Université Grenoble Alpes

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/lpro/rims_fr.html
cnms_en.html

Cours de sécurité
M33-5. Stratégies et politique de sécurité
Audit

M33-5. Stratégies et politique de sécurité, Audit

- 5.1 Politiques de sécurité, normes
- 5.2 Acteurs de la sécurité
- 5.3 Audit
- 5.4 Synthèse
- 5.5 Conclusions

One of the rules of a security manager

- In security, you should know!
- Be at the good state of the art => to implement « good practices »
- We should prove than we have done/implemented the best regarding the state of the art. => it means that it should be documented
- Everything which is needed should be explicitely authorized. Everything which is not authorized is by default forbidden

Université Grenoble Alpes

5.1 Politiques de sécurité, normes

5.1 Introduction

- Etablir une stratégie de sécurité est une étape essentielle pour protéger et sécuriser un réseau
  - Besoin de procédures
  - Précision des comportements appropriés
  - Consensus opérationnel et de gestion
  - Mesures à prendre en cas de comportement inacceptable (interne entreprise, action en justice…)
  - **Rôle et responsabilités** de chaque groupe dans la sécurisation de l'entreprise
  - Définition des outils requis – dépenses en matière de sécurité

5.1 Définition de la politique de sécurité

- Simple et compréhensible
- Adoptable par un personnel préalablement sensibilisé voire formé
- Aisément réalisable
- De maintenance facile
- Vérifiable et contrôlable (périodiquement)
- Configurable et personnalisable (selon les profils des utilisateurs, les flux, le contexte, la localisation des acteurs)
- Dimension temporelle : jours ouvrés, heures de travail
- Dimension spatiale : nomadisme de certains utilisateurs

5.1 Certification ISO et sécurité (1/4)

- ISO 17799/27001/27002/… (*Information technology - Security techniques - Code of practice for information security management*),
  - 27005: Information security risk management
    - www.iso.org

- Planification de la continuation de l'activité
  - L'entreprise doit continuer à fonctionner normalement suite à une défaillance ou un incident majeur
- Contrôle de l'accès au système
  - Définit comment contrôler les informations
  - Définit comment détecter les activités non autorisées
- Développement et maintenance des systèmes
  - Processus de sécurisation des systèmes, logiciels, données
- Sécurité physique et environnementale
  - Protéger contre tout accès non autorisé ou action nuisible

5.1 Certification ISO et sécurité (2/4)

- Conformité
  - À la loi
  - Aux règles de sécurité
- Sécurité du personnel
  - Risque d'erreurs humaines
  - Vols
  - Mauvaise utilisation
- Organisation de la sécurité
  - Décrit comment la maintenir et la gérer
- Gestion des ordinateurs et des opérations
  - Décrit comment augmenter la sécurité
- Classification et contrôle des biens
  - Appliquer et maintenir le degré de protection approprié aux données et informations de l'entreprise

5.1 Certification ISO et sécurité (3/4)

- Adoption de la norme favorisée par le fait que certaines compagnies d'assurance l'imposent
  - Basée sur la gestion des risques
- Code de pratique pour la gestion de la sécurité et identification d'exigences de sécurité
  - Mais ne précise pas les manières de les réaliser
- Cette norme aborde les aspects organisationnels, humains, juridiques et technologiques
- Etape de conception, mise en œuvre et maintien de la sécurité
- www.iso.org

5.1 Certification ISO et sécurité (4/4)

Domaines de sécurité des normes

1. Politique de sécurité
2. Organisation de la sécurité
3. Classification et contrôle des outils
4. Sécurité et gestion des ressources humaines
5. Sécurité physique et environnementale
6. Exploitation et gestion de systèmes et de réseaux
7. Contrôle d'accès
8. Développement et maintenance des systèmes
9. Continuité de service
10. Conformité

5.1 Gouvernance de la sécurité avec les norms ISO 270XX

- ESS27 : Essentiels ISO 27001 & 27002
- IO27LA: ISO 27001 Lead Auditor
- ISO27LI: ISO 27001 Lead Implementer
- ISO27RM: ISO 27005 Risk Manager
- ISO27004: Indicateurs et Tableaux de bord Cybersécurité
- ISO 27035: Gestion des incidents de sécurité

5.1 Methods (1/2)

- Méthodes préconisées par le CLUSIF (*Club de la Sécurité de l'Information Français)* :
  - Marion (*Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau /* Method for the Analysis of the Data-processing Risks and Optimization per Level)
  - Méhari (*Méthode Harmonisée d'Analyse des Risques* / Harmonized Method for Risks Analysis)
- Méthodes de la DCSSI (*Direction centrale de la sécurité des systèmes d'information)*
  - EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
  - Melisa (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information)

5.1 Méthodes (2/2)

- AFAI (Association Française de l'Audit et du Conseil Informatique), branche française de l'ISACA (Information Systems Audit and Control Association) => méthode de gouvernance et d'audit des systèmes d'information (CobiT : Control objectives for information and Technology)
- Méthode Octave (Operationally Critical Threat, Asset, and Vulmnerability Evaluation)
  - Cramm (CCTA Risk Analysis and Management Method)

5.1 D'autres guides

- CERT (Computer Emergency Readiness Team, www.cert.org) propose un « Guide to system and network practices »
- NCSA (National Center for Supercomputing Applications, www.ncsa.edu) propose un « guide to enterprise security »
- Internet Security Alliance (www.isalliance.org) propose un « Common sense guide for senior manager »
- Information Security Forum (https://www.securityforum.org/) propose « the standard of good practice for information security »
- The 60 minutes network security guide (first stage towards a secure network environment), SNAC (System and Network Attack Center, USA)

Université Grenoble Alpes

5.2 Acteurs de la sécurité

5.2 Acteurs de la sécurité (1/4)

- Responsable sécurité
  - (directeur ou responsable de la mission sécurité, administrateur …)
  - Fonction plus organisationnelle que technique
    - Contrôle de la gestion et l'administration des moyens et des mesures de sécurité mises en œuvre sur les différentes cibles de la sécurité
    - Définition des privilèges d'accès aux ressources pour chaque catégorie d'utilisateurs
    - Réévaluation régulière des privilèges d'accès
    - Élaboration et maintien des documents administrateur et utilisateur
    - S'assurer que les cibles de sécurité sont sous surveillance, participer à l'analyse d'incidents éventuels et décider, avec les acteurs concernés, des actions nécessaires pour remédier aux défaillances constatées

5.2 Acteurs de la sécurité (2/4)

- Responsable des ressources humaines (RRH)
  - Effectuer les contrôles nécessaires avant l'engagement de nouveaux collaborateurs
  - Sensibiliser les nouveaux collaborateurs face à leur responsabilité en matière de sécurité (directives de sécurité, comportement éthique, charte d'utilisation des ressources, clauses de non divulgation et confidentialité)
  - Faire signer la déclaration de secret professionnel, de non reproduction des informations et leur approbation de la politique de sécurité
  - Coordonner les activités avec le responsable de sécurité lors d'une rupture de contrat d'un collaborateur

5.2 Acteurs de la sécurité (3/4)

- Chefs de service
  - Veiller à ce que leurs collaborateurs ou consultants soient informés de la politique de sécurité afin qu'ils en respectent les directives
  - Informer les administrateurs de la sécurité concernés de toutes les modifications ayant un impact potentiel sur le niveau de sécurité et sa gestion
  - Analyser, valider et prendre position par rapport aux demandes d'accès aux ressources émanant de leurs collaborateurs
  - Recenser et récupérer les informations sensibles détenues par un collaborateur qui quitte sa position dans l'organisation

5.2 Acteurs de la sécurité (4/4)

- Utilisateurs (maillon faible)
  - Respecter les règles pratiques définies par la politique de sécurité
  - Ne divulguer aucune information confidentielle
  - Utilisation des ressources informatiques de l'entreprise uniquement à des fins professionnelles
  - Obligation d'informer le responsable sécurité de tout élément ayant un impact potentiel sur la sécurité
    - ! Certains risques se concrétisent de manière progressive !

5.2 Mesure du niveau de conscience des utilisateurs vis-à-vis de la politique de sécurité

- Est-ce que votre entreprise vous a informé de sa politique de sécurité ?
- Avez-vous une copie de cette politique ?
- Consultez-vous cette politique fréquemment ?
- Savez-vous ce que signifie « être conscient de la sécurité » ?
- Avec quelle fréquence votre entreprise conduit des sessions de formation ou de rafraîchissement de la sécurité ?
- Considérez-vous que votre formation à la sécurité vous a apporté les connaissances suffisantes pour prendre en compte (détecter, réagir…) les incidents de sécurité ?
- Etes-vous conscient de ce qui peut être considéré comme un incident de sécurité ?
- Quelles actions entreprendriez-vous si vous savez qu'un incident a eu lieu ?
- A qui déclareriez-vous cet incident ?
- Vous sentez-vous à l'aise pour prendre en compte les incidents de sécurité ?

Université Grenoble Alpes

5.3 Audit/certification de la sécurité

Principes de base des audits

- Ce n'est pas :
  - arrivée inopinée de contrôleurs qui viennent à l'improviste faire tout et n'importe quoi
- C'est :
  - Ecrire noir sur blanc les opérations à réaliser
  - Prévenir les personnes concernées et régler en amont toute difficulté avant qu'elles ne deviennent ingérables
  - Démarche ISO 19011 :
    - décrit toutes les étapes de l'audit
      - Depuis la planification
      - Jusqu'à l'approbation du rapport final
    - Principes fondamentaux que doit respecter l'auditeur

Principes de l'audit

- Déontologie (respect de la confidentialité des informations reçues)
- Impartialité : factuel
- Conscience professionnelle : mission très précise à accomplir en un délai fini
- Indépendance : ne pas être juge et partie
- Approche fondée sur la preuve : chercher les preuves avérant les faits

Pourquoi un audit ?

- Inventorier
- Achat d'une filiale
- Nouvelle application métier
- Certification
- Relation client-fournisseur (contractuel)
- Forensic (aspect légaux)
- Polices d'assurance...

Déroulement d'un audit (1/3)

- 1. Premier contact, analyse des enjeux
- 2. Revue de documentation (audit conceptuel)
- 3. Plan d'audit
- 4. Réunion d'ouverture : expliquer aux acteurs ce qui va se passer

Déroulement d'un audit (2/3)

5. Activités d'audit
   - Analyses:
   - Architecture
   - Vulnérabilité
   - Application
   - Composant
   - Configuration
   - Tests de Pénétration,
   - Analyses des risques / Plan Action

Déroulement d'un audit (3/3)

- 6. Réunion de clôture
- 7. Après l'audit
  - Rapport d'audit
  - Validation
  - Procédures de contestations

Travail de groupe

- MEHARI : Manuel de référence des services de sécurité
- Par groupes de 3, chaque groupe en responsabilité d'un domaine
- Préparer un compte-rendu/Planches de 5 minutes du « Domaine » qui vous est attribué
- Organisation groupe : leader, rapporteur

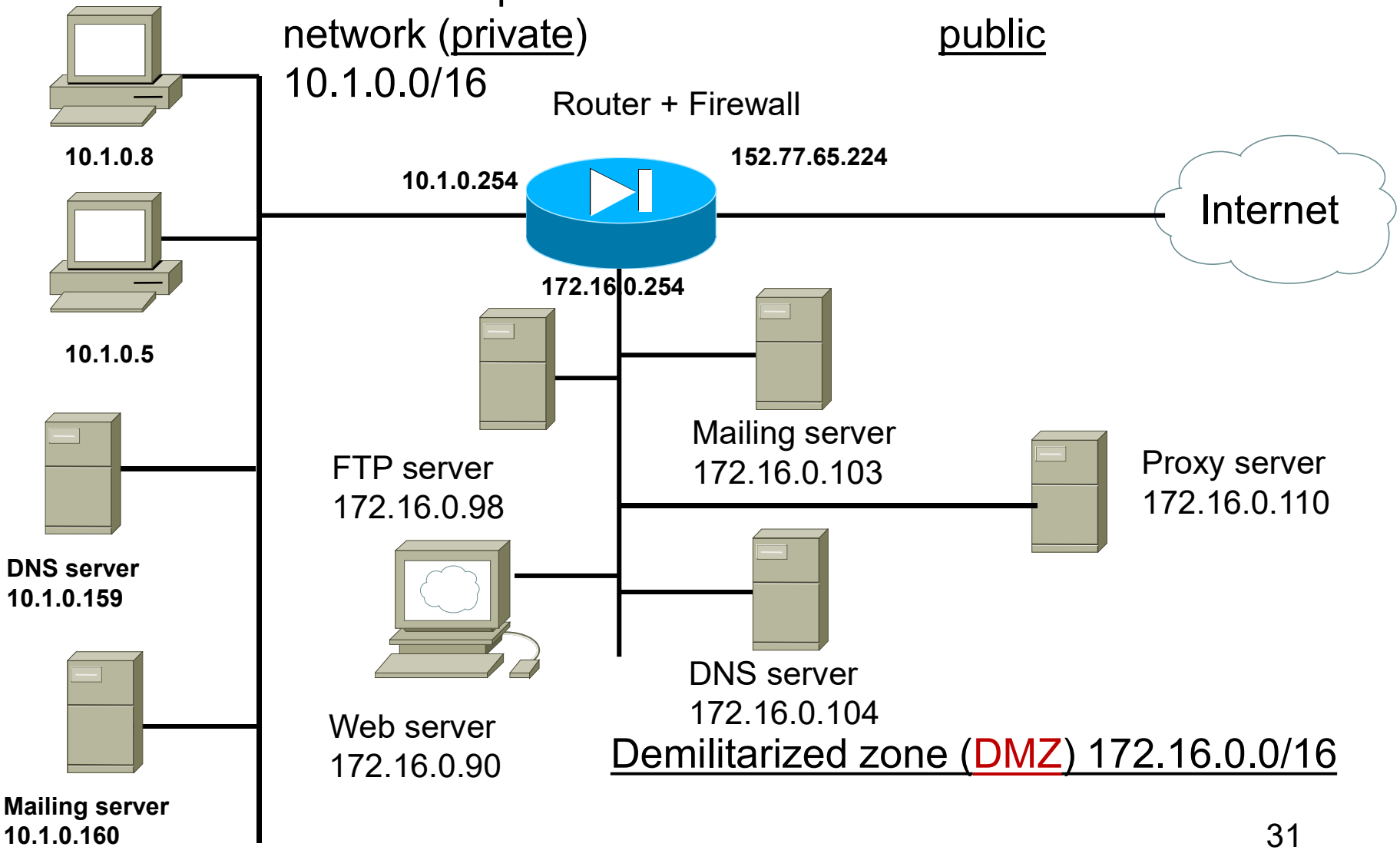
Université Grenoble Alpes

5.4. Synthèse – Politique de sécurité

Principe de base pour la configuration d'un pare-feu => applicable à la sécurité de manière générale

- Moindre privilège : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le peer-to-peer dans le cadre d'une entreprise
- Interdiction par défaut : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement intercepté
- Défense en profondeur : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau
- Goulet d'étranglement : toutes les communications entrant et sortant du réseau doivent transiter par le pare-feu. Il ne faut pas de points d'entrée ou de sortie du réseau non contrôlés, comme par exemple des modems sauvages
- Simplicité : les règles de filtrage du pare-feu doivent être les plus simples et les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- Participation des utilisateurs : les utilisateurs doivent être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu seront ainsi mieux acceptées.

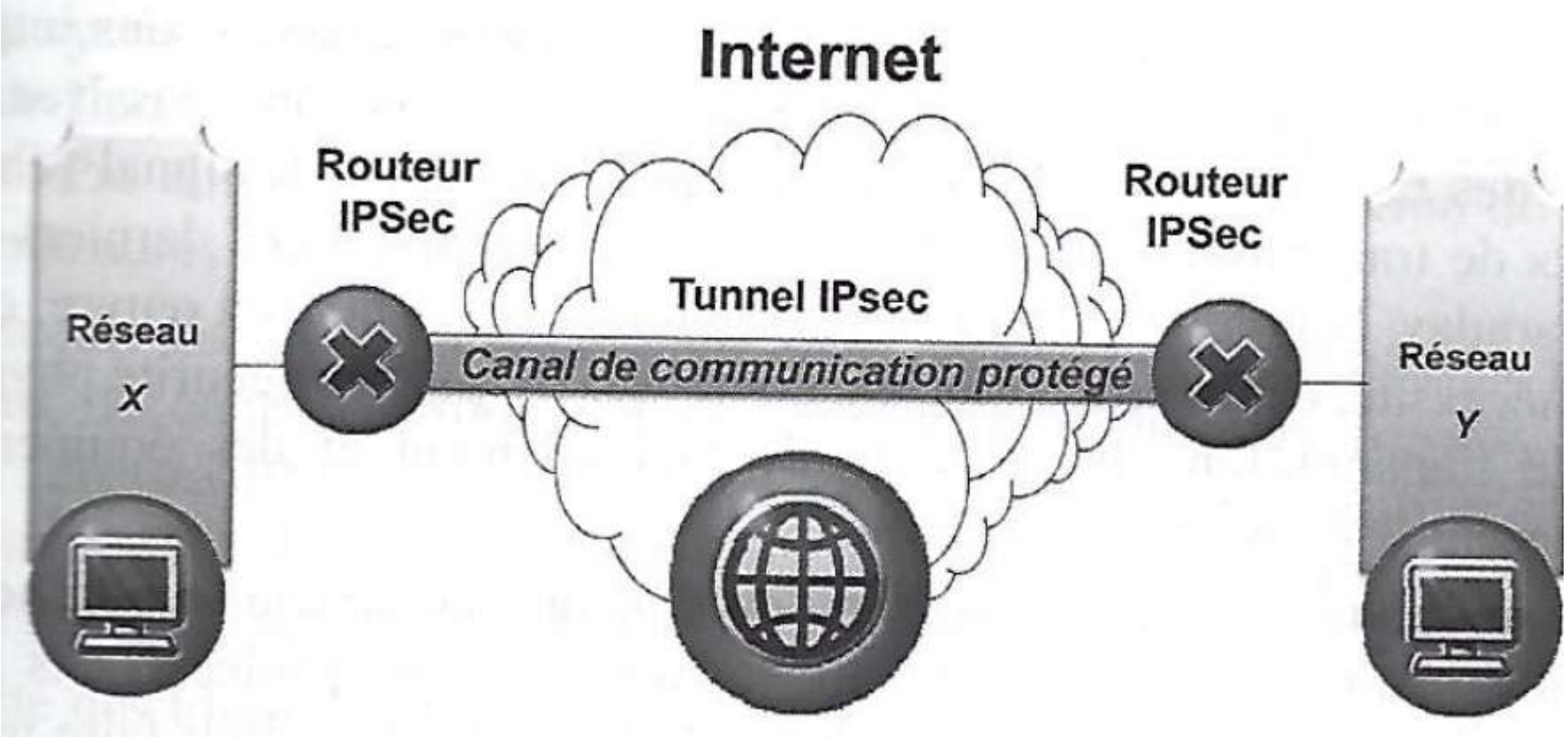
Une architecture sécurisée…



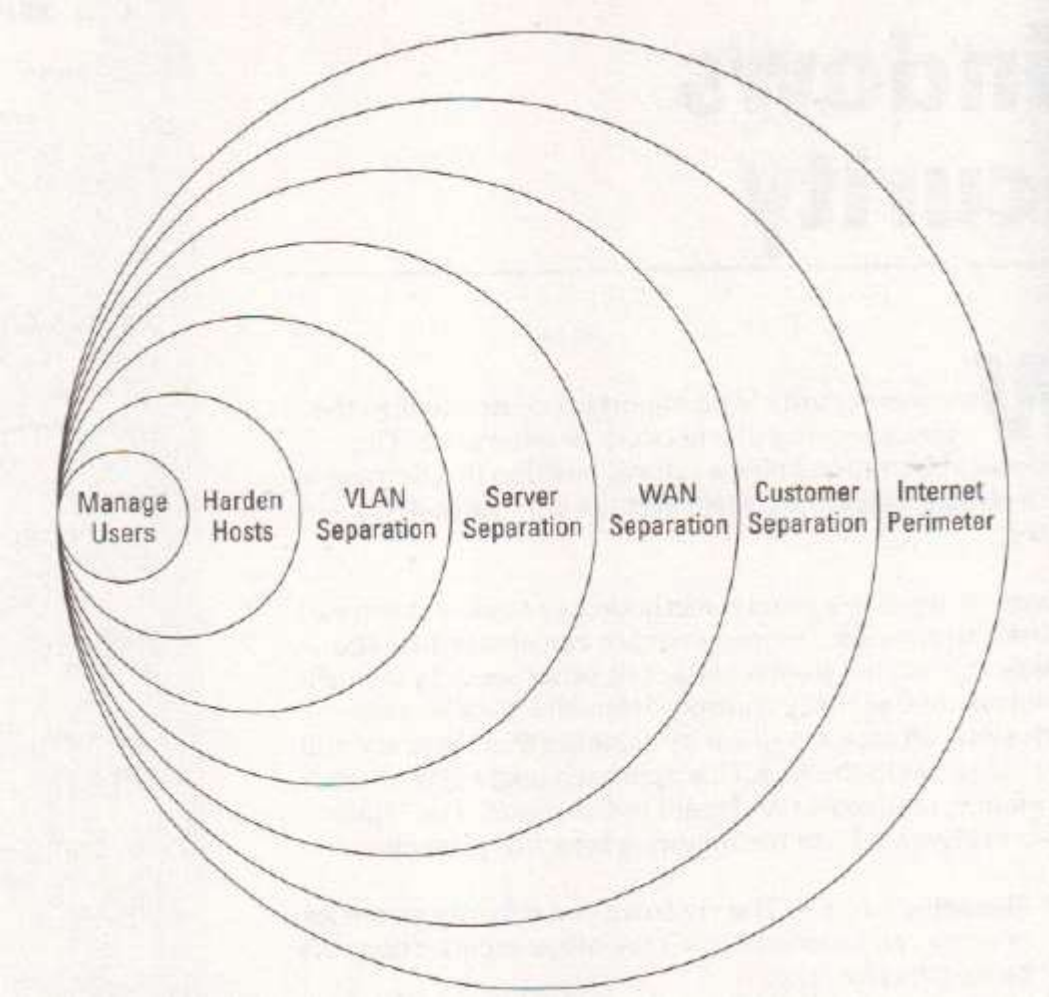
Applications de la cryptographie

- Protéger des données ou connexions sensibles (fonction de l'analyse de risques)
  - Cryptage (Confidentialité)
  - Signature numérique (intégrité, authenticité)
  - Qualité de service, temps réel
  - Confiance (Trustability)

Protocoles de sécurité : Ex de Mode tunnel de IPSec

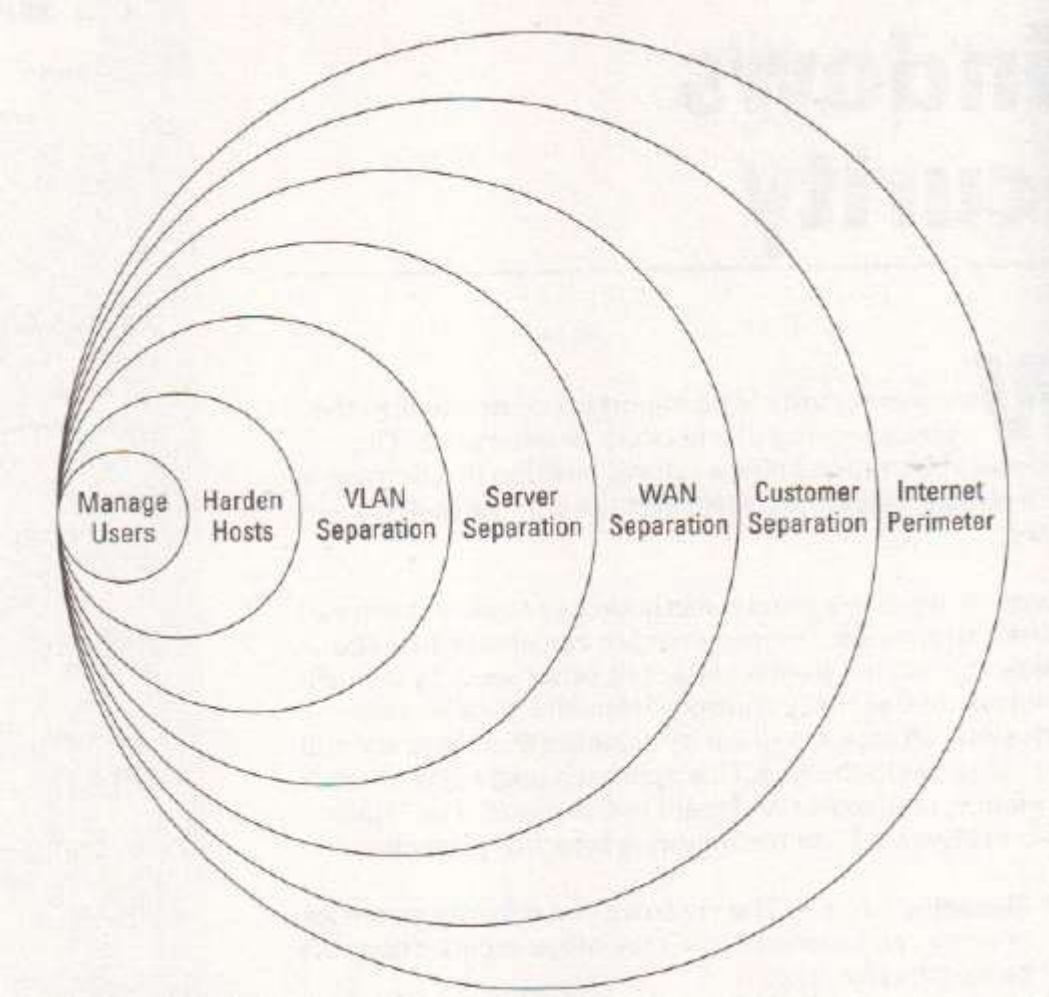


Méthodologie de défense en profondeur



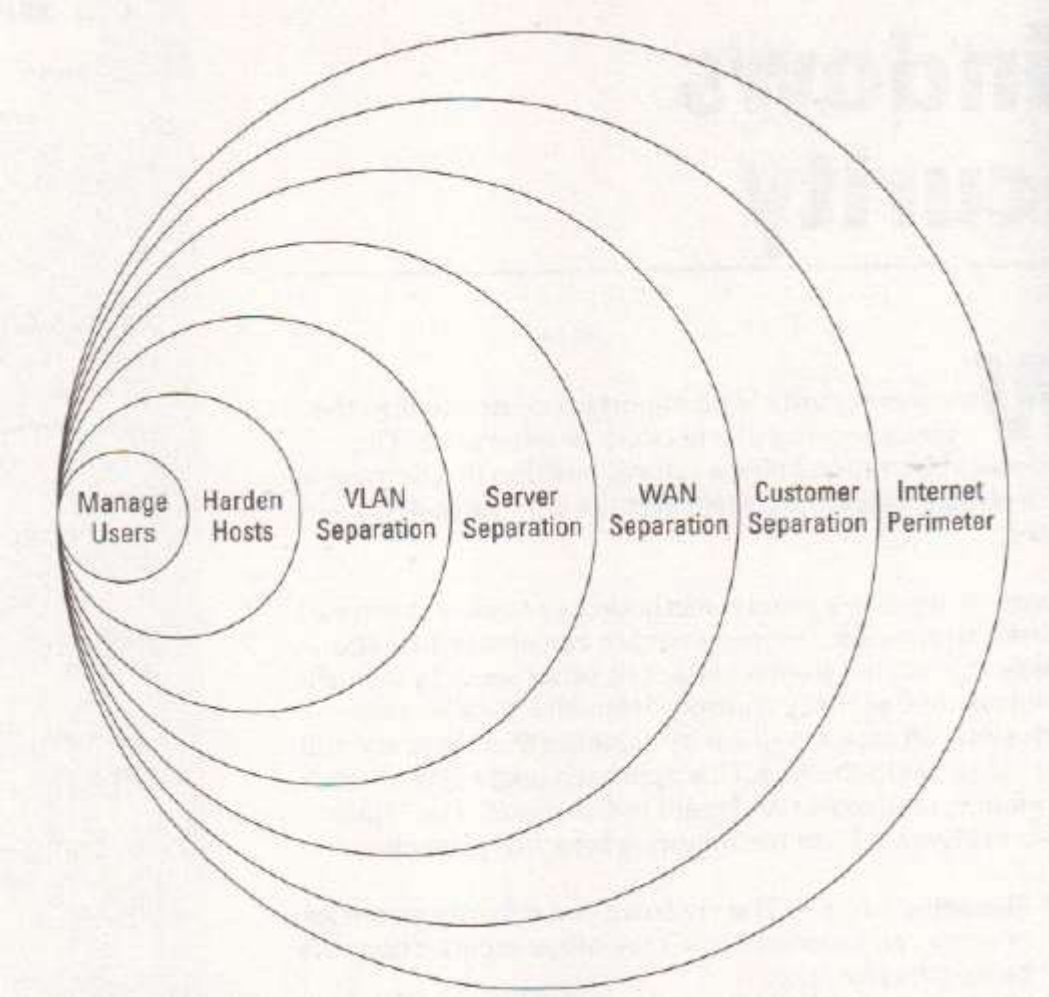
- Managing users
  - La vigilance et la formation des utilisateurs peuvent être cruciales pour une bonne efficience des autres contrôles de sécurité
- Harden hosts (renforcer les machines)
  - Les configurations par défaut sont les premières cibles des attaquants et sont toujours dans le Top 10 des listes de vulnérabilités
- VLAN separation
  - Confiance mais séparation – personne à l'exception des administrateurs ne doit être en mesure de joindre des serveurs stratégiques

Méthodologie de défense en profondeur



- Server separation
  - Prévoir un endroit avec de la sécurité avancée pour les cibles à forte valeur
- WAN separation
  - Etablir des critères d'accès (authentification) entre les hôtes et les serveurs
- Customer separation
  - Considérer que n'importe quel utilisateur ou machine hors du périmètre sécurisé est non sécurisé
- Internet perimeter
  - L'internet contient de nombreuses menaces mais de nombreuses attaques viennent de l'intérieur

Méthodologie de défense en profondeur



Cible opportune

Attaquant Découragé, prix à « payer » pour l'attaque…

Cible de choix

Mettre en œuvre plusieurs couches pour réussir à détecter l'attaque avancée…

Université Grenoble Alpes

5.5 Conclusion

5.5 Se protéger c'est possible

- Techniques de protections multiples
  - Mais toutes possèdent des failles
  - La plupart viennent des configurations
  - Les autres viennent des failles des logiciels
- Le piratage est de plus en plus facile
  - Exemple :
    - Pirater un réseau WIFI avec un PDA
      - Avec google : sniffer Windows CE → Retina
- Les risques sont de plus en plus grands
  - Travail distant, Travail mobile
  - Outils communicants
- Données vitales pour les entreprises

5.5 Une "bonne" sécurité

- Une « bonne sécurité »
  - Maîtriser toutes les configurations
    - Serveurs
    - Equipement réseau
    - Clients
  - Maîtriser les « gadgets »
    - Téléphone, PDA avec bluetooth, WIFI
  - Utiliser les sondes
  - Utiliser les logs
    - Avec un serveur de LOG

5.5 Des certitudes ?

- On n'évitera pas le piratage
  - Mais on protégera les données
    - Sauvegarde
    - Plan de reprise après incident
  - On le saura à temps pour intervenir
    - Nécessite une astreinte (automatisée ?)
- Sensibiliser les utilisateurs
  - Aux risques
  - Aux conséquences
  - Exemple :
    - Skype interdit dans l'éducation nationale
- Rappel
  - Gérer la sécurité c'est rester curieux attentif et ouvert
  - Ne pas céder à la paranoïa

Devoirs surveillés M25 et M33

- Aucuns documents autorisés
- Questions de cours ou d'applications du cours
- M33 : Questions d'ordre général sur une politique de sécurité

- Bonne chance !

Références (1/2)

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- A. Fernandez-Toro, management de la sécurité de l'information, implémentation ISO 27001 et 27002
- C. Davis, M. Schiller, K. Wheeler – IT auditing : using controls to protect information assets
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013.
- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Course of Jean-Luc Noizette, ESSTIN, Nancy.
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006
- Presentation of Eric WIESS
- VPN, mise en œuvre sous Windows Server 2003, P. Mathon, 2004

Références (2/2)

- Compression et cryptage des données multimedia, X. Marsault, Hermès, 1995
- SSL VPN, Understanding, evaluating and planning secure, web-based remote access – J. Steinberg & T. Speed, 2005.
- P. H. Oechlin, LASEC/EPFL
- http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- SSH, le shell sécurisé, D. J. Barrett et R.E. Silverman, O'Reilly, 2001
- Hacking interdit, IIème édition, Micro Applications, 2007
- D. Vergnaud – Exercices et problèmes de cryptographie, Dunod, 2015
- CEH, Certified Ethical Hacker, Matt Walker, McGrawHill, 2017
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.
- Collectif sous la Direction de Y. Fouratier & L. Petre-Cambacedes – Cybersécurité des installations industrielles – Cepadues, 2015.

- L’utilisation des méthodes décrites dans ce cours engage la responsabilité des utilisateurs !