ATGBM 2018

Les réseaux et les protocoles de communication

Denis Lebeuf
Responsable de la sécurité de l'information
CISSS de Laval

28 avril 2018

En guise d’introduction

- On a mis dans le texte de présentation de cet atelier :

  "Venez apprendre les bases du réseau axé sur les équipements biomédicaux et non les ordinateurs."

- Je rectifie :

  Les équipements biomédicaux SONT des ordinateurs!

  De les traiter autrement mène à de sérieux problèmes.

Des protocoles? Et alors?

- Définition :
  Ensemble de règles définissant le mode de communication entre deux ordinateurs
- Approche pragmatique :
  Nous mettrons l'emphase sur l'impact de ces protocoles sur votre travail quotidien

Adressage

- Sur un réseau, permet de livrer l'information au bon équipement
- Adresse physique (MAC)
  - spécifique à un appareil
  - exemple : 6c:f0:49:00:b2:24
- Adresse réseau (IP)
  - particulière à un réseau
  - exemple : 10.44.8.122

→ Enregistrer l'adresse MAC dans l'inventaire des équipements

DHCP

Dynamic Host Configuration Protocol

- Définit les paramètres de communication avec les autres équipements du réseau
- Adresses :
  - fixe
  - réservée
  - dynamique

préférable

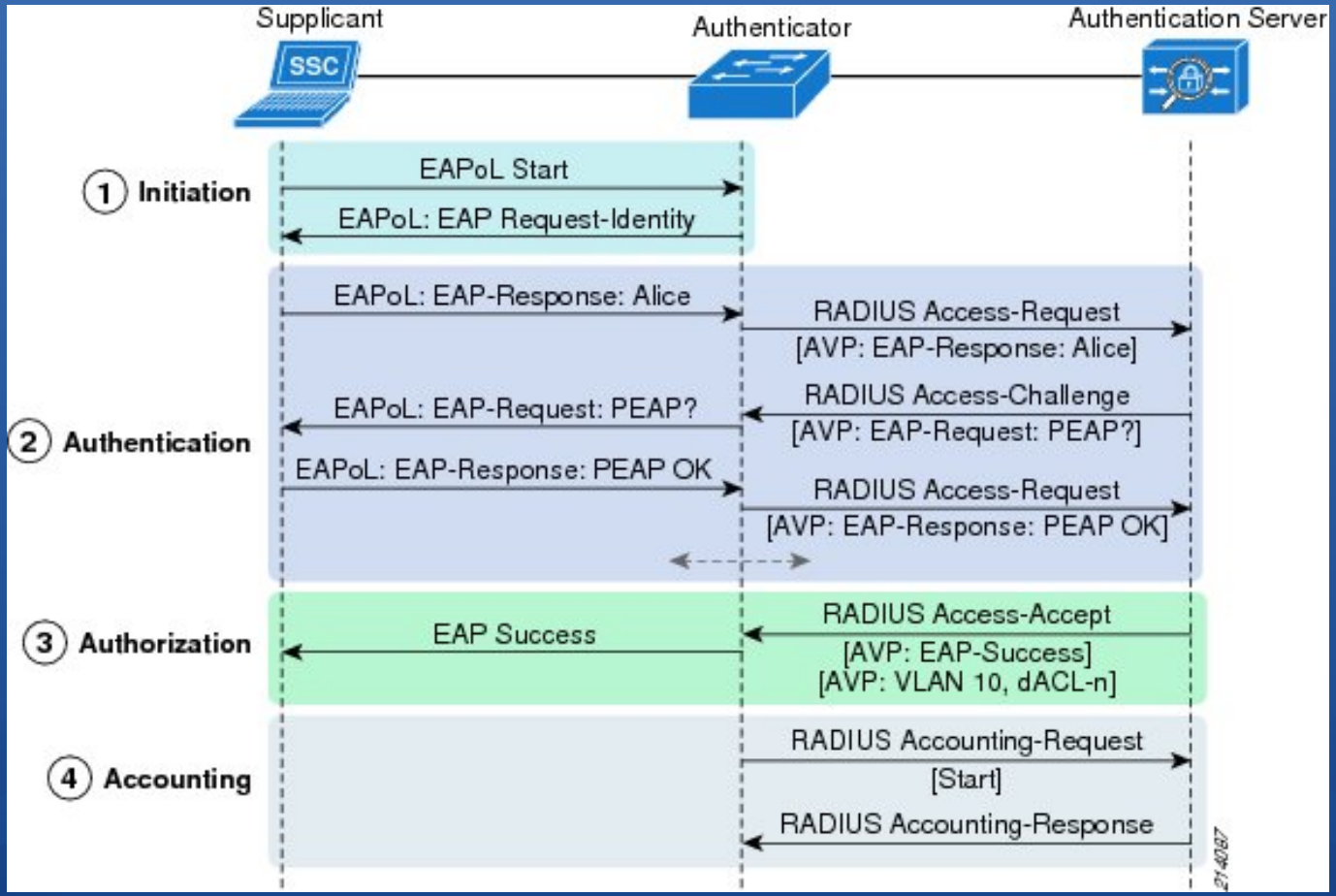
Éviter les adresses fixes : difficiles à gérer à long terme

802.1x

- Élément important pour accroître la sécurité d’un réseau
  - contrôle l’accès au réseau
  - permet une grande visibilité des activités sur le réseau
- Relativement peu déployé dans le réseau de la santé
  - CHUM, CUSM, Laval (peut-être d’autres)

→ Difficile à implanter car peut parfois causer des problèmes de connectivité avec certains équipements

Communications 802.1x



Utilisation du sans-fil

- Avant de mettre en place un réseau sans-fil, il faut faire une évaluation :
  - des interférences possibles avec les appareils bio-médicaux
    - constitue de moins en moins un problème en ce qui concerne les appareils cellulaires
    - considérer entre autre un réseau 5GHz plutôt que 2.4GHz
  - des risques de propagation des infections
    - contact avec l'usager ou son environnement en contexte clinique
  - du niveau critique du projet
    - la connexion peut-elle être interrompue sans conséquences graves?

WIFI 802.11 a/b/g/n/ac

Protocole	GHz	Mbps	Pour	Contre
802.11	2.4	2	Bonne couverture	Lent (peu implanté)
812.11b	2.4	11	Bonne couverture	Interférences
802.11a	5	54	Peu d'interférences	Plus courte distance (1/4) Bloqué par obstacles
802.11g	2.4	54	Bonne couverture	Interférences Coût plus élevé de production
802.11n	2.4	300	4 antennes (MIMO) Moins affecté par les interférences	Génère plus d'interférences
802.11ac	5	870 1730 6700*	8 antennes (MIMO) Connexions simultanées (MU-MIMO)	Coût plus élevé de production Nombreuses variations dans les produits

802.11i - WPA2

- Norme développée pour corriger les défauts de sécurité des réseaux sans-fil 802.11

  WEP ➪ WPA ➪ WPA2

- Comprend trois principales composantes de sécurité :
  - 802.1x: mécanismes d'authentification du client
  - AES: encryption forte des données échangées
  - RSN: gestion du passage d'un point d'accès à un autre
  - le chiffrement de la négociation initiale a été abandonné

→ KRACK : faille récente nécessitant une mise à jour des équipements

HL7

Healthcare Level 7

- Définit le format des messages échangés entre applications dans le domaine médical
- Plusieurs versions du protocole
  - v2.x : très répandue, nombreuses extensions ad hoc
  - V3 : beaucoup plus structurée, complexe et lourde à implanter

→ Nécessaire pour inter-opérabilité, mais pas suffisant

→ En général : v2 intra-établissement, v3 infrastructure (DSQ)

Message HL7v2

MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||
ADT^A01^ADT_A01|01052901|P|2.5

EVN||200605290901||||200605290900

PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-
9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35
209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O |||||||
0105I30001^^^99DEF^AN

PV1|||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||
67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||
13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||200605290900

OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F

OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F

AL1|1||^ASPIRIN DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

DICOM

Digital imaging and communications in medecine

- Encadre le stockage et l'échange d'images médicales
  - définition de l'objet image
  - définition des services pour gérer ces images
- Les informations relatives au sujet sont couplées avec l'image
- Est à la base du développement des PACS (Picture Archiving and Communication Systems)
- Standard bien défini et très bien implanté

→ Bonne assurance d'inter-opérabilité au niveau du transfert d'images

CCOW

Clinical Context Object Workgroup

- Protocole visant l'intégration visuelle et le partage de contexte entre des applications cliniques s'exécutant sur un même poste de travail.
- Réduit les risques d'erreurs et assure la cohérence des données entre les applications
- Comprend trois parties :
  - partage de contexte utilisateur (gestionnaire centralisé)
  - protection d'applications
  - passage de contexte clinique entre applications

Demande un haut niveau de maturité technologique

Environnements virtuels

- Un serveur physique est utilisé pour émuler plusieurs serveurs distincts
- Chaque serveur émulé ne s'aperçoit pas qu'il partage les ressources avec d'autres
- Plusieurs plateformes existent :

  Vmware, KVM, VirtualBox, …
- Permet de mettre en production beaucoup plus rapidement

→ Danger de prolifération incontrôlée des serveurs

Conteneurs

- Virtualisation axée sur le déploiement rapide de services
- Plusieurs plateformes existent, mais la plus populaire est Docker
- Un grand nombre d’instances peuvent être démarrées sur un même serveur
- Mécanismes automatiques de distribution de charge et de reprise

→ Évolution très rapide

→ Mécanismes de sécurité encore à raffiner

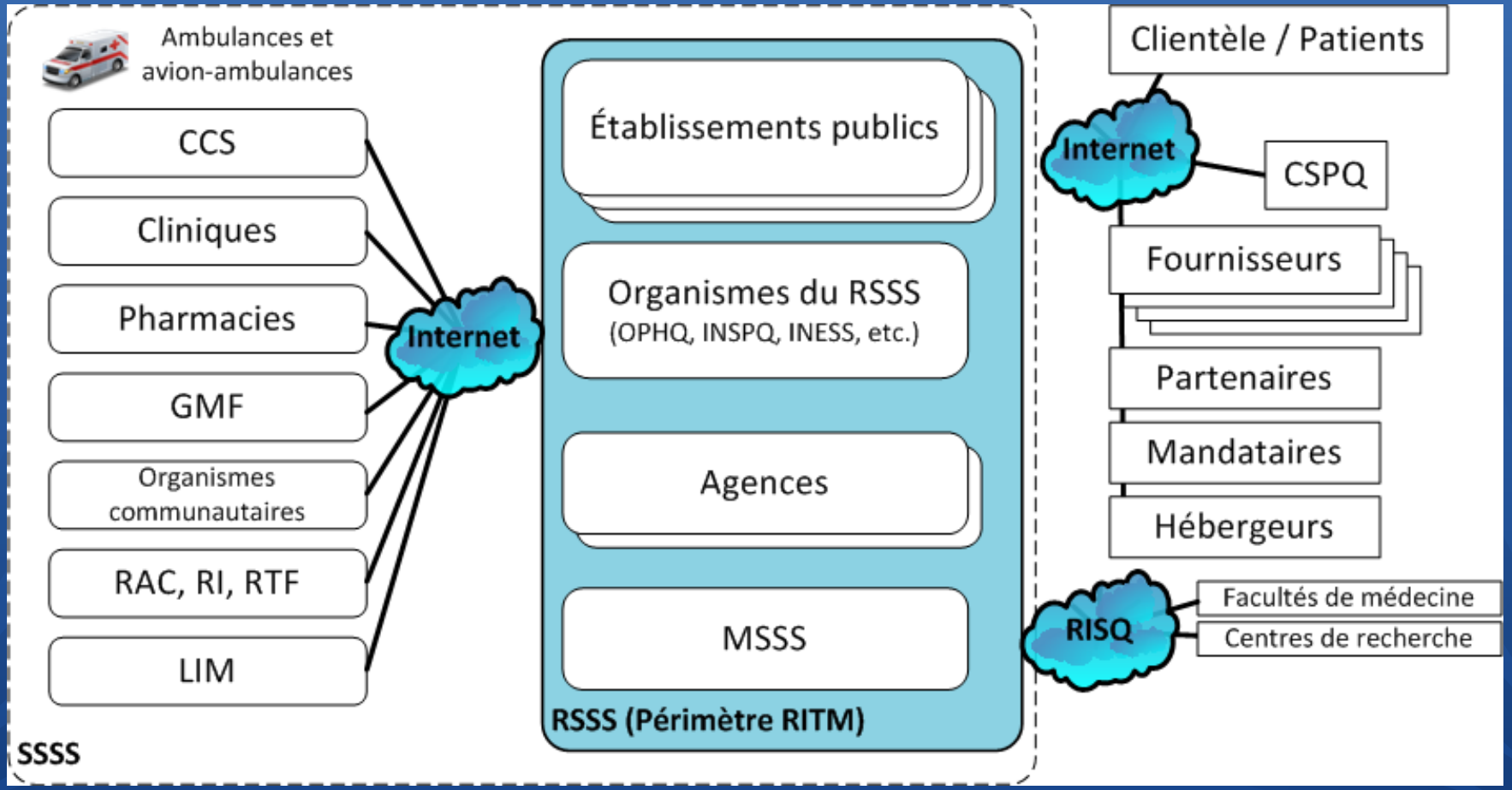
RITM

Réseau intégré de télécommunication multimédia

- Réseau privé reliant les établissements de santé du Québec
- Isole les établissements de santé de l’Internet
  - courriel Outlook et infonuagique brisent cette barrière de sécurité
- Accès distant régi par la DGTI du MSSS
  - authentification forte pour les utilisateurs et les fournisseurs

→ S’assurer que les fournisseurs utilisent le service F-VPN

Schéma du RITM



Une jungle d’acronymes

- On branche de plus en plus d’équipements au réseau
- En déchiffrer les spécifications devient un défi en soi
- Avoir une connaissance en réseautique est nécessaire pour voir au-delà des affirmations des fournisseurs