Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 – Sécurité et Réseaux

TD/TP n°1

Exercice 1 : Authentification

Alice souhaite s'authentifier auprès de Bob, et Trudy est un attaquant (Man In The Middle : MITM) qui écoute et analyse les trafics du réseau via l'outil ***Wireshark***. Trouver les faiblesses dans les mécanismes d'authentification suivant en complétant le schéma à droite (dans la mesure du ***possible*** !):

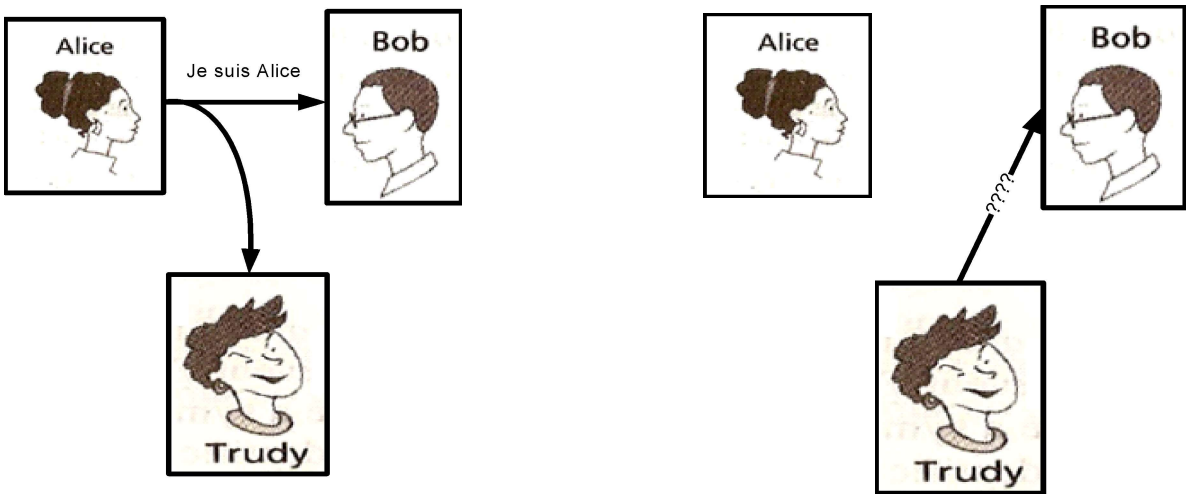

Figure 1 : Protocole d'authentification pda 1.0

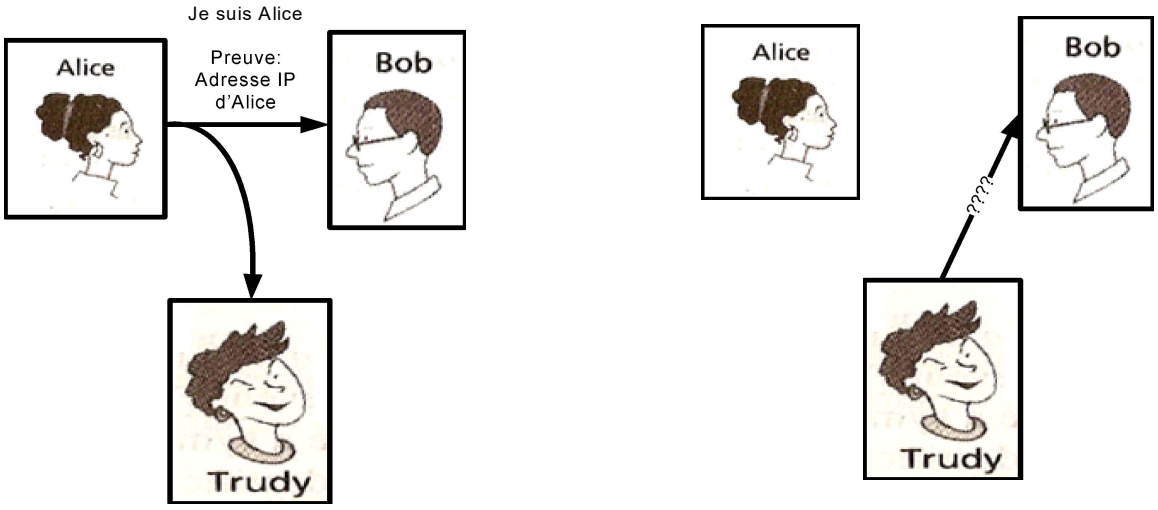

Figure 2 : Protocole d'authentification pda 2.0

Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 – Sécurité et Réseaux

TD/TP n°1

Figure 3 : Protocole d'authentification pda 3.0

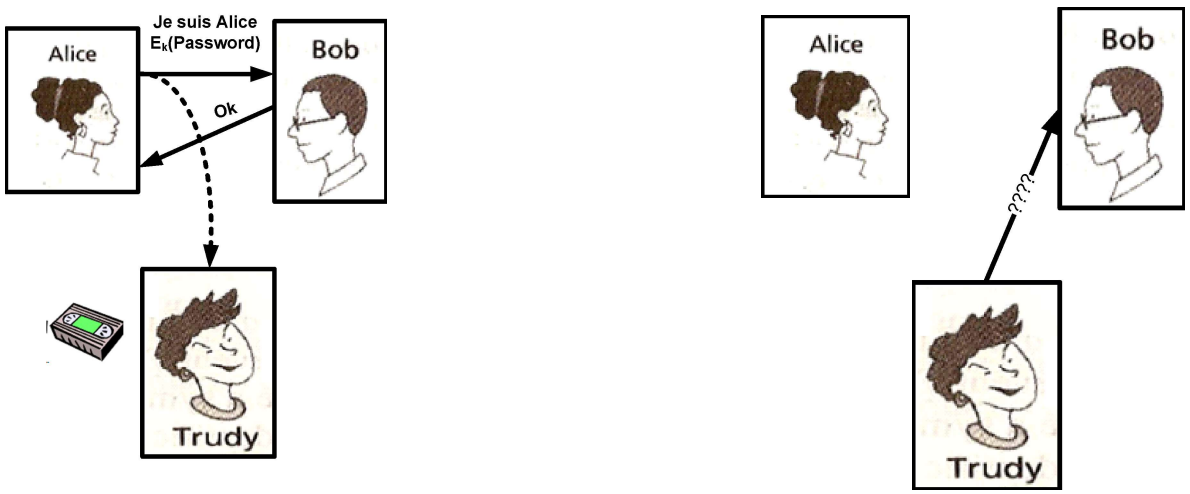

Figure 4 : Protocole d'authentification pda 4.0

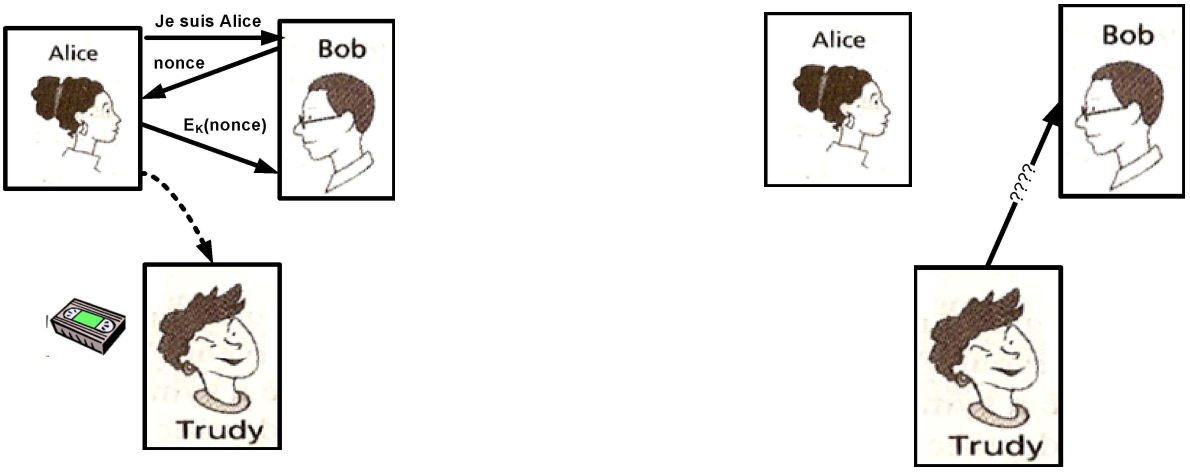

Figure 5 : Protocole d'authentification pda 5.0

Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 – Sécurité et Réseaux

TD/TP n°1

Exercice 2 : Services de sécurité

Trouvez la correspondance entre les services de sécurité (a à f) et les éléments proposés (1 à 6). Sur le texte, il suffira de traces des traits pour rejoindre la lettre et le chiffre associé.

a. Confidentialité	1. Message arrive intact
b. Intégrité d'un message	2. Etre sûr de l'origine du message
c. Autorisation	3. Envoyer un message privé
d. Authentification	4. Mot de passe
e. Non-répudiation	5. Vérifier le privilège de modifier un fichier
f. Contrôle d'accès	6. L'action ne peut plus être niée une fois effectuée

Exercice 3 : Substitution

La substitution suivante a été utilisée pour chiffrer un message confidentiel :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
R	H	N	Y	C	Q	F	U	W	A	J	O	Z	X	M	K	S	I	T	G	P	D	V	B	L

Déchiffrer ce message confidentiel et trouver le texte en clair :

PXGWCXTERPGZWCPVSPCYCPVGPORPIRT

Exercice 4: code de César

Pour protéger des données confidentielles, on utilise un système de chiffrement dit de César (qui consiste à décaler les lettres de l'alphabet d'une constante). Montrer qu'il est très aisé de déchiffrer le message suivant (écrit en français) :

PINIYRIZEYXTEWPEGLERHIPPI

Exercice 5 : cryptanalyse

On considère un système de chiffrement symétrique avec une clé de 64 bits. Vous cherchez à casser le système sans aucune connaissance de la clé : vous essayez de manière exhaustive toutes les clés. On suppose que vous avez à votre disposition un ordinateur puissant capable de tester une clé (et de dire si c'est la bonne !) en une picoseconde (pico=10^{-12}sec).

1. Combien de clés y a-t-il ? Combien de clés en moyenne essaierez-vous ?
2. Combien de temps en moyenne vous faudra-t-il pour trouver la bonne clé ?
3. Quelles solutions préconisez-vous pour lutter contre la cryptanalyse par force brute ?

Exercice 6 : conséquences des erreurs de transmission

On utilise un mécanisme de chiffrement par bloc de 128 bits.

1. Quelle sera la conséquence d'une erreur de transmission non détectée sur un bit lors du déchiffrement ?
2. Quelle sera la conséquence d'un ajout ou d'une perte d'un bit lors de la transmission ?

Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 – Sécurité et Réseaux

TD/TP n°1

Exercice 7 : Chiffrement de Vigenère

Vous avez intercepté ce message chiffré avec l'algorithme de Vigenère. Déchiffrer le message sachant que la clé est ″RPS″ :

CXFKTFKXGEKSLIDVUSZI

Exercice 8 : Auto-chiffrement

Déchiffrer le message texte suivant, sachant qu'il est chiffré avec l'algorithme d'auto-chiffrement et que la clé utilisée est ″RPS″.

CPUCYRKYCTLLSPCKXPSKEDVWHGUCRKCGNRDYFEEYW

Exercice 9 : Auto-chiffrement

Déchiffrer le message suivant, sachant qu'il est chiffré avec l'algorithme d'auto-chiffrement, et qu'il y a eu une indiscrétion (clé de chiffrement : ″DESCARTES″) :

OEKVEXTRGRRSILOERGZUEUHQVIHTVWJRQEEEEJUYLVZEHWRIYXNZWMFAAXUE

Exercice 10 : Chiffrement de PlayFair

Soit un système polyalphabétique qui utilise une matrice 5x5 avec un *mot-clé* suivi des autres lettres de l'alphabet (avec W et X dans la même case). Chaque groupe de 2 lettres est codé par la lettre à l'intersection de la ligne de la première et la colonne de la seconde puis à l'intersection de la ligne de la seconde et de la colonne de la première. Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de droite (avec rotation circulaire) ; Si les deux lettres tombent sur la même colonne, on remplace chacune par celle de dessous (avec rotation circulaire). En cas de lettre double et en cas de lettre unique (nombre total de lettres impair), une lettre ″parasite″ est insérée (W).
Étant donné qu'il y a eu une indiscrétion, vous connaissez la clé : ″Intelligent″.
Déchiffrer le message suivant :

IL OP IL NI IZ NE QP YO IQ XI IL FS LA TY

Exercice 11 : Chiffrement de Rail Fence

Rail Fence est une forme de transposition qui consiste à écrire les lettres en "Zig-Zag". Déchiffrer le message suivant, sachant que la clé est 3 (niveau=3).

LOSST ERLEE XRSEH MENIS NEDMU ETIRS TGUED OTSMA ETENB EANI

Exercice 12 : Chiffrement via transposition de la matrice

L'exemple ci-dessous utilise un système de chiffrement avec transposition de colonnes pour protéger des données confidentielles :

*MGCDECSSFTSENN*EEOELEATII*

Étant donné qu'il y a eu une indiscrétion, vous connaissez la clé 31542.
Déchiffrez le message : pour le chiffrement, on écrit le message en ligne et on le lit en colonnes.