

### I. PRESENTATION

Ce document décrit la situation actuelle des implémentations IPsec les plus courantes. Certains points faibles ont déjà été rapportés comme les attaques brute force sur les clés partagées ou sur les authentications XAUTH. D'autre part des méthodes de fingerprinting efficaces sont applicables à la majorité des implémentations VPN comme l'utilisation des empreintes de backoff ou le lookup de vendor-id. Mais ce document met en avant certains comportements qui favorisent la mise en œuvre de ces attaques et permettent une identification précise des équipements utilisés alors qu'une protection est possible dans la majorité des cas.

Ce document décrit pourquoi la majorité des implémentations VPN souffrent d'une « vulnérabilité » de type information disclosure.

### II. INTRODUCTION

Les accès VPN vers les réseaux d'entreprise sont largement répandus. De nombreuses autres technologies répondent à la demande croissante de mobilité, comme les portails web de messagerie (OWA, eNotes ...), les VPN SSL ou encore BlackBerry. Néanmoins les accès IPsec depuis des postes nomades permettent souvent un accès privilégié à tout ou partie du réseau interne de l'entreprise. IPsec utilise IKE afin de négocier les différents paramètres de sécurité nécessaires à l'établissement d'un tunnel authentifié et chiffré.

Bien que cette méthode d'accès soit robuste, celle-ci présente certains risques. On peut classifier les risques en trois catégories principales :

- Attaque contre les données (cryptanalitique) → Vol de données
- Attaque contre les accès au réseau (preshared key crack, auth crack, postes clients) → Intrusion
- Fingerprinting (backoff, vendor id) → Reconnaissance, identification

On peut noter que les méthodes de fingerprinting donnent des résultats précis et surtout très fiable en comparaison avec d'autres techniques comme OS fingerprinting.

### III. ATTAQUES CONTRE LES DONNEES :

En ce qui concerne ce premier point, bien que l'élément ne soit pas négligeable, la mise en oeuvre d'une attaque est complexe. Il sera tout d'abord nécessaire de pouvoir observer la communication entre le client et le point d'accès VPN. De plus une attaque de type cryptanalytique devra être effectuée afin d'avoir accès aux données échangées, qui peuvent n'avoir que peu d'intérêt au final. Rappelons également que les clés de chiffrement sont changées sur une base régulière et que la puissance de calcul nécessaire reste aujourd'hui encore importante. C'est pourquoi l'utilisation d'AES en remplacement de 3DES n'est pas encore requise pour des raisons de sécurité (AES offre néanmoins de meilleures performances)

### IV. INTRUSIONS :

Les intrusions peuvent être effectuées grâce à diverses attaques.

#### i. Sécurité du poste client

La sécurité du poste client est le point le plus sensible. Il existe de nombreux moyens d'attaquer un poste client connecté directement à internet. Les efforts se concentrent donc sur la mise en place de diverses solutions visant à limiter le risque d'attaque sur le poste client via l'implémentation de firewall personnels, d'antivirus, de systèmes de détection d'intrusions, de systèmes de contrôle d'intégrité de donnée et la désactivation du split tunneling (la désactivation du split tunneling ne permet pas de protéger le réseau interne contre des attaques virales !).

Une configuration idéale serait le blocage de toute communication autre que le flux IPsec vers le gateway d'entreprise en utilisant des filtres bas niveaux ; le seul risque serait alors l'exploitation d'une faille applicative du client VPN ou du stack IP de la machine.

#### ii. Les failles ike

En mode agressif, mode requis pour les connexions VPN de type Dial-up, l'authentification repose sur un seul élément lorsque xauth n'est pas mis en oeuvre : le secret partagé. Bien entendu cela ne concerne pas les configurations IKE mettant en oeuvre des certificats, mais celles-ci ne sont pas encore majoritaires. Cette attaque a été reportée dans « PSK Cracking using IKE Aggressive Mode » de Michael Thumann et Enno Rey, ainsi que par Roy Hill de NTA monitor, auteur de ike-scan et psk-crack. De plus un document récapitulatif très complet a été publié par SANS début 2004. Ces différents documents sont disponibles sur [www.netsec.ch/ressources/wp](http://www.netsec.ch/ressources/wp) ; Les références des documents originaux sont indiquées en annexe.

Voici un petit rappel des faits ...

## Targeting IKE

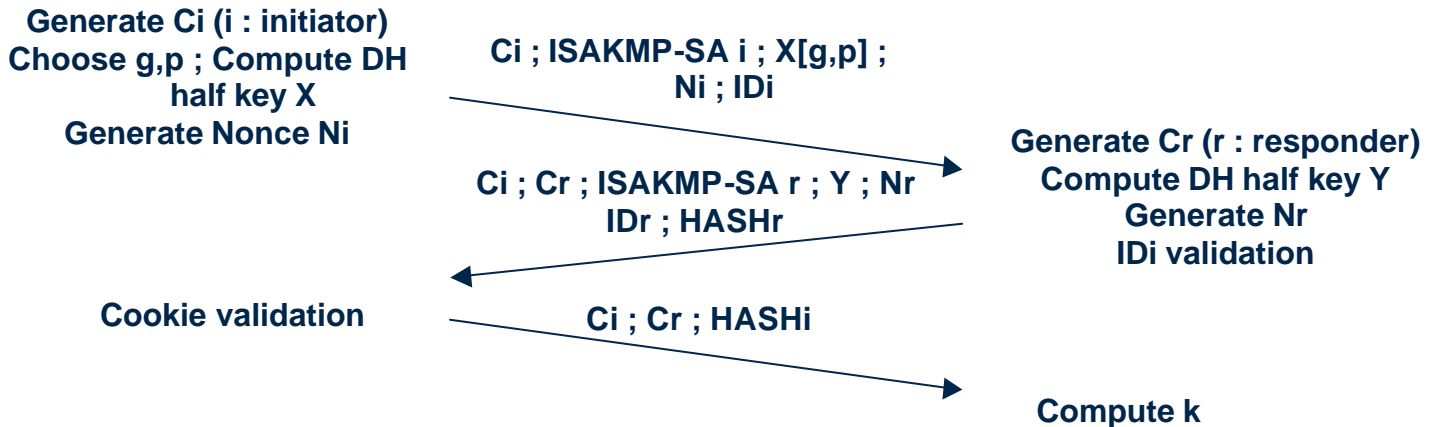
Florent TRUPHEME – florent@netsc.ch



### RAPPEL

L'observation du seul 2<sup>ème</sup> paquet de la phase 1 IKE permet d'obtenir toutes les informations nécessaires à la préparation d'une intrusion.

### Echange de la phase 1 IKE en mode agressif :



En effet le secret partagé est le paramètre principal de l'authentification de la machine cliente lors de l'établissement IKE; L'authentification est effectuée par la validation d'un « hash » (empreinte) de différents paramètres concaténés et le secret partagé est le seul paramètre non visible sur le réseau.

#### KEY GENERATION METHOD

( $k$  : DH generated key ; PSKEY : preshared key)

$SKEYID = HASH(PSKEY, N_i | N_r)$

#### HASH<sub>r</sub> VALUE GENERATION METHOD

$HASH_r : HASH(SKEYID, X | Y | C_r | C_i | ISA | ID_r)$

On voit tout de suite comment le secret partagé va être trouvé. Cette attaque est très bien décrite dans les documents cités en référence. En voici un bref rappel :

### PHASE 1

Le but ici est donc de trouver le secret partagé utilisé en effectuant une attaque de type brute force sur le hash échangé, connaissant les autres paramètres impliqués dans son calcul. Le temps nécessaire au crack de la clé dépend de sa taille, de sa complexité en terme de caractères utilisés ainsi que de la puissance de la machine utilisée. Mais les clés utilisées sont souvent générées manuellement (bien que la majorité des équipements proposent une méthode de génération de clé automatique) et il n'est pas rare que des suites de mots soient utilisées, associés à quelques chiffres ; Ou encore une phrase relativement longue mais une phrase au sens propre, attaquant par dictionnaire. Cette attaque ne laisse d'ailleurs que peu de

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



traces sur le gateway VPN ; Du moins l'événement «retransmission limit has been reached » attire que rarement l'attention des administrateurs.

Différents outils permettent d'effectuer ce genre d'attaque, notamment psk-crack de nta-monitor (\*nix, windows) ou cain (windows).

Notes :

Les caractères de brute force par défaut sont souvent les minuscules ainsi que les chiffres de 1 à 9. Il est donc bien requis d'utiliser des caractères spéciaux et d'avoir une longueur de clé d'au moins 30 caractères.

Si nous sommes chanceux et que la clé partagée peut être trouvée, il sera facile de négocier correctement la phase 1 avec le gateway puisque tous les autres paramètres de la négociation sont connus (adresse IP du gateway, identificateur IKE, vendor-id du client et du gateway)

D'ailleurs l'obtention des vendor-id permet d'identifier de manière précise les types d'équipements VPN utilisés. Les clients VPN de ces différents éditeurs ne sont pas difficiles à obtenir et ne poseront pas de problème d'incompatibilité.

Un autre paramètre intéressant de la phase 1 est la négociation de xauth qui est déterminé par le type d'authentification négocié : Type 3 pour clé partagée seulement ; Type 65001-65100 pour clé partagée + eXtended AUTHentication (XAUTH) ...

Une fois la phase 1 atteinte, la négociation de la phase 2 peut commencer.

### PHASE 2

1)  
La voie facile ... Le type d'authentification négociée est le type 3. Mise à part l'utilisation du bon domaine d'encryption (qui n'est pas forcément synonyme d'échec de la phase2 si non identiques), cette phase ne présente aucune autre opération que la génération des SAs IPsec. Le domaine d'encryption est généralement composé de AnyIP (255.255.255.255/32) comme identificateur local et un réseau privé de type 192.168.1.0/24 ou 10.x ou 172 ...

Des tentatives de négociation espacées dans le temps resteront peu détectables, surtout si elles sont effectuées en portant attention au fuseau horaire du gateway VPN afin que la connexion de l'utilisateur identifié par notre id IKE soit plausible.

2)  
Authentification par usr/pwd statique ... Une attaque par brute force peut être tentée mais sa réalisation pose plusieurs problèmes : Les gateway VPN ne renverront pas d'information permettant de déterminer si un nom d'utilisateur existe ou non (Bien que certains produits le permettent). Une attaque par brute force ne passera pas inaperçue dans les logs du gateway.

3)  
Authentification pas usr/pwd dynamiques ... Ce type de configuration ne peut être attaqué de cette manière.

## Targeting IKE

Florent TRUPHEME – florent@netsec.ch



Notons que si xauth est utilisé, la réussite de l'attaque est complètement aléatoire et peu probable. Attention peut être portée à l'identificateur ike puisque celui-ci peut reprendre le nom d'utilisateur xauth ; En effet pour la majorité des éditeurs, si les utilisateurs xauth sont définis localement, la configuration est assimilée à celle de l'utilisateur ike et le nom reste le même.

Il s'agissait notamment du comportement de Firewall-1, vulnérabilité relevée par Roy Hill. Les détails sont fournis à l'adresse suivante : <http://www.nta-monitor.co.uk/news/checkpoint-tech.htm>. Mais il existe d'autre équipement qui renvoient le message INVALID-ID-INFORMATION lorsqu'un mauvais identificateur est reçu. Bien que la RFC préconise l'envoi de ce message, on peut se demander du bien fondé de son envoi dans certain cas.

### V. IDENTIFICATION

Trop d'éditeurs ne proposent pas d'implémentations suffisamment strictes en terme de négociation. Ces comportements permettent une reconnaissance efficace des systèmes utilisés, facilitant l'exploitation de failles connus (ou à venir) de manière ciblée. De plus ces attaques peuvent être facilement effectuées à distance, avec des résultats très précis en terme de fingerprinting.

#### i. Le mode agressif :

L'attaque contre le secret partagé décrite ci-dessus implique que le gateway VPN réponde à la requête IKE effectuée par l'attaquant. Sur ce point, tous les éditeurs ne proposent pas un comportement commun, rendant plus ou moins facile l'attaque, même impossible à distance dans certains cas :

Rappelons que les identificateurs utilisés sont transmis en clair, rendant possible l'acquisition d'un identificateur ike valide en observant une négociation légitime. Cette méthode par sniffing est rendue plus facile par la forte émergence des réseaux wireless ouverts dans les aéroports, gares, restaurants, hotels ... et c'est de là que certains utilisateurs nomades vont se connecter. Mais ces cas ne représentent pas la majorité des attaques qui souvent sont effectuées à distance.

Lors d'une attaque à distance, l'attaquant n'a pas connaissance des id valides. Si le gateway VPN ne répond pas à sa requête, celui-ci n'aura pas l'occasion de craquer le secret partagé et ne pourra pas non plus obtenir de vendor-id, permettant une identification souvent précise de l'équipement.

Lors d'une négociation en mode agressif, l'id est envoyé dans le premier paquet de la phase 1, et quel que soit le mode d'authentification (secret partagé, digital signature, encryption). De ce fait, si le gateway VPN ne reconnaît pas l'id IKE envoyé par l'initiateur, celui-ci ne devrait pas répondre. Ce comportement permettrait d'éviter la majorité des attaques dont l'auteur n'a pas pu identifier un id valable au préalable.

Tous les gateway devraient donc ne pas répondre à des requêtes IKE en mode agressif lorsque l'id reçu n'est pas reconnu. Mais tous les éditeurs n'appliquent pas cette mesure de protection.

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



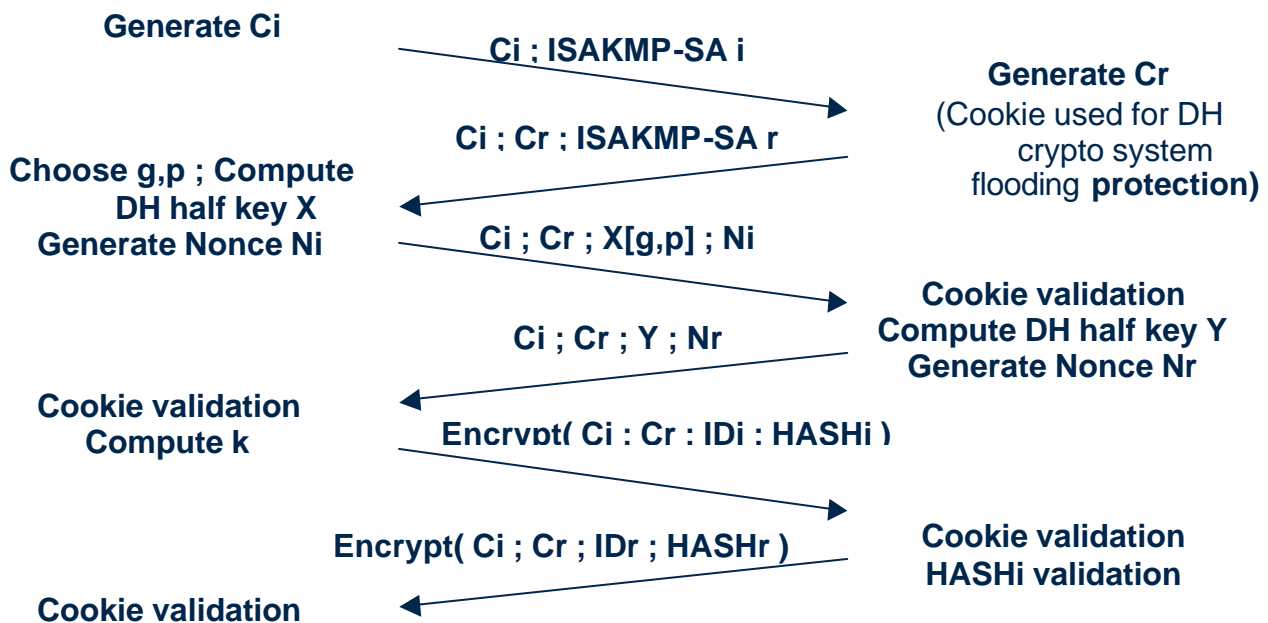
### ii. Le mode main

En ce qui concerne le mode main, on se rend compte que tous les gateway VPN peuvent être identifiés de manière précise par deux méthodes connues, présentées par Roy Hills et utilisées par ike-scan, à savoir le backoff et le vendor-id.

Le backoff permet une identification de l'éditeur alors que le vendor id permet souvent d'identifier en plus de l'éditeur, une version précise de l'application !

Mais connaissant l'attaque, il semble qu'une analyse du comportement n'ait pas été effectuée de manière critique envers les éditeurs de solutions VPN mais que ce comportement a été considéré comme une fatalité du protocole, ce qui n'est pas le cas. En effet, lors d'une négociation en mode main, un gateway VPN ne devrait pas répondre à une requête IKE lorsque l'adresse IP de l'initiateur n'est pas reconnue et qu'un secret partagé est utilisé.

Afin de comprendre, regardons l'échange de la phase 1 en mode main (PSK) :



On voit que les paquets 5 et 6 sont chiffrés ; Or la clé de chiffrement est dérivée depuis, entre autres, le secret partagé. Comme aucun identificateur n'est transmis dans les paquets 1 à 4, le seul moyen pour le gateway VPN de connaître le secret partagé qu'il doit utiliser pour dériver les clés est l'adresse IP de l'initiateur IKE.

Rappelons que le seul 2<sup>ème</sup> paquet de la phase 1 permet d'identifier de manière précise l'équipement VPN. On peut donc dire que la majorité des implémentations VPN souffrent d'une « vulnérabilité » de

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



type information disclosure. (Le débat sur le terme vulnérabilité n'est pas intéressant ; On a bien un comportement contraire aux règles basiques de sécurité).

L'attaquant pourrait utiliser une requête avec une authentification de type public key (signature ou encryption), mode pour lequel ce raisonnement n'est pas applicable. Néanmoins, si une telle méthode n'est pas supportée (configurée) sur le gateway VPN, la réponse renvoyée par le gateway sera de type NO-PROPOSAL-CHOSEN et ni l'empreinte de backoff, ni le vendor id pourront alors être obtenus.

### iii. Conclusion

On se rend compte ici que les implémentations IKE permettent une identification simple et très fiable depuis internet. Ce comportement n'est pas techniquement justifié, mais s'explique peut être par l'absence de recommandation sur ce point dans les RFCs liées à IKE.

Pour le mode agressif, aucun gateway VPN ne devrait négocier avec un client dont l'identificateur n'est pas reconnu, et ce quel que soit le mode d'authentification.

Pour le mode main, étrangement, seul le mode d'authentification PSK peut se protéger contre cette attaque, une implémentation utilisant un système de clés publiques reste vulnérable.

Il est donc important que les éditeurs prennent en compte le risque d'identification et corrigent ce comportement. C'est dans ce but que ce document a été rédigé et c'est également dans ce but que NETwork Security Consortium publie de nouvelles signatures de vendor-id manquantes dans les fichiers de signatures actuels.

Merci d'envoyer vos commentaires/questions à l'adresse suivante : [wp@netsc.ch](mailto:wp@netsc.ch)

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



### VI. REFERENCES

D.Harkins and D.Carrel, RFC2409 “The Internet Key Exchange (IKE)”,  
(<http://www.ietf.org/rfc/rfc2409.txt>)

R.Hills, “NTA Monitor UDP Backoff Pattern Fingerprinting WhitePaper”  
(<http://www.nta-monitor.com/ike-scan/whitepaper.pdf> ,January2003)

Michael Thumann and Enno Rey ; PSK Cracking using IKE Aggressive Mode  
(<http://www.ernw.de/download/pskattack.pdf>)

John Pliam: ”Authentication Vulnerabilities in IKE and Xauth with Weak Pre-shared key  
(<http://www.ima.umn.edu/~pliam/xauth/> )