Sécurité des systèmes d'exploitation

Éléments pratiques

Plan

- *Active Directory*
  - Présentation (simplifiée)
  - Impact sur la sécurité d'un système Windows
- Protocoles d'administration distante
- Lutte contre les vulnérabilités
- Guides de sécurisation

Active Directory

- Introduit dans Windows 2000 Server en remplacement des domaines NT4 (type Samba <=3)
  - Déploiement *On Premise* ou *cloud* (Azure AD)
  - Renommé en *Active Directory Directory Services* (AD DS) depuis Windows Server 2008
- Regroupement administratif de ressources
  - Machines, utilisateurs, groupes, imprimantes, …
  - Ressources organisées dans un annuaire

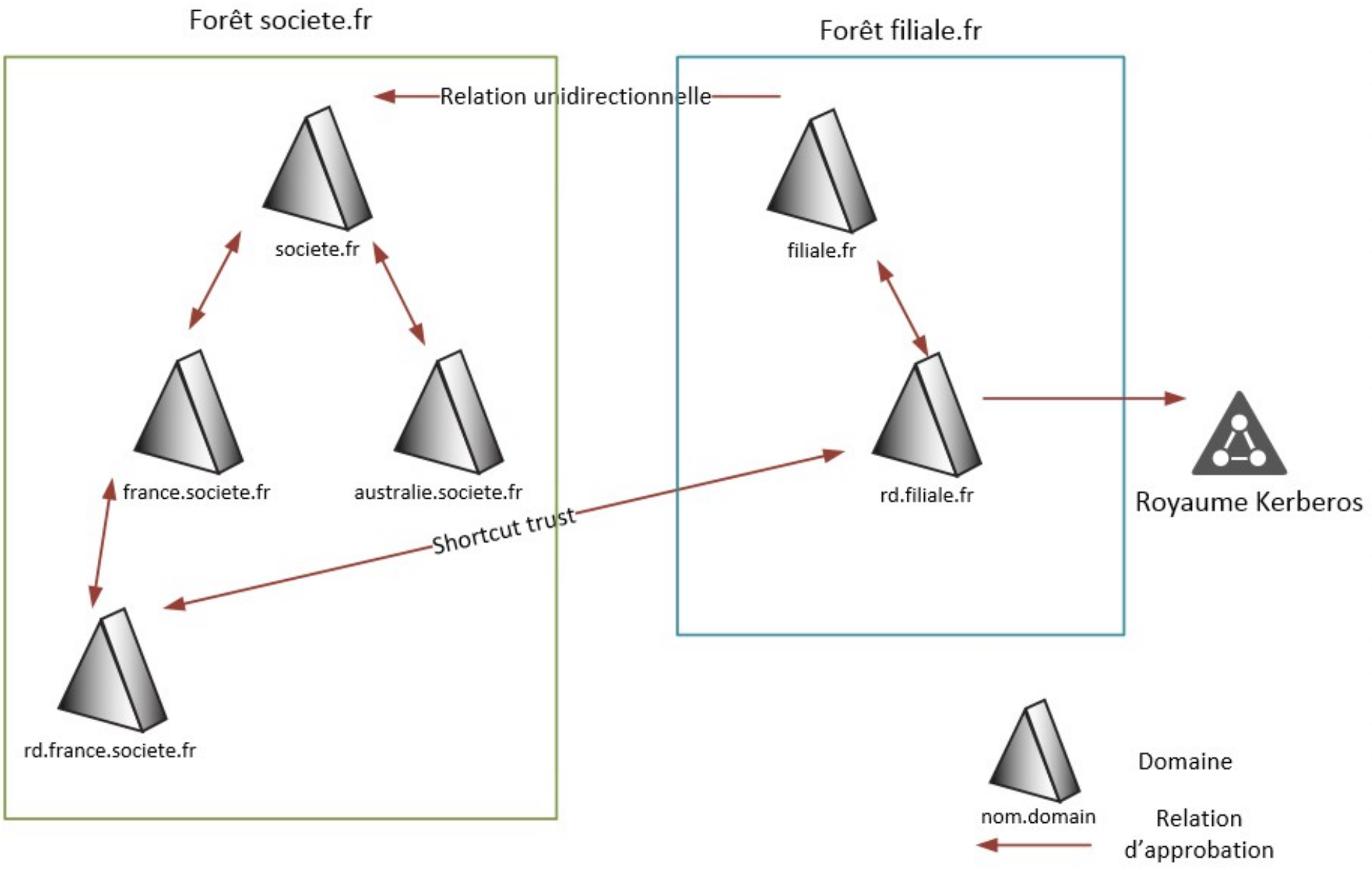
Active Directory

- Repose sur un ensemble de services qui utilisent a minima (liste étendue selon version)
  - des protocoles standards sur Internet
    - DNS : 53/TCP/UDP
    - SNTP : 123/UDP
    - LDAP (ou LDAPS): 389/TCP/UDP, 636/TCP, 3268/TCP, 3269/TCP
    - Kerberos v5 (avec des extensions) : 88/TCP/UDP et 464/TCP/UDP
  - mais pas uniquement
    - SMB/CIFS : 445/TCP
    - RPC Windows : 135/TCP, 49152-65535/TCP
    - NTLM (peut se désactiver sous certaines conditions)

Active Directory

- Un contrôleur de domaine (rôle « AD DS » depuis Windows Server 2008) héberge
  - l'annuaire Active Directory
    - Annuaire type LDAP
  - un serveur Kerberos (AS et KDC)
    - Authentification centralisée
    - Domaine AD <=> Royaume Kerberos
  - des fichiers (scripts et *Group Policy Objects*) partagés avec les membres du domaine
    - Utilisés pour l'administration et la configuration (y compris politique de sécurité) des machines membres
- Les contrôleurs de domaine se répliquent entre eux (réplication multi-maître)

Active Directory



Active Directory

- Un domaine fait toujours partie d'une forêt
  - La forêt porte le nom du domaine racine (le premier domaine créé)
- Une forêt contient un arbre de domaines
  - Cet arbre peut être constitué d'un seul domaine
- La forêt constitue une frontière de sécurité
  - Les domaines d'une même forêt sont liés automatiquement par des relations d'approbations bidirectionnelle
    - Racine/arbre
    - parent/enfant

Active Directory

- Les relations d'approbations sont des liens de confiance
  - elles permettent à un sujet d'un domaine A d'accéder à une ressource d'un domaine B
- Les relations d'approbation peuvent être constituées manuellement
  - Unidirectionnelle ou bidirectionnelle
  - Entre 2 domaines de forêts différentes
    - Entre 2 domaines racines de forêts différentes : relation de forêt
  - Entre 2 domaines issus de branches différentes au sein d'une même forêt ou issus de 2 forêts liées par une relation de forêt : *shortcut trust*

Active Directory

- Les objets contenus dans l'annuaire ont des attributs de sécurité :
  - ACL (contrôle d'accès et audit) et un propriétaire
    - les opérations possibles varient en fonction des objets, par ex. :
      - Mettre à jour le mot de passe d'un utilisateur
      - Lier une GPO à une unité d'organisation
  - Les principaux ont un identifiant de sécurité (SID)
- Modèle de contrôle d'accès par défaut : DAC
  - Complété par un modèle ABAC (*Attribute Based Access Control*) à partir de Windows Server 2012
- Délégation de droits via les ACL

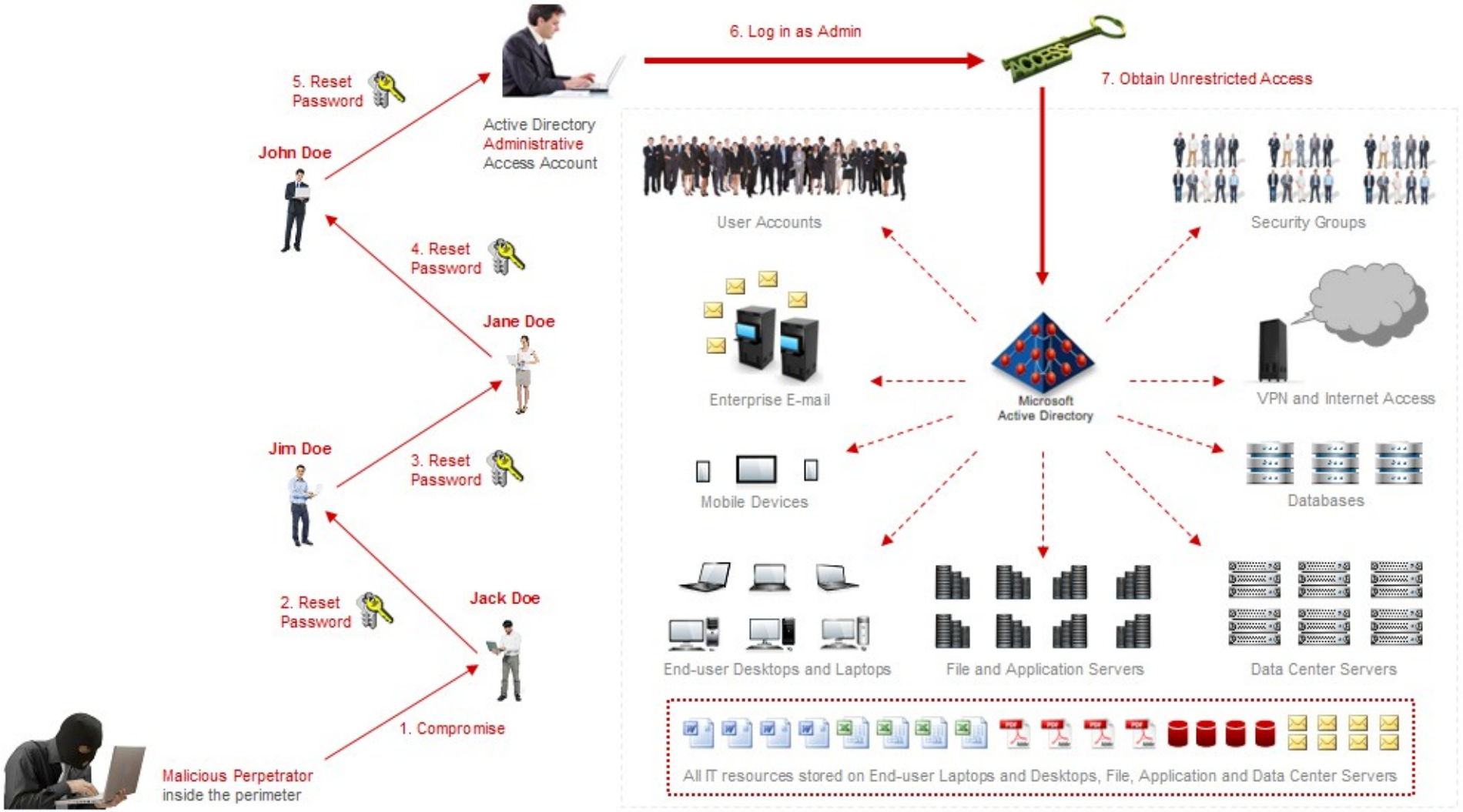
Impact sur la sécurité d'un système Windows

- Relation de confiance d'un membre du domaine envers le domaine
  - Utilisateurs et groupes
    - Y compris les comptes à privilèges
  - Configuration diffusée via les GPO
    - Politique de sécurité
      - Authentification, sécurisation de protocoles réseau, attribution des droits Windows, journalisation, filtrage réseau, configuration IPsec, contrôle applicatif,
    - Configuration de logiciels
    - Scripts (démarrage/extinction du poste, ouverture/fermeture de session)
    - Tâches planifiées

Impact sur la sécurité d'un système Windows

- Risque majeur : compromission d'un AD
  - Vol d'éléments d'authentification (*credentials*) jusqu'à obtenir un accès privilégié
    - Par ex., en cherchant dans la mémoire du processus LSASS d'une machine compromise
    - Un compte privilégié n'est pas nécessairement administrateur du domaine (furtivité)

Impact sur la sécurité d'un système Windows



Source : Paramount Defenses

Impact sur la sécurité d'un système Windows

- Quelques points d'attention sur la sécurité
  - Les contrôleurs de domaine
    - Y compris les services privilégiés présents sur ces machines : client AV, client de gestion (par ex., solution de télédéploiement), agent de sauvegarde
    - Compte krbtgt
  - Comptes et groupes privilégiés
  - Relations d'approbation
  - Stratégies de sécurité au sein des GPO
  - Canaux de communications entre les machines et les contrôleurs de domaine

Protocoles d'administration distante

- En environnement Linux
  - SSH
    - Couche de transport chiffrée
      - Utilisée pour véhiculer différents canaux
      - Authentification du serveur
    - Authentification utilisateur
      - Mot de passe, GSS-API (prise en charge de Kerberos), paire de clés, basée sur l'hôte
        - Formats pour les clés publiques : SSH, OpenPGP, X509v3
      - Module PAM
    - Fonctionnalités
      - Session interactive de type CLI
      - Relais X11
      - Relais de trafic réseau
      - Transfert de fichiers (2 protocoles possibles, SCP ou SFTP)

Protocoles d'administration distante

- Points d'attention
  - Protection des éléments secrets
    - Contrôle d'accès sur les clés
    - Protection de la mémoire du processus (ptrace() !)
  - Vérification de l'empreinte du serveur
  - Contrôle des machines et des utilisateurs autorisés
    - Root ?
      - Préférer des comptes nominatifs avec une délégation sudo
  - Protection contre les attaques sur l'authentification
    - pam_tally2 ou fail2ban ?
  - Cryptographie
  - Fonctionnalités de relais autorisées : réseau, X11 ?

Protocoles d'administration distante

- En environnement Windows
  - RPC
    - Plusieurs couches de « transport »
      - SMB, TCP, UDP, HTTP, NetBIOS *over* {IPX, TCP, NetBEUI}, AppleTalk
        - SMBv2 prend en compte l'authentification des utilisateurs et la signature des messages, SMBv3 (Windows 8 & +) apporte le chiffrement (AES128-GCM ou AES128-CCM)
    - Très utilisé : consoles de gestion graphiques, outils en ligne de commande, WMI (*Windows Management Infrastructure*)
    - Utilisation de ports réseaux dynamiques
    - Sous certaines conditions (par ex. objets DCOM), il possible de positionner des ACL pour filtrer l'accès

Protocoles d'administration distante

- WinRM (*Windows Remote Management*)
  - Repose sur la spécification *WS-Management Protocol* qui repose sur des messages SOAP
  - Couche de transport HTTP
    - Chiffrement en activant HTTPS
  - Authentification utilisateur
    - Authentification sur base HTTP (Basic, Digest) y compris NTLM et Kerberos
  - Fonctionnalités
    - Session interactive de type CLI
    - Transfert de données (encapsulées dans des messages SOAP...)
- SSH ?
  - Pas en natif, travaux en cours
- Powershell utilise aussi bien RPC que WMI ou WinRM

Protocoles d'administration distante

- RDP (Remote Desktop Protocol)
  - Couche de transport chiffrée
    - Chiffrement propriétaire ou TLS
      - TLS repose sur l'implémentation SChannel (commune à divers composants Windows : serveur web, navigateur, ...)
    - Authentification du serveur par certificat X509 en mode TLS
  - Authentification utilisateur
    - Utilisation des mécanismes natifs de Windows
      - Peut prendre en compte une carte à puce
      - Présence d'éléments d'authentification en mémoire !
        - Sauf en cas d'utilisation du mode *RetrictedAdmin*
    - Peut être précédée d'une authentification réseau (*Network Level Authentication*) entre le client et le serveur avant d'autoriser une ouverture de session
  - Fonctionnalités
    - Session interactive graphique (inclut transfert de fichiers)
    - Montage de périphériques distant

Protocoles d'administration distante

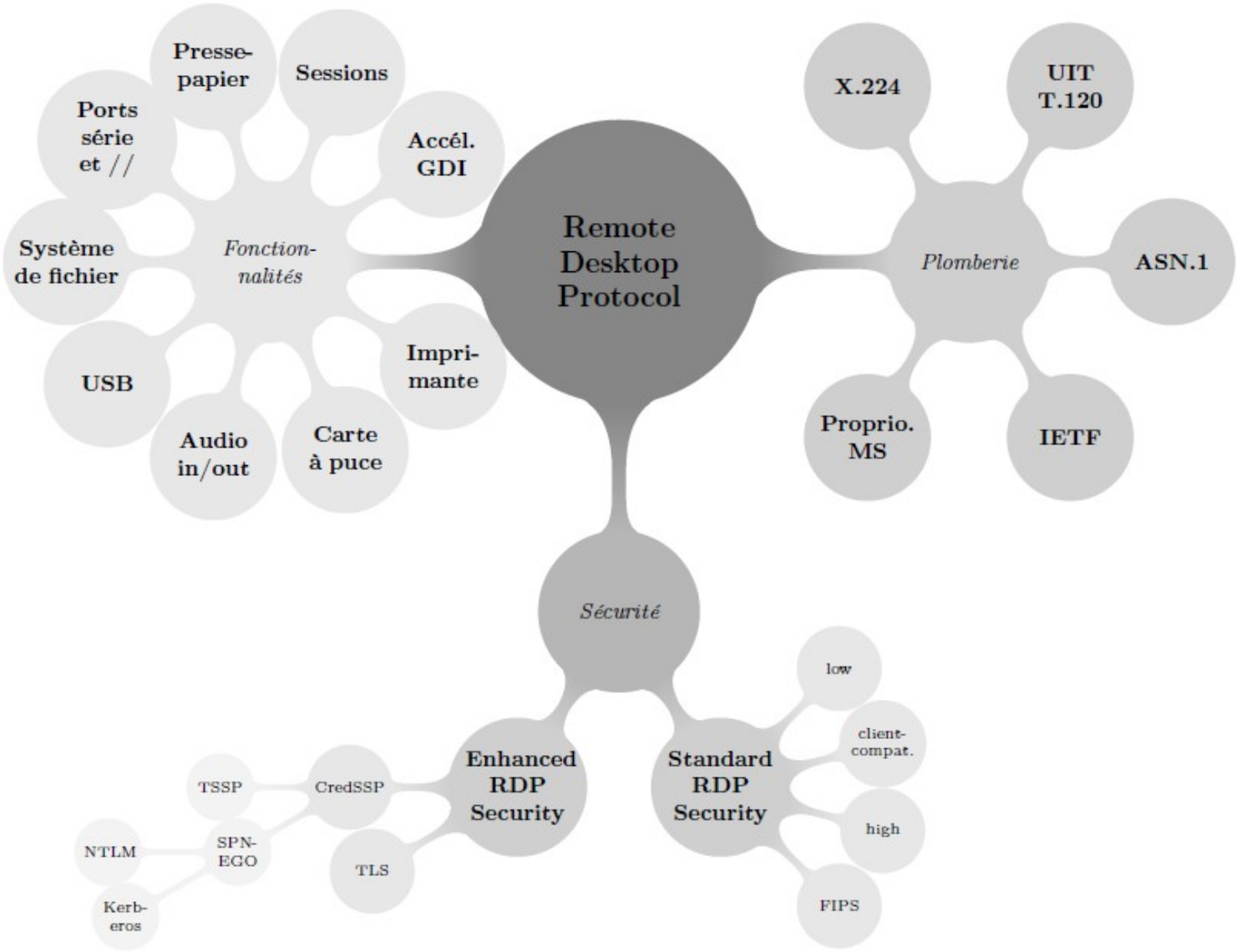


FIGURE 1. Vue d'ensemble du protocole

Source : Bordes et al.

Lutte contre les vulnérabilités

- Actions préventives
  - Réduire la surface d'attaque
    - Appliquer le principe du moindre privilège
    - Désactivation de services inutiles
    - Désactiver les protocoles non-sécurisés ou obsolètes
    - Plus complexe, limiter le code privilégié
      - Restreindre les modules chargés (liste noire) au strict besoin
      - Modification des options de construction du noyau Linux
        - Y compris pour supprimer les modules noyau inutiles
        - Travail de suivi du noyau à quantifier
  - Limiter l'impact
    - Activer les mécanismes de protection du système d'exploitation (noyau et applications)
    - Renforcer le contrôle d'accès, par exemple avec des mécanismes MAC

Lutte contre les vulnérabilités

- Mettre à jour le système
  - Y compris les éléments tiers
    - BIOS (UEFI ou non), micrologiciel de périphériques
    - Pilotes de périphériques (code noyau)
  - Paquetages des distributions Linux
    - Suivi des vulnérabilités par les mainteneurs ?
    - Origine et intégrité du paquetage ?
    - Logiciels hors paquetages (compilés depuis les sources ou fournis en version binaire) ?
  - Systèmes Windows
    - Windows Update ou ses relais pour entreprise (WSUS, SCCM, ...)
      - Sécurité de ces relais ?

Lutte contre les vulnérabilités

- Exemples de vulnérabilités Windows
  - Vulnérabilités, publiées par ShadowBrokers, ciblant le protocole SMBv1 (comme Eternal Blue),
    - Eternal Champion
      - Exploite une *race condition* dans la manière dont le protocole SMBv1 gère les transactions
      - Permet une fuite d'information de structures de données du noyau et une exécution de code à distance dans le noyau
      - Cible Windows XP à Windows 7 toute version et Windows 8 32 bits
    - Eternal Synergy
      - Exploite une mauvaise gestion des informations présente dans en-têtes SMB des messages d'une transaction
      - Permet une exécution de code à distance dans le noyau
      - Cible Windows XP à Windows 8
    - SMBv1 est désactivable depuis 10 ans !

Lutte contre les vulnérabilités

- Exemple de vulnérabilité du noyau Linux
  - CVE-2017-6074
    - Exploite une vulnérabilité de type *use-after-free* dans l'implémentation du protocole DCCP (Datagram Congestion Control Protocol) présente dans le noyau Linux
    - Permet une élévation de privilège locale
    - Présente depuis, au moins, le noyau 2.6.18
    - Protocole présent sous forme de module noyau dans les distributions courantes (Debian, Red Hat, Ubuntu)
      - La désactivation du module noyau DCCP supprime la vulnérabilité
        - Par défaut, le noyau Linux d'Android n'intègre pas DCCP
      - Une politique SELinux adaptée peut bloquer l'exploitation de la vulnérabilité

Lutte contre les vulnérabilités

- Attention, le traitement préventif ne marche pas pour tous les cas
  - Points non-spécifiques aux systèmes d'exploitation
    - Mettre en place un processus de gestion des vulnérabilités
    - Préparer la réaction
      - Journalisation
      - Détection d'intrusion
      - Analyse forensique

Guides de sécurisation

- La sécurisation d'un système d'exploitation nécessite une très bonne connaissance :
  - De son fonctionnement ;
  - De son modèle de sécurité ;
  - Des services applicatifs déployés.
- Ces connaissances sont indispensables pour
  - Déploiement initial et gestion/défense dans le temps
  - Audit
- Elle nécessite aussi une politique de sécurité
  - Dérivée d'une réglementation ou du résultat d'une analyse de risque

Guides de sécurisation

- Il existe des référentiels de configuration sécurisée issus de différentes sources, notamment
  - « Éditeur » du système d'exploitation : Debian, Microsoft, Red Hat, etc.
  - Agences gouvernementales : ANSSI, NSA, etc.
  - Groupements industriels : NERC, PCI-DSS, etc.
  - Communautés d'experts techniques : CIS, SANS, etc.
- Mise en œuvre parfois fastidieuse (i.e. plusieurs centaines de recommandations à appliquer)
  - Facilitée par l'existence d'outils de contrôle utilisant des scripts, des référentiels SCAP, etc.

Pour aller plus loin

- Active Directory Security, Sean Metcalf
- Bonnes Pratiques, ANSSI
- Sécurité de RDP, Aurélien Bordes et al., SSTIC 2012

Questions ?