Applications

Cours MPRI niveau 1

Initiation à la cryptologie

15 et 22 mai 2006

Louis Granboulan

Première partie

Canal sécurisé

15 mai 2006

Louis Granboulan

Plan du cours

1. Principes
   a. Entité et identité
   b. Chaîne de confiance
2. Outils
   a. Génération de pseudo-aléa
   b. Partage de clef
   c. Signature
   d. Chiffrement
3. Exemples
   a. IPSec
   b. SSL
   c. SSH
   d. GSM, GPRS, UMTS
   e. WiFi (WEP, WPA, WPA2)

Bibliographie

- Un cours donné au Royal Holloway
  - http://www.isg.rhul.ac.uk/msc/teaching/iy5511/ic3.shtml
  - Regarder surtout les parties 4 à 8
- Références : RFC
  - 2402, 2406, 2409 (pour IPSec)
  - 2246 (pour TLS)
  - 2284, 2716, 2869 (pour authentification WPA)

Principes

- Entité
  - Objet, personne, groupe de personnes, … dans le monde «réel».
- Identité
  - Valeur numérique identifiant une entité, dans un certain contexte.
  - Une identité a des droits (d'accès, de certification, …) dans un certain contexte.
  - Une entité peut avoir plusieurs identités.

Lien entité–identité

Ne peut être fait que dans le monde «réel».

Something that you have

- Lien fait à l'aide de matériel inviolable, e.g. puce sécurisée, token, dongle, …

Something that you know

- Code secret, mot de passe, …

Something that you are

- Lien fait à l'aide de la biométrie.

Éventuellement plusieurs à la fois

- Carte à puce à clef biométrique et à PIN code.

Cryptographie

- C'est la «science du secret»
  - La notion d'identité ne peut exister sans secret.
- Caractéristiques d'une identité
  - L'identité est une valeur publique.
  - Un détenteur de l'identité possède un secret associé à cette valeur publique.
  - Parfois le secret n'est pas explicite.
    Par exemple : comment avoir un doigt reconnu par le détecteur biométrique.

Chaîne de confiance

- La confiance est héritée
  - À une identité est associée des droits dans un certain contexte.
  - On y fait confiance car cette association a été annoncée par une ou plusieurs identité(s) de confiance.
- Ce n'est pas spécifique au monde numérique
  - Par exemple le commerçant fait confiance à une carte bancaire, héritée d'une confiance en la banque, héritée d'une confiance en l'état et la justice, etc.

Architecture de confiance

- PKI (Public Key Infrastructure)
  - Une identité «maître» est de confiance, a priori (root certificate)
  - Elle certifie d'autres identités, pour certaines applications, pouvant elles-même certifier d'autres identités : arborescence
  - Une révocation peut être publiée : CRL (certificate revocation list)
    Datation, timestamping
  - La certification peut être partagée (signatures de groupe)
- PGP web of trust
  - Un exemple de PKI décentralisée : chacun est sa propre racine dans son arborescence de confiance, la réunion des arborescences format un graphe.

Outils

Outils : pseudo-aléa

- Principe
  - Une petite graine aléatoire sert à fabriquer une quantité plus élevée de pseudo-aléa
- Usages
  - Pour dériver des sous-clefs à partir d'une clef maître
- Mise en œuvre
  - Chiffrement de flot
  - Mode compteur d'une fonction de hachage

Outils : génération de clef

- Principe
  - Deux identités A et B (chacune ayant son secret) créent un nouveau secret commun au deux.
- Problème
  - Man-in-the-middle : les communications entre A et B doivent avoir leur expéditeur authentifié
- Remarques
  - Génération tri-partite ?
  - Minimisation du nombre de communications
  - Imprédictibilité de l'aléa, rejeu

Outils : signature

- Principe
  - Protocole faisant intervenir un signataire et un vérifieur
  - Seule une certaine identité est capable de faire des signatures valides
- Variantes
  - On-line (interactive) ou off-line
  - Vérifieur désigné ou non répudiation
- Mise en œuvre
  - Asymétrique : signature à clef publique
  - Symétrique : signature à clef secrète (i.e. MAC)

Outils : chiffrement

- Principe
  - Protocole faisant intervenir un chiffreur et un déchiffreur
  - Seule une certaine identité est capable de déchiffrer
- Mise en œuvre
  - Asymétrique : chiffrement à clef publique
  - Symétrique : chiffrement de flot ou mode d'opération d'un chiffrement de blocs

Composition

- Question fondamentale
  - Doit-on signer le message chiffré, ou bien chiffrer le message signé ?

Exemples

Exemples : IPSec

- Canal sécurisé au niveau «réseau».
  - Mode «transport» : sur un réseau gérant IPSec
  - Mode «tunnel» : machines intermédiaires, ne gérant pas IPSec
- Fonctionnalités
  - Authentification et/ou confidentialité : AH et ESP
  - Politique de sécurité : SPD et SAs
  - Génération de clef : IKE

IPSec : AH

- AH : Authentication Header (RFC 2402)
  - Authentification de l'émetteur et intégrité des données
  - Authentifie tout le *payload* IP et une grande partie du *header* (e.g. pas le TTL)
- Utilisation
  - Empêcher *IP spoofing*
  - Empêcher les rejeux (les paquets ont des numéros de séquence)
- Outils cryptographiques
  - MAC (HMAC-MD5-96, HMAC-SHA1-96, …)

IPSec : ESP

- ESP : Encapsulating Security Protocol (RFC 2406)
  - Authentification et/ou confidentialité des données
  - Uniquement le *payload* IP
- Utilisation
  - Confidentialité, y compris éventuellement de la longueur du *payload* (par un *padding*)
- Outils cryptographiques
  - MAC et chiffrement symétrique (e.g. à base de DES, 3K-TDES, RC5, IDEA, …)

IPSec : numéros de séquence

- IP est un protocole par paquets
  ⇒ arrivent dans le désordre

- Numéros de séquence
  - 32 bits, initialisés à 0
    ⇒ changement de clef si overflow
  - Authentifiés mais pas chiffrés
  - Réordonnés à l'arrivée avec une «fenêtre glissante», de longueur conseillée 64
    ⇒ refus de certains paquets si les délais/latences sont trop longs.

IPSec : SPD

- SPD : Security Policy Database
  - Basée sur des SA (Security Association) indiquant les préférences (algorithmes, mode transport/tunnel, état courant) pour chaque catégorie de paquets
  - Plusieurs SAs peuvent être associées à une catégorie de paquets (e.g. AH + ESP)

IPSec : gestion des clefs

- De nombreuses clefs partagées
  - Une pour chaque SA
  - Une SA pour chaque {ESP,AH} x {tunnel,transport} x {émetteur,récepteur}
- Deux sources
  - Création et partage manuels
  - IKE (adaptation de Oakley et ISAKMP)

IPSec : IKE

- IKE : Internet Key Exchange (RFC 2409)
  - Authentification mutuelle
  - Création d'un nouveau secret partagé
  - Résiste au DoS (cookies)
  - Négociation des algorithmes utilisés
  - Options avancées
    - Protection contre la comprimission : *Forward Secrecy*
    - Répudiation : *Deniable Authentication*
    - Anonymat : *Identity protection*

IPSec : IKE

- Phase 1
  - Négociation de la SA principale
  - Pour les autres SA, les erreurs et la gestion
  - Canal bidirectionnel
  - Canal ISAKMP (IPSec Key Management Protocol)
- Phase 2
  - Négociation des SA de données
  - Plus rapide

IPSec : IKE phase 1

- Deux modes
  - Mode principal, lent (6 messages)
  - Mode agressif, moins sûr (4 messages)
- Modes d'authentification
  - Quatre modes pour chacun
    - Signature
    - Chiffrement à clef publique
    - Chiffrement à clef publique modifié
    - Clef pré-partagée
  - Nonces pour éviter le rejeu
  - Certificats pour les clefs publiques
- Authentifient un partage de clef Diffie-Hellman
  - Cinq groupes différents, ou bien *new group mode*

IPSec : IKE mode principal

1. I→R : cookie, SA
2. R→I : cookie, SA
3. I→R : cookie, 1/2 Diffie-Hellman, nonce
4. R→I : cookie, 1/2 Diffie-Hellman, nonce
5. I→R : cookie, (certificat, signature) chiffrés
6. R→I : cookie, (certificat, signature) chiffrés

IPSec : etc.

- Pour plus de détails
  - Sur le site de la DCSSI
    http://www.formation.ssi.gouv.fr/stages/documentation/architecture_securisee/vpn.html
  - La partie 5 du cours de Kenny Paterson
    http://www.isg.rhul.ac.uk/msc/teaching/iy5511/ic3.shtml

Exemples : SSL

- SSL : Secure Sockets Layer
  - v1 : non diffusée ; v2 : avec failles ; v3 : à peu près OK
  - TLS : Transport Layer Security
  - TLS 1.0 = SSL 3.1 (3.0 légèrement modifié)
  - TLS défini par RFC 2246
- Deux niveaux
  - SSL Record Protocol, construit sur TCP
  - Upper Level, construit au dessus
    - SSL Handshake Protocol
    - SSL Change Cipher Spec. Protocol
    - SSL Alert Protocol
    - Other applications, e.g. HTTP

SSL Record Protocol

- Notion de session
  - Créée par le Handshake
  - Fixe les paramètres cryptographiques
  - Transporte plusieurs connexions
- Notion de connexion
  - Caractérisé par les clefs partagées, l'état courant, …
  - Les clefs sont créées à partir de la clef maître, de session

SSL Handshake Protocol

- Quatre méthodes de partage de clef
  - Chiffrement RSA
  - Fixed Diffie-Hellman (ne dépend que des clefs publiques)
  - Ephemeral Diffie-Hellman
  - Anonymous Diffie-Hellman (vulnérable au man-in-the-middle)
- Authentification
  - Capacité au déchiffrement RSA
  - Signature DSS ou RSA
- Dérivation de clef
  - À base de MD5 ou SHA1

SSL Handshake Protocol

1. ClientHello
   - Numéro de version, Nonce, liste de Ciphersuite (e.g. TLS_RSA_WITH_3DES_EDE_CBC_SHA)
2. ServerHello, ServerCertChain
   - Version, Nonce, Session ID, Ciphersuite
   - Certificat de clef publique
3. ClientKeyExchange, ClientFinished
   - Clef de session, authentification
4. ServerFinished
   - Authentification

SSL Handshake Protocol

- Particularités
  - Changements de paramètres cryptographiques possible en cours de session
  - Plusieurs connexions peuvent partager les mêmes paramètres (e.g. les pages d'un même site web)
- Différences entre SSL 3.0 et SSL 3.1/TLS 1.0
  - MAC : HMAC et non une variante
  - Dérivation de sous-clefs basée sur HMAC
  - Padding de taille variable (pour cacher la longueur des messages)
  - etc.

Failles de TLS

- Génération d'aléa
  - Faille pour certaines implantations
  - Goldberg, Wagner, 1996
- Messages d'erreur
  - Donnent de l'information sur le message
  - Canvel, Hiltgen, Vaudenay, Vuagnoux, 2003
- Temps de réponse
  - Peuvent donner la clef secrète du serveur (OpenSSL)
  - Boneh, Brumley, 2003

Exemples : SSH

- Secure Shell
  - v1 : avec failles ; v2 : OK
  - En cours de normalisation par l'IETF
- Trois niveaux
  - SSH Transport Layer Protocol
    - Authentification du serveur
    - Chiffrement
  - SSH Authentication Protocol
    - Authentification du client
  - SSH Connection Protocol
    - Plusieurs connexions sur une session

SSH : faiblesses de la v1

- SSH v1 Insertion attack
  - Mauvais algorithme d'intégrité (CRC32)
  - Longueur des paquets non protégée
- SSH v1.5
  - Attaque théorique retrouvant la clef de session
  - Man-in-the middle (avec dnssniff)
  - Denial of Service

Exemples : GSM, GPRS, UMTS

- 2ème génération de téléphonie mobile
  - Global System for Mobile communications
    - Norme européenne (CEPT puis ETSI)
    - Fonctionnement en circuit (facturation au temps)
  - GPRS : General Packet Radio Service
    - 2.5G
    - Fonctionnement en paquets (facturation au volume)
  - Sécurisé (contrairement à la 1G)
  - Radio TDMA : Time Division Multiple Access
- 3ème génération
  - UMTS : Universal Mobile Telecommunications System
  - Mieux sécurisé
  - Radio W-CDMA : Wideband Code Division Multiple Access

GSM : SIM

- Subscriber Identity Module
  - Hardware inviolable contenant un secret de 128 bits : Ki
  - Sert à l'authentification (facturation) et à la confidentialité
- Clef secrète partagée
  - L'opérateur (AuC : Authentication Centre) connaît les Ki
  - Authentification par preuve de connaissance de Ki
  - Confidentialité par génération d'une clef de session Kc
- Anonymat
  - À l'aide d'identités temporaires

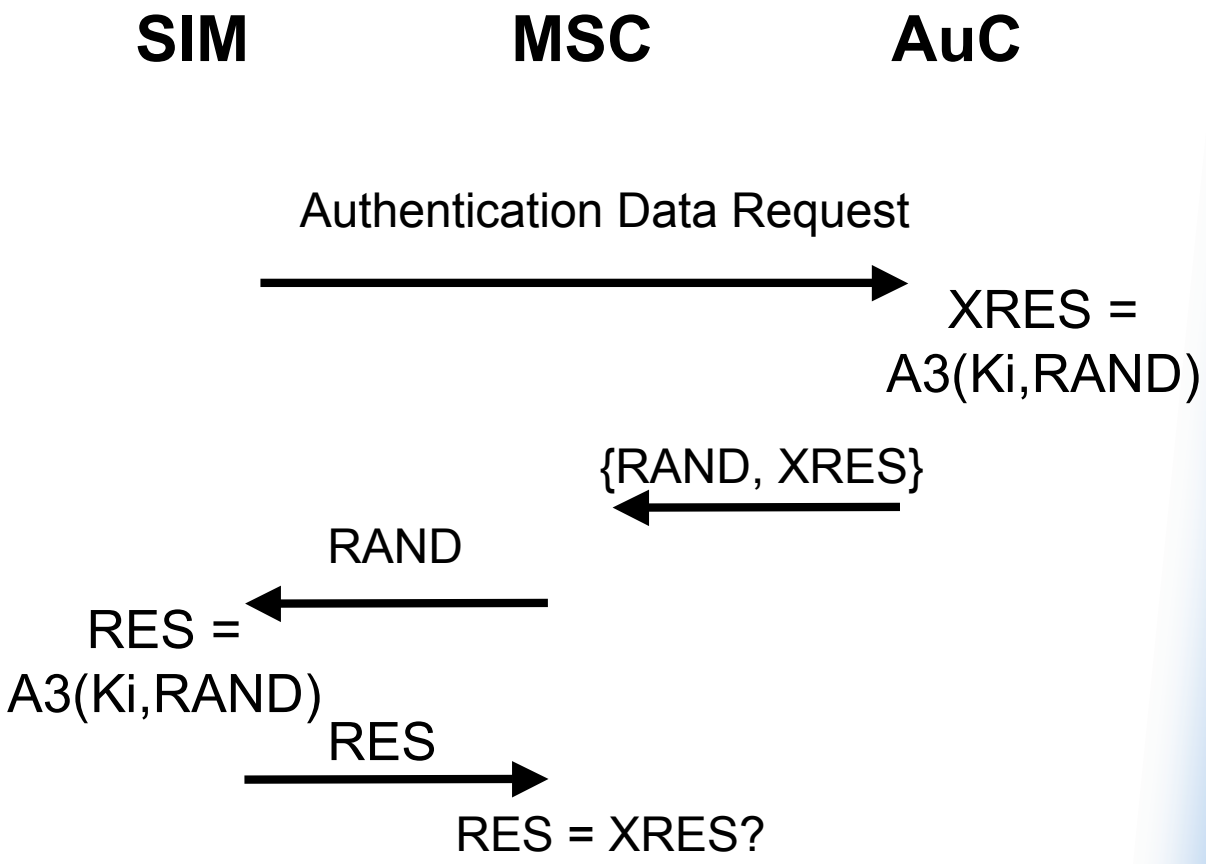
GSM : anonymat

- Premier accès à un opérateur : envoi de IMSI
  - International Mobile Subscriber Identity
  - Envoi par l'opérateur d'une TMSI, chiffrée
  - Temporary Mobile Subscriber Identity
- Accès suivant : envoi de TMSI
  - Envoi par l'opérateur d'une nouvelle TMSI, chiffrée

GSM : authentification

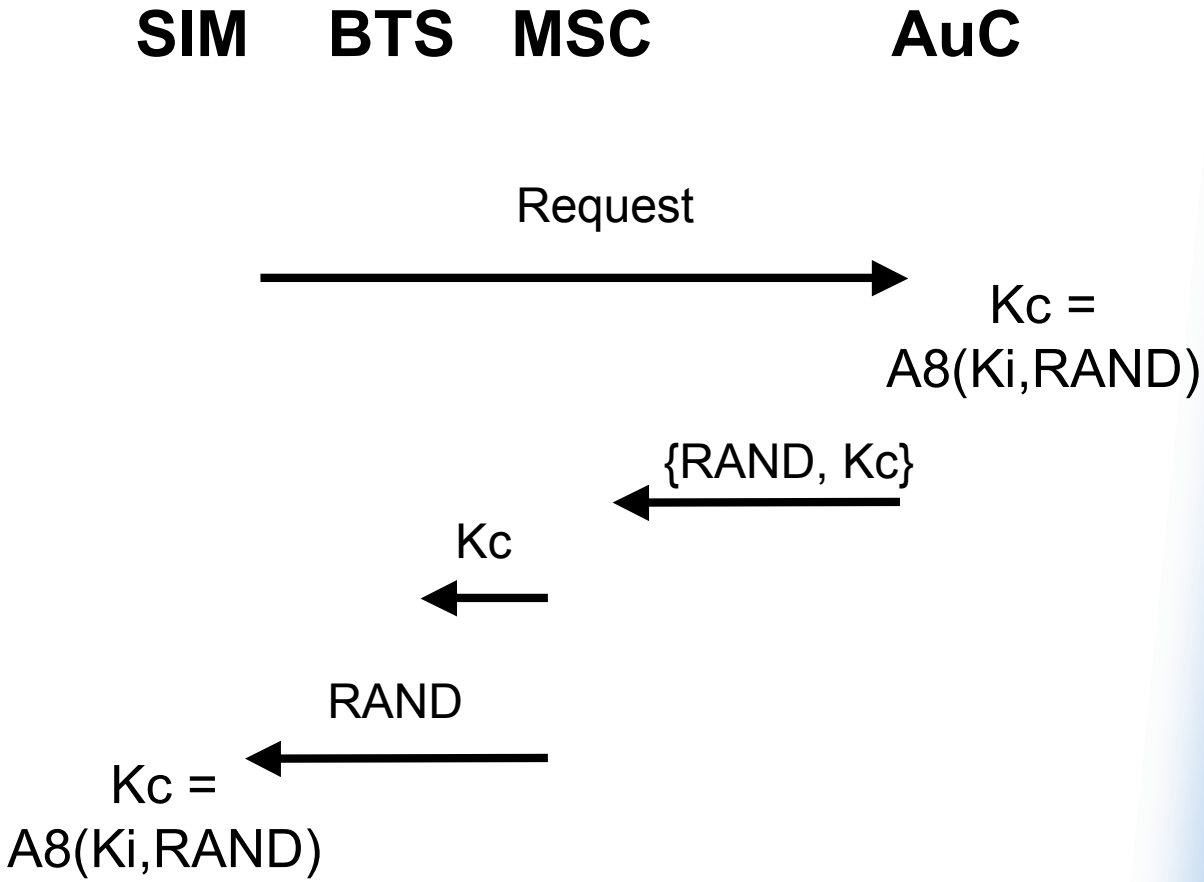
- Algorithme A3
  - Prend en entrée Ki (128 bits) et RAND (128 bits)
  - Renvoie RES (32 bits)

- SIM : mobile
- MSC : réseau local
- AuC : réseau d'abonnement



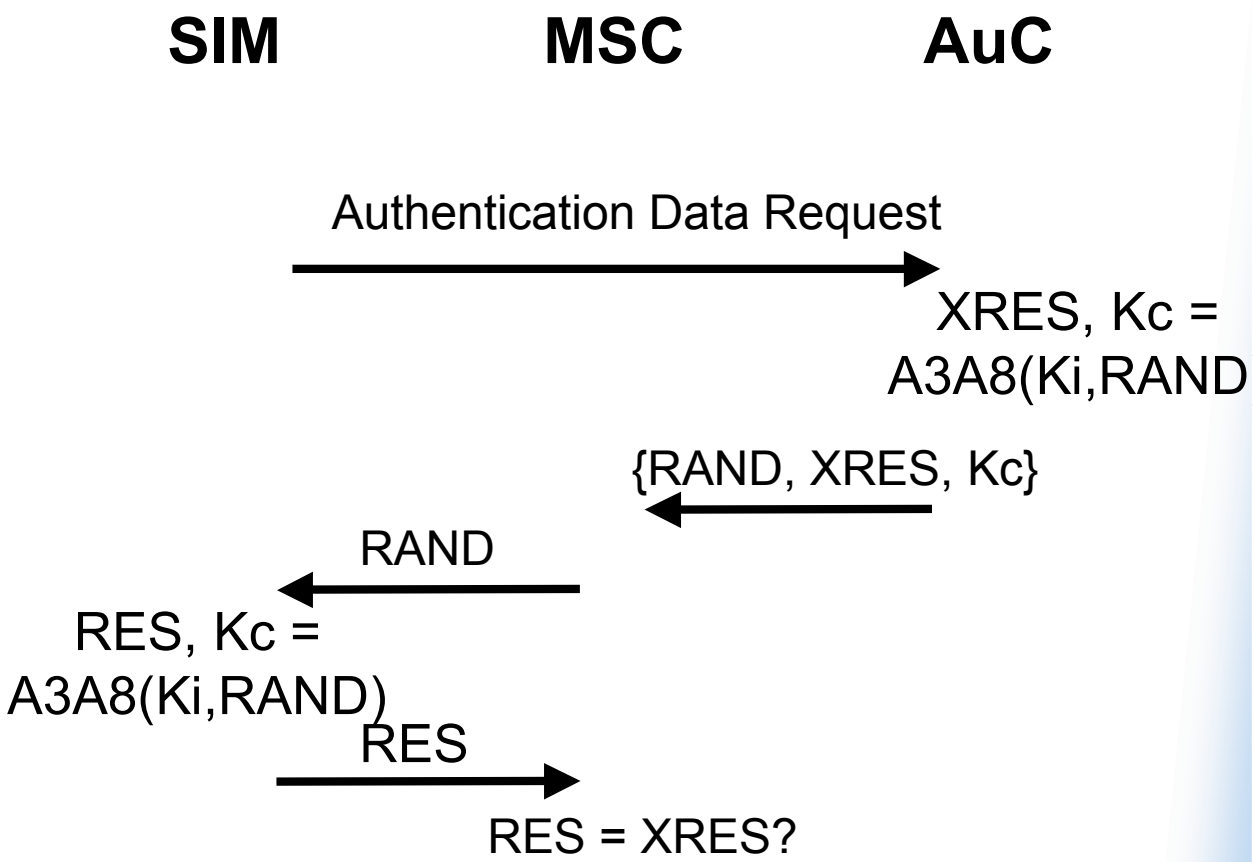
GSM : clef de session

- Algorithme A8
  - Prend en entrée Ki (128 bits) et RAND (128 bits)
  - Renvoie Kc (64 bits)
- BTS : station de base



GSM : A3/A8

- Les deux sont simultanés
  - Prend en entrée Ki (128 bits) et RAND (128 bits)
  - Renvoie RES (32 bits) et Kc (64 bits)
- Peuvent dépendre de l'opérateur
  - Souvent c'est COMP128 qui est utilisé
  - Mauvais algorithme (Ki déduit de 50000 challenges choisis)



GSM : confidentialité

- Algorithme A5 (spécifications non publiques, mais connues)
  - A5/0 : pas de chiffrement
  - A5/1 : chiffrement « fort »
  - A5/2 : chiffrement « faible »
- Chiffrement de flot
  - Très peu consommateur de courant
  - Flot engendré avec un « frame counter »
- Sécurité
  - Kc fait 64 bits doit 10 nuls : recherche exhaustive possible
  - Une recherche exhaustive en 2^{40} est possible (taille des registres)
  - Une attaque en temps réel est possible (TMTO)
  - L'insertion du « frame counter » est linéaire
  - Le même Ki est utilisé que ce soit A5/1 ou A5/2

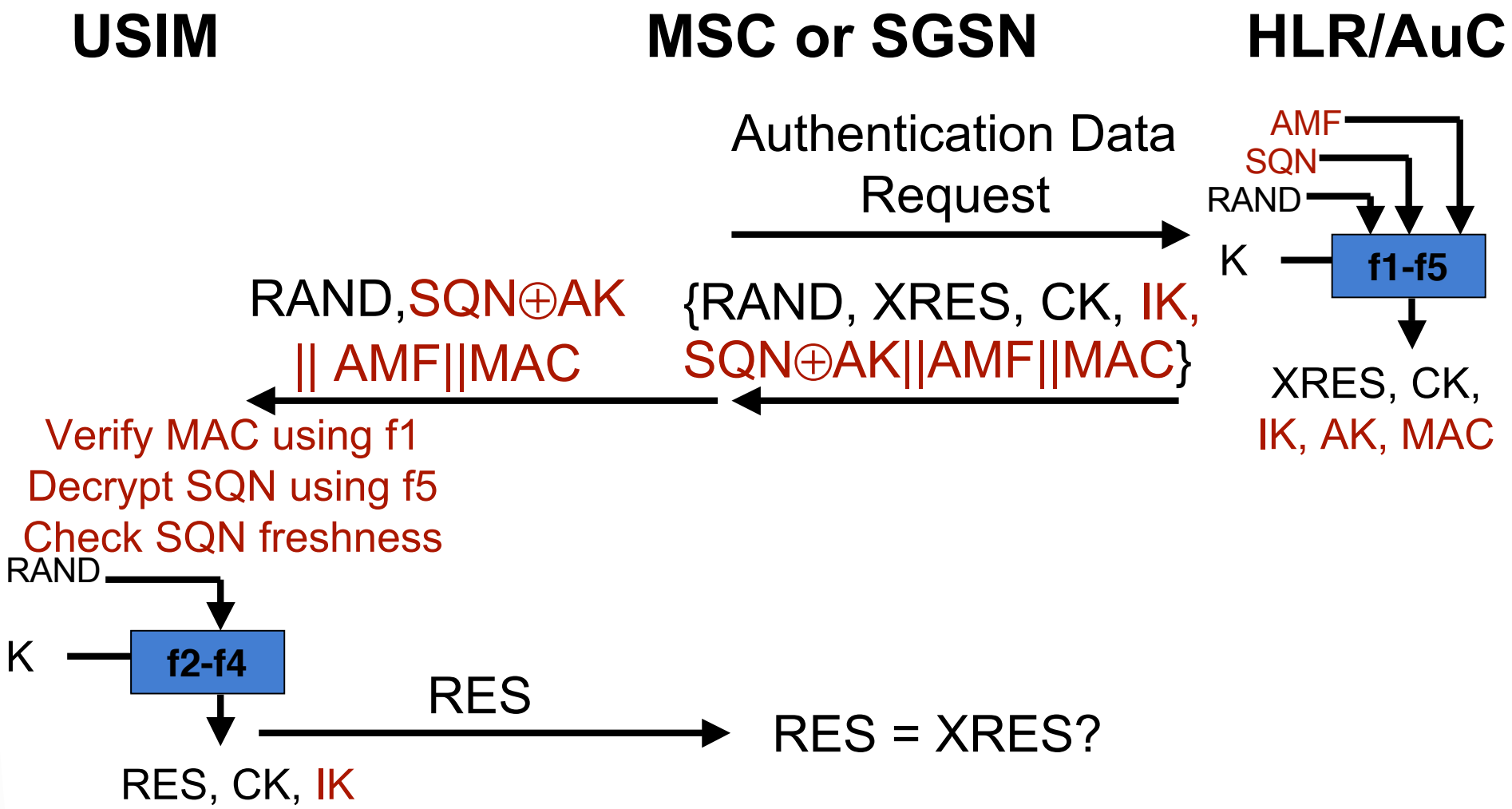
GPRS

- Même authentification que GSM
- Chiffrement
  - Confidentialité plus profond que la station de base
  - Algorithmes GEA1, GEA2 et GEA3 de spécifications non publiques
  - Le numéro de « frame » ne se répète plus au bout de 3.5 heures

UMTS

- Anonymat
  - Même technique que GSM/GPRS
- Confidentialité
  - Nouvel algorithme, public : mode d'opération du chiffrement par bloc KASUMI
  - Clef plus longue (128 bits)
- Intégrité des données
  - Utilise une clef secrète (MAC) au lieu d'un simple checksum
  - Algorithme public, basé sur KASUMI
- Authentification
  - Mutuelle
  - Algorithmes dépendant de l'opérateur
  - Algorithme conseillé MILENAGE, public, basé sur RIJNDAEL

UMTS : authentification



Exemples : WiFi

- WLAN
  - Wireless Local Area Network
  - WiFi : 802.11
- Spécifications radio
  - 802.11b (jusqu'à 11 Mbps)
  - 802.11a (jusqu'à 54 Mbps)
  - 802.11g (jusqu'à 54 Mbps, compatible 802.11b)
  - 802.11n (Jusqu'à 200 Mbps, pour fin 2006)
- Spécifications sécurité
  - WEP : Wired Equivalence Privacy
  - WPA : Wi-Fi Protected Access
  - 802.11i, aka. WPA2

WiFi : WEP

- Confidentialité
  - Clef partagée
  - Chiffrement basé sur RC4-64
  - 40 bits de clef
  - 24 bits d'IV (5 heures à 11 Mbps)
- Authentification
  - Clef partagée
  - AP envoie nombre aléatoire, le client le renvoie chiffré
- Intégrité
  - Checksum CRC32
  - Calculé avant le chiffrement !

WiFi : WEP

- Ce mode d'utilisation de RC4 est mauvais
  - Force brute si 40 bits !
  - Beaucoup d'IV sont faibles
  - Les premiers octets du clair sont connus
  - Outils opensource pour attaquer WEP
  - Si pas assez de trafic pour l'attaque, rejeu de paquets ARP
  - etc.

WiFi : WPA

- Correction de WEP
  - Corrige les trous de sécurité
  - Fournit de nouvelles fonctionnalités
  - Compatible avec le hardware WEP
- Deux modes de gestion des clefs
  - Pre-shared (comme WEP)
  - Enterprise (utilise EAP : Extensible Authentication Protocol, avec un serveur RADIUS, qui gère par exemple des certificats)
  - Inclus dans 802.1x
- Chiffrement TKIP
  - RC4 utilisé avec une nouvelle clef par paquet
  - Ces clefs sont engendrées à partir de la clef maître
  - CRC32 remplacé par MIC (Michael Integrity Code)

WiFi : 802.11i

- Amélioration de WPA
  - Appelé aussi WPA2
  - N'est pas encombré par la compatibilité avec WEP
  - Moins vulnérable au DoS que WPA
  - Extensible
- Aspects cryptographique
  - Basé sur AES

Fin

Seconde partie

Autres applications

22 mai 2006

Louis Granboulan

Plan du cours

1. Contrôle d'accès
   a. Windows (LanManager, NTLM, NTLMv2)
   b. Unix Password
   c. Kerberos
   d. EMV
2. Sécurisation de documents
   a. E-mail (S/MIME et PGP)
   b. Fichiers (PGP)
   c. Partitions (PGP, Filevault)

Windows : LanManager

- Type de protocole
  - Authentification challenge/réponse
  - Mot de passe comparé à un haché
  - Fonction de hachage basée sur DES
  - Cf. http://www.wikisecure.com/index.php/LanManager_Hash
- Failles
  - Découpe le mot de passe en blocs de 7 caractères
  - Caractères choisis dans un petit ensemble (majuscules, chiffres, ponctuation + 32 caractères spéciaux)
  - Cf. http://geodsoft.com/howto/password/nt_password_hashes.htm

Windows : NTLM

- Type de protocole
  - Apparu avec NT, puis 2000 et XP
  - Comme LanManager : challenge/réponse
  - Basé sur MD4 suivi d'un chiffrement DES
- Amélioration
  - 14 caractères, minuscules acceptées
- Faille
  - Un bloc de DES n'est quand même pas assez grosse
  - Jusqu'en 2001, désactiver LM n'empêche que l'accès, mais ne supprime pas le stockage des hachés sur le disque !

Windows : NTLMv2

- Protocole
  - Apparu avec NT 4.0 SP4
  - Basé sur HMAC-MD5
  - Cf. http://curl.islandofpoker.com/rfc/ntlm.html
- Amélioration
  - L'espace du hachage fait 128 bits
  - Encodage Unicode
- Question
  - Unicité des caractères ?

Windows : conclusion

- Seuls Windows 2000 et XP font une authentification acceptable (NTLMv2 et surtout Kerberos)
  - Les mises à jour de 95, 98 et Me ne sont pas stables
  - NT 4.0 ne peut pas faire de Kerberos
- Ne pas utiliser les vieilles versions, mais… il y a souvent une compatibilité ascendante qui affaiblit le système, par exemple :
  - Samba utilise LanManager
  - Même si samba est désactivé, MacOS X stocke les hachés LM quelque part
  - …

Unix password

- Protocole
  - Authentification challenge/réponse
  - Utilisation d'une *salt* pour éviter les attaques par dictionnaire
  - 25 chiffrements DES consécutifs à partir du clair 0 et en utilisant la *salt* pour choisir parmi 4096 variantes
- Shadowing
  - À l'origine, le mot de passe haché était dans /etc/passwd lisible par tous
  - Désormais, caché et lisible par root uniquement

Kerberos

- Protocole de partage de clef
  - Développé au MIT, basé sur Needham-Schroeder
  - Basé sur du chiffrement DES
  - Nombreuses versions (actuellement v5)
  - Cf. http://www.isi.edu/gost/publications/kerberos-neuman-tso.html
- Principes
  - Trois partenaires : client, serveur et AS (serveur d'authentification)
  - Tickets fabriqués par l'AS à chaque demande de nouvelle connexion, en utilisant la clef secrète
  - Pour éviter que la clef secrète soit utilisée trop souvent : une indirection supplémentaire (TGS : ticket granting server)
- Problèmes
  - Vulnérable aux attaques par dictionnaire (off-line)

EMV

- Cartes bancaires
  - Eurocard Mastercard Visa (2001)
  - Spécification pour cartes à puce
- Crypto
  - Authentification symétrique (DES, 2k3DES) ou asymétrique (RSA)

E-mail

- Bases communes
  - Communication
    - MUAs et MTAs
    - Protocole SMTP (texte sur TCP/25)
    - POP (RFC 1939) et IMAP (RFC 2060)
  - Format
    - RFC 822 : format en-tête/corps de mail
      - Date de 1982, ASCII seulement
    - MIME : Multipurpose Internet Mail Extensions
      - RFC 2045-2049

E-mail : SSL

- La protection de la communication est faite par encapsulation dans SSL
  - SMTP : assez rare
  - POP et IMAP : très courant, mais pas partout
  - HTTP : presque partout, mais en option quand même
- Ne suffit pas
  - Problèmes avec les firewalls
    - SMTP : TCP/25 SMTPS : TCP/465
    - HTTP : TCP/80 HTTPS : TCP/443
    - POP3 : TCP/110 POP3S : TCP/995
    - IMAP : TCP/143 IMAPS : TCP/993
  - Le message une fois reçu n'est plus protégé

E-mail : S/MIME

- Historique
  - Développé par RSA en 1995, repris en RFC 2630-2634
  - Présent dans tous les MUA modernes
- Fonctionnalités
  - Signature asymétrique (avec non-répudiation)
  - Chiffrement asymétrique hybride
  - Algorithmes variés : DES, 3DES, RC2, RSA, ElGamal, SHA1, MD5, RSA, DSS
  - Chaînes de certificats X.509
    - Le même format que SSL et IPSec

E-mail : PGP

- Historique
  - Développé par Phil Zimmerman en 1991, plusieurs variantes libres (OpenPGP, GnuPG) et commerciales (PGP corp.)
  - Plugins pour tous les MUA modernes
- Fonctionnalités
  - Signature asymétrique (avec non-répudiation)
  - Chiffrement asymétrique hybride
  - Algorithmes variés : DES, 3DES, AES, …, RSA, ElGamal, SHA1, MD5, …, RSA, DSS, ECDSA, …
  - Web of trust
    - Confiance accordée individuellement par un algorithme élaboré
  - Keyring pour les clefs publiques et la confiance accordée
  - Clef secrète chiffrée par mot de passe

Fichiers

- En ligne de commande
  - GnuPG, OpenSSL
  - Utilisent les outils développés pour un autre usage
- Logiciels dédiés
  - WinZip, WinRar
  - Ajout du chiffrement à des fonctions d'archivage
- Problématique spécifique
  - Ajout de données à la fin, modification au milieu
  - Habituellement : il faut tout chiffrer/signer de nouveau

Disques

- Problématique spécifique
  - Tout le temps modifiés : on ne peut se permettre de tout chiffrer à chaque changement
  - Habituellement : chiffrement/authentification secteur par secteur
    - Une clef commune, numéro de secteur comme paramètre
    - Concept cryptographique inventé pour modéliser cela : *tweakable block cipher*
- Outils
  - Images disque chiffrées (PGPdisk, Drivecrypt, Truecrypt, Filevault, …)
  - Disques externes incluant du chiffrement…

Fin

Exercices

Quelques protocoles

- **Question :**
  pour chacun des protocoles décrits ci-après, faire des propositions de
  - Modèle formel de sécurité
  - Construction à partir de primitives ou autres protocoles cryptographiques

Password-authenticated Key Exchange

- Description (PAK)
  - Protocole à deux partenaires
  - Un petit secret partagé (peu de bits d'entropie) : mot de passe
  - Objectif : créer un gros secret partagé
  - Contrainte : résister à la recherche exhaustive sur le mot de passe
- Références
  - http://www.cs.ut.ee/~helger/crypto/link/protocols/pak.php

Oblivious transfer

- Description (OT)
  - Protocole à deux partenaires
  - Alice connaît un bit et l'envoie à Bob avec probabilité 50%
  - Alice ne sait pas s'il a été envoyé
  - Bob sait s'il l'a reçu
- Ou bien (1-out-of-2 OT)
  - Alice connaît deux bits b_0 et b_1 et en envoie un à Bob
  - Alice ne sait pas lequel a été envoyé
  - Bob sait lequel il a reçu
- Références
  - http://www.cs.ut.ee/~helger/crypto/link/protocols/oblivious.php

Private Information Retrieval

- Description (PIR)
  - Il s'agit de faire des requêtes dans une base de données sans indiquer quelle a été la requête
  - La donnée est une chaîne de bits $x_1 \ldots x_n$
  - La requête est un indice i
  - Il y a k serveurs
  - Le client doit trouver x_i sans publier i
  - Objectif : on veut minimiser la quantité d'information transmise à chaque requête
- Références
  - http://www.cs.umd.edu/~gasarch/pir/pir.html
  - http://citeseer.ist.psu.edu/499507.html

Memory checking

- Description
  - Le vérifieur a une petite zone de mémoire privée
  - Il a accès en lecture et écriture à une grande zone de mémoire non-fiable
  - Il veut savoir si la mémoire non-fiable a changé
- Références
  - Le cours donné par Moni Naor ces dernières semaines http://www.wisdom.weizmann.ac.il/~naor/COURSE/ens.html