Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

R&D en sécurité des systèmes d'information Orientations et enjeux

Direction Centrale de la Sécurité des Systèmes d'Information

F. Chabaud

SSTIC - 6 juin 2008

PREMIER MINISTRE
S·G·D·N

Plan

- La sécurité des systèmes d'information : un enjeu de souveraineté
- Défense en profondeur en SSI
- Forces et faiblesses de la recherche française
- Les thématiques techniques prioritaires
- Conclusion

Un enjeu de souveraineté

Souveraineté :

- Pouvoir suprême reconnu à l'État, qui implique l'exclusivité de sa compétence sur le territoire national et son indépendance internationale, où il n'est limité que par ses propres engagements
  - Le petit Larousse illustré, 2005, 100ème édition.
  - ✓ Protéger l'autonomie de décision de l'État
    - ➢ au delà des frontières, même numériques.
  - ✓ Rôle protecteur de l'État pour ses citoyens.

Et la souveraineté dans tout ça…

- Juillet 2007 : Lorsque Windows Vista se connecte à l'Internet, 20 utilitaires et services transmettent des informations utilisateur à Microsoft.
  - ✓ Et 47 autres se contentent de stocker des données localement, pour ne communiquer qu'environ 50% de leur collecte.
  - ✓ Pour plusieurs outils, la justification n'est pas claire : NAT sur Ipv6, gestionnaire de périphériques, Plug and Play, associations de fichiers, observateur d'événements, icône de statut de connexion…
  - ✓ A chaque fois qu'il utilise ces services, l'utilisateur partage ses informations avec la firme de Redmond.
  - ✓ Une ligne le rappelle dans le contrat de licence Vista : « En utilisant ces services, vous acceptez la transmission de cette information. »
- Selon une étude publiée par Softpedia, les 47 autres outils archiveraient un volume de données qui mettrait en danger le respect de la vie privée…

Et la souveraineté dans tout ça… (2)

- Novembre 2007 : Le site cryptome.org a publié une liste d'adresses IP de la NSA (National Security Agency).
  - ✓ Parmi les commentaires, l'auteur de la note précise qu'elles sont utilisées notamment pour «la mise sur écoute de téléphones intelligents (« smart phones ») équipés de Microsoft Mobile».
  - ✓ Les privilèges d'administration à distance ouvrent une porte dérobée sur les systèmes d'exploitation Microsoft, via les ports TCP / IP 1024 à 1030.
  - ✓ Ceci est souvent activé lors de visites sur les serveurs de mise à jour Microsoft.
  - ✓ Une fois les privilèges d'administration établis, il est possible d'accéder aux machines à distance et à volonté…

Et la souveraineté dans tout ça… (3)

- *Mars 2008 :* Au marché noir de la cyberdélinquance, Message Labs a découvert un programme d'affiliation avec rémunération pour infecter des ordinateurs.
  - ✓ Très complet, ce site affiche une liste de prix en dollars pour 1 000 machines compromises :
    - 100 dollars pour un lot situé en Australie,
    - 60 pour un lot au Royaume-Uni ou en Italie,
    - 50 pour les États-Unis,
    - 25 en France, et…
    - 3 dollars seulement en Asie.
- Les webmestres participants sont invités à insérer du code qui piège leurs pages !
  - ✓ Ce code appelle en cascade des scripts hostiles hébergés sur des sites compromis, ou des réseaux de machines zombie.
  - ✓ En cas de test réussi sur une vulnérabilité, un code léger est exécuté sur le poste victime.
    - Ce code charge des chevaux de Troie, modifiés tous les trois jours pour éviter la détection.
    - Activé 15 à 30 minutes après installation, il ira télécharger d'autres codes malveillants tout en comptabilisant une unité à l'actif du webmestre malveillant.
- La « revente » de machines compromises (infectées par des espiogiciels) est désormais monnaie courante sur le marché noir de la cyber-délinquance.
- De nombreux réseaux de machines zombies sont loués pour diverses tâches.

Et la souveraineté dans tout ça… (4)

- Mars 2008 : La chaîne de magasins d'alimentation américaine Hannaford a été victime d'une attaque informatique
  - ✓ Les informations de plus de 4,2 millions de cartes ont été dérobées au cours des trois derniers mois
  - ✓ L'attaque utilisait un espiogiciel qui a été découvert dans la totalité des magasins de la Nouvelle-Angleterre et de l'État de New York, ainsi que dans la majorité des magasins Sweetbay de la chaîne en Floride.
  - ✓ Ce logiciel interceptait les données des cartes de crédit et de guichet des clients, au moment où elles étaient transmises aux banques par les magasins pour approbation.

Et la souveraineté dans tout ça… (5)

- Avril 2008 : découverte et saisie de certains matériels réseau Cisco contrefaits fabriqués en Chine
  - ✓ livrés aux agences gouvernementales et militaires américaines.
  - ✓ une enquête ouverte par le FBI craint que les attaquants chinois aient placé des portes dérobées indétectables dans ses infrastructures réseaux.
    - ➢ En effet, la proportion importante de routeurs et de switchs Cisco contrefaits installés ces dix-huit derniers mois dans les réseaux des agences compromet leur sécurité face à des attaques ciblées..

Et la souveraineté dans tout ça… (6)

- Mai 2008 : Microsoft dévoile une clé USB capable d'extraire des éléments de preuves importantes lors d'enquêtes judiciaires.
  - ✓ Microsoft a mis au point une mini-clé USB destinée aux services de police amenés à analyser le contenu de disques durs.
  - ✓ Le Computer Online Forensic Evidence Extractor (COFEE) peut être utilisé dans le cadre des enquêtes de police afin de lire des disques durs et de déchiffrer des mots de passe sans avoir à éteindre l'ordinateur et à effacer des preuves.
  - ✓ La clé compte 150 commandes et peut se connecter au disque dur, vérifier l'historique de navigation et déchiffrer certains mots de passe.
  - ✓ Microsoft distribue sa clé gratuitement depuis l'année dernière et estime qu'elle serait utilisée par plus de 2 000 représentants des forces de l'ordre dans 15 pays différents…

Mais que fait la RECHERCHE ?

- Il y a un manque de perception de ces enjeux
  - ✓ Domaine technique nouveau
  - ✓ Difficile à comprendre
- La culture de la sécurité est peu présente
  - ✓ La société française y est globalement réfractaire
  - ✓ Il y a un manque de formation
    - ➢ La SSI c'est une spécialité de fin de cursus
    - ➢ Alors que la SSI ce sont des principes applicables à tous les niveaux
- **<u>Face à cela la recherche a un rôle important à jouer</u>**

Défense en profondeur

Les six idées les plus stupides en matière de Sécurité des Systèmes d'Information…

- Un grand merci à Marcus Ranum pour son article humoristique mais profondément sérieux de 2005 intitulé :
  - ✓ ***The Six Dumbest Ideas in Computer Security***
- Ce qui suit est un résumé traduit de cet article
  http://www.ranum.com/security/computer_security/editorials/dumb/index.html

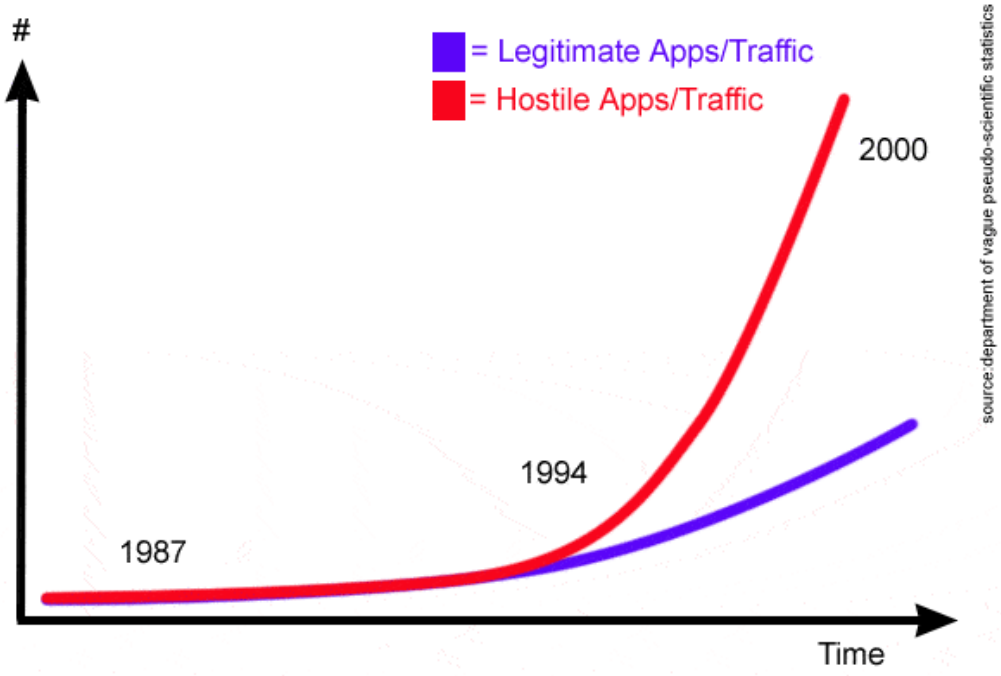
Idée stupide n°1
L'autorisation par défaut

- Tout ce qui n'est pas explicitement interdit est autorisé
- C'est malheureusement le cas général de tous les systèmes
- Parce que c'est le plus confortable
  - ✓ Exemple type : tout programme est exécutable sauf si mon anti-virus l'interdit
  - ✓ D'autant plus stupide que le nombre d'applications couramment employées sur un poste donné est étonnamment faible (<30)
- Le symptôme le plus évident de cette situation :
  - ✓ C'est lorsqu'on se retrouve dans une situation de course à l'échalote avec les hackers
  - ✓ Car cela signifie que ce que vous ne connaissez pas PEUT endommager vos systèmes
- L'approche contraire
  - ✓ Est beaucoup plus difficile à concevoir et réaliser
  - ✓ Mais est aussi beaucoup plus sûre

Tout ce qui n'est pas explicitement autorisé est interdit !

Idée stupide n°2
Recenser les vulnérabilités

- Principe de la détection de signature (anti-virus, détection d'intrusion…)
- Là encore c'est la solution de facilité
- Cela évite d'avoir à savoir exactement comment son système fonctionne
- C'est en fait un cas particulier de l'idée n°1 mais qui rapporte beaucoup d'argent !



Recenser oui… mais quand il y a peu de vulnérabilités !

Idée stupide n°3
Pénétrer et corriger

- Tester ou faire tester les vulnérabilités d'un système et le corriger au fur et à mesure
- Le problème c'est que si un programme est mal conçu, rajouter du code n'arrangera rien !
  - ✓ Si cette idée fonctionnait alors Internet Explorer serait sûr depuis le temps !
- Le symptôme le plus évident de cette situation :
  - ✓ Si vous êtes obligés d'appliquer systématiquement les derniers patchs du mois c'est que votre système est vulnérable à tout nouveau bug

Corriger oui… mais quand cela a du sens et qu'on en a les moyens techniques !

Idée stupide n°4
Le hacking c'est super !

- C'est là un effet de mode
- Encouragés par les médias qui aiment valoriser l'intelligence et la technicité des hackers et protégés par le sentiment d'anonymat, des informaticiens timides peuvent devenir de vrais criminels
- Mais c'est aussi lié à l'enseignement de l'informatique
  - ✓ Il vaudrait mieux enseigner à concevoir des systèmes sûrs
  - ✓ Qu'enseigner à identifier les failles dans un système
- Le modèle économique actuel (cf. idée n°3) encourage malheureusement dans le mauvais sens

Cela n'empêche pas d'étudier les méthodes d'attaque !

Idée stupide n°5
Sensibiliser les utilisateurs

- Si cela avait dû marcher, cela aurait déjà marché !
  - ✓ La moitié des utilisateurs mâles cliquera sur un lien annonçant Anna Kournikova en tenue d'Eve !
- En fait, si on compte sur l'utilisateur, c'est qu'on est déjà dans une logique de « permission par défaut ».
  - ✓ L'utilisateur a-t-il vraiment besoin de pouvoir recevoir des pièces jointes ?
  - ✓ Et quand bien même, pourquoi est-ce dangereux pour votre système ?

Sensibiliser les utilisateurs non, les décideurs oui !

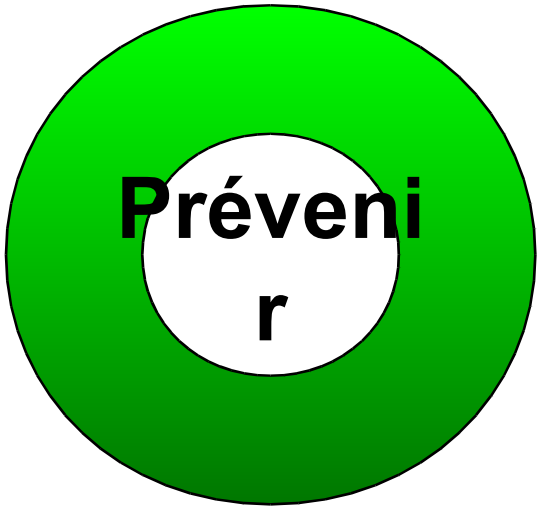
Idée stupide n°6
Il vaut mieux agir que ne rien faire

- Il y a deux races de directeurs informatiques
  - ✓ Les « tout nouveau tout beau »
    - ➢ qui vont déployer les nouvelles technologies dès leur apparition
  - ✓ Les « il est urgent d'attendre »
    - ➢ qui vont prendre le temps de la réflexion et du retour d'expérience
- Sur le plan de la sécurité, il n'y a pas photo car :
  - ✓ **Il est toujours plus facile de ne pas faire quelque chose d'idiot que de faire quelque chose d'intelligent**

Mais ne rien faire dans des pans entiers de la SSI c'est suicidaire !

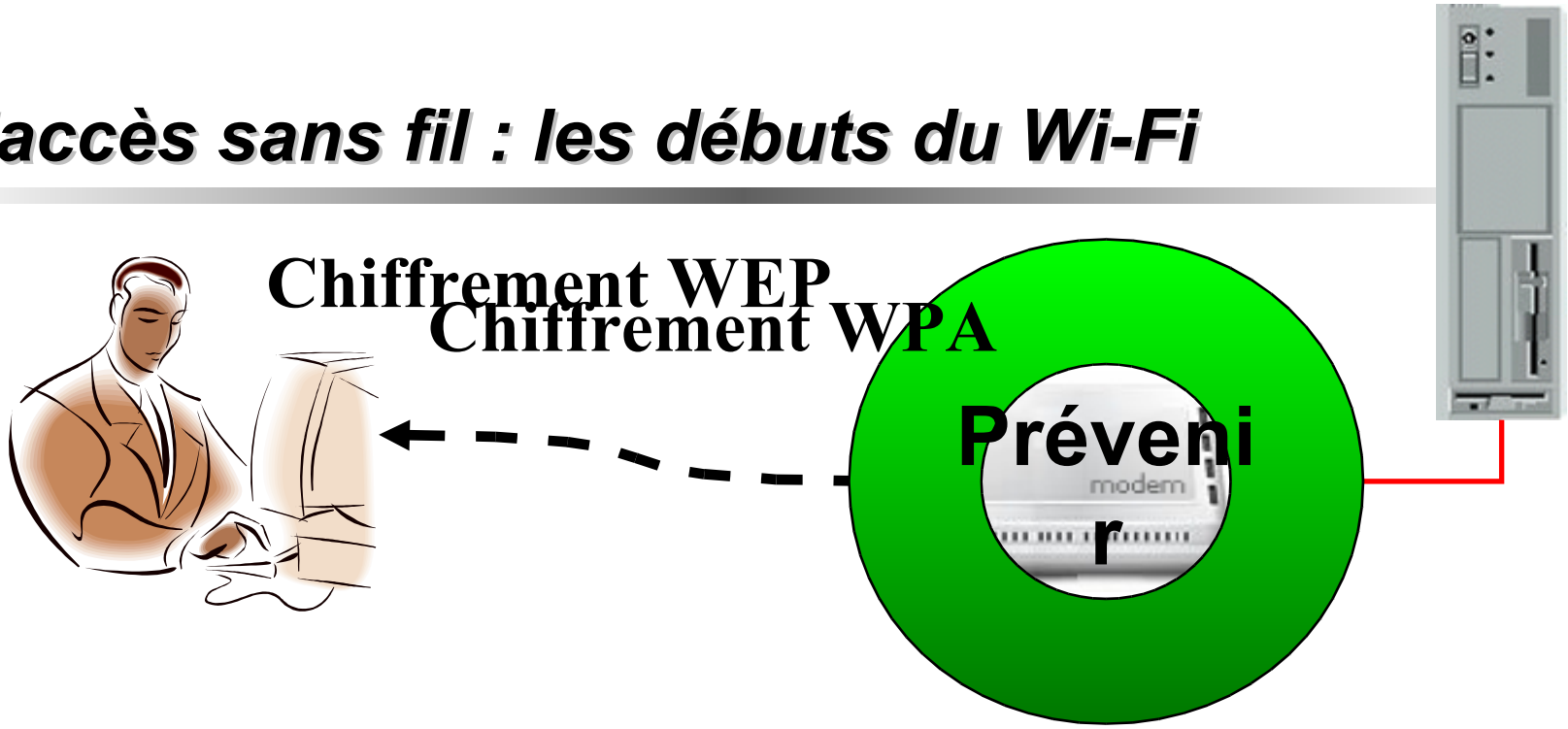
Défense en profondeur et SSI

- **La défense en profondeur dans le domaine de la SSI doit être développée**



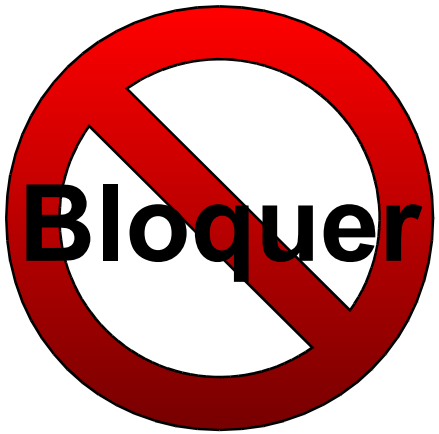
- éviter
  - ✓ la présence
  - ✓ l'apparition
- de failles dans les constituants du système d'information

L'accès sans fil : les débuts du Wi-Fi



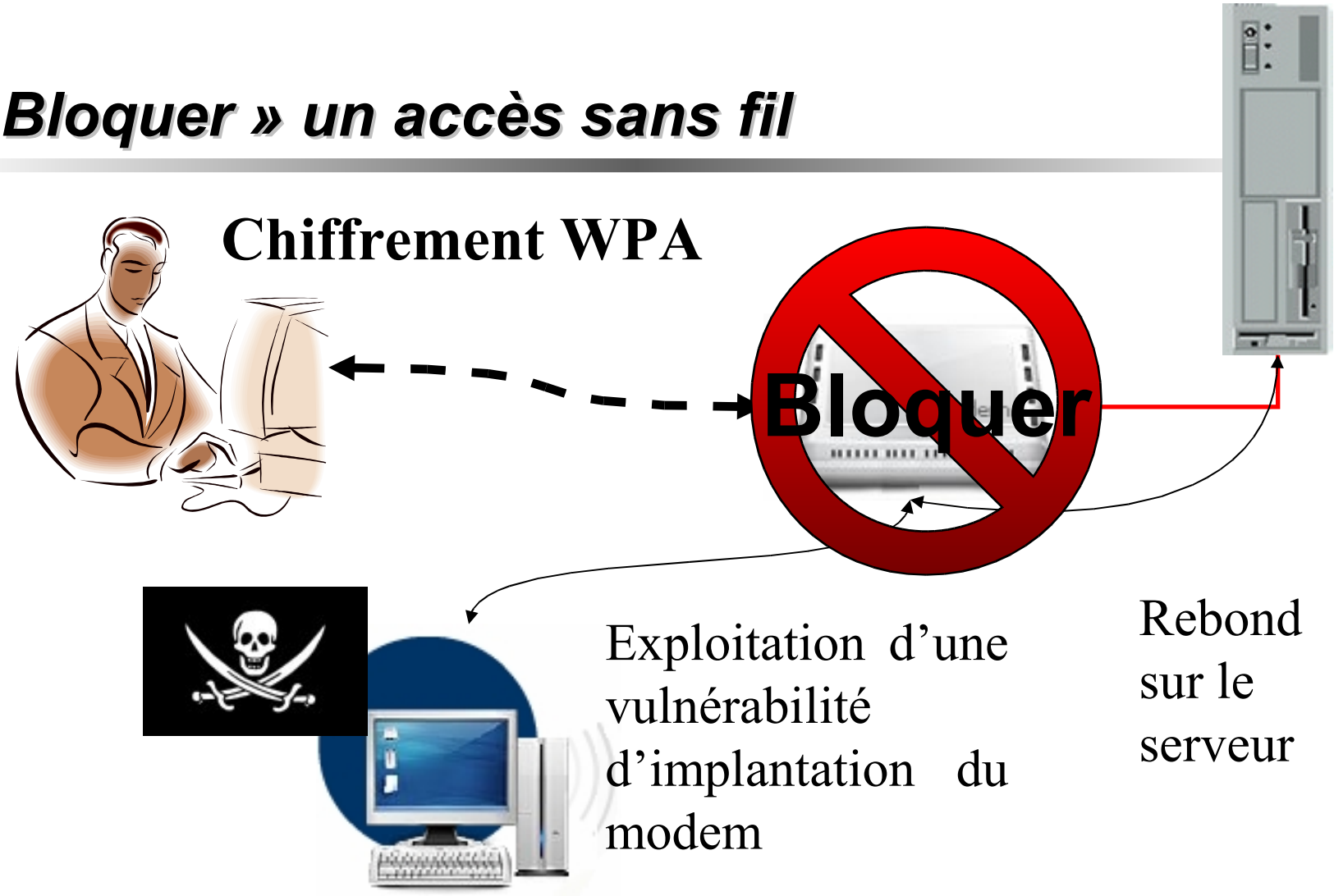
On « découvre » que le WEP est vulnérable…

Défense en profondeur et SSI

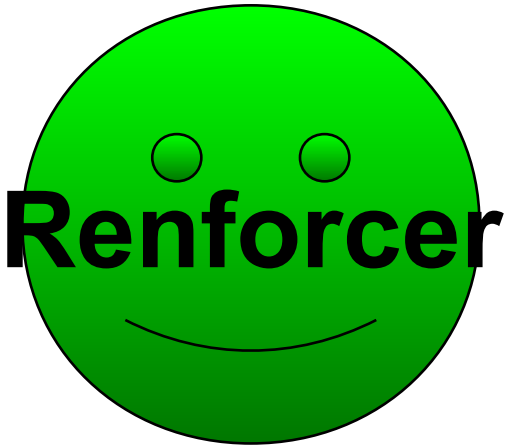


- empêcher les attaques
  - ✓ sur les composants sensibles
  - ✓ sur les composants vulnérables
- du système d'information
- réduire les chances de succès des attaques ciblées

« Bloquer » un accès sans fil

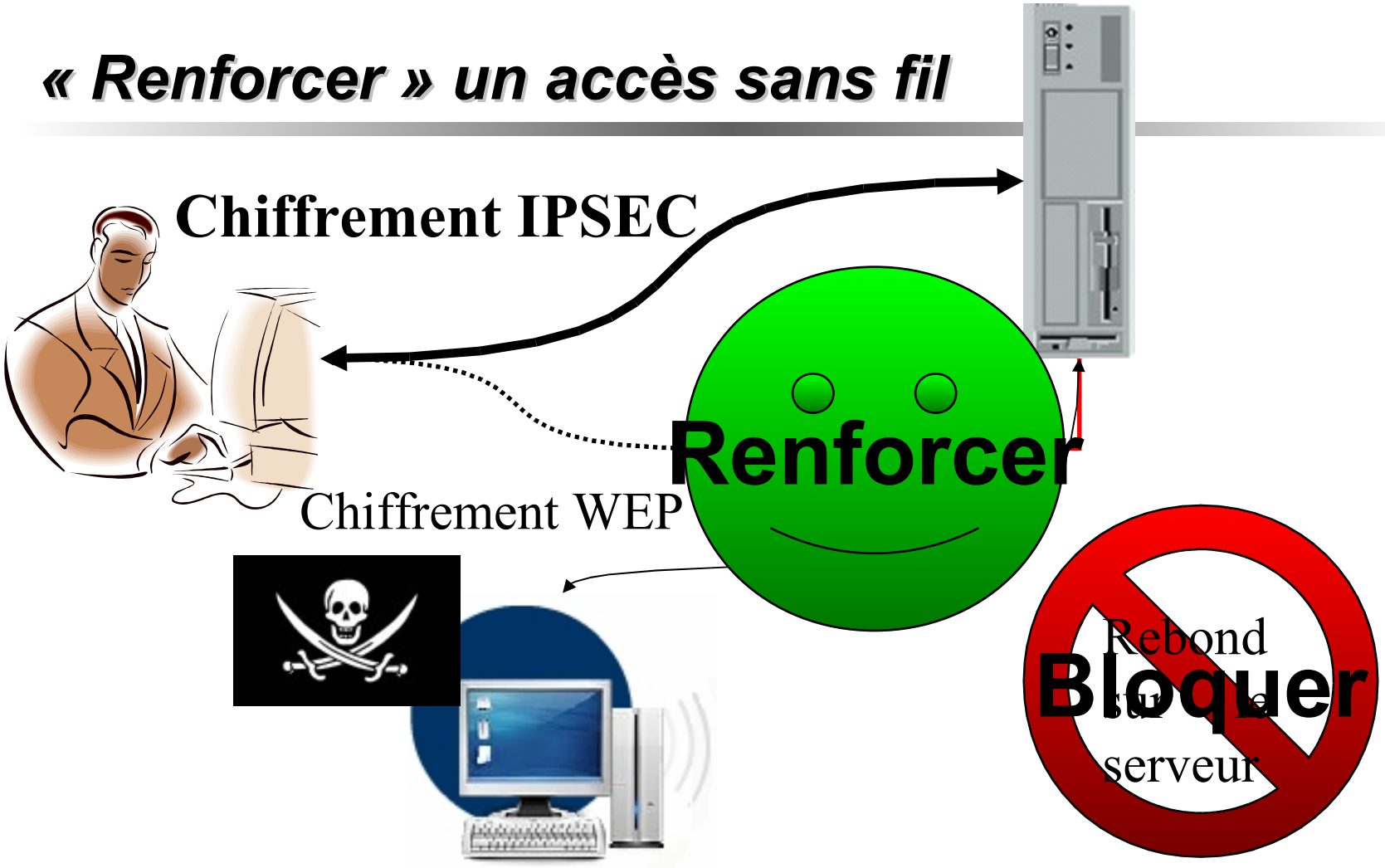


Défense en profondeur et SSI



- limiter les conséquences
  - ✓ d'une compromission
  - ✓ d'une attaque
- de l'un ou l'autre des composants du système d'information

« Renforcer » un accès sans fil

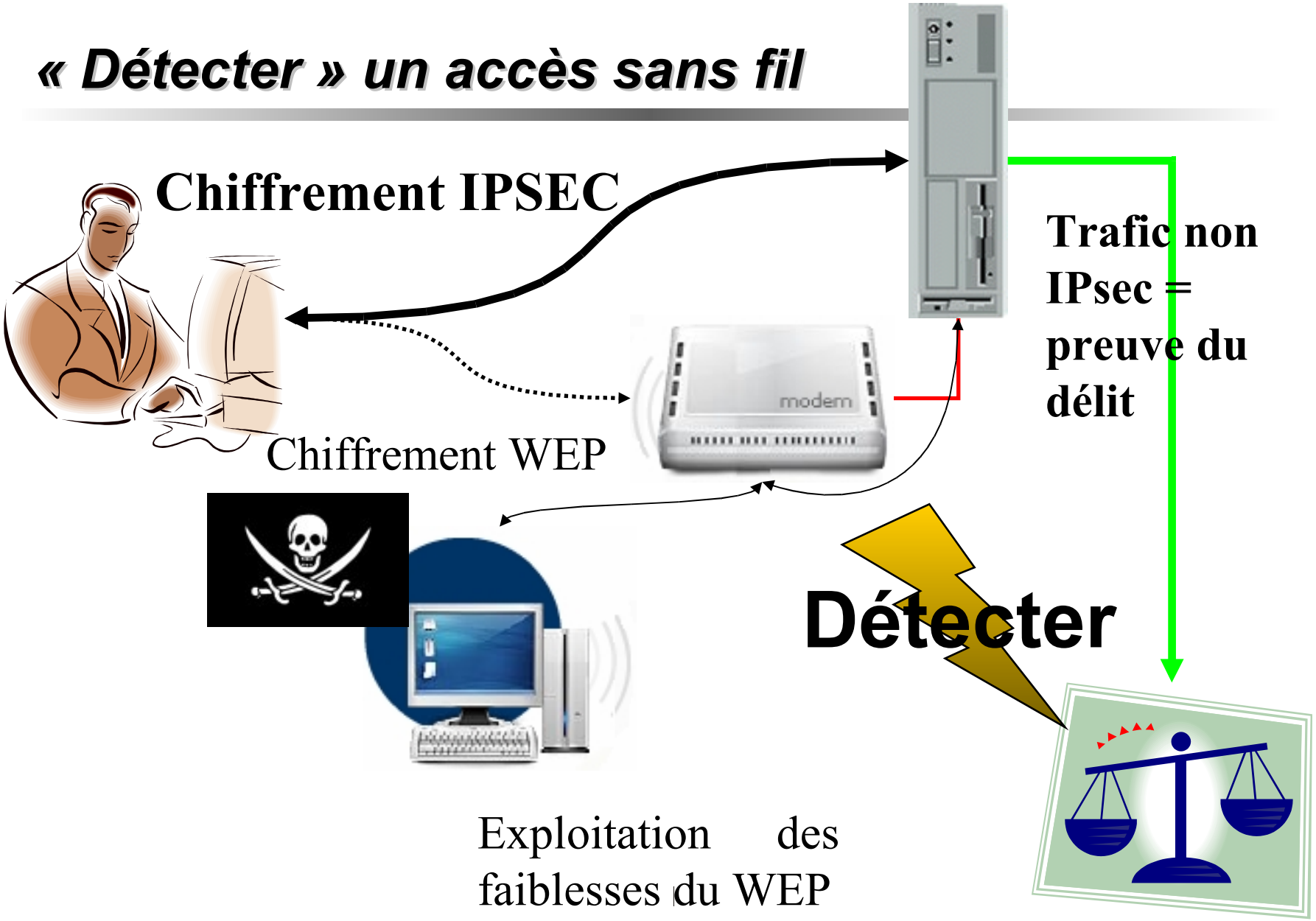


Exploitation des faiblesses du WEP

Défense en profondeur et SSI

- pouvoir
  - ✓ identifier,
  - ✓ en vue d'y réagir,
- les incidents ou compromissions survenant sur le système d'information

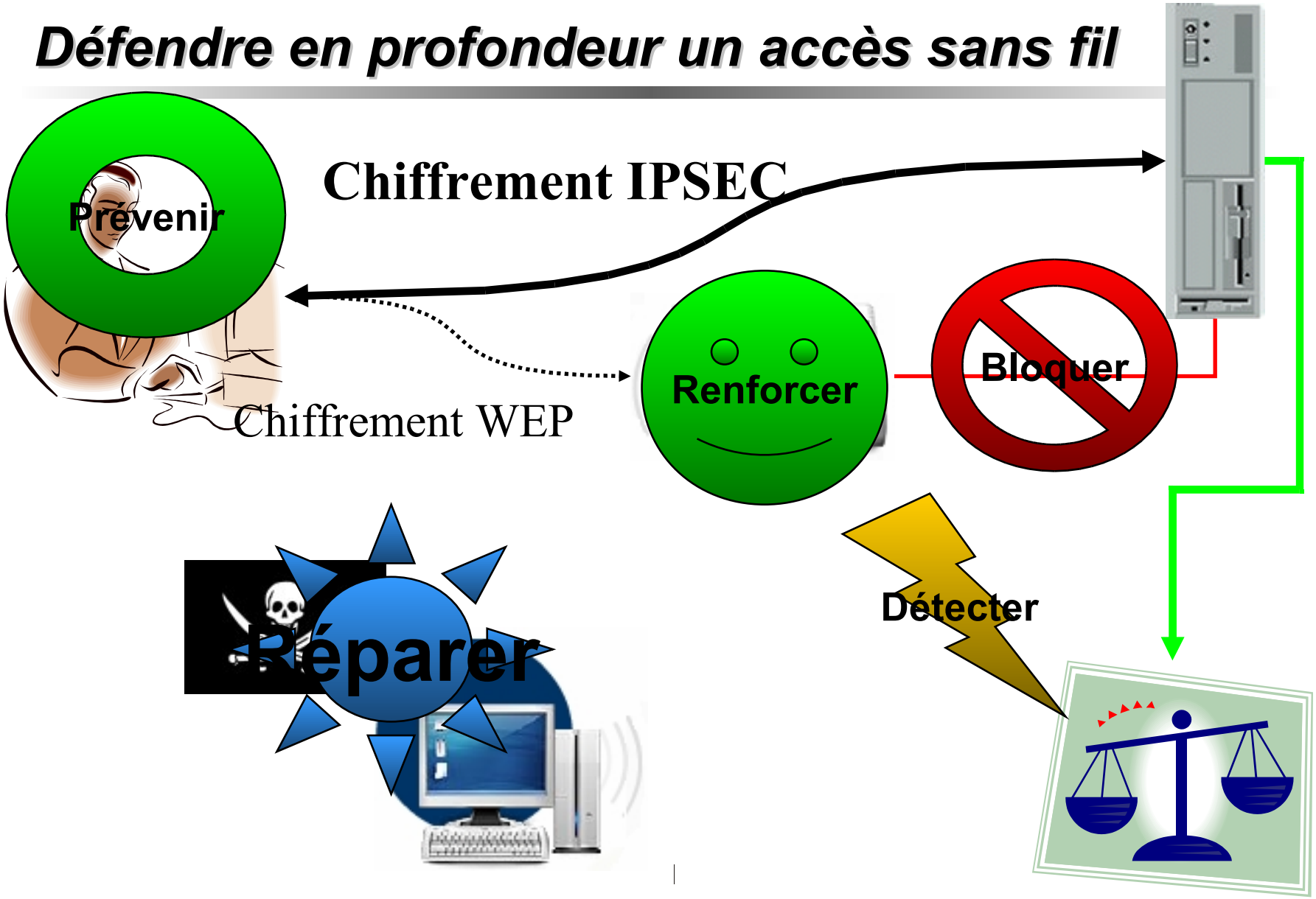
« Détecter » un accès sans fil



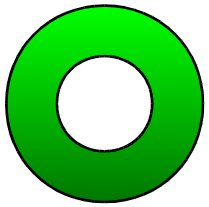
Défense en profondeur et SSI

- disposer de moyens pour remettre en fonctionnement le système d'information suite à
  - ✓ un incident
  - ✓ une compromission

Défendre en profondeur un accès sans fil



De manière générale…

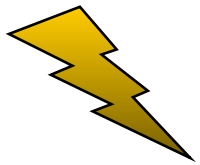


- On est mauvais en prévention
  - ✓ Mise à jour des systèmes inefficace
    - ➢ Combien de systèmes Windows 95 encore utilisés ?
    - ➢ Combien de systèmes d'exploitation sûrs ?

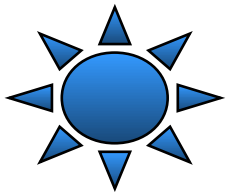
  - On mise tout sur le blocage
    - ✓ Chiffrement des réseaux
    - ✓ Firewalls
  - **Or, le blocage n'existe pratiquement plus dans les systèmes actuels massivement interconnectés**

- On est mauvais en tolérance aux agressions
  - ✓ Les systèmes applicatifs ne résistent pas à la chute de cette première barrière

De manière générale…



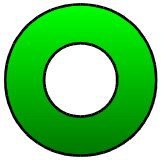
- On commence à faire de la détection
  - ✓ Mais basée sur des outils peu maîtrisés
    - ➢ Anti-virus
    - ➢ Sondes réseau
    - ➢ Détection d'intrusion

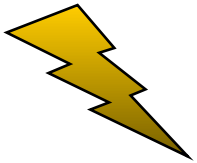
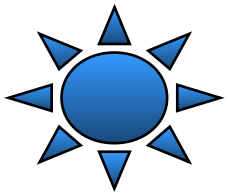


- La capacité de réparation est faible
  - ✓ Les cibles potentielles sont difficiles à modifier : systèmes d'exploitation, cartes à puce, bientôt les téléphones mobiles
  - ✓ Le cycle de réparation éventuel est long quand il existe
    - ➢ Songez qu'une carte de paiement dure deux ou trois ans
      - Mais au moins elle a été évaluée
    - ➢ Songez qu'un téléphone mobile est utilisé entre 6 mois et… 6 ans !
      - Mais au moins… euh non !

Recherche et développement en SSI

- Développer la sécurité de nos systèmes d'information sera un **effort de longue haleine nécessitant d'investir dans la durée**
- Nous avons pris du retard dans la compréhension et la maîtrise de la conception de la sécurité dans les nouvelles technologies
- Les problèmes que nous rencontrons sont liés à des erreurs dans la conception de nos systèmes
  - ✓ Les briques à développer en priorité : des systèmes d'exploitation
    - ➢ Moins vulnérables
    - ➢ Tolérants aux vulnérabilités
    - ➢ Avec une capacité de développement nationale pour que
      - la détection de tentatives d'attaque
      - et la correction de vulnérabilités
    - ➢ **ait un <u>sens</u>**



Un pot de miel pour tous !

- Les pots de miel sont utilisés dans la détection des nouvelles attaques
- Ils emploient toutes les techniques de la défense en profondeur
  - ✓ En particulier, par définition, ils doivent être « tolérants » aux attaques
  - ✓ Leur comportement « normal » est encadré pour pouvoir détecter l'anomalie
  - ✓ Ils exploitent tous les développements en cloisonnement, virtualisation, contrôle d'intégrité, etc.
- Or, paradoxalement, ces outils robustes ne sont que des simulateurs et ne protègent aucune information
- Les vraies informations restent sur des systèmes ouverts à tout vent et respectent parfaitement toutes les idées les plus stupides de la SSI selon Marcus Ranum

Forces et faiblesses de la recherche française

Les atouts de la recherche française

- Les deux mamelles de la recherche française en matière de sécurité des systèmes d'information :
  - ✓ Cryptographie
  - ✓ Méthodes formelles
- Malheureusement, les systèmes utilisés :
  - ✓ Utilisent une cryptographie standardisée RSA, AES
  - ✓ Utilisent rarement les méthodes formelles
- La qualité de la recherche française dans ces domaines… a donc trop peu d'impact sur les systèmes opérationnels
  - ✓ Une exception notable : la carte à puce
    - ➢ Par exemple une carte Gemalto a été certifiée par la DCSSI avec une machine Java en partie formellement prouvée
      - Mais est-elle utilisée ?

Les faiblesses de la recherche française

- On constate un déséquilibre grave : des compétences cruciales ne sont pas couvertes
  - ✓ Systèmes d'exploitation
  - ✓ Protocoles réseaux
  - ✓ Architectures matérielles
- Une enquête menée par le ministère de la recherche en 2007 confirme ce point
- En outre, les laboratoires académiques, *a fortiori* leurs travaux, sont peu connus du tissu industriel qui, globalement :
  - ✓ a peu d'activité de R&D
  - ✓ a un niveau faible car ne couvrant pas non plus l'éventail des compétences requises
    - ➢ On retrouve là une conséquence de l'absence de prise en compte de la sécurité dans les cursus de formation

Rééquilibrer la recherche en SSI

- Comme la cryptographie en son temps, la SSI doit être théorisée, apprise, enseignée et constituer une école de recherche vivace et reconnue au niveau international
  - ✓ Pour cela, il faut que les « bonnes » équipes s'intéressent aux problématiques SSI
- La R&D en SSI nécessite un investissement humain important du fait de la grande dispersion des domaines de compétence à couvrir
  - ✓ La sécurité d'un SI résulte de facteurs extrêmement divers touchant à des domaines très variés :
    - ➢ Cryptographie, informatique, électronique, micro-électronique, protocoles, physique, mécanique, chimie des matériaux, etc.
  - ✓ Seuls quelques grands groupes industriels pourraient espérer atteindre la capacité d'innovation requise en SSI… mais avec un retour sur investissement non évident

Besoin d'une communauté SSI

- La recherche académique doit donc garantir la capacité d'innovation de notre tissu industriel et former ses ingénieurs et ses chercheurs en SSI.
- Les industriels doivent pouvoir identifier facilement les équipes académiques susceptibles de les aider dans ce domaine
- Des structures d'échange rassemblant industriels et académiques doivent être mises en place pour que les compétences critiques puissent être partagées

Thématiques prioritaires

Les missions de la DCSSI

- Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale, en matière de sécurité des systèmes d'information
  - ✓ Assurer la fonction d'autorité nationale de régulation pour la SSI
  - ✓ Assister les services publics en matière de SSI (conseils, Inspections, CERTA…)
- Développer l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics

  http://www.ssi.gouv.fr/fr/sciences/publications.html
- Former et sensibiliser à la SSI
  - ✓ Assurer la coordination interministérielle de prévention et de protection contre les attaques en SSI

Orientation de la recherche en SSI

- Suite au travail d'un groupe piloté par la DCSSI associant des représentants des ministères, de l'INRIA, du CNRS, du CEA, de l'ANR, d'Oséo, un rapport d'orientation a été publié le 30 novembre 2006 et actualisé le 10 avril 2008.
- Décrivant les enjeux
  - ✓ Souveraineté
  - ✓ Protection de la vie privée
  - ✓ Disponibilité
  - ✓ Imputabilité des accès
- Identifiant des évolutions en cours qui impactent la SSI
- Analysant en fonction de ces évolutions les domaines techniques à maîtriser

Rapport d'orientation de la R&D en SSI

- Première édition en 2006 disponible en ligne :
  http://www.ssi.gouv.fr/fr/sciences/fichiers/rapports/rapport_orientatio

- n°2571/SGDN/DCSSI/SDS du 30/11/2006
  « Préparé par la commission interministérielle pour la sécurité des systèmes d'information (CISSI), ce rapport public constitue une référence à caractère incitatif pour orienter les choix stratégiques en matière de recherche et de développement dans le domaine de la sécurité des systèmes d'information. »
- La réactualisation du rapport est prévue annuellement

  http://www.ssi.gouv.fr/fr/sciences/fichiers/rapports/rapport_orientatio

  n°757/SGDN/DCSSI/SDS du 10/04/2008
  - ✓ Peu de changements
    - Renforcement des enjeux
    - Bilan de la recherche actuelle
    - Les thématiques scientifiques restent les mêmes

Architectures

- Architectures des produits et systèmes
  - ✓ Les architectures sont beaucoup plus pérennes que les technologies dans le domaine de l'information (cf. PC ou TCP/IP).
  - ✓ Choisir dès le début des architectures saines au plan de la sécurité est crucial.
  - ✓ Bien anticiper les évolutions des architectures largement répandues est indispensable
- Enseigner à concevoir des architectures saines
  - ➢ Cf idée n°4 de Marcus Ranum
- D'autant que nous pouvons nous appuyer sur des compétences en architectures auto-organisantes
  - ✓ Réseaux ad-hoc, grilles de calcul, pair-à-pair, autant d'architectures nouvelles où l'hypothèse classique en SSI de l'enceinte à protéger d'un extérieur hostile est battue en brèche.

L'informatique de confiance

- Trusted Computing Group
  - ✓ Le futur des architectures de PC
    - ➢ Qu'on le veuille ou non !
  - ✓ Des impacts sur toutes les technologies majeures :
    - ➢ Ordinateurs
    - ➢ Mobiles
    - ➢ Stockage
  - ✓ Un impact économique potentiellement important
    - ➢ L'industrie de la carte à puce est en première ligne
  - ✓ Une représentation française notoirement insuffisante
    - ➢ Initiative de la DCSSI en cours pour faire mieux connaître ces travaux et y participer
- Pour éviter la politique de l'autruche…

Cryptographie et gestion des clés

- Ne pas se reposer sur ses lauriers !
- La cryptographie c'est ce qui reste quand toutes les autres protections ont disparu
- C'est aussi ce qui est le plus difficile à changer dans un système opérationnel !
  - ✓ Non pas en théorie, mais en pratique
- Un exemple : IGC/A

- Vendredi 13/12/2002 : génération de deux bi-clés RSA2048 et DSA1024
  - ✓ Choix dicté par l'existant des navigateurs
- Cinq ans de travaux juridiques
  - ✓ Ordonnance n° 2005-1516 du 8/12/2005
    - ➢ RGI
    - ➢ RGS
  - ✓ Publication au Journal Officiel de la Rép. Fr. le 17/02/2007
- Incorporation dans les magasins de certificats (Mandriva, Microsoft) en 2007
- Au fait… et SHA-1 ?
  - ✓ RSA 4096 – SHA 256
  - ✓ EC-DSA
  - ✓ D'ici 2010.
- Mais la clé RSA2048 survivra vraisemblablement !

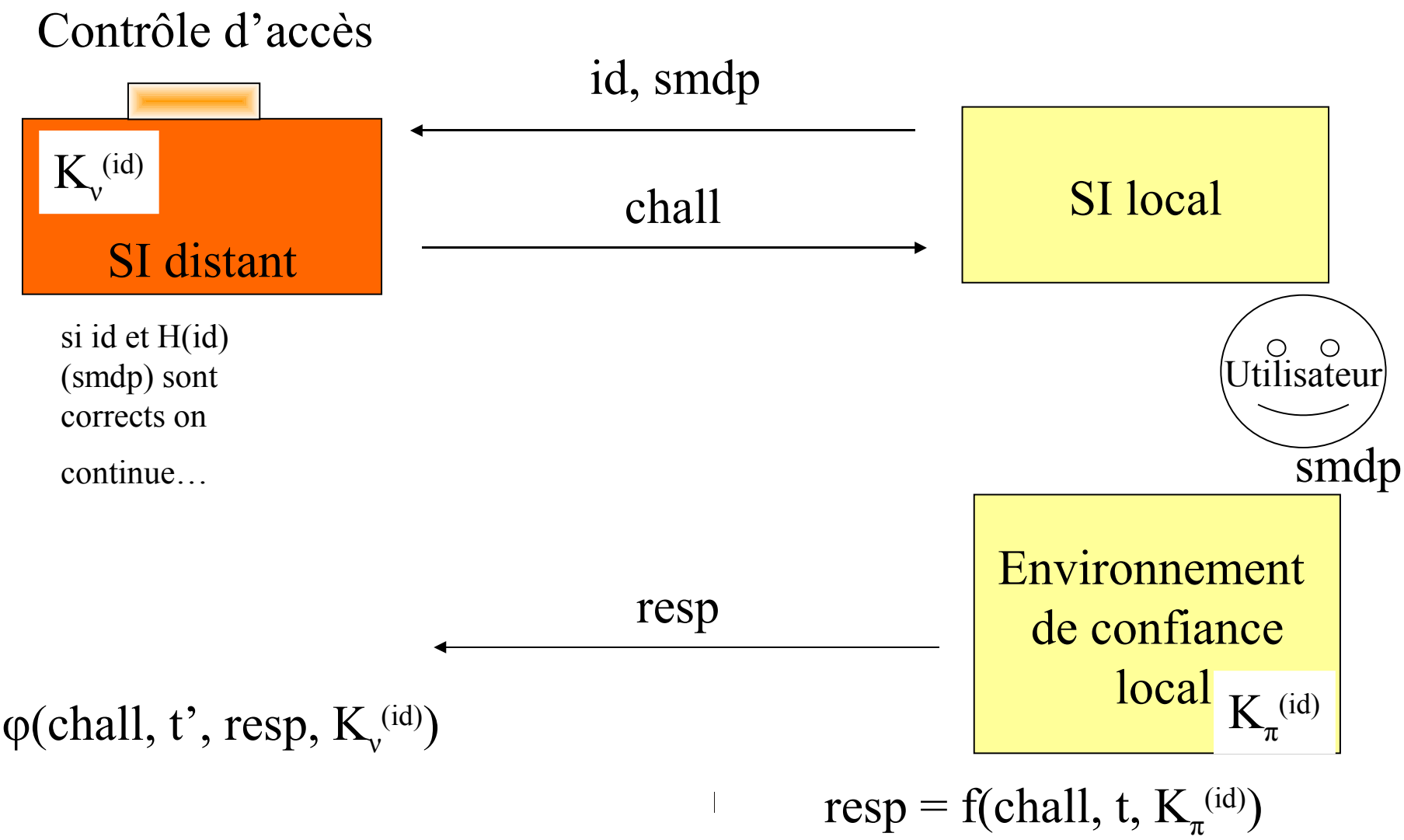
Faciliter la SSI : ergonomie et supervision

- Ergonomie
  - ✓ Faire reposer tous les systèmes sur une seule architecture est un bon moyen de préparer les catastrophes.
    - ➢ Proposer de nouvelles architectures permet de contribuer à l'info-diversité
  - ✓ L'amélioration de l'ergonomie des solutions de SSI de haut niveau de sécurité faciliterait leur généralisation.
  - ✓ La simplicité d'emploi est aujourd'hui quasiment absente
- Supervision
  - ✓ La haute technicité de la SSI fait qu'elle passera sans doute par la mise en place de services de supervision opérés par des sociétés de confiance, dont la sécurité reste à concevoir dans le respect des enjeux.

Fédération d'identités

- Typiquement une réponse à la problématique d'ergonomie et de supervision
- Problématique de l'authentification distante
  - ✓ Cruciale pour la sécurité des systèmes d'information
  - ✓ Technologies actuellement utilisées battues en brèche par le hameçonnage (« phishing »)
  - ✓ Enjeu fort de protection de la vie privée
- Là encore éviter la politique de l'autruche !
- Et en plus il y a vraiment de la recherche à faire
  - ✓ Référentiel de la DCSSI sur l'authentification distante
    - ➢ Proposition en cours pour normalisation AFNOR
  - ✓ Modélisation de l'authentification distante
    - ➢ Mécanismes cryptographiques (machines)
    - ➢ Mécanismes de déverrouillage (personne)

Modèle général du mot de passe à usage unique



Fondations de la SSI

- Formats de données – protocoles
  - ✓ La communication généralisée se fera en respectant des normes qui restent encore à établir, surtout au plan de la sécurité
- Systèmes d'exploitation
  - ✓ Le futur est fait d'objets de plus en plus intégrés dans les systèmes d'information
  - ✓ Tous ces objets embarquent des systèmes d'exploitation qui doivent être variés et dont la sécurité est une problématique complexe
    - ➢ **Les anti-virus doivent être éradiqués !!!**

Défi « SEC&SI »

- Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute
- Appel à projets de l'ANR d'un type nouveau
  - ✓ Six mois de conception pour proposer une configuration linux
    - ➢ Dédiée à l'internaute
    - ➢ Dédiée à ses opérations « sensibles »
      - Banque en ligne
      - Télé-déclaration des impôts
      - Messagerie signée
  - ✓ Six mois d'évaluation
    - ➢ Par attaque théorique ou pratique des solutions entre elles
    - ➢ Arbitrée par la DCSSI
  - ✓ Deuxième année scindée par trimestre en deux périodes successives de conception/évaluation
- Début du défi en septembre 2008
  - ✓ Trois challengers retenus
    - ➢ OSOSOSOS : OSOSOSOS is a Secure Open Source Operating System which Ought to be Simple
    - ➢ Safe OS
    - ➢ SPACLik : Security Properties for Application Control within a Linux Kernel
  - ✓ Un site de référence sera prochainement ouvert et le règlement du défi publié

Conclusion

- La structuration de la recherche en matière de sécurité des systèmes d'information doit se poursuivre
- Des thématiques dans ce domaine sont orphelines en France
  - ✓ Alors même que des compétences voisines existent
  - ✓ Des efforts d'adaptation sont donc nécessaires
  - ✓ Et en plus des sauts technologiques comme l'utilisation des méthodes formelles sont possibles
    - ➢ À condition de se donner aussi des cas concrets à étudier
- Ignorer des initiatives sous des prétextes idéologiques est stupide
  - ✓ **Toute technologie de sécurité a ses bons et ses mauvais côtés**
  - ✓ **La recherche doit dans ce domaine jouer un rôle citoyen**
    - ➢ **En alertant le niveau politique**
    - ➢ **En lui donnant des arguments objectifs**
    - ➢ **Pour qu'il puisse corriger d'éventuels travers**