Olivier MOUNEU
FIA-5

FOAD Sécurité des systèmes

Accès distants et TD SSH

Questions :

Comparaison en terme de complexitté et coût financier

Solution	Cout financier		Complexité		Protection des données	
	Note	Critères	Note	Critères	Note	Critères
Infrastrucuture dédiée	9	Besoin matériel très important (coût infrastructure) Temps et ressources nécessairesà la mise en place importants	10	Installation, paramétrage et assurer la sécurité des équipements et de l'infrastructure	9	Le transfert des données se limite à l'infrastructure dédiée, ce qui limite l'exposition à des attaques On pourrait ajouter des solutions de chiffrement pour prévenir du sniffing
Traversée libre du réseau internet	2	Réseau facilement accessible peu couteux à rejoindre	3	Peu de configuration nécessaire	0	Aucune protection des données n'est assurée que ce soit en confidentialité, intégrité et authentification des données
VPN IPSec	6	Nécessite matériels adaptés (routeurs) ou matériel supportant ce protocole	7	Plus complexe à mettre en place qu'un VPN SSL en terme de paramétrage VPN IPSec est plus adapté pour la connexion site-to-site	8	Avec le protocole IPSec (configurer avec protocole ESP), on rend totalement indéchiffrable le contenu du paquet (protocole utilisé et données), les adresses IP d'origine et de destination L'authentification, l'intégrité et la confidentialité sont assurées
VPN SSL	5	Un navigateur peut suffire à établir un tunnel VPN SSL Besoin seulement d'un routeur prenant en charge protocole VPN SSL (logiciel) pour fonctionner	6	Idéal pour mise en place d'un accès distant à des salariés Nécessite configuration SSL (certificats)	7	Permet d'authentifier des utilisateurs et permet aisin un contrôle plus fin dans la gestion des accès des utilisateurs

Le MAC ESP dans le paquet IPSec permet d'authentifier un message, on s'assure que le paquet reçu provient bien de la source attendue.

Le passage à l'échelle est la faculté d'un système à pouvoir changer de taille en fonction de l'évolution des besoins. Dans le cadre du partage des clés, IPSec prend cette contrainte en compte grâce au protocole Internet Key Exchange (IKE), IKE assure la Security Association. IKE prend en charge l'authentification grâce à l'échange de clé pré-partagées, signature ou clé publique (ex. certificat X.509). L'échange de clé symmétrique pour la communication entre les deux appareils se fait grâce à la méthode Diffie-Hellman.

TD

L'addition est donc équivalente à un OU exclusif (XOR) et la multiplication à un ET (AND).

Addition

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication

x	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Extention de corps de Galois $Z/2^m$