

# Targeting IKE

Florent TRUPHEME – florent@netsc.ch



## I. PRESENTATION

This document describes the actual situation of most deployed IPsec implementation. Many points have already been releases in earlier documents like pre-shared key cracking attack, xauth password brute force cracking ... Also accurate fingerprinting methods have been discussed, based on IKE backoff and vendor id lookup.

But the key point of this document is the analyses of the behavior of most VPN gate that make easier attacks enounced before.

This document explain why major VPN vendor are suffer of an information leakage “vulnerability” that allow very accurate fingerprinting form internet without particular knowledge of the service offered.

## II. INTRODUCTION

IPsec VPN accesses to the enterprise network are largely implemented. Many other technologies answer to the actual mobility requirement like webmail portals, SSL VPN or some BlackBerry. However, IP often allow privileged access to the network with less or no service restriction. IKE is often the protocol used to negociate IPsec tunnels ; It allow authentication, key exchange, some attack protection by relying on several integrated protocols.

Even if IKE is robust i such way, some flow exists, that can be classified in the following way :

- Attack against data (cryptanalitic) → Stole of data
- Attack against network access (preshared key crack, auth crack, clients host) → Intrusion
- Fingerprinting (backoff, vendor id) → Identification

We can note that fingerprinting method give very accurate result with ike gateway, far bettern than OS fingerprinting !

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



### III. ATTAQUES CONTRE LES DONNEES :

Concerning this first point, it is not a big issue for us because of the complexity of attack. First, IPsec traffic has to be sniffed from network. Plus cryptanalytic attacks consume many resources and there is no guarantee that the data obtained have a bit of interest.

Additionally, encryption keys are changed regularly during data exchange. That's why the question 3DES or AES do not make sense at this time except for performance reason.

### IV. INTRUSIONS :

Several attacks could lead to intrusion :

#### i. Client host security

Client host security is the most sensible element. There is many ways to attack client host that is directly connected to the Internet. That's why there is a race to put all possible software on labtop like personal firewall, HIDS, antivirus, integrity checker program ... We also often hear about split tunneling, but keep in mind that split tunneling (configuration that avoid having both connections possible to/from the internet and to/from the enterprise network at the same time) do not avoid virus propagation !

It seems that the best configuration for such host is to have no other communication that IPsec tunnel to the enterprise network ; Forcing the use of secured enterprise internet gateway for any access to the web. The only risk would then be a flow in the VPN client application or in the client OS TCP/IP stack.

#### ii. IKE flow

With aggressive mode, authentication only relies on the pre-shared key (abstract of xauth). Sure it did not concern certificate-based implementation, but there are not so many deployed at this time. This attack has already been reported in «PSK Cracking using IKE Aggressive Mode » de Michael Thumann et Enno Rey, and also by Roy Hill form NTA monitor, ike-scan et psk-crack author. Plus a very complete document that resume all attack and theory has been released by SANS in 2004. For convenience, all this documents are directly available from [www.netsc.ch/ressources/wp](http://www.netsc.ch/ressources/wp).

Here is a quick resume ...

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



### RAPPEL

The observations of the only 2nd IKE packet in an aggressive mode exchange allow obtaining all required information to start the attack.

### IKE aggressive mode exchange :

<b>Generate Ci (i : initiator)</b>		
<b>Choose g,p ; Compute DH half key X</b>	<b>Ci ; ISAKMP-SA i ; X[g,p] ; Ni ; IDi</b>	
<b>Generate Nonce Ni</b>		
	<b>Ci ; Cr ; ISAKMP-SA r ; Y ; Nr ; IDr ; HASHr</b>	<b>Generate Cr (r : responder)</b>
		<b>Compute DH half key Y</b>
		<b>Generate Nr</b>
		<b>IDi validation</b>
<b>Cookie validation</b>	<b>Ci ; Cr ; HASHi</b>	
		<b>Compute k</b>

The pre-shared key is THE parameter for client authentication during ISAKMP SA establishment. Authentication is based on the HASH validation, that was computed with several parameters but that are all visible on network except the PSK.

And when we look at the key generation method :

#### KEY GENERATION METHOD

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

SKEYID = HASH (PSKEY, Ni | Nr)

#### HASHr VALUE GENERATION METHOD

HASHr : HASH (SKEYID, X | Y | Cr | Ci | ISA | IDr)

Now we imagine immediately how we can find the famous pre-shared key ...

### PHASE 1

The goal here is to find the pre-shared key used by load a brute force attack on the pre-shared key. The time needed to crack such key depends of the key and of the character used in it. However the key are often manually generated by human, and unfortunately many time with human logic behind : Only basic character set are used (lower case letter and some number), the psk length is poor and some time very long but composed with nice words ... A piece of cake for dictionary attack.

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



Also attack against IKE negotiation does not let not many traces in the log and “retransmission has been reached” message unfortunately does not impact administrators.

Several tools allow such cracking operation on psk. The two best known are psk-crack de nta-monitor (\*nix, windows) and cain (windows).

Note :

Default brute force characters set are often lower case and number. So it is a big step to use a minimum pre-shared length of 30 char and use special character.

If we are lucky and that pre-shared key can be recovered, it will be easy to establish phase1 SA.

Also at this point, vendor ids have already been obtained, giving opportunity to identify the gateway type. VPN client of various editors can be easily found ; This way interoperability issue are far behind.

Another interesting parameter of the phase1 negotiation is xauth, which is determined by negotiated authentication type : Type 3 for pre-shared key only ; Type 65001-65010 for pre-shared + eXtended AUTHentication (XAUTH) ...

Once phase1 is established, phase2 negotiation can start.

### PHASE 2

1)  
The easy way... The negotiated authentication type is 3 (pre-shared only). Except the use of the good encryption domain (assuming the this is a critical negotiation parameter, which is not the case for some vendors), there are no other operations than key generation, and algorithm negotiation. For the encryption domain, the remote part should be a private IP range.

2)  
XAUTH used with static uid/pwd ... Brute force attack can be tried but success is really unsure even if editors do not follow best security practices on this point. Check the last NTA-Monitor white paper ...

Additionally such attack will be noisy in log.

3)  
Authentication with dynamic usr/pwd ... This type of configuration is not concerned by such attack. Only vulnerabilities in the xauth process could allow intrusion.

### V. IDENTIFICATION

Too many VPN editors do not propose IKE implementation strict enough in term of negotiation. This behavior allows very easy fingerprinting activity, from the Internet, without any particular knowledge of any parameter requirement. This leads to information leakage, which should be avoided by security vendor.

#### i. Aggressive mode :

The pre-shared key attack described above rely on the fact that VPN gateway answer to the IKE request of attacker. On this point, not every vendor offers the same level of protection against such attack. Some of them do not protect against attack from Internet (without valid id).

The following element should be taking into account concerning aggressive mode negotiations. All parameters involved in the negotiation are passed in clear text on the wire. This allow attacker to easily sniff valid ike id, especially now that many open wifi access are offered in airport, restaurant ... Place from which potential VPN users will start negociating. However this is not representative of the total number of attacks, which are often loaded from the Internet.

When trying to scan ike gateway, attacker do not know any valid ike id. If the VPN gateway does not respond to this request, attacker would be unable to get vendor id and then identify the presence of a VPN gateway and worse, what is the VPN vendor.

With aggressive mode negotiations, the id is always present in the first packet sent by initiator ; This is valid for any authentication type. Then if the received ike id is not successfully lookup in the VPN gateway internal ISAKMP peer list, no response must be sent back to the initiator !

All VPN gateways MUST not respond to ike aggressive mode negotiation request until ike id has been received and validated.

#### ii. main mode

Concerning main mode, we quickly saw that majority of VPN vendor can actually be fingerprinted with two method reported by Roy Hills and used by ike-scan, which are backoff and vendor id lookup.

Backoff allow editor identification and vendor id often allow to identify a specific version of the running software version as well as the editor !

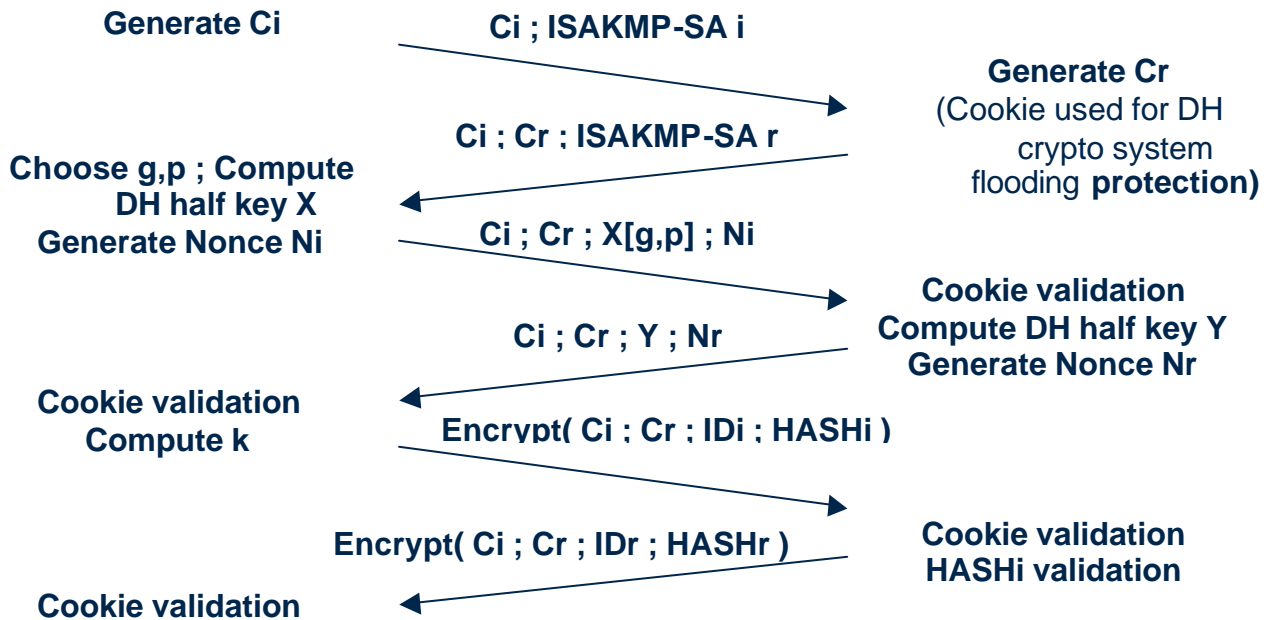
Even if this attack has been reported for a long time, it seems that no analyses point on editor responsibilities but that this behavior is only tied to IKE protocol, which is a wrong assessment. When speaking of main mode negotiation with pre-shared key, VPN gate should not answer to initiator if the source IP address is not known.

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



To better understand, we have to take a look at the phase 1 exchange (Main mode with pre-shared key).



We can see that packet #5 and #6 are encrypted ; However the encryption key is derived from (but not only) the pre-shared key. Since no identification data was sent before the exchange of these two packets, the only way for the VPN gateway to know what pre-shared key have to be used is the source IP address of the IKE initiator.

Be aware that the only 2<sup>nd</sup> packet allows fingerprinting with both backoff and vendor-id. Then we could claim that answering to main mode request when proposal specify PSK authentication type and source IP address is not know is a flow !

The question “vulnerability or not” is not the key point here. All VPN vendors that accept to negotiate with unknown IP offer information disclosure to any attacker on the Internet.

Attacker could use proposal with public key encryption as authentication type but if such authentication type is not supported or configured on the VPN gateway, the answer will be NO-PROPOSAL-CHOSEN, which will not allow attacker to identify gateway vendor and version.

### iii. Conclusion

We saw here that many IKE implementations allow very accurate fingerprinting without specific knowledge of the environment. This behavior leads to scan from Internet ; Scan that could allow mapping of exact version of gateway device, which will be sometime the enterprise firewall. The attackers just have to wait release of vulnerability on such version.

## Targeting IKE

Florent TRUPHEME – florent@netsc.ch



Concerning aggressive mode, all authentication modes can be protected against such scan with no valid ID.

Concerning main mode, only pre-shared key authentication can be protected against such fingerprinting activity. Public key encryption authentication modes are still vulnerable since the ike initiator IP address can be dynamic with such authentication mode.

Vendor should take this into account and revise IKE implementation to only negotiate with authorized peer. Some statement on this should have been found in the RFC.

Administrators should deploy only aggressive mode with public key encryption authentication. For main mode with public key encryption, the flow is really tied to IKE. However PSK is the only main mode authentication type that could be protected against fingerprinting.

To help vendors to take that issue into account, NETwork Security Consortium will try to add news entries to the ike-scan backoff pattern file and vendor-id pattern file.

Thanks to send any comments to : [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/> )