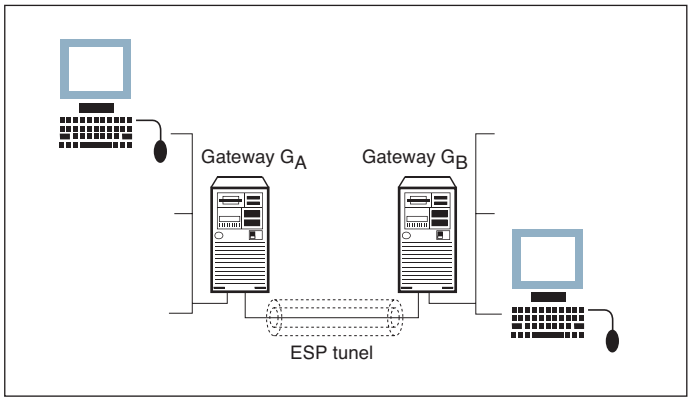
Závažný průlom do virtuálních privátních sítí a protokolu IPSec (1)

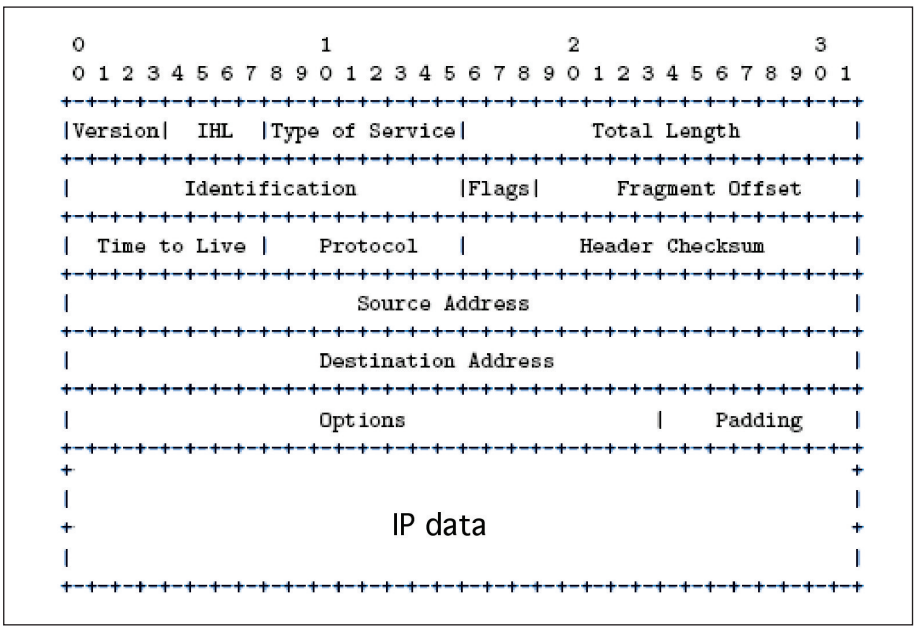
Virtuální privátní sítě (VPN) založené na protokolu IPSec jsou nemyslitelnou součástí internetu. Šetří ohromné náklady, které by firmy a jednotlivci museli vynaložit, kdyby nemohli pomocí nich vzdáleně a přitom bezpečně komunikovat. Až dosud VPN tento problém řešily šifrováním. Teď jsou vážně ohroženy. Ukážeme prakticky proveditelný útok, jehož výsledkem je kompletní dešifrovaná komunikace. Útočník nepotřebuje žádnou významnou výpočetní kapacitu ani čas. Luštění provádějí stroje, kterých se to týká, bezděčně samy! Jediné, co útočník potřebuje, je manipulovat se zašifrovanými daty na kanálu. Uvádíme příčinu tohoto stavu a účinnou obranu.



Obr. 1 VPN – šifrované spojení pomocí IPSec (ESP tunel)

Princip útoku

Tentokrát se nejedná o žádné chyby administrátorů ani programátorů. Kde je chyba, když IPSec používá kvalitní šifry? Zrádcem je kupodivu protokol IP na přijímací straně, který je příliš upovídaný. Chytrému útočníkovi na komunikačním kanálu, který se ho šikovně ptá, nakonec všechna otevřená data bezděčně vyzradí a odšifruje. A to i přesto, že odpovědi IP-protokolu jsou také šifrované protokolem IPSec. IPSec proti tomu nemůže žádným způsobem zasáhnout, neboť jen přenáší (šifruje) data, která jsou mu předávána. Pokud je některá ze stran vyzradí, nemůže to nijak ovlivnit. Avšak „upovídanost“ protokolu IP je jeho základní vlastností, kterou nemůžeme zakázat, aniž bychom omezili funkčnost internetu. Lze však poměrně jednoduše v zařízeních IPSec zakázat použití šifrování bez autentizace. To zamezí manipulacím se šifrovanými daty, což je zde základní nástroj útočníka.



Obr. 2 Obsah IP-paketu = (IP-hlavička, data), bity jsou číslované od 0 do 31

Souhrnné údaje o útoku

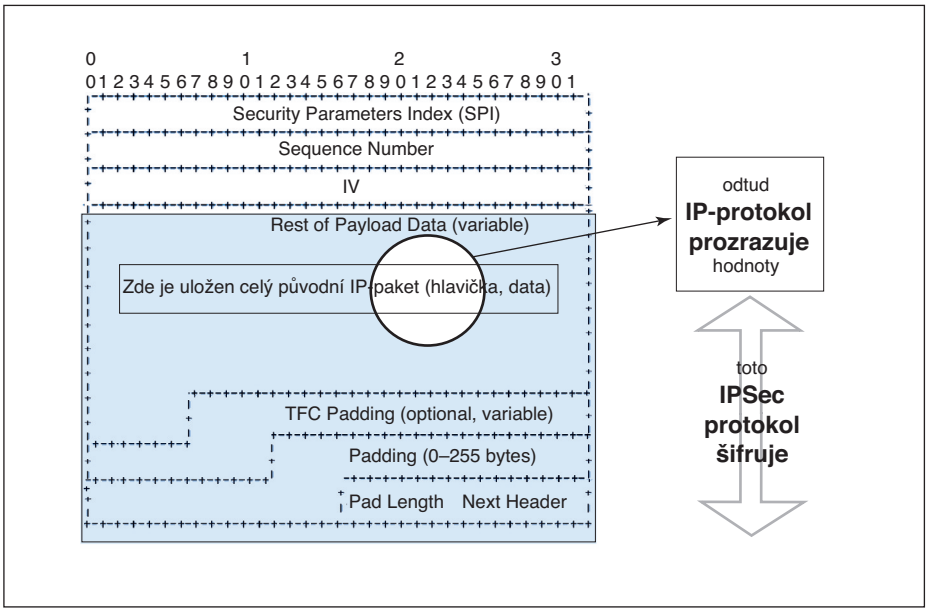
- útok je prakticky proveditelný a použitelný na všechna zařízení IPSec, která jsou realizována podle platných standardů IPSec (starých RFC 2401-12 i nových RFC 4301-4309)
- útok byl experimentálně ověřen na konkrétní VPN (Open Solaris), dešifrování jednoho bloku (8 nebo 16 bajtů) zašifrované komunikace trvá desítky sekund
- nezáleží na použité blokové šifře (AES, TripleDES, v CBC modu)
- platí pro tunelový i transportní modus
- odhaluje i maskování délek paketů (zakrývání toku dat)

Princip útoku si ukážeme na tunelovém modu se šifrováním bez autentizace (*obr. 1*). Host H_A v lokální síti zde posílá IP-paket hostovi H_B ve vzdálené lokální síti. Obsah tohoto paketu (podle RFC 791) vidíme na *obr. 2*. IPSec před něj předřadí svoji hlavičku (SPI, seq. number, IV) a za něj umístí patičku (TFC padding, padding, Pad Length (PL), Next Header (NH)) a celý původní IP-paket včetně své patičky zašifruje pomocí IV a dané blokové šifry (v modu CBC) (*obr. 3*).

Mistrně využitá „upovídanost“ protokolu IP

K demonstraci ideje útoku použijeme položku „Time to Live (TTL)“ v hlaviče IP. Pomocí ní se v internetu například zajišťuje, aby pakety sítí nebloudily po příliš dlouhých cestách. Vezměme si nešifrovaný paket. Při sestavování cesty nastaví zdroj jeho položku TTL (obvykle) na hodnotu 64, a když se paket vrátí zpět jako nedoručený, tak jasně vidí, že na své cestě překonával příliš mnoho směrovačů. Každý router totiž při průchodu takového IP-paketu (pokud není určen jemu) snižuje položku TTL o jedničku, a když nastane TTL=0, paket se zahodí a zpět k příjemci je o tom v řídicím protokolu ICMP vyslána zpráva. Tyto „testovací“ pakety jsou zjevně velmi důležité pro chod internetu. Při definici IP-protokolu se nezdálo nijak divné, že by tato vlastnost mohla nějakým způsobem později škodit. A přesto. Přidejme nyní do cesty ony dvě brány na *obr. 1*, které šifrují celý původní průchozí paket. Předpokládejme pro ilustraci, že TTL byla při odesílání paketu rovna 1. Brána G_A původní paket (viz *obr. 1*) obalí novou (šifrovací) hlavičkou protokolu IPSec (ESP) a zašifruje ho jako payload (viz *obr. 2*). Brána G_B ho přijme, odšifruje, zjistí, zda jsou správné hodnoty Padding, PL, NH, a pokud ano (pokud ne, nic nevyzrazuje a paket zahodí), odstraní ESP hlavičku a patičku a předá původní vnitřní paket protokolu IP (mi-

mochodem, že se ten paket má předat protokolu IP, říká položka NH s hodnotou 4). IP-protokol zjistí, že není určen pro lokální síť, ale jiný router, a tak sníží pole TTL o jednu a za normálních okolností ho pošle dalšímu routeru. V našem případě však hodnota TTL je nula, což znamená, že paket se potuloval příliš dlouho internetem a nedospěl do cíle. Proto IP-protokol vystaví služební zprávu (tzv. ICMP zpráva), že čas TTL vypršel („TTL exceed“), a pošle ji zpět zdroji, který původní paket odeslal. Podstatné je, že tato zpráva je velmi krátká – její paket má pouze sedm bloků. Paket je zašifrován branou G_B a putuje do brány G_A. Pokud útočník vidí, že G_B odpovídá G_A zprávou, která má sedm bloků, nepochybně ví, že obsah původního pole TTL byl jednička. To, co jsme právě popsali, je postranní kanál, kterým IP-protokol na přijímací straně útočníkovi sděluje, jaká je hodnota specifického bajtu otevřeného textu! Tuto ukázku jsme uvedli pro ilustraci principu luštění a aby bylo vidět, že „upovídanost“ protokolu IP je přirozená a nezbytná, ale že současně prozrazuje něco, co mělo být utajeno. Principem je, že obsah bajtu TTL byl šifrován protokolem IPSec a protokol IP ho vyzradil. Zdá se, že takové vyzrazení nikomu nevadí – pole TTL je nezajímavé. V příštím čísle si ukážeme, jak jednoduchou aplikací tohoto principu odhalit přímo data. Připomeňme, že postranní kanály jsou nejúčinnější kryptoanalytickou metodou dneška a kryptoanalytici pomocí nich umí takříkajíc „zničehož nic uplést bič“. K reálnému útoku na IPSec je použito několik postranních kanálů.



Obr. 3 Obsah ESP paketu, který prochází mezi G_A a G_B, a princip luštění

Závěr

V klíčové práci [1] byl ukázán velmi praktický útok na šifrovací protokol IPSec. V důsledku toho bude většina šifrátorů IP neúčinná, pokud nebude kromě šifrování používat také autentizaci. Velmi doporučujeme všem správcům takových zařízení, aby co nejdříve své sítě překonfigurovali. Jsou-li však k šifrování IP-kanálů použity speciální šifrátory, které neumožňují zapnout také autentizaci přenášených dat, bude lépe je odevzdat jako druhotnou surovinu do šrotu. Šifrování bez autentizace by mělo být od nynějška v IPSec přísně zakázáno.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Degabriele, J. P., Paterson, K. G.: Attacking the IPSec Standards in Encryption-only Configurations, Crypt. ePrint Archive Rep. 2007/125, http://eprint.iacr.org/2007/125.pdf