Chapitre 2 : Sécurité des communications

SÉcurité et Cryptographie
2013-2014

Sup Galilée INFO3

Objectifs,vulnérabilités et menaces

C'est bien d'assurer la sécurité d'un système informatique, mais le problème devient plus ardu lorsqu'il s'agit d'assurer la sécurité de communications entre un système et un autre, ou encore lorsqu'il s'agit d'assurer la sécurité des communications d'un système connecté à un réseau de télécommunication, comme Internet.

Objectifs,vulnérabilités et menaces

À la base les questions qui se posent sont toujours les mêmes :

- Confidentialité : Comment s'assurer que les messages que mon système envoie n'arrivent pas à des personnes ou des systèmes non autorisés ? En supposant qu'il est facile d'intercepter des messages, comment être raisonnablement sûr qu'ils ne pourront pas être interprétés par d'autres personnes que celles auxquelles ils étaient destinés ?

Objectifs,vulnérabilités et menaces

- Intégrité : Comment être sûr que mon message arrivera bien à destination ? Comment être sûr qu'il ne subira pas d'altération ou si cela se produit, que cela sera détecté ?

Objectifs,vulnérabilités et menaces

- Authenticité : Suis-je sûr de la validité des messages que je reçois ?
Comment détecter qu'un message est un faux ?

Objectifs,vulnérabilités et menaces

- Disponibilité : Il existe des cas où il est vital que les communications puissent être assurées. Le refus de service puet être un problème majeur pour le fonctionnement d'un système. Un exemple : le système de contrôle du trafic aérien.

Objectifs,vulnérabilités et menaces

Vulnérabilités

- Selon le médium utilisé pour les communications, l'interception est plus ou moins aisées : il est par exemple très facile d'intercepter des conversions téléphoniques ou des communcations en WIFI, alors qu'il devient plus difficile d'intercepter des communications sur fibre optique.

- Les nœuds de télécommunication sont particulièrement vulnérables. Un commutateur ou un routeur endommagé peut gravement nuire au bon fonctionnement d'un réseau.

- Les connexions des systèmes aux réseaux sont vulnérables : il y a la menace des intrusions.

Objectifs,vulnérabilités et menaces

Menaces

Quelques termes choisis pour identifier les menaces contre la sécurité d'un réseau de communication :

- Mascarade : Un imposteur prétend être un utilisateur autorisé.

- Play-back : Quelqu'un intercepte un message valide et l'envoie de nouveau. Cela peut être gênant pour une banque lorsqu'une telle action survient lors d'un transfert informatique de fonds.

- Répudiation : Le destinataire d'un message nie avoir reçu celui-ci ou l'émetteur nie l'avoir transmis.

- Refus de service : La disponibilité du réseau est mise en cause, soit accidentellement, soit intentionnellement.

Objectifs,vulnérabilités et menaces

Menaces

L'interception des communications est également une préoccupation :

- Interception passive : C'est une menace contre la confidentialité. On y trouve par exemple les écoutes téléphoniques.

- Interception active : C'est encore plus grave, puisqu'on attaque l'authenticité et l'intégrité des informations transmises par exemple en les modifiant (mais aussi "man-in-the-middle").

Objectifs,vulnérabilités et menaces

Contre-mesures

Comment faire pour se protéger ? Quatre approches peuvent être envisagées :

- Protéger les équipements de télécommunications, ce qui suppose soit de posséder l'intégralité des équipements, soit de supposer que l'opérateur de télécommunication fait de même avec ses propres équipements. C'est souvent la seconde option qui est mise en pratique pour les réseaux informatiques : utilisation de firewalls.

- Protéger les donnés qu'on envoie. Les techniques de chiffrement (abordées dans la suite du cours) permettent de répondre au problème de confidentialité, d'authenticité et même d'intégrité. Le protocole IPv6 permet de chiffrer, avec IPsec en natif, les communications de bout en bout.

- Appliquer des principes d'administration sûre. De même qu'un système d'exploitation offre des moyens de contrôler les accès des utilisateurs, on peut appliquer des contrôles d'accès sur le réseau.

- Configurer son réseau local de façon sûre. Un exemple de ce que l'on peut faire : isoler son système (ou un sous-réseau) et de le connecter derrière un firewall (coupe-feu) : DMZ ou zone démilitarisée.

Quelques généralités sur les systèmes de chiffrement

Un algorithme de chiffrement est une fonction mathématique utilisée pour le chiffrement et le déchiffrement des données. La plupart des algorithmes modernes sont à clefs. L'algorithme de chiffrement et de déchiffrement est connu, mais dépend des clefs qui sont propres à chaque utilisateur.

- Les algorithmes à clef secrète : La clef (qui permet de chiffrer et de déchiffrer) n'est connue que du seul émetteur d'un message et de son destinataire.

- Les algorithmes à clef publique : Le destinataire possède deux clefs : sa publique, connue de tout le monde, et sa clef privée (qu'il est le seul à connaître). L'émetteur d'un message chiffre ce dernier avec la clef publique du destinataire.

Quelques généralités sur les systèmes de chiffrement

La gestion des clefs est un problème délicat à résoudre : comment créer des clefs ? comment les échanger ? comment authentifier une clef reçue par un autre utilisateur ? comment les stocker ? combien de temps les utiliser ?