GCM: Nové zabezpečení IPSec

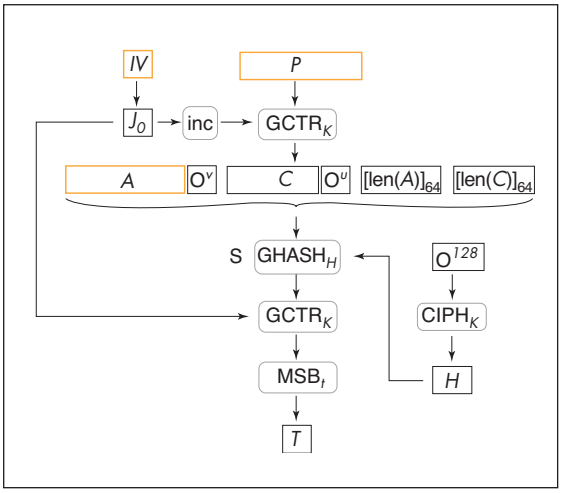
Velkým nešvarem současných implementací protokolů IPSec je použití šifrování bez autentizace. To je častá konfigurace zařízení a programů, která IPSec realizují, protože šifrování paketů připadá administrátorům jako dostatečná ochrana, a autentizace se zdá být nadbytečnou a zdržující. To je veliký omyl, k němuž se v Kryptologii pro praxi ještě vrátíme. Autentizační kódy byly donedávna velmi výpočetně náročné, stejně jako vlastní šifrování paketů. V článku popisujeme novou normu a metodu, která definuje velmi rychlý autentizační kód společně se šifrováním paketů.

Galois/Counter Mode

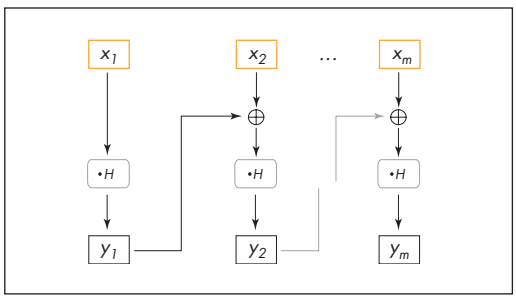
Použití nového autentizačního kódu umožňuje šifrovat a autentizovat pakety až do rychlosti 10 Gb/s v hardware a je také velmi vhodné pro SW implementaci. Šifrování probíhá pomocí blokové šifry (doporučována *AES*) v čítačovém módu (viz ST 9/2003) a autentizace pomocí autentizačního kódu založeného na rychlém násobení v konečném tělese GF(2^{128}). Obě techniky popisuje dokument SP 800-38D amerického úřadu NIST [1]. Tyto speciální publikace (SP) mají statut standardů, a proto uvedená metoda byla rychle rozpracována, například do RFC 4106 [2].

Šifrování a autentizace paralelně

Metodu nejlépe popisuje *obr. 1.* Blok dat (*P* jako Payload) je zašifrován pomocí blokové šifry *AES* (s klíčem *K*, který sdílejí obě komunikující strany) v čítačovém módu (algoritmus $GCTR_K$, viz dále) na stejně dlouhý šifrový text (*C*) a ten, tak jak vzniká, může paralelně vstupovat do výpočtu zabezpečovacího kódu $GHASH_H$. Velkou předností této metody je, že kromě šifrového textu do zabezpečovacího kódu mohou vstupovat i otevřená data návěští *A* (Autentizovaná data), která se nešifrují (nemusí šifrovat). Jde zejména o hlavičku paketu, která obsahuje IP-adresy, číslo paketu apod. Tím je umožněna ochrana proti modifikaci i těchto otevřených dat, aniž by se musela šifrovat. Do výpočtu zabezpečovacího kódu (tag *T*) vstupují tedy tato otevřená data, šifrový text dat (obojí definovaně doplněné nulovými bity na bloky délky 128 bitů) a nakonec ještě délky těchto dvou bloků (64bitová binární čísla len(*A*) a len(*C*)) jako opatření proti dalším útokům. Z celého tohoto řetězce, jehož délka je násobkem 128 bitů, se vypočte zabezpečovací kód (signature *S*), který se zašifruje (pomocí čítačového módu) a vybere se z něho požadovaný počet bajtů (*t*) do zabezpečovacího řetězce *T* (označovaného jako *ICV*, Integrity Check Value). Ten se pak přenáší společně se šifrovaným paketem příjemci. Činnost příjemce je zřejmá – nejprve odšifruje hodnotu *T* a získá signaturu. Pak signaturu vypočte z obdržených dat *A* a *C* a porovná je. Pokud souhlasí, paket nebyl narušen a může být odšifrován. Ve skutečnosti probíhá odšifrování průběžně tak, jak jsou data přijímána paralelně s výpočtem *S*. Po kontrole S se pak data prohlásí za platná nebo se zahodí.



Obr. 1 Šifrování a autentizace pomocí GCM



Obr. 2 Rychlý zabezpečovací kód GHASH

Výpočet zabezpečovacího kódu

Výpočet zabezpečovacího kódu opět nejlépe ilustruje *obr. 2.* Vstupem procedury je posloupnost 128bitových bloků *X* a výstupem je poslední 128bitový blok *Y*. Konstanta *H*, kterou se násobí v příslušném Galoisově tělese, je tajná a je odvozena od klíče *K*. Na rychlou realizaci násobení existují odpovídající algoritmy, ve skutečnosti je zabezpečovací kód lineárním kódem s konstantní maticí, která je ovšem mohutná, tajná a závislá na klíči *K*, tedy něco jako tajný kód *CRC* o délce 128 bitů.

Šifrování pomocí GCTRK

Popis algoritmu šifrování v čítačovém módu *GCTRK* je jednoduchý. Počáteční hodnota registru J_0 vzniká z inicializačního vektoru *IV* (ten se vybírá z hlavičky paketu) určitou jednoznačnou transformací (prodloužení nebo kryptografické zkrácení, detaily nejsou tak podstatné, viz literatura). Potom se zašifruje blokovou šifrou (*AES*) s klíčem *K* a výsledné heslo zašifruje (operací xor) signaturu *S*. Potom se registr J_0 inkrementuje (pouze jeho dolní 32bitové slovo, modulo 2^{32}) a tato hodnota po průchodu blokovou šifrou tvoří heslo k zašifrování prvního bloku otevřeného textu (payloadu *P*). Další blok *P* se šifruje blokem hesla, který odpovídá další inkrementované hodnotě registru J_0, atd.

Bezpečnost

Základní podmínkou bezpečnosti GCM je, aby klíč *K* byl generován náhodně a nikdy se nestalo, že by pro tentýž klíč byla použita stejná inicializační hodnota *IV*. Z ní se totiž generuje heslo pro čítačový modus, které by bylo v tomto případě stejné, což se nesmí stát. Hodnota *IV* musí být proto volena také náhodně a nejlépe v rámci jednoho platného klíče je vhodné kontrolovat, že použité hodnoty *IV* byly různé. Ještě lépe je klíče generovat náhodně a v rámci jednoho klíče použít jen jednu hodnotu *IV*.

V literatuře naleznete detaily rychlého algoritmu výpočtu zabezpečovacího kódu, testovací hodnoty a další podrobnosti.

Závěr

Po delší době je k dispozici neobtěžující zabezpečovací kód, který umožňuje šifrování a autentizaci pro vysokorychlostní přenosy. Není sice příliš silný, ale pro výše uvedené účely se jeví NIST jako dostatečný. Příslušná funkce $GHASH_H$ se však nesmí používat jako hašovací funkce pro žádné jiné účely.

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

LITERATURA

[1] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication, NIST Special Publication 800-38D, DRAFT (April, 2006)

[2] RFC 4106: The Use of Galois/Counter Mode (GCM) in Ipsec Encapsulation Security Payload (ESP)