morin met en avant l'incompatibilité du BYOD avec certains impératifs de sécurité. Il s'agit d'une pratique inadaptée, le concept même du BYOD accentue ce problème de maîtrise. En effet, si l'employeur n'est pas le propriétaire du terminal, il n'a pas les moyens d'imposer les restrictions et les règles de sécurité nécessaires à la protection de ses données. Pour y remédier, les solutions existantes à ce jour se présentent souvent comme des applications qui encapsulent des outils et données professionnelles, et ne nécessitent aucune modification des terminaux. Mais cette approche, consistant à mettre les biens sensibles sous le contrôle d'un environnement hostile, apparaît comme structurellement inadaptée. L'alternative proposée par Benjamin Morin est celle du UYED (*Use Your Employer Device*). Elle postule l'utilisation d'un terminal professionnel permettant d'accomplir des tâches personnelles et non l'inverse.

Une autre solution réside dans l'application d'une gestion multi-niveau dans l'utilisation du BYOD. Le multi-niveau doit garantir l'isolation entre des environnements à exécution séparée, et permettre de séparer le domaine personnel du domaine professionnel. Ce système s'appuie sur un socle de confiance et des primitives de cloisonnement garantissant l'étanchéité entre les domaines. Mais pour être efficace les primitives de cloisonnements doivent être implantées dans les couches logicielles basses des terminaux Si cette solution est séduisante en théorie, elle est compliquée à mettre en place puisqu'elle implique de modifier en profondeur les systèmes d'exploitation, opération difficilement envisageable sur un mobile dont le propriétaire n'est pas l'employeur. En partant de l'hypothèse d'un OS de smartphone nativement équipé de ces primitives de cloisonnement, on pourrait envisager deux configurations sécurisées : le BYOD multi-niveau qui suppose une confiance mutuelle et dans laquelle l'employeur a la possibilité d'imposer des règles de sécurité, ou le UYED multi-niveau.

On voit arriver aujourd'hui des technologies matérielles ARM Trustzone. De même l'utilisation de DRM pourrait s'appliquer au BYOD en protégeant les données de l'employeur même en cas de compromission du terminal.

Ces solutions n'excluent pas pour autant certaines interrogations quant à la personnalisation et à l'administration de l'environnement sécurisé, aux garanties d'isolation au sein de l'environnement sécurisé ou au contrôle de l'environnement d'exécution sécurisé. Pour conclure, si Benjamin Morin n'est pas fondamentalement opposé au BYOD, en l'état actuel de la technologie, il ne le recommande pas.

Dominique Mouchet (Altetia) La consumérisation du marché de l'informatique et le BYOD

Dominique Mouchet a commencé par rappeler ce qu'il convient d'appeler consumérisation. Il y a encore peu de temps, les usages informatiques professionnels influençaient ceux de la sphère privée, or aujourd'hui cette tendance s'inverse et ce sont les connaissances et les outils personnels des employés qui sont mis au service du monde professionnel. S'il convient de souligner le danger du BYOD en termes de transfert de données, il ne faut pas occulter le fait que celui-ci puisse être un facteur d'enrichissement de l'entreprise.

Les enjeux du BYOD se situent à différents niveaux. Pour les collaborateurs, il s'agit d'acquérir une meilleure maîtrise de la performance individuelle et de faciliter le mouvement entre la vie privée et la vie professionnelle. Pour l'entreprise, l'enjeu consiste à disposer de moyens de collaboration interpersonnels directement utilisables, et à proposer des informations disponibles depuis n'importe quel lieu et à tout moment. Pour les DSI, l'idée est d'apporter de nouveaux usages en maintenant le SI opérationnel tout réduisant le coût d'infrastructure.

Il existe plusieurs profils de demandeurs de BYOD, et cette pratique s'ouvre à des secteurs dans lesquels on ne l'attendait pas. Les populations qui doivent collaborer au-delà de leur entreprise font un usage du BYOD qui vise à accroître la performance, mais qui induit une prise de risque forte.

En termes d'impacts d'usages, on est confronté à la nécessité de gérer une multitude de systèmes tout en évitant de créer un empilement de passerelles. Il s'avère également nécessaire de renforcer la sécurité, ce qui nécessite avant tout une meilleure hygiène de sécurité dans les entreprises, ainsi que la mise en conformité des réseaux avec les usages BYOD et la localisation des

ressources sensibles. Le BYOD doit être considéré comme une première étape, les DSI vont être amenées à définir et à appliquer une politique liée aux objets mobiles.

Loup Gronier (LEXSI) Retour d'expériences issues des audits

Loup Gronier nous a présenté les résultats obtenus dans le cadre d'audit d'équipements, d'applications mobiles et de MDM ayant trait au BYOD. Il a souligné la difficulté suivante : il n'est pas possible d'auditer un terminal qu'avec l'accord de son propriétaire, or dans le cas du BYOD, l'entreprise n'est pas propriétaire des équipements et le détenteur peut donc s'opposer à l'audit. Ainsi seul le matériel professionnel est concerné par les résultats présentés.

Le premier postulat, en termes d'audit, est que l'on cherche ce que l'on l'a déjà trouvé au moins une fois. Or la mobilité utilise beaucoup de technologies connues et renvoie donc à des problèmes déjà vus.

Dans le cas de l'audit d'un *laptop*, on trouve par exemple rarement un disque dur complètement lisible, des comptes mot de passe stockés en clair ou mal chiffrés, un accès direct au bureau ou l'absence de verrouillage de session. On rencontre par contre relativement souvent des cas de *post-boot* sans protection, de disques durs partiellement chiffrés, des hashs de connexion stockés en local et des failles classiques qui ne sont pas spécifiquement liées à la mobilité comme des applications personnelles ou un répertoire de téléchargement bien rempli.

Les audits de smartphones ou de tablettes attestent de l'absence de *pincode*, de l'absence de verrouillage en cas d'inactivité, de cas de *smartphone jailbreaké*, d'une version OS un peu ancienne, d'ajout d'applications, de *malware*, de traces d'usages connexes, de la présence de très nombreux SMS, de pont Wifi mal sécurisé, de données non chiffrées...

Lors d'audits d'applications mobiles on est parfois confronté à l'absence de contrôle des caractères saisis, à l'authentification et la gestion de droits sur le terminal et non pas sur l'application distante et ses corollaires, au stockage en clair d'informations sensibles sur l'équipement, à des fichiers de configuration comportant des anomalies et à des *webservices* mal sécurisés. Il est fréquent de trouver de mauvaises gestions de la mise en sommeil de l'application, le manque d'exhaustivité des contrôles de saisies ainsi que le manque d'exhaustivité de l'effacement de données en cache.

Dans les cas d'audits de MDM les risques détectés sont parfois liés à l'emploi d'un produit insuffisamment mature, d'une configuration trop permissive ou d'une configuration poussée mais modifiable sur *smartphone*, ou encore liés à un produit installé sur des socles mal sécurisés. Il est plus courant de rencontrer le cas de services ouverts sur le réseau interne.

Au-delà de ces résultats, Loup Gronier nous rappelle qu'il ne faut pas s'arrêter à ce que l'on trouve le plus fréquemment aujourd'hui lors de ces audits. En effet, les vulnérabilités liées à l'usage de *smartphones* sont et seront toujours utilisées par des attaques, et la sécurisation se doit de s'adapter aux évolutions de celles-ci. En outre, les failles ne relèvent pas que d'un usage mal maîtrisé des divers équipements. Il convient en effet de rappeler que les réseaux sans fil sont quasiment tous écoutables, et que les ondes sont perturbables ce qui les rend peu fiables.

La mobilité combine donc de nombreux risques et les résultats d'audits nous montrent que de nombreuses failles techniques sont en réalité des failles classiques dues à l'inexpérience des utilisateurs, au *time to market*, au manque de tests et à des configurations laxistes.

Sébastien Bombal (AREVA) Le problème posé dans un Groupe industriel

Sébastien Bombal nous a soumis le problème du BYOD dans un groupe industriel. Aujourd'hui les limites de sécurité sont de plus en plus floues et incertaines, les menaces sont de plus en plus agressives ce qui implique la remise en cause du modèle de sécurité utilisé. Or le marché a évolué dans le sens contraire, tout y est discrétionnaire, ce que l'on tente de compenser en ajoutant des briques de sécurité. Détection et réaction restent néanmoins les parents pauvres de la sécurité.

Il est nécessaire d'identifier les besoins de BYOD. Sont-ils liés à des enjeux de productivité, au recrutement, à une mobilité accrue... ? Les questions de sécurité, de coûts cachés et de qualité doivent rester au centre des préoccupations du groupe. Il convient également de tenir compte de la problématique d'obsolescence inhérente à l'utilisation de ces outils, et de définir la façon dont elle doit être prise en compte.

Sébastien Bombal nous présente ensuite les termes de la mobilité en vigueur chez Areva : la possibilité de se connecter en 3G n'est offerte que sur leur site, le choix de terminaux a été fait en fonction de la possibilité de les maîtriser, et si les tablettes sont utilisées, c'est uniquement pour la gestion de stocks. La gestion des différents outils restent entièrement sous le contrôle d'Areva.

On peut alors se demander quelle est leur approche du BYOD. La réponse apportée par Sébastien Bombal est qu'elle n'est actuellement pas jugée compatible en terme de sécurité et de qualité de service, ni en terme économique avec l'activité d'Areva. Avant d'envisager le BYOD il faut pouvoir qualifier la demande et considérer les alternatives existantes comme le multi-niveau, ce qui nécessite de revoir le parc applicatif afin qu'il puisse supporter de nouveaux terminaux. Or un tel projet doit être anticipé avant sa mise en place effective.

Cela implique de nouvelles réflexions, notamment en termes d'ergonomie et de rapport aux données, avant de pouvoir envisager le BYOD de façon sûre.

Sid Lazizi (Mobile Iron) Le MDM les tendances et évolutions

Sid Lazizi est venu nous parler du MDM. L'adoption massive des pratiques BYOD vaut essentiellement par l'usage d'applications internes ou disponibles sur un *AppStore*. Dans la configuration actuelle des choses, la domination d'un OS sur les autres étant incertaine, les DSI se doivent de pouvoir supporter le multi-OS. Le recours aux *AppStore* entraîne par ailleurs certaines exigences en termes de sécurité puisque leur utilisation peut faire courir un risque à l'entreprise. Il convient de protéger le terminal sans entraver l'expérience utilisateur qui est au cœur des attentes du consommateur.

Les sociétés les mieux adaptées sont celles qui réfléchissent en premier lieu aux questions de mobilité, ce qui leur permet de mettre en place les moyens nécessaires et adaptés. Tout verrouiller n'est pas une solution viable, il faut passer par une solution d'infrastructure et non par un système tiers.

L'enjeu se situe dans la séparation entre données privées et professionnelles sans altérer l'expérience utilisateur. Celle-ci peut être réalisée par l'accès à une plateforme disponible sur le *Cloud* ou une installation au niveau du SI, le but étant de proposer une solution qui ne frustre pas l'utilisateur, tout en donnant de la visibilité et du contrôle au DSI.

Sid Lazizi nous décrit un avenir du MDM dont les clés seront le support de plusieurs OS, la recherche d'une qualité d'expérience primant sur le choix des marques, l'usage d'applications développées en externe et la maîtrise de la sécurité sur le réseau. C'est cette grille d'infrastructure mobile que Mobile Iron souhaite pouvoir apporter à ses utilisateurs

Patrick Borras (UCOPIA) Internet et les obligations légales, la réponse UCOPIA

Patrick Borras a apporté un éclairage sur les obligations légales à respecter, en lien avec deux lois en vigueur.

La première est la loi contre le terrorisme, en vigueur depuis 2006 et appliquée dans la plupart des pays européens. Elle stipule que tout organisme fournisseur de contenu Internet doit sécuriser son réseau et conserver une trace des données qui y sont échangées, ce qui comprend la traçabilité des connexions d'utilisateurs, les informations concernant la session de connexion, l'identification du matériel utilisé, la nature de l'activité sur le réseau, et les données permettant d'identifier le ou les destinataires de la communication. Ces données doivent être conservées pendant un an.

Depuis 2009, la loi Hadopi assure la protection des droits sur Internet. Aujourd'hui il n'y a pas de produit qui permette d'interdire totalement les contenus illégaux, mais il faut néanmoins pouvoir retrouver les utilisateurs qui ne seraient pas en conformité avec la loi.

Ucopia fournit des contrôleurs d'accès à destination des nomades en accord avec la législation. Il a été constaté que 40% des connexions nomades étaient établies depuis des smartphones et des tablettes. Ucopia permet de sécuriser le réseau et de tracer l'activité pour fournir des journaux de connexion selon un procédé validé par l'ANSSI.

Elle offre la possibilité de gérer des accès en internes, du `BYOD` et des invités. La création de compte peut être faite par l'entreprise ou de façon autonome par l'utilisateur. La sécurisation passe par l'authentification des utilisateurs rattachés à un profil, ce qui permet de gérer plusieurs types de population avec des droits d'accès différents, ainsi que le trafic des connexions. L'accès nomade ne nécessite aucune configuration afin d'être le plus accessible possible pour l'utilisateur.

Il existe donc aujourd'hui plusieurs solutions permettant d'être en conformité avec la législation et de fournir un réseau sécurisé ainsi que des fonctions de sécurité en mobilité.

Pascal Michel, Thierry Bôle (IFPen) et Christophe Corlay (IFP SChool) IFP Energies nouvelles et IFP School : deux points de vue sur la mobilité

IFPEN est un établissement public de recherche, d'innovation et de formation. Les enjeux de mobilité auquel il est confronté sont liés aux déplacements de plus en plus fréquents des cher-

cheurs et à leur nécessité d'accéder aux ressources IFPEN de façon sécurisée. La politique de sécurité de l'information comporte plusieurs facettes. Pour les DSI, l'enjeu principal est la sécurité de l'information, pour les DQSE la sécurité des biens et personnes prime, et le RSSI coordonne et supervise, il est garant de l'application de la politique de sécurité, de la sensibilisation à la sécurité du SI et du respect des chartes mises en place.

Techniquement, l'IFPEN doit pouvoir offrir la possibilité de se connecter depuis l'extérieur en répondant à des configurations Windows et Linux et en chiffrant les données. L'accès VPN est soumis à des vérifications préalables afin de s'assurer de la conformité du poste. L'accès au SI est limité en fonction de la population identifiée. Les obligations de traçabilité et de *reporting* mensuel doivent être respectées.

L'accès au réseau est possible via un terminal Blackberry IFPEN. Les terminaux sont chiffrés, la configuration est gérée en central et appliquée à l'ensemble des terminaux, on est donc dans le cas de terminaux professionnels mis à disposition de certains utilisateurs. L'accès au SI en condition de mobilité dans certains pays peut s'avérer problématique en termes de confidentialité des données. L'IFPEN peut donc dans certains cas mettre à disposition un poste vierge et procède ensuite au rapatriement des seules données utiles lors du déplacement de l'utilisateur concerner.

Dans le cas d'accès au SI via un poste non IFPEN, l'utilisateur passe par un portail permettant la continuité d'activité : VPN SSL et bureau Citrix. L'utilisateur retrouve complètement son environnement, affranchi de son poste personnel. Cette solution est utilisée en cas de besoin par l'IFPEN, mais pourrait aussi répondre à une situation de télétravail. Ce type d'accès peut passer par un portail détaché VPN SSL pour un accès à l'intranet uniquement et via une authentification forte, ou par un portail *webmail reverse proxy*, qui permet un accès à la messagerie, aux contacts, à l'agenda. L'utilisation de ce second type de portail est restreinte à certaines populations responsabilisées.

Les besoins identifiés ici sont la mutualisation des ressources et des moyens, avec une contrainte à respecter : il faut pouvoir gérer des populations différentes. Une infrastructure `Wifi` est dédiée à ces accès pour assurer la sécurisation et traçabilité.

Dans le cas de l'IFP School, l'accès au réseau concerne le personnel et les étudiants (qui peuvent se trouver à l'étranger), les enseignants non permanents et les anciens diplômés. Cela nécessite une application disponible tout le temps et partout, et accessible à plusieurs populations. La solution adoptée par l'IFP School est l'hébergement complet extérieur en *datacenter*. La sécurité du serveur est sous le contrôle de l'IFPEN. L'accès doit être compatible avec tous les supports, tous les navigateurs, tout type de matériel. L'IFP School propose également le développement d'applications, applications métiers et l'attribution d'une adresse e-mail disponible à vie.

Les perspectives sont aujourd'hui le déploiement à destination des tablettes et smartphones. Ici le `BYOD` répond à un besoin réel lié à la diversité des étudiants et des supports employés.

Yvic Le Scouezec et Frederic Buisson (CISCO) La gestion de la mobilité et des équipes en interne

Frédéric Buisson est revenu dans un premier temps sur les changements rapides et profonds liés à l'usage des smartphones et des tablettes, et à leur passage de la sphère privée à la sphère professionnelle. Des changements auxquels il est important de réfléchir en amont pour pouvoir les initier dans de bonnes conditions. Le `BYOD` se doit d'être un projet d'entreprise, il convient d'éviter les approches en silos et de le penser globalement en fédérant le projet.

Pour cela il faut commencer par définir comment adresser ces besoins. Se posent alors les problèmes d'infrastructures *wireless*, de sécurité, de gestion de parc de terminaux. Le plus grand

dénominateur commun à ces questions est le réseau. Bien entendu le BYOD aura un impact différent en fonction des organisations, il faut pouvoir l'envisager depuis un environnement nécessitant des contrôles stricts jusqu'à l'implication de nouveaux services d'applications métier optimisées.

Les enjeux soulevés sont les suivants : il faut être en mesure de sécuriser les accès, de délivrer une expérience de qualité et de gérer la complexité que cela engendre, ce qui implique un accès unifié pour centraliser l'authentification, la traçabilité, l'accès... et donc de passer par un seul réseau.

La politique de sécurité doit tenir compte de différents critères : identifier l'utilisateur et l'équipement connecté, valider sa conformité et décider de l'accès donné. Cette politique doit se retrouver n'importe où, ce qui signifie qu'elle doit être présente dans le *Cloud* et pas uniquement en interne.

Enfin, un réseau unique permet de regrouper les questions de management et d'administration.

Yvic Le Scouezec est ensuite intervenu pour nous présenter le BYOD chez Cisco. La mobilité y est encouragée : moins de 50% des employés travaillent dans les locaux et les managers ne sont que rarement sur les mêmes sites que leurs équipes. L'organisation mondialisée induit un équilibre difficile à trouver. Au-delà de la question des technologies employées, Cisco est confronté à une question de culture d'entreprise : comment peut-on fournir les mêmes *process* partout dans le monde.

Chez Cisco, le BYOD est utilisé uniquement pour les tablettes et les *smartphones*. Il n'est pas proposé sur d'autres supports pour lesquels il ne représente pas de gain. Le choix des OS se porte majoritairement sur Mac, et s'il n'y a pas de moyen efficient qui permette de mesurer une augmentation de productivité, les utilisateurs déclarent un gain de temps. Pour pallier à la question du coût, Apple étant plus onéreux que les PC, il a été décidé de mettre en place un support communautaire pour les utilisateurs de Mac afin d'en réduire les frais. Dans la même optique, concernant les *smartphones*, les employés se voient proposer un terminal de base, mais ils ont la possibilité de mettre plus de leur poche pour obtenir un autre modèle. Au final, les coûts pour l'entreprise sont un peu moins élevés, les employés utilisant de plus en plus souvent des terminaux personnels. On constate sur le même principe une augmentation du nombre d'utilisateurs et du matériel mis au service de Cisco.

Par mesure de sécurité, pour se connecter au réseau depuis ces terminaux il faut s'enregistrer afin que l'entreprise puisse identifier l'utilisateur du terminal. L'usage est de la responsabilité de l'utilisateur, même lorsqu'il s'agit de terminaux personnels utilisés dans le cadre professionnel. De même, toute perte ou vol du terminal doit être signalé à Cisco afin de pouvoir procéder au plus vite à l'effacement complet des données qui y sont stockées. L'enjeu est de parvenir à créer un consensus sur la réglementation appliquée. Pour que les utilisateurs acceptent les règles, il convient de trouver un équilibre entre ce que souhaite l'utilisateur et les besoins de l'entreprise. Grâce à ces mesures, la sécurité progresse tout en gardant une certaine souplesse.

Concernant l'utilisation des applications, très utilisées sur ces nouveaux outils, l'enjeu est de pouvoir les faire correspondre à tous les types de terminaux. La solution adoptée par Cisco est le Cisco Store qui propose des applications développées par l'entreprise et proposées librement aux employés via le *store*.

Demeure la question de sauvegardes régulières et automatiques des données qui sont utilisées sur ordinateur, mais qu'on ne sait pas encore mettre en œuvre sur tablette ou *smartphone*. Se pose le problème de restauration des données en cas de casse ou perte.

Cisco propose une expérience optimisée, la mise en place de règles simples, une gestion simplifiée, un déploiement *zero touch*, qui en font une expérience unique pour ses utilisateurs.

Laurent Gydé (Renater) La mobilité sécurisée par les services RENATER

Laurent Gydé est venu nous présenter deux des services proposés par Renater, infrastructure réseau et portefeuille de services à destination de l'enseignement et de la recherche.

Le premier point abordé est la fédération d'identité pour la mobilité numérique Comment adapter les systèmes d'authentification à l'échelle requise dans un contexte qui voit le paysage de l'enseignement supérieur et de la recherche se consolider, les réseaux autoriser l'accès massifs aux ressources distantes, la possibilité d'utiliser à distance les services de plusieurs organisations et l'offre de services mutualisés de développer ?

L'idée de Renater est de mettre en place une fédération éducation/recherche qui dispose d'une infrastructure nationale, d'une l'authentification web, et d'un mécanisme de fédération d'identité. Celui-ci fonctionne de la manière suivante : l'utilisateur se présente au service, qui lui demande de s'identifier via un portail `WAYF` (*where are you from*), et le mécanisme de fédération le redirige vers le serveur d'authentification associé. Le fournisseur d'identité renvoie alors une confirmation au fournisseur de service, avec les paramètres d'accès associés. Ainsi le mot de passe ne circule pas du tout. On utilise pour cela un fonctionnement préexistant, interopérable, qui permet de contrôler les échanges.

Cette fédération donne accès à des différents services : des ressources documentaires, de l'e-learning, l'accès au `Wifi`, à des applications métiers mutualisées, à l'extranet, à la distribution de logiciels, à des applications et à des services nationaux. Cette démarche s'inscrit également dans une initiative européenne d'inter-fédération qui favorise les échanges et l'accès de ressources internationales.

Actuellement, Renater travaille à l'amélioration de l'ergonomie de ses services, à la qualité des référentiels d'identité, ainsi que sur la concentration des risques sur les IDP.

Eduroam pour l'accès `Wifi` fédéré Le second service présenté par Laurent Gydé est l'accès `Wifi` fédéré `eduroam`, une opération nationale visant à développer l'utilisation du `Wifi` afin de faire face aux pratiques actuelles de mobilité et de collaboration. Il s'agit donc de pouvoir fournir un accès `Wifi` partout, pour tous, sans multiplier les efforts.

La solution consiste en une connexion `Wifi` sécurisée, utilisable dans l'établissement d'origine ou en situation de nomadisme (même à l'étranger) via la saisie du *login* habituel, après une configuration initiale du client. En Europe 36 pays sont couverts par `eduroam`, et on dénombre 54 pays utilisateurs dans le monde, soit plus de 6000 sites.

Le système fonctionne par la hiérarchie de serveurs `radius`, comprenant un serveur par établissement, un serveur national et plusieurs serveurs mondiaux. Il s'agit donc plus d'une question d'organisation que de technique de pointe.

Restent à traiter certaines questions, telles que l'harmonisation des protocoles d'authentification, la configuration nécessaire sur les postes clients, le filtrages mis en œuvre sur les accès `eduroam`, la mise en place d'une extension d'`eduroam` vers les réseaux d'opérateurs et la création d'un support pour accompagner l'utilisateur.

Jacques Le Rest (Ifremer) Solution d'accès Wifi UCOPIA

J. Le Rest nous a fait la présentation du système d'accès `Wifi` visiteur à l'Ifremer. Il concerne les 26 sites repartis sur tout le littoral métropolitain et les Dom Tom et propose le même service informatique partout, *via* Orange, depuis un seul accès Internet basé à Brest. Le service informatique comprend 20 personnes dont 3 ingénieurs télécoms.

Chaque lieu répond à des normes interdisant le déploiement massif, le `Wifi` étant accessible uniquement en salle de réunion et dans les ateliers. La gestion est entièrement centralisée WLC Cisco par le biais d'un peu plus de 50 bornes et la diffusion de 2 `SSDI` : un pour le visiteur et un pour l'intranet. Ces accès `Wifi` disposent de sécurisation `TTLS` et par l'authentification via un *login* et un mot de passe.

Le visiteur bascule vers un portail captif Ucopia, une solution qui permet de respecter la législation en vigueur et de savoir qui est connecté, quand et pour quoi faire. Le portail captif ne nécessite aucune configuration sur les PC, et offre la possibilité d'interfacer avec différentes bases, et de gérer les droits en fonction du type d'authentification. Pour finir l'interface proposée est simple et multilingue.

Dans le cas de création de compte pour des visiteurs ne disposant pas d'authentifiant, l'Ifremer à choisi de faire confiance aux utilisateurs. Tout agent Ifremer peut accéder à une page de délégation sur laquelle sont notés le nom du visiteur, son numéro de téléphone, et son adresse *e-mail*, ce qui permet la création d'un identifiant de connexion `Wifi` qui est envoyée directement par `SMS` à la personne concernée. Il est également possible de s'authentifier par fédération d'identité `WAYF` (*where are you from*).

Philippe Breider (Vmware) VXI

Philippe Breider nous a présenté Wmware, un outil de virtualisation. Si la solution historique de virtualisation d'un poste de travail existe depuis 2006, il s'agit d'une solution limitée pour des questions technico- économiques.

Une seconde solution, rendue possible par le rachat de Mirage par Wmware, permet de gérer des environnements physiques ou portables ainsi qu'une gestion par couche du poste de travail. Il s'agit d'une approche assez novatrice, qui plait par son côté tout en un. Il en découle trois grands usages : la gestion du poste de travail au sens large, la gestion des sauvegardes et de la restauration de données utilisateur, et la migration du parc vers Windows 7. L'utilisation de Mirage permet une gestion centralisée et une exécution locale. Le couplage de View et Mirage permet une gestion centralisée unifiée.

Philippe Breider nous a ensuite présenté rapidement quelques unes des propositions de Wmware. Horizon Mobile reprend le principe de virtualisation et l'applique au mobile, en créant une passerelle entre un usage personnel et professionnel. Le projet Octopus est une reprise du principe de la Dropbox, il permet le stockage des données dans un *Cloud privé*, comprenant différents niveaux de droit d'accès et la possibilité de travailler en collaboration.



Chapitre 3

Présentations

3.1 Benjamin Morin (ANSSI)

BYOD : maîrise et sécurité

Benjamin Morin est le chef du laboratoire architectures matérielles et logicielles, sous-direction expertise, à l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

BYOD, maîtrise & sécurité
Séminaire Aristote

Benjamin Morin
ANSSI/SDE/ST/LAM

7 février 2013

Acte I

Mise en situation

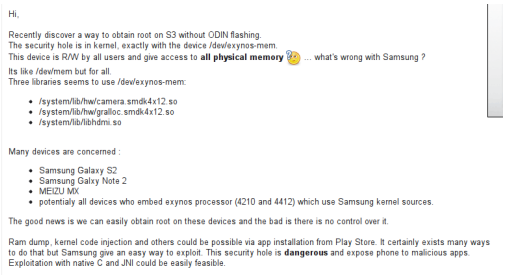
Rappels sur les risques et les menaces associés à la mobilité

- Vol de données sensibles
  - Risque amplifié en cas d'usage mixte des terminaux (personnel et professionnel)
- Prise de contrôle à distance
- Vecteur d'accès à d'autres systèmes
  - Système d'information d'une entreprise
  - Services en ligne
- Espionnage
- Perte, vol, ou emprunt du terminal
- Applications malveillantes, indiscrètes et/ou vulnérables
- Failles du système et/ou du matériel
- Maîtrise limitée des terminaux

Quelques mots au sujet des applications...

- Applications malveillantes
  - Phénomène en pleine explosion
  - Plus de 14000 nouveaux codes malveillants apparus au 1er trimestre 2012
- Applications « indiscrètes »
  - Collecte illégitime ou injustifiée de données
  - Cf. divulgation des UDID et des données de porteurs d'iPhone
- Applications vulnérables
  - Risque de prise de contrôle à distance des terminaux
  - Cf. `jailbreakme.com`

Un exemple récent sur le réalisme de la menace



Hi,

Recently discover a way to obtain root on S3 without ODIN flashing.
The security hole is in kernel, exactly with the device /dev/exynos-mem.
This device is R/W by all users and give access to **all physical memory** 🤔 ... what's wrong with Samsung ?
Its like /dev/mem but for all.
Three libraries seems to use /dev/exynos-mem:

- /system/lib/hw/camera.smdk4x12.so
- /system/lib/hw/gralloc.smdk4x12.so
- /system/lib/libhdmi.so

Many devices are concerned :

- Samsung Galaxy S2
- Samsung Galxy Note 2
- MEIZU MX
- potentialy all devices who embed exynos processor (4210 and 4412) which use Samsung kernel sources.

The good news is we can easily obtain root on these devices and the bad is there is no control over it.

Ram dump, kernel code injection and others could be possible via app installation from Play Store. It certainly exists many ways to do that but Samsung give an easy way to exploit. This security hole is **dangerous** and expose phone to malicious apps.
Exploitation with native C and JNI could be easily feasible.

`http://forum.xda-developers.com/showthread.php?p=35469999`

Exigences de sécurité et maîtrise des terminaux

- Les employeurs doivent prendre les mesures de sécurité adéquates pour protéger les biens sensibles présents sur les terminaux
  - Opter pour des terminaux sécurisables ;
  - Interdire l'installation d'applications non validées ;
  - Imposer une authentification robuste du porteur ;
  - Empêcher l'accès à des services ou des réseaux non maîtrisés ;
  - etc.
- Les employeurs doivent donc contrôler / maîtriser autant que possible les terminaux

Aparté sur la question de la maîtrise des smartphones

- Les acteurs du secteur des smartphones sont nombreux et ont des exigences (de sécurité) différentes
  - voire incompatibles d'un contrôle exclusif des terminaux par leur propriétaire
  - car l'utilisateur final est considéré comme un attaquant potentiel dans certains modèles de sécurité
- La multiplicité des acteurs industriels dilue le contrôle que le propriétaire d'un smartphone peut exercer sur son terminal.

Répercussions sur les utilisateurs finaux

- Un défaut de maîtrise bride les possibilités de sécuriser un système et limite la confiance que l'on peut/doit lui accorder.
- Les *smartphones* échappent en grande partie aux mesures de sécurité classiquement employées sur des terminaux « standards ».
- La sécurité des smartphones doit toujours être considérée à l'aune de ce problème de maîtrise.
- Cette vigilance s'applique à plus forte raison sur les services distants (informatique en nuage).

Acte II

De l'incompatibilité du BYOD avec la sécurité

(ou pourquoi le BYOD est fondamentalement inadapté à une protection robuste des informations professionnelles sensibles)

BYOD et maîtrise

- Le BYOD accentue le défaut de maîtrise de l'employeur sur les terminaux et le prolonge jusque dans l'administration du parc
  - Par définition du BYOD, l'employeur n'est pas le propriétaire des terminaux des employés
  - Il ne peut donc pas légitimement imposer des restrictions fortes sur les terminaux
- Le BYOD est donc fondamentalement inadapté à une protection robuste des informations professionelles sensibles
  - Les usages professionnels devraient être réalisés sur un terminal dont l'employeur a la maîtrise,
  - c'est-à-dire sur un terminal dont l'employeur est le propriétaire.

Solutions BYOD existantes

- De nombreuses solutions BYOD sont implémentées sous la forme d'une application dédiée
  - Encapsulation des outils et des données professionnels
  - Ne nécessitent aucune modification des terminaux des employés
  - ... ce qui simplifie grandement leur déploiement.
- Cette approche consiste moralement à mettre les biens sensibles sous le contrôle d'un environnement hostile
  - (ou qui doit être considéré comme tel)
  - La séparation entre les domaines professionnel et privé est réalisée en espace utilisateur
  - une application malveillante peut donc potentiellement accéder aux données sensibles de l'application professionnelle (éventuellement via une élévation de privilèges)
- Ces solutions sont donc structurellement inadaptées à la protection de données sensibles

Acte III

Soyons constructifs

(ou quelques pistes de réflexion pour rendre le BYOD acceptable)

Acte III -- Scène 1

Un concept innovant : le UYED

« Use Your Employer's Device »

Retournons le problème

Finalement, de quoi les employés ont-ils besoin ?

- d'un terminal personnel qui leur permette d'accomplir des tâches professionnelles ?

Retournons le problème

Finalement, de quoi les employés ont-ils besoin ?

- ~~d'un terminal personnel qui leur permette d'accomplir des tâches professionelles ?~~
- ... ou d'un terminal professionnel qui leur permette d'accomplir des tâches personnelles ?
  - Avec une maîtrise du terminal par l'employeur
  - Et des mesures de sécurité adaptées

Acte III -- Scène 2

Le multiniveau ~~contre le~~ au secours du BYOD

Systèmes multiniveaux

- Le rôle d'un système multiniveau est de garantir l'isolation entre des environnements d'exécution séparés
  - Accéder à des données ou des services de niveaux de sensibilité hétérogènes depuis un même terminal
  - En l'occurrence, séparer un domaine « personnel » et un domaine « professionnel »
- Les systèmes multiniveau s'appuient sur un « socle de confiance » et des primitives de cloisonnement robustes
  - Le rôle de ces primitives est d'empêcher un domaine d'interférer avec un autre
  - ... ou plus précisément, de contrôler les interactions autorisées entre ces domaines

Instanciation de systèmes multiniveaux

- Pour être robustes, les primitives de cloisonnement doivent être implantées dans les couches logicielles basses des terminaux
  - typiquement, le système d'exploitation et son noyau.
  - voire dans les couches inférieures (hyperviseurs)
- Séduisant en théorie, mais complexe à réaliser en pratique actuellement
  - Nécessite une modification en profondeur du système d'exploitation
  - Difficilement envisageable sur un terminal qui ne serait pas la propriété de l'employeur
  - Voire impossible sur les modèles qui interdisent le chargement d'un système alternatif (via des dispositif de boot sécurisé).

Vision prospective

- Admettons que les OS pour smartphones soient nativement équipés de ces primitives de cloisonnement
  - *i.e.* il « suffit » de les configurer pour les utiliser
- Deux configurations de mobilité sécurisée sont envisageables
- La moins bonne : BYOD avec smartphone multiniveau
  - L'employé « prête » un compartiment à son employeur
  - Au sein duquel l'employeur dispose des privilèges requis pour imposer ses règles de sécurité
  - Suppose une confiance mutuelle dans le socle de confiance
  - Satisfaisant tant que l'employé n'est pas malveillant
- La meilleure : UYED avec smartphone multiniveau

Acte III -- Scène 3

Autres solutions...

Trusted Execution Environments (TEE) (1/2)

- Technologie matérielle ARM/TrustZone
- Séparation de l'environnement d'exécution en deux domaines
  - Un domaine dit « non sécurisé » (l'OS de l'utilisateur) et un domaine « sécurisé »
  - Protection en intégrité et en confidentialité des applications qui s'exécutent dans le domaine sécurisé contre le domaine non sécurisé
  - y.c. en cas de compromission du noyau du domaine non sécurisé
- Cas d'application types
  - Applications de paiement, DRM, etc.
  - Cas d'application du BYOD pour des applications professionnelles ?

Trusted Execution Environments (TEE) (2/2)

Des interrogations subsistent sur ce type de technologie

- Technologie encore fermée
- Quid de la personnalisation de l'environnement sécurisé ?
- Quid des garanties d'isolation au sein de l'environnement sécurisé ?
- Qui contrôle l'environnement d'exécution sécurisé ?

Épilogue

Conclusion

- Les menaces auxquels sont exposés les terminaux mobiles imposent une protection robuste des informations sensibles
  - En complément des mécanismes de sécurité dont disposent nativement ces terminaux
  - Éventuellement au détriment des attentes fonctionnelles des utilisateurs
- La mise en place de ces protections requiert une maîtrise des terminaux par l'employeur
  - Ce qui tend à supposer qu'il en est le propriétaire
- Des solutions techniques émergent pour satisfaire les exigences de sécurité
  - Mais les solutions actuelles sont majoritairement inadaptées

Merci

Questions ?

3.2 Dominique Mouchet (Altetia)

La consumérisation du marché de l'informatique et le BYOD

ALTETIA

La consumérisation du marché de l'informatique et Le BYOD

Séminaire ARISTOTE
7 Février 2013

ALTETIA
183 avenue Georges Clémenceau
92024 Nanterre
0155692121
www.altetia.com
dominique.mouchet@ altetia.com

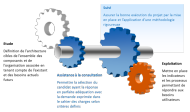
Plan de la présentation

- Présentation Altetia (rapide c'est promis ;-)
- Point de situation :
  - Une définition de la consumérisation de l'IT
  - Les enjeux de la consumérisation
  - Nous sommes tous dans la consumérisation…
  - Des secteurs s'ouvrent au BYOD là où on ne l'attendait pas…
  - Les impacts apparents sur la DSI
- Prise en compte d'un projet lié à la consumérisation :
  - Schéma général de planification du projet
  - Perspectives de la consumérisation de l'IT

ALTETIA

ALTETIA en quelques mots

Expérience avérée



Large spectre de projets

- Audiovisuel
- visioconférence
- Déménagement
- Service télécom : mobile, data, voix
- Infrastructure
- Aménagement de salles
- datacenter
- Raccordement des bâtiments (GC , fibre hertzien)
- Infrastructure à l'intérieur des bâtiment
- Réseau
- Service opérateurs Maintenance
- Outsourcing, Infogérance
- Immeuble intelligent
- …

Quelques références

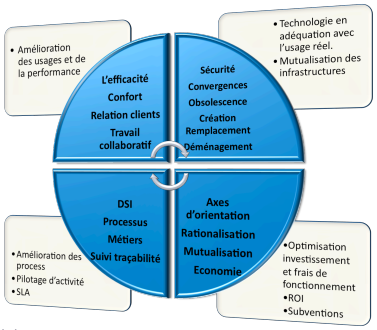
Les domaines d'activité

Réseau, Téléphonie, collaboratif, audiovisuel

- Refonte système
- Création
- Modernisation
- Déménagement

ALTETIA

Pourquoi faire appel à un Conseil ?



ALTETIA

Consumérisation de l'informatique : une définition

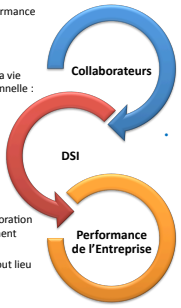
Définition wikipedia : "Consumerization is an increasingly accepted term used to describe the growing tendency for new information technology **to emerge first in the consumer market** and **then spread into business** and government organizations. The emergence of **consumer markets as the primary driver of information technology innovation** is seen as a major IT industry shift, as large business and government organizations dominated the early decades of computer usage and development."

Formellement, le BYOD n'est qu'une partie de la consumérisation…

ALTETIA

Les enjeux de la consumérisation de l'IT

- **Pour les collaborateurs :**
  - Meilleure maîtrise de sa performance individuelle :
    - Mobilité,
    - Accès à l'information
  - Facilité de mouvement entre la vie professionnelle et la vie personnelle :
    - Réduction de la frontière d'horaires et d'activités
- **Pour l'entreprise :**
  - Disposer de moyens de collaboration entre les personnels directement utilisables :
    - Accès à l'information en tout lieu par les collaborateurs,
    - Accès permanent aux informations Business,
    - Résilience de moyens,



- **Pour les DSI :**
  - Apporter de nouveaux usages :
    - Applications collaboratives,
    - Favoriser l'agilité des organisations : nouveaux projets, …
  - Maintien du SI opérationnel :
    - Charge,
    - Sécurité,
  - Réduire les coûts d'infrastructure :
    - Par la réduction du nombre de terminaux,
    - Pour coller à l'évolution de l'activité : terminaux et stockage

ALTETIA

Nous sommes tous dans la consumérisation…

Le BYOD, une maladie plus répandue qu'on ne pense :

- **Le Haut Potentiel qui refuse d'intégrer une entreprise « ringarde » :**
  - Exige de pouvoir faire une visio avec ses équipes en déplacement depuis sa nouvelle Surface,
  - Poste sur Google+ depuis les réunions
  - Rédige les comptes-rendus de réunion avec MindMap
- **Le VIP qui a reçu son IPAD à Noël :**
  - ✓ « Vous me faites tourner ça avant 11h avec mes emails et mon agenda »,
  - ✓ « ca marchait chez moi et ça ne marche plus… »
- **Le Chef de Projets qui collabore sur Dropbox :**
  - ✓ Parce qu'un sous traitant lui a posé un fichier à 22h30 la veille,
  - ✓ Parce qu'il en a marre des outils corporate qui ne marchent jamais…

L'OVNI

Le ressourçophage

Le sécuricide

11/02/13

ALTETIA

Des secteurs s'ouvrent au BYOD là où on ne l'attendait pas…

- **Secteur public : Médecin de PMI, assistante sociale, Employé d'intervention … :**
  - **à qui on refusé un smartphone**
  - **Qui doit faire des allers retours avec son centre technique pour prendre connaissance du mail indiquant son prochain RDV**
  - ➢ exemple d'usage BYOD qui précède une généralisation sur des outils corporate
- **Les populations qui doivent collaborer au-delà de leur entreprise : équipes projet, commerciaux, avocats pour réponse à des appels d'offre … :**
  - ➢ exemple d'usage BYOD qui vise à accroître la performance…avec une prise de risque forte

11/02/13

ALTETIA

Les impacts apparents sur la charge des DSI

- **Nécessité de gérer une multitude de systèmes / terminaux :**
  - **IOS, Android, Windows, Linux**
  - **Et comment je rejoins la conférence vidéo avec mon skype ???**

La solution à l'arrivée du BYOD ne passe pas par un empilement de passerelles

- **Nécessité de renforcer la sécurité :**
  - **Accès aux ressources réseau de l'entreprise,**
  - **Prévenir les fuites d'informations,**
  - **Prévenir les infections par supports amovibles.**

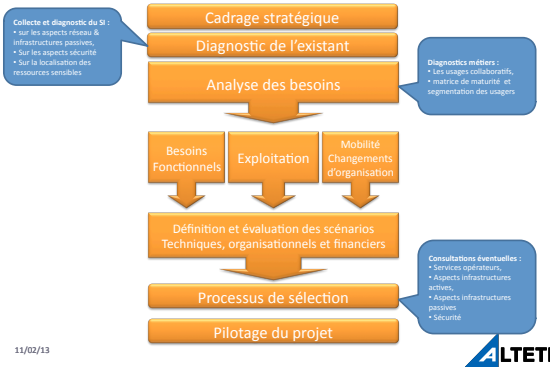
« En France, 21 % des données sont stockées dans un cloud, 11 % sont sur des terminaux mobiles et 23 % des utilisateurs y accèdent via un smartphone ou une tablette »
Enquête Symantec – 11/2012

La solution à l'arrivée du BYOD passe par une meilleure « hygiène » de sécurité dans les entreprises

11/02/13

ALTETIA

Schéma général de planification du BYOD



11/02/13

ALTETIA

Réflexions sur la consumérisation…

- **Le BYOD comme première étape :**
  - **Les usages évoqués sont légitimes dans la stratégie d'entreprise, et vont donc s'imposer comme vecteurs de croissance,**
  - **Le mouvement BYOD préfigure des demandes pour la connexion d'objets communiquants de plus en plus divers (wearable devices)**
  - ➢ Les DSI vont devoir définir et appliquer une politique liée aux objets mobiles, avec des volumétries d'accès sans commune mesure avec la situation actuelle : lien avec le Big Data.
- **Les impacts réels du BYOD apparaissent encore mal maîtrisés :**
  - **Les pertes potentielles liées à la sécurité sont plus souvent chiffrées que les gains de performance liés au BYOD,**
  - **Le BYOD ne doit pas occulter les formations et l'accompagnement au changement.**
  - ➢ La clé de la performance est la capacité à collaborer, et dans une moindre mesure la dextérité dans la manipulation des outils.

11/02/13

ALTETIA

Merci de votre attention !

Des questions ?

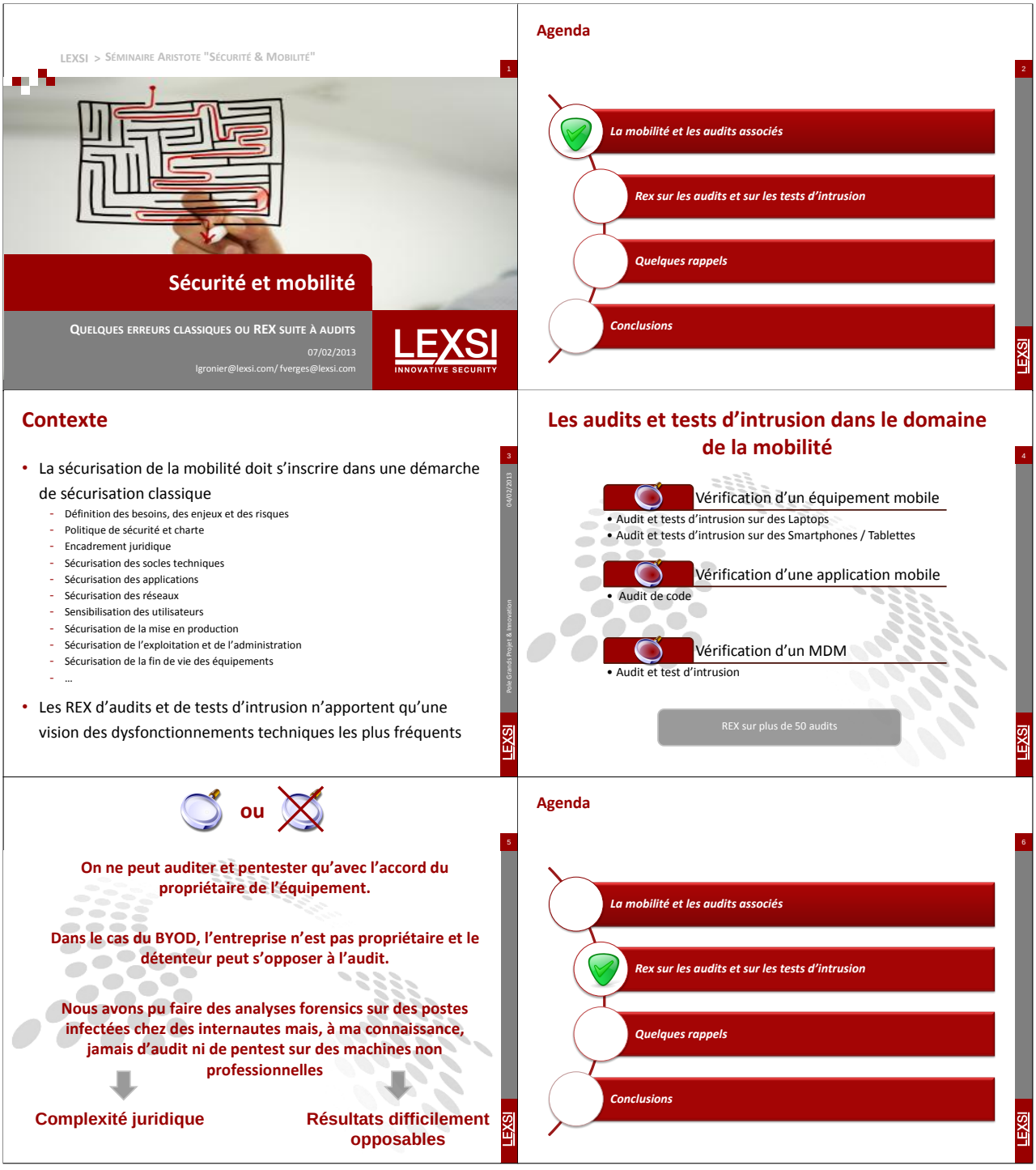
11/02/13 12

ALTETIA

3.3 Loup Gronier (LEXSI)

Retour d'expériences issues des audits

LEXSI, société de conseil spécialisée en sécurité des systèmes d'information réalise depuis plusieurs années des audits et des tests d'intrusion dans le domaine de la mobilité. Les audits et les tests d'intrusion doivent permettre de mesurer finement l'efficacité des mesures de sécurité mais également d'assurer une évangélisation tant les problèmes rencontrés sont récurrents et parfois triviaux. Cette intervention présente un retour d'expérience sur les résultats de ces contrôles et matérialise les failles les plus souvent constatées par nos auditeurs et pentesteurs.



Rex sur les audits

Postulats

Ce que l'on cherche, on l'a déjà trouvé au moins une fois. La mobilité utilise pour beaucoup des technologies connues.

Lorsqu'un pentester ou un auditeur prouve une nouvelle technique d'attaque, elle se retrouve dans la liste de ce que l'on cherche.

L'imagination d'un pentesteur n'a pas de limite mais les erreurs sont souvent… les mêmes.

7 LEXSI

Audit ou pentest de laptop

- Ce que l'on trouve… rarement
  - Un disque dur complétement lisible
  - Des comptes / mots de passe stockés en clair ou mal chiffré
  - Accès direct au bureau (BYOD, vous avez dit BYOD…)
  - Absence de verrouillage de session
- Ce que l'on trouve… souvent
  - Le poste boot sans protection et on se retrouve sur la mire windows (ou Linux)
  - Un disque dur partiellement chiffré et des données dans les répertoires cache des applications
  - Des hashs de connexion stockés en local
  - Du classique pas lié à la mobilité
    - > Des applications « personnelles »
    - > Un répertoire « téléchargement » bien rempli

8 LEXSI

Audit ou pentest de smartphone ou tablette

- Ce que l'on trouve… parfois
  - L'absence de pincode
  - L'absence du verrouillage en cas d'inactivité
  - Un smartphone jailbreaké
  - Une version d'OS un peu ancienne et buggée sans les correctifs
  - Des applications supplémentaires et pas toujours inoffensives
  - Des malwares
  - Des traces d'usages connexes
  - Des SMS, des SMS, des SMS (attention à la vie privée)
  - Un pont wifi mal sécurisé
  - Des données non chiffrées
    - > Globalement
    - > Dans des espaces de cache
  - Des informations dans la configuration des applications
    - > URL, compte, mot de passe…

9 LEXSI

Audit ou pentest d'application mobile

- Ce que l'on trouve… parfois
  - L'absence de contrôle des caractères saisis
  - L'authentification/gestion de droits sur le device, pas sur l'application distante et ses corrolaires :
    - > Le login/mot de passe générique stocké en local
    - > La capacité à changer de profil
  - Le stockage en clair d'information sensible sur l'équipement
  - Des fichiers de configuration comportant des anomalies
  - Des webservices mal sécurisés permettant de récupérer des informations sur l'application ciblée
- Ce que l'on trouve… souvent
  - Une mauvaise gestion de la mise en sommeil de l'application
  - Un manque d'exhaustivité des contrôles des saisies
  - Un manque d'exhaustivité de l'effacement des données en cache

10 LEXSI

Audit ou pentest de MDM

- Ce que l'on trouve… parfois
  - Un produit pas mature
    - > Interfaces non sécurisées
    - > Bugs et Buffer Overflow…
  - Des configurations trop permissives
    - > Pas de contrôle sur le pincode
    - > Pas de contrôle sur le jailbreak
    - > Pas de contrôle sur le temps avant extinction
    - > …
  - Des configurations poussées mais modifiables sur le smartphone
  - Des produits installés sur des socles mal sécurisés
- Ce que l'on trouve… souvent
  - Des services ouverts sur le réseau interne
  - Des bannières et des informations techniques

11 LEXSI

Agenda

1. *La mobilité et les audits associés*
2. *Rex sur les audits et sur les tests d'intrusion*
3. *Quelques rappels*
4. *Conclusions*

12 LEXSI

Attaque d'un smartphone

Une vulnérabilité sur un smartphone

Un agresseur identifie un vecteur pour utiliser la vulnérabilité
- ❑ Mail (éventuellement avec un attachement piégé)
- ❑ Site web avec code actif
- ❑ …

Ouvre le mail et lit l'attachement
Accède au site web
…

Est alors sous le contrôle de l'attaquant y compris les SMS

Les équipements ont eu et auront des vulnérabilités, les attaques les utiliseront

La sécurisation de la mobilité doit évoluer selon les attaques

Le CERT Lexsi a démontré la faisabilité de ce type d'attaque depuis l'envoi d'un PDF infecté jusqu'au BOT actif sur le smartphone

13 LEXSI

Attaque d'un poste chiffré

Un poste éteint est laissé accessible

L'agresseur accède au poste et y installe un mouchard

L'utilisateur accède au poste et tape son mot de passe qui est récupéré par le mouchard

L'agresseur accède au poste une deuxième fois et récupère le mot de passe

L'agresseur a accès à l'ensemble des données du disque dur

Le logiciel permettant cette attaque est disponible librement sur Internet

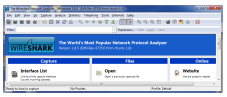
En face de chaque mesure de sécurité, des attaques se développent

La sécurisation de la mobilité doit évoluer selon les attaques

14 LEXSI

Attaque des réseaux sans fil

Nos équipements mobiles utilisent classiquement 3 types de réseaux sans fil : Wifi, Bluetooth et GSM/3G



Créer un sniffer Bluetooth ? C'est simple comme bonjour !

27th Chaos Communication Congress
We come in peace

Wideband GSM Sniffing

Mais également …

Sniffing DECT Phones – The Details

En face de chaque technologie, des attaques se développent : sniffer, ManInTheMiddle…

La sécurisation de la mobilité doit évoluer selon les attaques

Réseaux sans fil et disponibilité ?

- Les ondes sont par essence perturbable

- La version grand public à « faible » portée

- La version professionnelle : une bulle de silence de 250 m de diamètre

Agenda

1. *La mobilité et les audits associés*
2. *Rex sur les audits et sur les tests d'intrusion*
3. *Quelques rappels*
4. *Conclusions*

Conclusions

- **Le monde de la mobilité combine les risques**
  - Terminaux mobiles, petits, faciles à perdre et à voler
  - Modèle de mise à disposition des softs peu onéreux
  - Terminal à la disposition de l'utilisateur, BYOD
  - Utilisation de technologies sans fil
  - …
- **Le terminal mobile devient de plus en plus un outil de « sécurisation »**
  - Envoi des mots de passe par SMS
  - SMS de confirmation
- **Le REX des audits nous montre beaucoup de failles techniques classiques :**
  - Dues à l'inexpérience et au manque de sensibilisation des utilisateurs
  - Dues au time to market et au manque de test des OS / Solution
  - Dues aux développeurs d'application
  - Dues à des configurations laxistes
- **Le constat doit être replacé dans une approche plus globale**

INNOVATIVE SECURITY

Pour vous aider à maîtriser vos risques

SIEGE SOCIAL :
Tours Mercuriales Ponant
40 rue Jean Jaurès
93170 Bagnolet
Tél. (+33) 01 55 86 88 88

www.lexsi.com

LEXSI LYON
Bois des Côtes 1 - Bâtiment A
300 route Nationale 6
69760 LIMONEST
Tél. (+33) 08 20 02 55 20

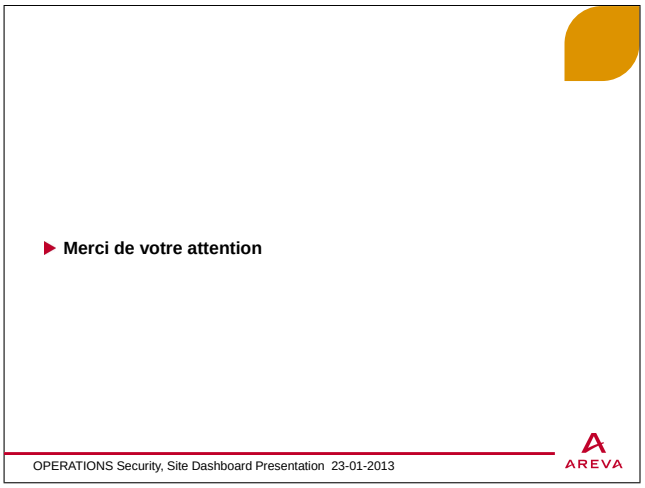
LEXSI CANADA
3446-202 rue St Denis
H2X 3L3 MONTREAL
Quebec
Tél. +1 514 903 6560

LEXSI SINGAPORE
46, East Coast Road
Eastgate - #07-06
428766 - Singapore
Tél. +65 63446926

3.4 Sébastien Bombal (AREVA)

Le problème posé dans un Groupe industriel

Sébastien Bombal est manager de la sécurité opérationnelle et des systèmes d'informations industriels pour le groupe AREVA. Il dirige également la spécialisation système, réseau et sécurité au sein de l'EPITA depuis 2006. Diplômé de l'EPITA et de l'école de guerre économique, il dispense régulièrement des conférences et est très engagé dans la cybersécurité et la cyberdéfense.


Merci de votre attention
OPERATIONS Security, Site Dashboard Presentation 23-01-2013
AREVA

3.5 Sid Lazizi (Mobile Iron)

Le MDM les tendances et évolutions

MobileIron a été fondée dans le but de simplifier le déploiement et la gestion des appareils mobiles intelligents en entreprise. Les tablettes et les smartphones, qu'ils soient sur iOS, Android, WinPhone, BB, Symbian sont en passe de devenir les principaux outils informatiques et de communication en milieu professionnel. Il sont toutefois assortis de coûts, de risques et de problèmes d'ergonomie que les stratégies de gestion des appareils mobiles conventionnels sont incapables de traiter. Notre approche consiste à simplifier la situation, tant pour les services informatiques ou financiers des entreprises que pour les utilisateurs finaux.

The Birth of Mobile IT

- User Driven
- Device Choice
- Micro-Mobile Apps
- User Experience
- Multi-OS Management
- Security
- Consumer Speed
- Compliance

MobileIron

Secure and manage mobile apps, documents, and devices

MobileIron

Purpose-built for Mobile IT

Our Mission:

To deliver the **Mobile IT Platform** companies need **today** to transform their business by **unleashing end user productivity** on any mobile device

8

MobileIron

Purpose-built for Mobile IT

Focused on customer success

4000+ customers globally

24x7 Operating globally

200+ of Fortune 500 / Global 2000

97% customer support satisfaction

7 of top 10 global pharma companies
4 of top 5 global automotive
3 of top 5 global retailers
5 of top 10 global law firms

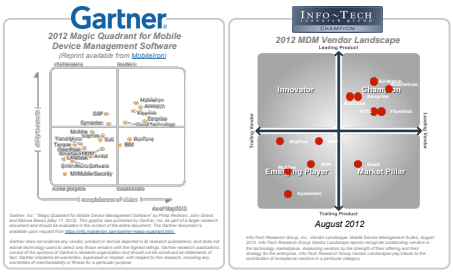
Strongest Mobile Ecosystem

9

MobileIron

Industry recognition

Gartner: Leaders Quadrant of 2012 MDM Magic Quadrant (May 2012)
Info-Tech: Champion in 2012 MDM Vendor Landscape (Aug 2012)
IDC: Fastest growing mobile enterprise management vendor (Sept 2012)
BusinessWeek: One of five hottest enterprise startups (Sept 2012)



10

MobileIron

Customer Success

4000 Customers

>70 Public Reference Customers

Financial Services

Government & Education

Healthcare / Pharma

Professional Services

Retail & Consumer Goods

Technology & Manufacturing

Travel and Hospitality

11

MobileIron

The MobileIron Platform Enables…

A End User Services

B Complete IT Mobile Management

To secure and manage mobile **apps, documents,** and **devices**

12

MobileIron

The MobileIron Platform Enables…

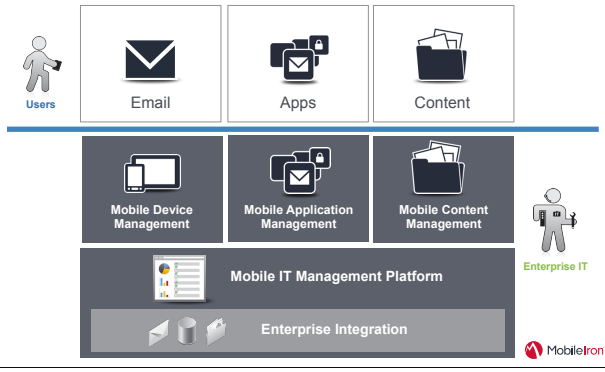
A End User Services

Device Choice | Secure Email | Apps | Content

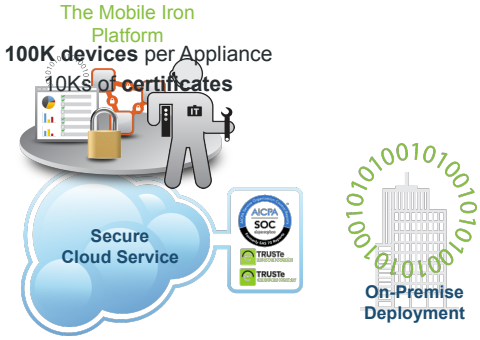
- Native Experience
- Secure
- Separation Between Enterprise & Personal

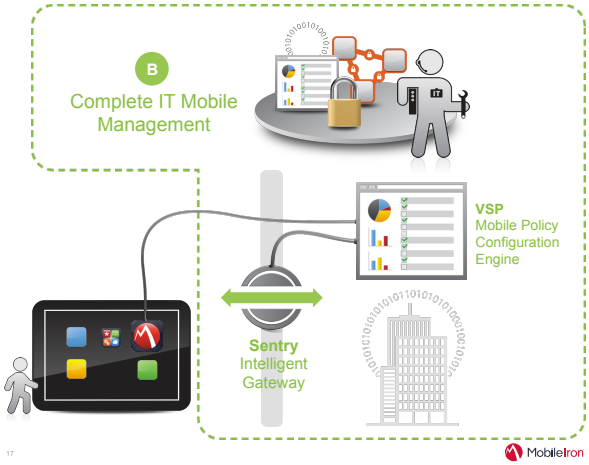
MobileIron

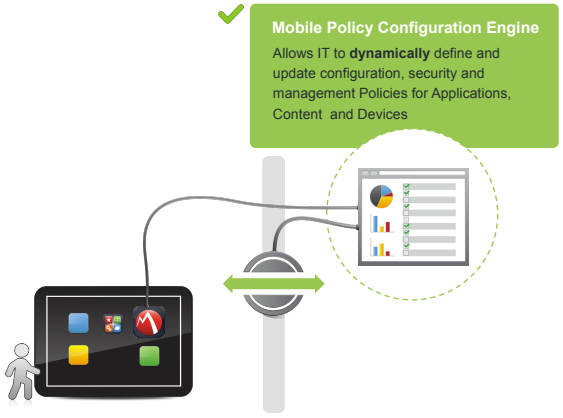
The MobileIron Platform

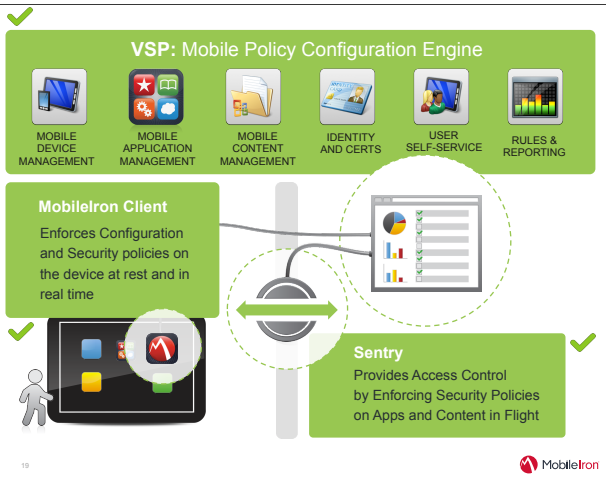


Cloud Deployment Flexibility

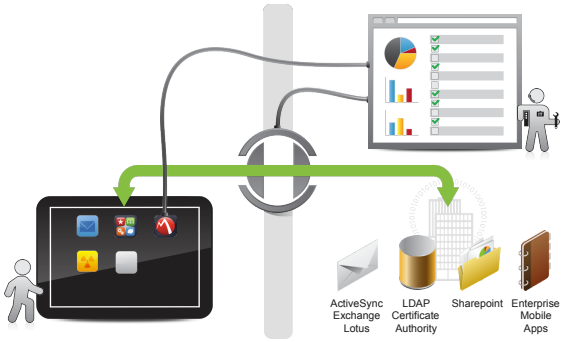




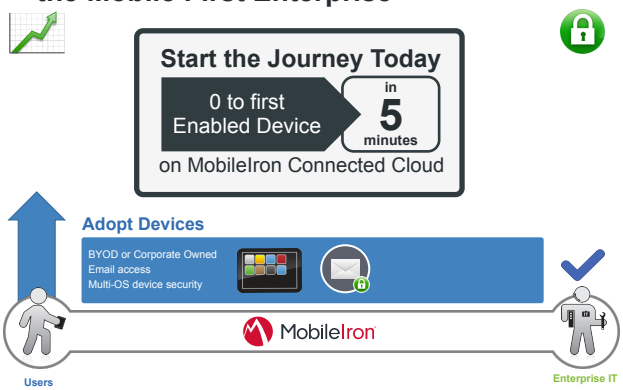




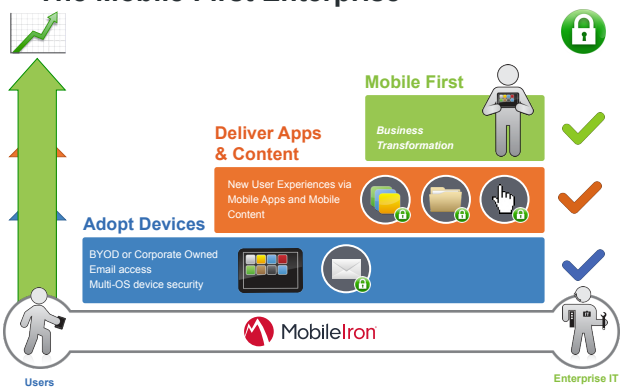
Integration with Enterprise Systems



The Journey to the Mobile First Enterprise



The Journey to The Mobile First Enterprise



The MobileIron Platform

End Users Value

- Device Choice
- Native Email
- Auto-Configuration
- WiFi Access
- Enterprise App Store
- Transparent App Security
- Intranet Access
- Mobile Access to Corporate Docs
- Online and Offline

Native Experience for BYOD and Corporate Devices
Separation of Corporate/Personal, SSO

Users

Mobile Device Management | Mobile Application Management | Mobile Content Management

Mobile IT Management Platform

Enterprise IT

23 MobileIron

The MobileIron Platform

IT Value

- Secure and Manage Devices Across Multi-OSes
- No-Touch Provisioning and Configuration
- Across Corporate Device or BYOD
- Store Front for In-House and Public Apps
- Dynamic Application-Level Policies/Config
- Separation Between Enterprise Persona
- App Tunneling
- Secure Enterprise Content Access (and SharePoint)
- Secure Email Attachment/DLP
- Secure Intranet Browsing
- Selective Wiping

Mobile Device Management | Mobile Application Management | Mobile Content Management

Mobile IT Management Platform

Enterprise IT

- Integration with Mail, Content, Identity, Directory, Certificates
- APIs for Enterprise Integration

24 MobileIron

The MobileIron Platform

Users

Email | Apps | Content

Advanced Management | AppConnect AppTunnel | Docs@Work

Mobile IT Management Platform (VSP, Connected Cloud)

Enterprise IT

MDM MAM MCM

25 MobileIron

Investment in Customer Success

World-class global technical support and services

Domain expertise around mobility best practices

Training and certification

MobileIron University

Best practice toolkits

BYOD, Apps, Android, Large Deployments

- Prepare
- Develop
- Roll Out
- Ssustain

Evaluation companion

Peer community

3 BEST PRACTICES FOR MOBILE IT

26 MobileIron

Why MobileIron

Best at Apps
Complete Application Management for *both* IOS and Android

Best at Enterprise Persona
Mobile Apps+Docs = Secure, Enterprise Persona

Best at Scale
100K devices per Appliance

Deployment Flexibility
Cloud and on-prem

27 MobileIron

Next Steps…

On Site Deep Dive

- Schedule an **On-site meeting** to discuss how MobileIron can help solve your mobile enablement needs

Deep Dive Webinar

- A **Deep Dive webinar** is held every week Thursday at 8am PST with live demos and answers to technical questions. register at: **deepdive.mobileiron.com**

Evaluation

- **Free 30 day evaluations** are available for customers at **evaluation.mobileiron.com**

MobileIron

3.6 Patrick Borras (UCOPIA)

Internet et les obligations légales, la réponse UCOPIA

Tout organisme désirant offrir un accès Internet au public est tenu de respecter des obligations légales. Cette présentation donne un aperçu des lois en vigueur liées à Internet et présente la solution UCOPIA qui apporte une réponse adaptée à ces obligations.

INTERNET ET OBLIGATIONS LEGALES, LA REPONSE UCOPIA

UCOPIA COMMUNICATIONS

SOMMAIRE

2

1. La législation relative à Internet
   - La Loi contre le terrorisme
   - La loi HADOPI
2. La solution UCOPIA en réponse aux obligations légales

11 février 2013 / Présentation Corporate 2013 UCOPIA

3

La législation

11 février 2013 / Présentation Corporate 2013 UCOPIA

La loi contre le terrorisme

Tout organisme fournissant un accès Internet à du public à partir de son réseau est tenu de mettre en œuvre les outils permettant de sécuriser son réseau et d'assurer la traçabilité des connexions utilisateur.

4

Loi n°2006-64 du 23 janvier 2006
Ou
Loi « Anti-terroristes »

11 février 2013 / Présentation Corporate 2013 UCOPIA

Que dit la loi contre le terrorisme?

- L'opérateur de communications électroniques est tenu de conserver…
  - Les informations permettant d'identifier l'utilisateur
  - Les données relatives aux équipements et terminaux utilisés
  - Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication
  - Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs
  - Les données permettant d'identifier le ou les destinataires de la communication

  (Décret n°2006-358 du 24 mars 2006, article R. 10-13 du CPCE)

5

- Les sanctions en cas de non respect de l'obligation de conservation des données sont…
  - **Un an d'emprisonnement et 75.000 euros** d'amende pour les personnes physiques et 375.000 euros pour les personnes morales. (Article L. 39-3 du CPCE)
- La durée de conservation des données est…
  - **D'un an pour le cas de la conservation des données relatives au trafic** lorsqu'il s'agit de la recherche, de la constatation et de la poursuite des infractions.
- Des données à délivrer aux personnes habilitées
  - Officier de Police, procureur de la République, …

11 février 2013 / Présentation Corporate 2013 UCOPIA

La loi HADOPI

HADOPI a pour objectif de favoriser la diffusion des œuvres et la protection des droits sur Internet

6

Loi 2009-669 du 12 juin 2009

11 février 2013 / Présentation Corporate 2013 UCOPIA

Que dit la loi HADOPI?

- Conservation des données utilisateur
- Des données à conserver pendant 1 an
- Sanctions sous forme d'amendes et coupure d'accès Internet
- Données à communiquer aux personnes habilitées

La législation en Europe

- La loi contre le terrorisme se décline dans bon nombre de pays Européen
  - Allemagne, Autriche, Belgique, Danemark, Italie, Pays Bas, …
- La durée de conservation des informations de connexion est variable suivant les pays
  - De 6 mois à 36 mois

UCOPIA, la réponse aux obligations légales

UCOPIA, qui sommes nous

- Leader européen sur le marché des contrôleurs d'accès haute performance
- UCOPIA sécurise les réseaux IP à destinations des utilisateurs nomades, visiteurs, ou employés
- Société créée en 2002
  - Par un essaimage de **l'Université Paris VI**
  - Soutenue par de **grandes institutions financières** (XAnge, LAU)
  - Siège social à Paris, bureaux à Munich, Londres, Milan
- 50% de croissance annuelle sur les six dernières années
  - Plus **de 7500 clients** dans tous les secteurs dont 75% du CAC 40
  - Un réseau de plus de **150 revendeurs européens**
  - Plus de **180 millions de connexions en 2012 sur nos solutions**
- 40% des connexions sur les solutions UCOPIA sont réalisées via des Smartphones / tablettes

Exemple du portail usine UCOPIA

UCOPIA, une réponse adaptée aux obligations légales

- UCOPIA répond aux besoins des organisations souhaitant s'équiper d'une connexion Internet sécurisée
  - Entreprises, hôtels, établissements d'enseignement, hôpitaux, administrations, …
- Conservation des données de connexions
- Service d'archivage des données
- Certification de Sécurité obtenue en 2010 de la part de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

01. UCOPIA COMMUNICATIONS EN BREF

UCOPIA sécurise le réseau en toute simplicité

*BYOD : Bring Your Own Device – Application mobile by Ucopia

Conclusion

- Les lois qui régissent Internet existent et sont appliquées
- Des solutions de mise en conformité à la législation existent
- UCOPIA est une réponse qui sécurise le réseau d'accès et qui apporte des fonctions de sécurité et mobilité
  - Authentification
  - Contrôle d'accès basé sur le lieu, le temps
  - Traçabilité
  - Simplicité du parcours client, confort d'utilisation
  - Application mobile
  - …

UCOPIA COMMUNICATIONS

Questions ?

+ 33 (0) 1 40 92 73 90
contactus@ucopia.com

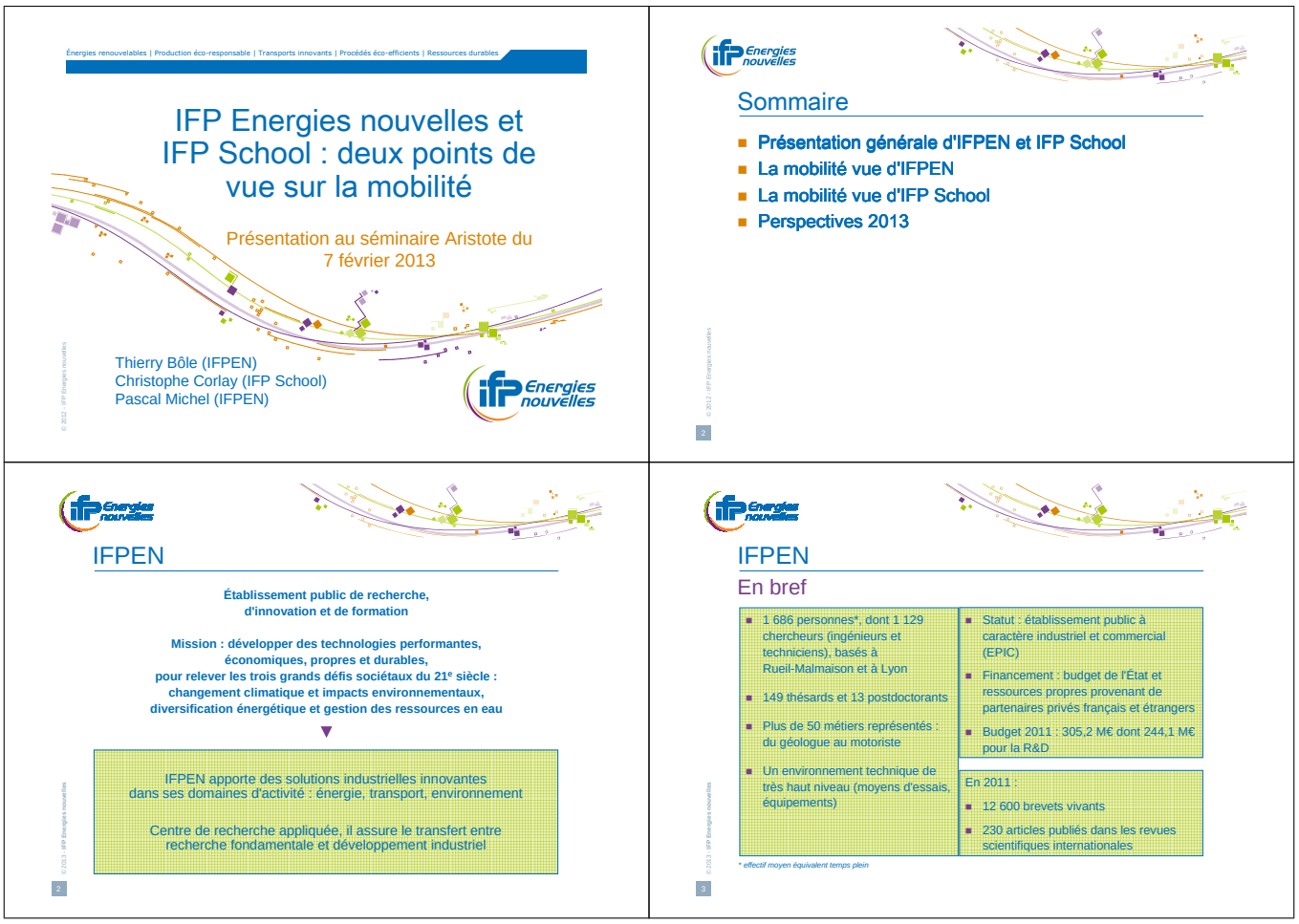
www.ucopia.com

3.7 Pascal Michel, Thierry Bôle (IFPen) et Christophe Corlay (IFP SChool)

IFP Energies nouvelles et IFP School : deux points de vue sur la mobilité

Thierry Bône est ingénieur sécurité de l'information à IFP Energies nouvelles. En relation avec le responsable de la sécurité du système d'information d'IFPEN, il étudie, met en place, contrôle et audite les éléments nécessaires à la sécurité de l'information. IFP Energies nouvelles présentera les solutions "classiques" mises en place pour permettre au chercheur d'accéder au système d'information en situation de mobilité depuis son poste IFPEN tout en garantissant un niveau de sécurité qui permet à l'entreprise de protéger son capital intellectuel. L'accès au SI d'IFPEN depuis le poste personnel de l'utilisateur est aujourd'hui limité à la messagerie et à quelques situations particulières.

Christophe Corlay est Responsable du système d'information d'IFP School. Chef de projet, il définit, pilote et assure le suivi de tous les projets de l'Ecole relatifs à l'utilisation d'outils informatisés d'aide à la formation et de gestion des élèves et des scolarités en relation avec le Comité de Direction d'IFP School. IFP School a fait le choix d'un système d'information externalisé qui permet de répondre au besoin de disponibilité 24/24 d'une l'école ouverte sur l'international. Le SI d'IFP School est accessible par toutes les parties prenantes (élèves, anciens, professeurs, personnel administratif) au travers d'un navigateur Web depuis le poste personnel de l'utilisateur



IFPEN
Positionnement stratégique

Le paysage énergétique

- Croissance de la demande et prix du pétrole
- Caractère par nature limité des énergies fossiles
- Changement climatique
- Difficile substitution massive et rapide des hydrocarbures pour les transports et la pétrochimie
- Tension sur les ressources humaines (nouvelles compétences, recrutement, formation)

Préparer la transition énergétique

Concevoir les solutions permettant d'optimiser l'utilisation des énergies fossiles tout en développant de nouvelles technologies et sources d'énergies pour répondre aux besoins sociétaux dans les domaines de l'énergie, du transport et de l'environnement

IFPEN
5 priorités stratégiques complémentaires

ÉNERGIES RENOUVELABLES	PRODUCTION ÉCO-RESPONSABLE	TRANSPORTS INNOVANTS	PROCÉDÉS ÉCO-EFFICIENTS	RESSOURCES DURABLES
DIVERSIFICATION ÉNERGÉTIQUE	RÉDUCTION IMPACT ÉCOLOGIQUE	EFFICACITÉ ÉNERGÉTIQUE		SÉCURITÉ DES APPRO.
	DÉCARBONATATION			
	CHANGEMENT CLIMATIQUE : RÉDUCTION ÉMISSIONS DE CO_2			
	DÉVELOPPEMENT DURABLE			
Produire, à partir de sources renouvelables, des carburants, des intermédiaires chimiques et de l'énergie	Produire de l'énergie en réduisant l'impact sur l'environnement	Développer des transports économes et à faible impact environnemental	Produire, à partir de ressources fossiles, des carburants et intermédiaires chimiques à faible impact environnemental	Proposer des technologies respectueuses de l'environnement et repousser les limites actuelles des réserves d'hydrocarbures

Transfert et diffusion du savoir
ENS du Pétrole et des Moteurs (IFP School)

- **IFP School : former les spécialistes de demain, capables de relever les défis associés à la transition énergétique**
- **Répondre ainsi aux besoins de talents en forte croissance dans l'industrie**
  - École d'application pour jeunes diplômés bac +4/+5 et professionnels
  - Délivrance d'un *Master of Science*
  - Près de 600 diplômés par an (ingénieurs, masters, etc.)
  - Près de 80 % d'élèves parrainés par l'industrie
  - 50 % d'élèves étrangers venant de plus de 45 pays
  - Taux de placement > 97 % à la sortie de l'École
  - 350 professeurs venant de l'industrie
  - 13 000 anciens élèves dans plus de 100 pays
  - Plusieurs formations diplômantes organisées dans des pays étrangers
  - Thèses : 150 étudiants en formation

IFP School

École d'application des métiers de l'énergie et des transports

Domaines :
- **Exploration-Production**
- **Procédés du secteur de l'énergie**
- **Motorisations et produits**
- **Économie-Management**

- Diplôme : diplôme d'ingénieur ou diplôme national de master
- Durée : 16 mois (standard)

Une forte intégration industrielle

- **80 %** des élèves parrainés et financés par l'industrie

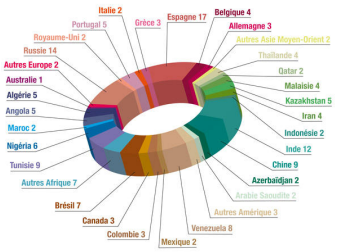
Arkema, Bosch, BP, Cepsa, CGG Veritas, Delphi, EDF, ExxonMobil, GDF Suez, Michelin, PDVSA, Perenco, Petrobras, PSA Peugeot Citroën, Renault, Saipem, Saudi Aramco, Schlumberger, Shell, Statoil, Technip, Total, Valeo, Volvo Powertrain...

- **350** enseignants issus de l'industrie

- Un taux de placement de **97 %** dès l'obtention du diplôme

Une École internationale

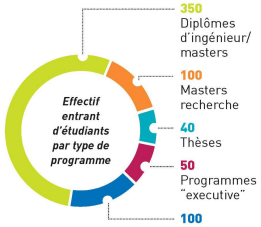
- Des programmes anglophones
- **50 %** d'étudiants internationaux
- **13 000** anciens étudiants en activité dans plus de **100** pays
- Des programmes joints avec des universités et écoles étrangères (Brésil, Canada, États-Unis, Norvège, Royaume-Uni, Russie)



Origine des étudiants
(promotion 2011, programmes orientés industrie)

Programmes

- Large gamme de 17 programmes de niveau master, en français ou en anglais
- Public : jeunes ingénieurs et professionnels de l'industrie
- Formations adaptées aux besoins de l'industrie et de la recherche appliquée
- Diplômes internationalement reconnus



Sommaire

IFPEN - Solutions autour de la mobilité

- Introduction
  - Besoins en matière de mobilité
    - Chercheurs fréquemment en déplacement dont pays avec législation spéciale aux passages de douane, besoins d'échanges croissants avec des entités tierces (structure collaborative des projets …), personnel IFPEN détaché à l'extérieur.
    - Besoins

    - d'accéder aux ressources IFPEN (dont messagerie, Intranet, zone fichiers, cluster HPC)
    - de sécurité : assurer la confidentialité des données, intégrité, traçabilité

IFPEN - Contexte organisationnel

- Politique de Sécurité de l'information IFPEN
  - Organisation :
    - DSI : Sécurité de l'information (aspects opérationnels)
    - DQSE : Sécurité des biens et des personnes
    - RSSI : Coordonne et supervise, garant de l'application de la Politique de Sécurité de l'Information
  - Sensibilisation à la sécurité du SI
    - Charte d'utilisation des ressources informatique mise à jour en 2012 qui traite des accès externes, des réseaux sociaux
    - Accueil "nouveaux arrivants", intervention DCRI
    - Guide des bonnes pratiques illustré avec des cas concrets
    - Guide du voyageur (inspiré de celui de l'ANSSI)

IFPEN - Accès au SI en mobilité

- Via un Portable IFPEN depuis l'extérieur

  - Configuration IFPEN Windows ou Linux
  - Chiffrement des données
  - Accès VPN soumis à des vérifications préalables
  - Accès limité au SI en fonction de la catégorie de population
  - Traçabilité et reporting mensuel
- Via un smartphone IFPEN

  - Terminaux chiffrés
  - Configuration gérée en central

IFPEN - Accès au SI en mobilité

- Cas du personnel en mission dans des pays spécifiques (dont Russie, Chine, Etats Unis)
  - Mise à disposition de poste "vierge"
  - Rapatriement des seules données utiles quant la législation du pays le permet

IFPEN - Accès au SI en mobilité

- Via un poste non IFPEN
  - Portail "Plan de Continuité d'Activité"
    - VPN SSL
    - Accès distant aux environnements bureautique et scientifique
  - Portail du personnel "Détaché"
    - VPN SSL
    - Accès Intranet seulement avec authentification forte
  - Portail Webmail
    - Reverse proxy
    - Accès à messagerie, contact, agenda
    - Restreint à certaines populations (responsabilisation et respects d'engagement pour synchronisation smartphone dont reset à distance et protection par code pin)

IFPEN – Infrastructure IFP School

- Besoin : mutualiser les ressources et les moyens
- Contraintes : gérer des populations différentes
  - Personnel de l'école et certains professeurs (=personnel IFPEN)
  - Population des étudiants présents sur le campus de Rueil
- Gestion administrative du personnel de l'école par le SI d'IFPEN
- Même réseau physique
  - Segmentation logique réseau (VLAN, ACL)
  - Segmentation logique Active Directory
  - Logiciels métiers pour les travaux pratiques (PC fixes dans les salles, service de fichiers)

IFPEN – Wifi Ecole

- Infrastructure Wifi dédiée pour accéder à Internet et au SI Métier de l'école
  - Authentification
  - Traçabilité
  - Accès depuis le Cyberclub sur des postes fixes
  - Accès depuis les portables et les terminaux personnels des élèves (et des professeurs) depuis n'importe où sur le campus IFP School …

Sommaire

- Présentation générale d'IFPEN et IFP School
- La mobilité vue d'IFPEN
- La mobilité vue d'IFP School
- Perspectives 2013

IFP School : différentes populations

- Le personnel IFP School (~60 personnes à Rueil)
- Les étudiants
  - **Ingénieurs (~ 350 /an, dont 50% d'étrangers) à Rueil**
  - **Masters recherche (~ 100 /an) à Rueil ou dans les universités partenaires**
  - **Essaimage (~ 150 /an) à l'étranger (Russie, Nigéria, Arabie Saoudite, ...)**
- Les enseignants non permanents (~350 français ou européens)
- Les anciens diplômés (~12 000 en activité répartis dans une 100e de pays)

IFP School : contraintes

- Applications du SI Ecole disponibles via internet, 24h/24, pour les étudiants / candidats venant de tous les pays, du Japon jusqu'à l'Amérique du Sud
- Gérer les différentes populations indépendamment d'IFPEN
  - **Hormis le personnel, les autres populations ne sont pas connues / enregistrées / gérées dans le SI IFPEN**

IFP School : solutions retenues

- Serveur / VM hébergés à l'extérieur (datacenter)
  - **Matériel propriété de l'École**
  - **Prestataire extérieur (Netwok-Studio)**
  - **Actuellement 9 VM installées**
- Annuaire LDAP indépendant pour gérer toutes les populations (typologie, droits, affectations, etc.) : OpenLdap / Meibo

IFP School : sécurité

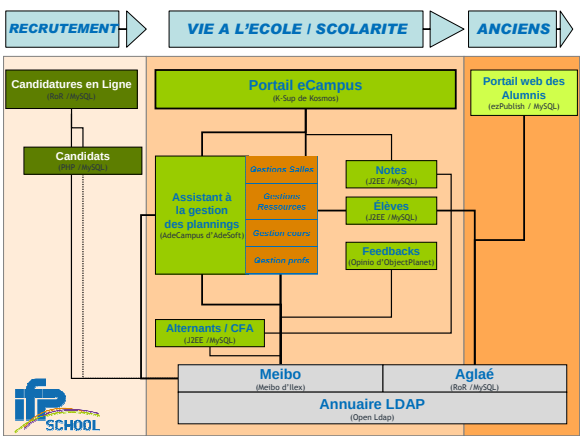
- Sécurisation du serveur :
  - **2 serveurs avec un SAN en redondance**
  - **Paire de switchs redondants**
  - **Firewall installé sur un NAS**
  - **Règles de contrôle sur les ports et protocoles**
  - **Accès SSH avec clés publiques et blacklistage**
- Sécurité du serveur sous contrôle IFPEN via des audits sécurité

IFP School : accès étendus

- Compatibilité tous supports (clients) :
  - **PC Windows/Linux, Mac, tablettes, smartphones**
- Compatibilité tous navigateurs (du moins les principaux) :
  - **Firefox, Chrome, Internet Explorer, Safari, ...**
- Compatibilité type de matériels (taille écran, écran tactiles, etc.) :
  - **Responsive design, applications mobiles**

IFP School : solutions mises en place

- Application métiers, la plupart en développements spécifiques:
  - **Pour les élèves : candidature, portail d'information (CMS), notes, feedbacks, plannings, etc.**
  - **Pour le personnel : candidats, CMS, notes, plannings, élèves, Meibo, Aglaé, etc.**
  - **Pour les personnes extérieures : Alternants, Alumni**
- eMail à vie (@ifp-school.com) :
  - **Attribué aux élèves et anciens diplômés**
  - **Alias vers leur email perso ou professionnel**



Sommaire

Perspectives 2013

- IFP School
  - Continuer le déploiement des applications sur tablettes et smartphones
- IFPEN
  - Renouvellement du smartphone IFPEN avec une solution centrale permettant de mieux gérer les smartphones personnels (cloisonnement des données)
  - Etude préliminaire BYOD (intérêts, enjeux, risques), problématiques légales en matière de droit social

Énergies renouvelables | Production éco-responsable | Transports innovants | Procédés éco-efficients | Ressources durables

Innover les énergies

www.ifpenergiesnouvelles.fr

3.8 Yvic Le Scouezec et Frederic Buisson (CISCO)

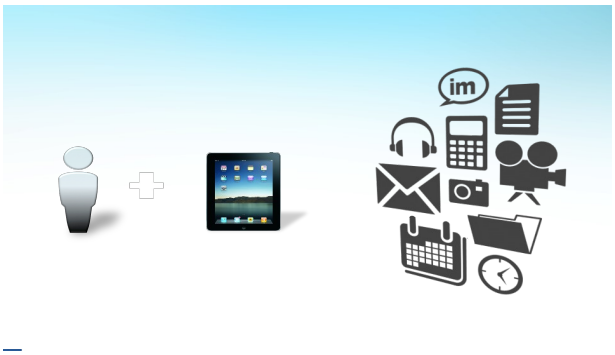
La gestion de la mobilité et des équipes en interne

Au delà du BYOD. L'expérience Cisco

Yvic Le Scouezec
Senior Manager, Cisco IT

Frédéric Buisson
Responsable des ventes produit sécurité
Secteur Public

BUILT FOR THE HUMAN NETWORK cisco



Un changement rapide et profond

BYOD: Un projet d'entreprise

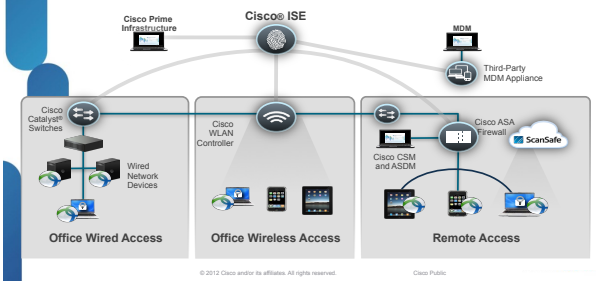
Comment adresser ces besoins ?

Spectre du BYOD

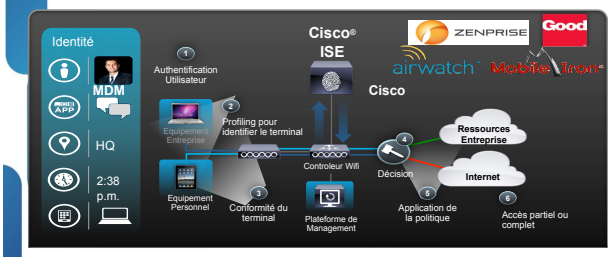
Limité	Basique	Amélioré	Avancé
Environnement nécessitant des contrôles stricts → Seuls les terminaux gérés par l'IT sont acceptés	Services basiques accessibles par tous → Variété des terminaux, mais accès limité (par exemple à internet)	Services différenciés Accueil des terminaux Accès sur site et à distance → Multiplicité des terminaux et des méthodes d'accès	Nouveaux services Applications métiers optimisées Collaboration → Multiplicité des terminaux Contrôle avancé

Les enjeux pour l'IT

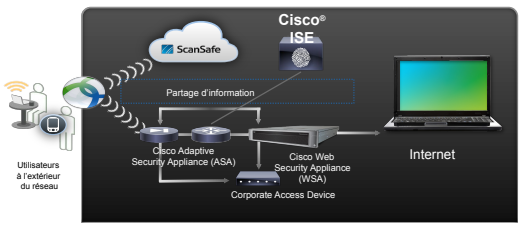
L'accès Unifié



One Policy



One Policy



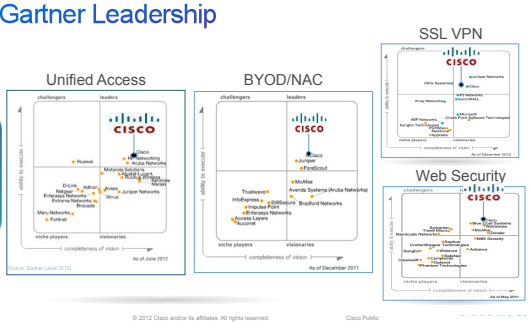
One Network : Offrir la meilleure expérience WiFi

Performance et Qualité	Eliminer les zones mortes. Cisco ClientLink
Prédictvité et robustesse	Protéger des interférences sans fil. Cisco CleanAir
Evolutivité	Supporter la vidéo haut débit. Cisco VideoStream
IPv6	Réseau sécurisé et proposant la Mobilité WiFi en IPV6

One Management

Monitoring de l'expérience	Visibilité de la performance applicative, simplifiant les opérations de diagnostic
Visibilité complète des clients connectés	Accéder aux informations cruciales sur la connectivité des clients, permettant un diagnostic rapide et efficace
Solution unifiée	Gérer de manière unifiée du cycle de vie complet filaire/wi-fi.

Gartner Leadership



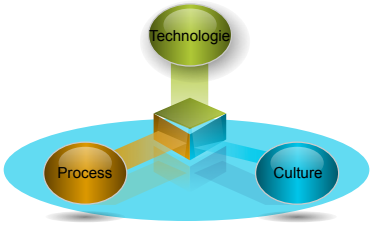
L'expérience Cisco

BUILT FOR THE HUMAN NETWORK cisco

CISCO en quelques Chiffres

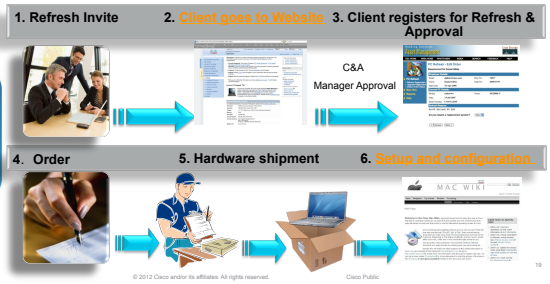
- 90 pays
- 450 bâtiments
- 50 salles serveurs
- 1000+ laboratoires
- 67,000 Employés
- 30,000 Prestataires
- 20,000 Partenaires
- 110+ Applications

Au-delà de la Technologie

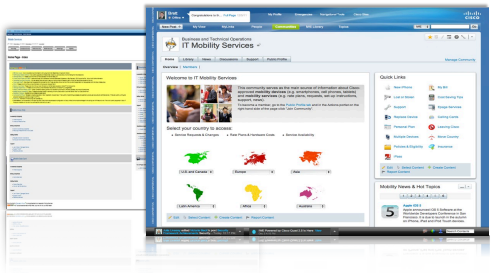


Un exemple client…

Process de refresh (incluant l'option Mac)



Social Support – Evolution Self-Service



BYOD : L'état des lieux

Platform*	August 2010	August 2011	August 2012
iPhone	5,895	17,337	24,779
iPad	677	5,933	11,863
BlackBerry	14,910	13,917	8,676
Android	209	3,822	6,798
Others	5,428	1,337	986
Total	**27,119**	**42,386**	**53,102**

*Includes devices with corporate plans, personal plans, and wi-fi only

Smartphones and Tablets at Cisco

Cisco's two year mobile device growth rate is **96%**

Créer un concensus

Implémentation de la politique

Corporate Policies
- Device Purchase
- Account Liability

Specific Directives
- Theater/Location
- Function/BU

Approvals
- Vice President for Corporate Liable
- Manager for Individual Liable

BYOD : Usage acceptable

Cisco Rules of Use

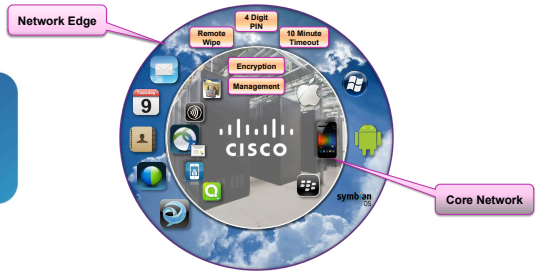
1) Allows Cisco to remotely wipe the device
2) Requires an acceptable password and 10 minute timeout
3) Require users to immediately report a lost or stolen device.

- All users must accept rules of use when signing up for service
- Trade off between employee trust and IT control
- There is no IT jargon – the rules are simple for end-users to understand

BYOD : Quelques métriques

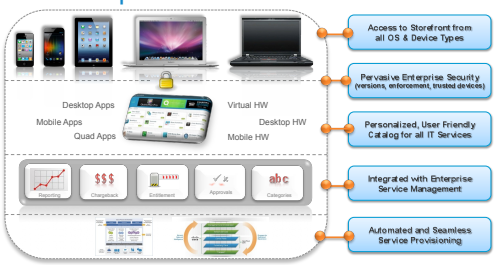
*2 year comparison

Modèle de sécurité pour l'accès distant



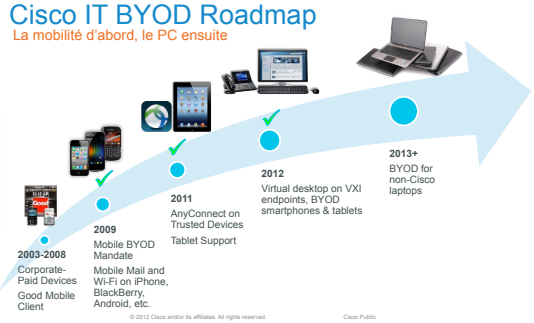
Cisco IT App Selection

Cisco Enterprise Store



Cisco IT BYOD Roadmap

La mobilité d'abord, le PC ensuite



One Network	Expérience utilisateur optimisée, au bureau ou en mobilité
One Policy	Une source unique pour la sécurité Des règles contextuelles
One Management	Une gestion simple Un déploiement "zero-touch"
Cisco on Cisco	Une expérience unique Des services innovants pour les utilisateurs Des mesures du succès

CISCO

3.9 Laurent Gydé (RENATER)

La mobilité sécurisée par les services RENATER

Laurent Gydé est directeur technique chez RENATER. La fédération d'identité pour la mobilité numérique, Eduroam pour l'accès wifi fédéré. RENATER, REseau NAtional pour la Technologie, l'Enseignement et la Recherche, relie entre eux et vers la communauté scientifique mondiale plus de 1300 sites d'enseignement et de recherche. Pour plus de 2 millions d'utilisateurs, RENATER répond depuis plusieurs années aux enjeux majeurs que sont la multiplication des services numériques entre établissements ainsi que l'accès réseau en situation de mobilité avec deux dispositifs complémentaires : la Fédération d'Identité Education-Recherche et le service d'accès réseau eduroam. Cette présentation fera un retour d'expérience sur ces deux déploiements au niveau national, ainsi que sur les extensions internationales en cours ou à venir.

RENATER
CONNECTEUR DE SAVOIRS

Séminaire Aristote
Sécurité et Mobilité

Retour sur les déploiements
eduroam et
Fédération Éducation/Recherche

7 février2013

RENATER
CONNECTEUR DE SAVOIRS

Agenda

- La communauté RENATER
- L'offre de service
- La mobilité numérique avec la Fédération Éducation/Recherche
- La mobilité réseau avec eduroam
- Conclusion

RENATER
CONNECTEUR DE SAVOIRS

La communauté RENATER

La communauté des utilisateurs 1/2

RENATER
CONNECTEUR DE SAVOIRS

Le BRGM : Bureau de la Recherche Géologique et Minière
Le CEA : Commissariat à l'Energie Atomique
IRSTEA : Institut National de Recherche en Sciences et Technologies pour l'environnement et l'agriculture
Le CIRAD : le Centre de coopération Internationale en Recherche Agronomique pour le Développement
Le CNES : Centre National d'Etudes Spatiales
Le CNRS : Centre National de la Recherche Scientifique
La CPU : La Conférence des Présidents d'Université
L'INRA : Institut National de la Recherche Agronomique
INRIA : Institut National de Recherche en Informatique et Automatique
L'INSERM : Institut National de la Santé et de la Recherche Médicale
L'IRD : Institut de recherche pour le développement
Le Ministère de l'Education nationale : Ministère de l'Education nationale
Le Ministère de l'Enseignement Supérieur et de la Recherche : Ministère de l'Enseignement Supérieur et de la Recherche
L'ONERA : le centre français de recherche aérospatiale

La communauté des utilisateurs 2/2

- Etablissements d'enseignement ou de recherche relevant d'autres tutelles (industrie, culture, agriculture, défense …)
- Fondations impliquées dans la recherche (Institut Curie, Institut Pasteur …)
- Grands établissements (CSI, IRCAM …)
- …

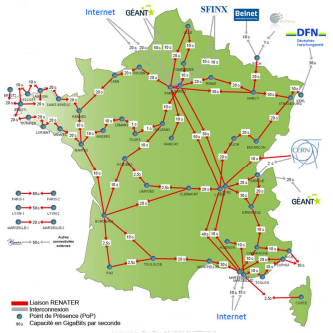
⇒1400+ sites
⇒2+ Mutilisateurs

L'offre RENATER

6

L' offre RENATER

Une infrastructure réseau



Un portefeuille de services pour l'enseignement et la recherche

- Services réseaux
- Services applicatifs
- La sécurité

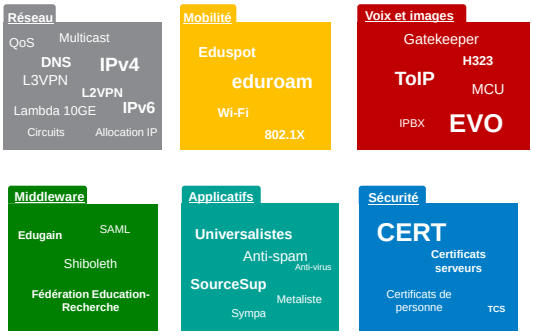
Quelques chiffres

Une couverture réseau complète

- 11 900 km de fibre optiques, 72 points de présence (NR)
- Réseau: 125 longueurs d'onde 10G
- Trafic: connectivité extérieure cumulée de près de 200Gbit/s, 100+Po échangés avec l'extérieur en 2012
- 1400+ prises en France métropolitaine et DOM/TOMs

Des services très utilisés

- 10 000 certificats électroniques délivrés au total
- 30 000 appels téléphoniques/an
- Antispam pour 800 000 comptes de messagerie, 2 000 000 d'emails filtrés par jour
- Accès WIFI eduroam : plus de 150 établissements opérationnels, 50 000 requêtes/jour en France
- Près de 20000 visioconférence RMS et EVO par an
- Le service de listes de diffusion Universalistes : 400 000 abonnés



La mobilité numérique :

La Fédération Education/Recherche

10

Le contexte :

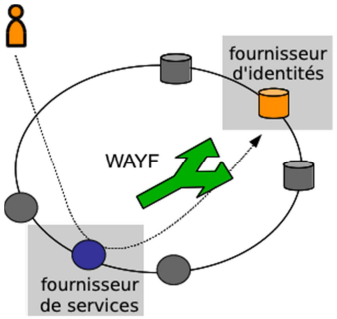
- Le paysage de l'enseignement supérieur et de la recherche se consolide
- Les réseaux autorisent désormais l'accès massif aux ressources distantes
- De plus en plus d'utilisateurs utilisent les services de plusieurs organisations
- Offres de services mutualisées de plus en plus nombreuses (PRES, UNR, …)
- De plus en plus de mutualisations au niveau national

⇒ **Comment passer à l'échelle pour l'authentification et l'accès ?**

La Fédération Education-Recherche

- **Infrastructure nationale**
- Pour **authentification web**
- Mécanismes de **fédération d'identités**
- Utilisant le logiciel **Shibboleth**
- Implémente le protocole **SAML**

Fédération / comment ça marche ?



Fédération / précisions

- Les mots de passe ne circulent pas
  - Juste une preuve d'authentification
- Authentification ET attributs utilisateurs
  - Utiles pour contrôle d'accès et personnalisation
- On ne réinvente rien
  - Branchement CAS et LDAP
- On est interopérable
  - Protocole SAML
- On contrôle les échanges
  - On peut restreindre le cercle de confiance

Les comptes CRU
Comptes Réseaux Universels

- IdP ouvert à tous les utilisateurs :
  - Création du compte en quelques minutes
  - Sans formalités
  - Ne nécessite qu'une adresse électronique valide
  - Permet d'accéder aux (nombreux) services qui les acceptent
- Mais …
  - Pas de vérification de l'identité

Fédération / Pour faire quoi ?

- Ressources documentaires
- E-learning
- Accès Wi-Fi
- Applications métier mutualisées
- Applications et services nationaux (dont RENATER)
- Extranet
- Distribution de logiciels
- …

Fédération / Qui l'utilise ?

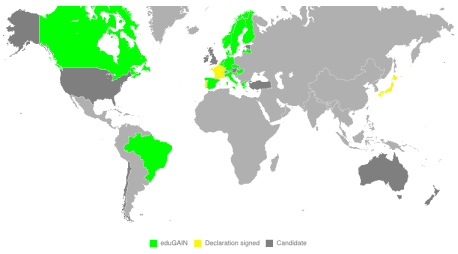
- En France *(février 2013)*
  - 169 fournisseurs d'identités
  - 337 ressources enregistrées
  - Des ressources locales non enregistrées
- RENATER
  - Migration progressive de tous les services (portails, visio, groupware …) vers une authentification fédérée
- Dans d'autres pays
  - https://federation.renater.fr/docs/autres_federations
  - Interopérables dans le cadre du projet européen eduGAIN

eduGAIN

- Initiative européenne d'inter-fédération
  - Ouverte aux fédérations non européennes
- Favorise l'échange et l'accès à des ressources internationales
- Norme SAML 2
- Fédération Education-Recherche en cours d'intégration (cible mi 2013)

eduGAIN

- Etat du déploiement dans le monde (février 2013)



Fédération / sujets en cours …

- Amélioration d'ergonomie à apporter
  - Intégration en mode SSO dans les ENT
- Qualité des référentiels d'identité utilisés pour les IDP
  - En liaison avec l'activité SupAnn de normalisation des annuaires de la communauté E/R
- Concentration des risques sur les IDP (identity provider)
  - Développement d'IDP avec authentification multi-facteurs
- Extensions internationales : eduGAIN

La mobilité réseau : eduroam

21

Le contexte :

- Différentes opérations nationales ont développé l'utilisation du WIFI pour les étudiants, les chercheurs et les personnels
- L'utilisation d'un ordinateur portable pendant les réunions est désormais banalisé (y compris pour le chat en support de la visio)
- Les collaborations entre établissements se multiplient, les personnels se déplacent …
- Les cursus communs se multiplient, les étudiants se déplacent …

⇒ **Comment fournir l'accès WIFI partout et pour tous sans multiplier l'effort correspondant ?**

eduroam pour l'utilisateur E/R

- C'est une connexion Wi-Fi
  - Sécurisée (802.1x)
  - Utilisable dans son établissement d'origine
  - Utilisable dans d'autres établissements
  - Utilisable à l'étranger
  - Saisie de son login habituel
  - Configuration initiale du client (PC/mac/tablette/smartphone …)

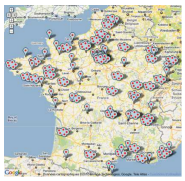
eduroam en 1:31 min

www.eduroam.org

http://vimeo.com/32210851

eduroam / où l'utiliser ?

- >150 établissements français membres
  - ~300 sites déclarés
  - 100.000 logins inter-etab en octobre 2010
- Europe
  - 36 pays couverts
  - 800+ organisations membres
  - 4500 sites déclarés
- Monde
  - 54 pays
  - Près de 6000 sites



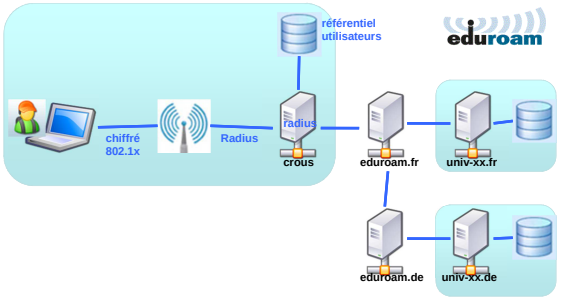
eduroam / où l'utiliser ?

- >150 établissements français membres
  - ~300 sites déclarés
  - 100.000 logins inter-etab en octobre 2010
- Europe
  - 36 pays couverts
  - 800+ org membres
  - 4500 sites déclarés
- Monde
  - 54 pays
  - Près de 6000 sites

eduroam / qui fait quoi ?

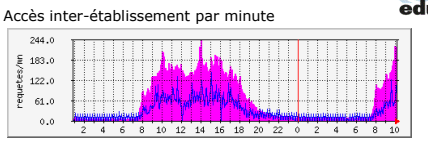
- L'infrastructure internationale
  - **Europe**, USA, Canada, Asie
  - Serveur radius racine
  - Organisation financée par l'UE dans le cadre du projet GN3
- eduroam en France
  - Opéré par RENATER
  - Un service radius proxy national (redondé)
- Les établissements
  - Opèrent un serveur radius pour leurs utilisateurs
  - Proposent des points d'accès Wi-Fi

eduroam / comment ça marche ?

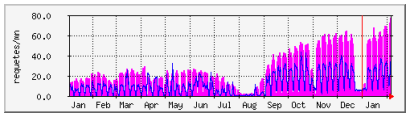


eduroam / utilisation en mobilité

- Accès inter-établissement par minute



- Augmentation visible sur 12 mois



eduroam / sujets en cours …

- Homogénéité des protocoles d'authentification 802.1x
  - Co-existence (ou pas) de TTLS et PEAP sur les sites
  - En cours d'harmonisation
  - ⇒ http://www.eduroam.fr/monitoring/monitoring.html
- Configuration des postes clients
  - Déploiement imminent d'un service de configuration au niveau européen
  - ⇒ https://cat-test.eduroam.org/
- Filtrages mis en œuvre sur les accès eduroam
  - Préconisation pour les sites
  - ⇒ https://services.renater.fr/ssi/_media/cert/pf-wifi-v6-1f.pdf
- Extension d'eduroam vers des réseaux d'opérateurs
- Support à l'utilisateur
  - To do (better)

Bonus !

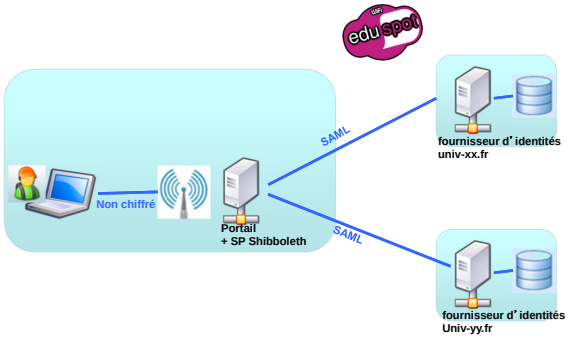
L'accès réseau nomade grâce à la Fédération Education/Recherche

31

eduspot … pourquoi ?

- eduroam ne répond pas à 100% des besoins
- Situation selon les établissements
  - eduroam pour tout le monde
  - eduroam pour enseignants et personnel
  - Pas d'eduroam
- Les autres solutions Wi-Fi
  - De type portails captifs
  - Authentification
    - locale (LDAP, CAS)
    - fédérée (Shibboleth)

Fonctionnement



eduroam vs. eduspot

	eduroam	eduspot
Sécurité	Flux radio chiffré (802.1x)	Flux radio non chiffré
Authentification	EAP / Radius (via proxies éventuellement)	Fédération d'identités (échange direct utilisateur⇔IdP)
Configuration	Configuration du poste utilisateur	Aucune (lancement navigateur)
Contraintes architecture	Serveur radius + raccordement au proxy	Portail + white list + SP Shibboleth
Ergonomie	Transparent (modulo profil standard)	Pas de configuration du poste. Plusieurs clics. Partage session ENT
Couverture	Internationale (arbre)	Nationale (cercle de confiance)
Comptes invités	Envisageable	Envisageable

Principaux enseignements

- Pour les services à l'utilisateur final, le passage à l'échelle dans la communauté E/R nécessite une organisation répartie
- La publicité du monitoring des services distribués favorise l'implication des acteurs locaux
- L'accompagnement de l'utilisateur final reste un défi à relever à tous les niveaux
- Le contexte (plateformes collaboratives, visio, BYOD, équipes réparties, services mutualisés …) et plus que jamais demandeur d'outils pour la mobilité.
- Dès les freins techniques levés, l'adhésion à ces services est toute naturelle pour les utilisateurs !

RENATER
CONNECTEUR DE SAVOIRS

1993 20 ANS 2013

Merci de votre attention !

www.renater.fr

3.10 Jacques Le Rest (Ifremer)

Solution d'accès Wifi UCOPIA

Ingénieur télécoms à Ifremer. Avec deux autres collègues, il définit et maintient à jour l'infrastructure réseau des 26 implantations qui constituent l'institut. Sa présentation portera sur la mise en œuvre du portail captif Ucopia pour les accès Wifi visiteurs dans le but d'être conforme à la législation française.

Ifremer

Portail captif Ucopia

Un accès wifi visiteur à Ifremer

Jacques LE REST – Ingénieur Télécoms – Ifremer
Séminaire Aristote « Sécurité & Mobilité » 7 février 2013

Séminaire Aristote « Sécurité & Mobilité »

Ifremer

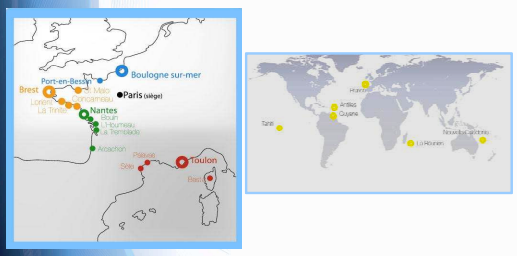
Institut français de recherche pour l'exploitation de la mer
- Connaître, évaluer et mettre en valeur les ressources des océans et permettre leur exploitation durable
- Améliorer les méthodes de surveillance, de prévision, d'évolution, de protection et de mise en valeur du milieu marin et côtier
- Favoriser le développement économique du monde maritime

Ifremer 2

Séminaire Aristote « Sécurité & Mobilité »

Ifremer - Implantations

26 sites répartis sur tout le littoral métropolitain et dans les DOM-TOM



Ifremer 3

Séminaire Aristote « Sécurité & Mobilité »

Organisation informatique

Réseau Privé Virtuel pour interconnecter les sites
- Orange

Accès Internet
- POP Renater de Brest 2

Le service informatique basé à Brest
- Effectif : 20 personnes
- Equipe réseau : 3 ingénieurs

Ifremer 4

Séminaire Aristote « Sécurité & Mobilité »

Le Wifi

Pas de déploiement massif
- Réservé au salle de réunion & ateliers

Gestion centralisée
- WLC Cisco
- ~ 50 bornes

2 SSID
- Visiteur & Intranet

Ifremer 5

Séminaire Aristote « Sécurité & Mobilité »

Wifi Intranet

Sécurisation TTLS
- Certificat annuel
- SecureW2 en XP, driver carte en Vista, W7

Authentification par login des agents Ifremer

Accès complet aux ressources de l'intranet

Ifremer 6

Wifi visiteur

En cour de bascule vers un portail captif Ucopia

Ancien accès
- Simple clé WEP affichée dans les salles
- Accès à Internet via un proxy
- Pas de log vraiment exploitation
- Non conforme à la Directive européenne 2006-24-CE et au Décret français du 24 mars 2006

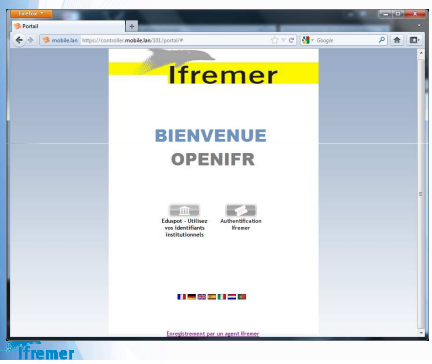
La solution Ucopia

Ce qui nous a séduit
- Conservation des données de connexions
  - sessions : qui s'est connecté quand ?
  - activité : qui a fait quoi ?
- Principe du portail captif
  - Interception du trafic HTTP
    - Zéro configuration sur les PC
  - https nécessite la prise en compte d'un proxy

La solution Ucopia

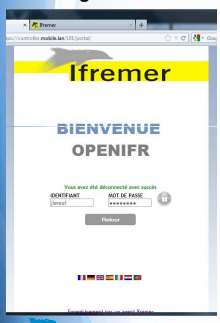
Ce qui nous a séduit (2)
- Connecteurs pour gérer les utilisateurs
  - Base interne, radius (eduroam), LDAP
  - Depuis juillet 2012 Shibboleth (eduspot)
- Gestion des droits en fonction du type d'authentification
- Interface et multi-linguisme

Le portail captif

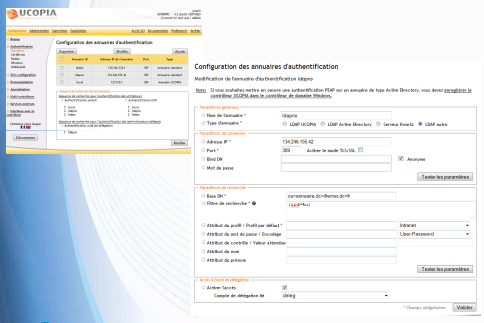


Authentification par annuaire

Interrogation de l'annuaire d'entreprise LDAP



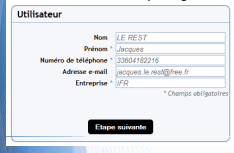
Configuration des annuaires



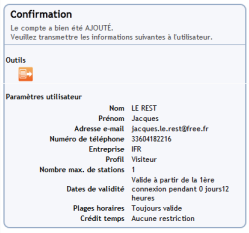
Compte visiteur : délégation

Compte visiteur : enregistrement

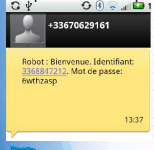
1 : Saisie de l'identité par agent Ifremer



2 : Ajout du compte dans la base



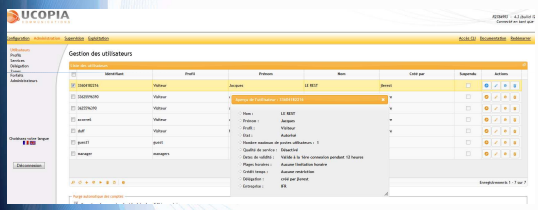
3 : Réception identifiant par SMS



Compte visiteur : base visiteur

Séminaire Aristote « Sécurité & Mobilité »

Base locale visiteur de l'Ucopia

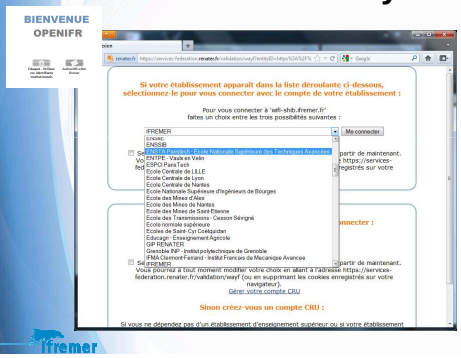


Ifremer

15

Authentification par la fédération d'identité : Wayf

Séminaire Aristote « Sécurité & Mobilité »



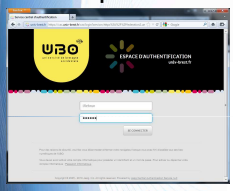
Ifremer

16

Authentification shibboleth

Séminaire Aristote « Sécurité & Mobilité »

Exemple Université Bretagne Occidental



ATTENTION: fermer cette fenêtre vous déconnectera.

Cliquez ici pour accéder à la page demandée

Identifiant	dominique.lebrun@univ-brest.fr
Profil	Visiteur
Services	HTTP, Mail
Zone d'entrée	Openifr
Plages horaires	Tous les jours
Validité	Toujours valide

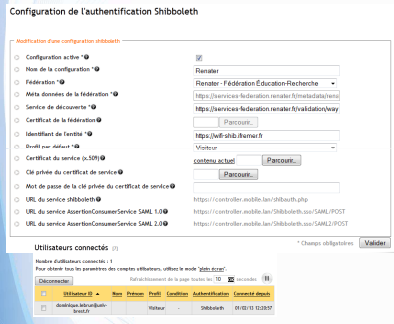
Déconnexion

Ifremer

17

Configuration shibboleth

Séminaire Aristote « Sécurité & Mobilité »



Ifremer

18

Des questions ?

Séminaire Aristote « Sécurité & Mobilité »

Ifremer

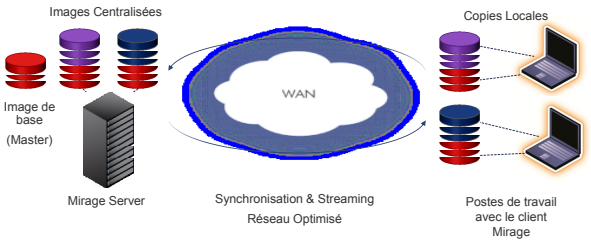
19

3.11 Philippe Breider (Vmware)

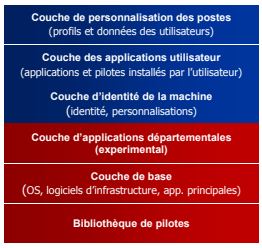
VXI

A l'heure où les tablettes graphiques et les PDA gagnent du terrain sur les PC traditionnels, où les utilisateurs développent de nouveaux usages basés sur les outils disponibles dans le cloud public et où la pression pour la réduction des coûts liés aux postes de travail n'a jamais été aussi forte, il est temps de moderniser les environnements de travail pour répondre à ces défis. L'environnement de travail utilisateur selon VMware c'est un ensemble de services : Services de postes de travail, Services applicatifs, Services de données et Services mobiles, gérés et accédés à travers un portail centralisé.

Mirage: gestion centralisée et execution locale



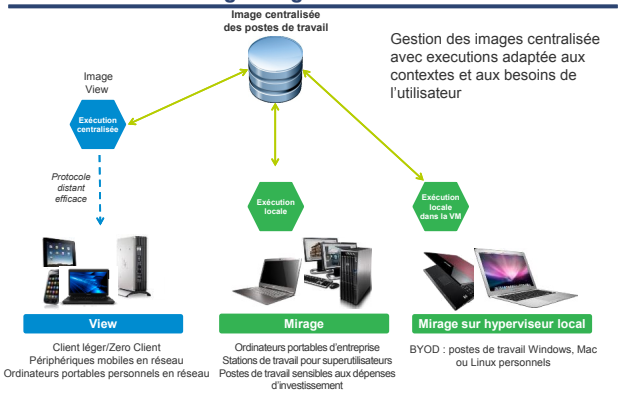
Gestion d'une image unique multi-niveau



VMware Mirage divise chaque point d'accès en couches logiques

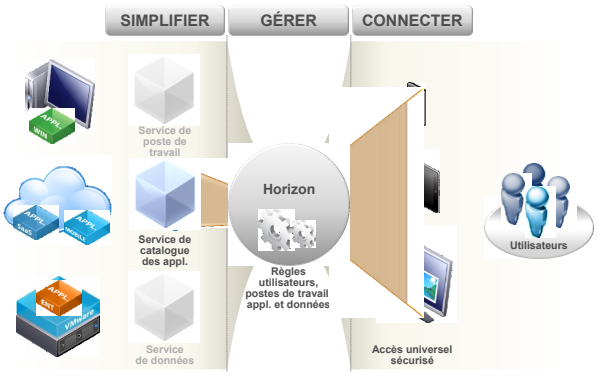
- Toutes les couches sont stockées dans le datacenter
- Les couches bleues sont sauvegardées en permanence à partir des points d'accès
- Les couches rouges sont gérées par le service informatique

VMware View + Mirage : la gestion centralisée unifiée



Gestion des images centralisée avec executions adaptée aux contextes et aux besoins de l'utilisateur

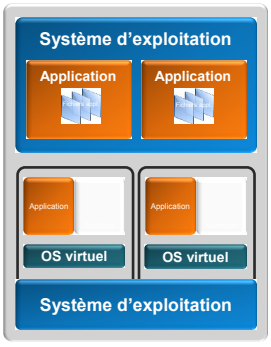
ThinApp et Horizon : la fourniture de catalogues de services applicatifs



Réduire les conflits d'applications et les coûts de support

ThinApp simplifie le packaging et le déploiement des applications

- Dissocier les applications et les données du système d'exploitation
- Supprimer les conflits entre applications (migration Win7, IE6 sous Win7, fin du support de XenApp5)
- Permettre plusieurs versions d'une même application sur un même poste
- Mettre en place des catalogues de services applicatifs à la demande
- Intégration facile aux outils de déploiement existants
- Compatible avec les postes traditionnels ou virtuels

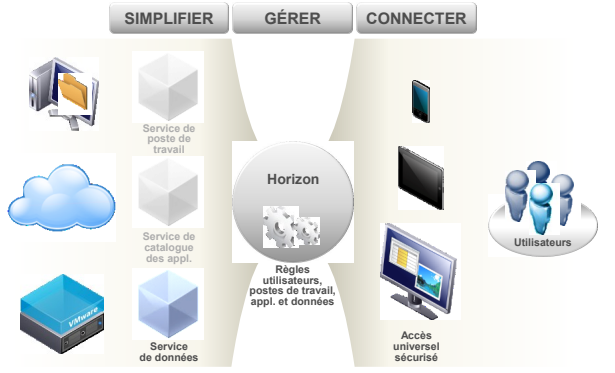


VMware Horizon : gestion unifiée des applications

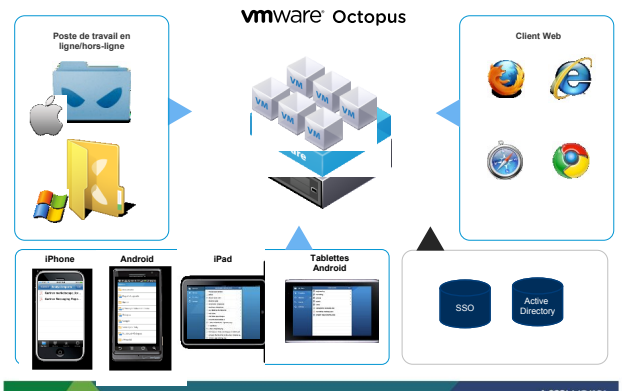
Diffusion de toutes les applications disponibles dans le Cloud

- Déploiement des applications SaaS, Web et Windows sur n'importe quel périphérique
- Gestion des droits, des règles d'accès associées aux application
- Catalogue d'applications unifié
- Rapports et surveillance en temps réel
- Gestion des application publiées avec Citrix XenApp (H1 2012)

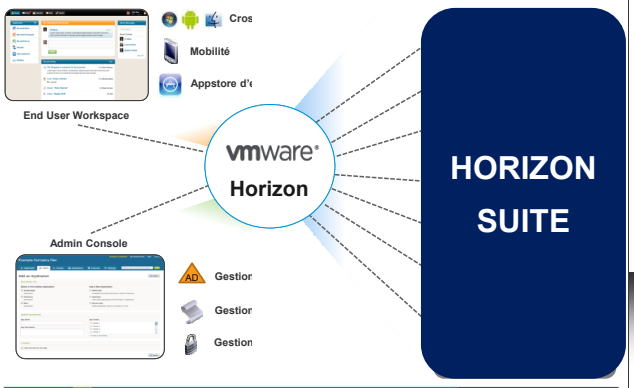
Projet Octopus : service de collaboration et de synchronisation de données sécurisé



Présentation d'Octopus



Horizon Suite – le Cloud Workspace de demain



vmware

vmware

Merci

ARISTOTE Association Loi de 1901. Siège social : CEA-DSI CEN Saclay Bât. 474, 91191 Gif-sur-Yvette Cedex.
Secrétariat : Aristote, École Polytechnique, 91128 Palaiseau Cedex.
Tél. : +33(0)1 69 33 99 66 Fax : +33(0)1 69 33 99 67 Courriel : Marie.Tetard@polytechnique.edu
Site internet http://www.association-aristote.fr