Internet Protocol Security – IPSec, zabezpečené připojení

Pozor, útok! (4. díl)

V již čtvrtém povídání o bezpečnosti na internetu vám přiblížíme množinu bezpečnostních protokolů Internet Protocol Security (IPSec).

V předchozích dílech seriálu „Pozor, útok!“, zaměřených na zajištění bezpečné výměny informací prostřednictvím internetu, jste se měli možnost seznámit s několika bezpečnostními protokoly. Nyní vám opět přinášíme nové informace z oblasti zabezpečení přenosu informací pomocí bezpečnostních protokolů a standardů: seznámíme vás s množinou bezpečnostních protokolů *Internet Protocol Security* definovaných pracovní skupinou IETF.

Co je IPSec?

Protokoly *Internet Protocol Security (IPSec)* jsou definovány a navrženy jako otevřená architektura s ohledem na poskytnutí bezpečnosti pro IPv4 a IPv6 využitím vysoce kvalitních šifrovacích mechanismů. Množina bezpečnostních služeb nabízených pro IPSec zahrnuje: 1. kontrolu přístupu (access control), 2. bezztrátovou integritu spojení (connectionless integrity), 3. ověření původu dat (data origin authentication), 4. utajení (confidentiality) – užitím šifrování, 5. zpětnou ochranu (protection against replays) – tj. zajištění proti útočníkovým snahám zachytit datagram a zaslat jej později zpět, 6. omezeně utajený tok dat.

Tyto služby jsou poskytovány na IP úrovni. Nabízejí tedy ochranu pro tuto a výše položené úrovně protokolů, např. pro TCP, UDP, BGP, ICMP atd.

IPSec tedy poskytuje bezpečnostní služby umožňující systému vybrat požadované bezpečnostní protokoly, určit algoritmy pro tyto služby a poskytnout šifrovací klíče požadované těmito službami. Protokoly IPSec mohou být úspěšně využity k ochraně jedné nebo více „cest“ mezi párem hostů, mezi párem bezpečnostních bran a mezi bezpečnostní bránou a hostem (viz obr. 1).

Architektura IPSec

Poté, co jste měli možnost seznámit se s úvodní charakteristikou IPSec, se nyní dozvíte základní informace o architektuře těchto protokolů, a to vyjmenováním a popsáním stavebních elementů IPSec. Těmi jsou následující protokoly:

IP Authentication Header (AH)

Cílem protokolu AH je poskytnutí bezztrátové integrity spojení (tj. poskytnutí spojení označovaného jako „per packet“), zajištění ověření původu dat pro IP datagramy pomocí autentizace a dále nabídnutí ochrany proti zpětnému zasílání datagramů s určitou časovou prodlevou.

Integrita dat je zajištěna pomocí kontrolního součtu generovaného prostřednictvím hashed message authentication code (HMAC), kombinovaného s tradičními hašovacími algoritmy, např. MD5 či SHA. Ověření původu dat je zajištěno užitím tajného klíče (secret key) pro potřebu autentizace. Zpětná ochrana je pak zajištěna sekvencí čísel pole uvnitř Authentication Header hlavičky.

Jako většina moderních protokolů je i protokol AH navržen pro aplikaci ve dvou modech. Prvním z nich je tzv. transport mode – v tomto modu je originální IP hlavička (= IP Header) datagramu vnější IP hlavičkou, je následována AH hlavičkou a následně informacemi obsaženými v originálním IP datagramu (tzv. Payload Data).

Druhou variantou je aplikace AH v tzv. tunnel mode – v tomto modu je generována nová IP hlavička pro užití vnější IP hlavičky výsledného datagramu.

IP Encapsulating Security Payload (ESP)

Protokol ESP zajišťuje utajení dat užitím šifrování a bezeztrátovou integritu navázaného spojení, ověřuje původ dat a chrání proti zpětnému zaslání datagramů. Protokol je navržen tím způsobem, že utajení dat poskytuje vždy, a to využitím symetrického šifrování. Zbývající složky ochrany naopak poskytuje volitelně. Protokol ESP může být aplikován stejně jako AH ve dvou modech. V *transport mode* je originální IP hlavička přenášena bez aplikování kompresních nebo šifrovacích mechanismů. Dále je následována ESP hlavičkou a TCP hlavičkou (viz obr. 3). Při

režimu v *tunnel mode* je opět generována nová IP hlavička. Originální IP datagram je zašifrován (viz obr. 4).

Poznámka: Authentication Header a Encapsulating Security Payload mohou být aplikovány samostatně nebo v kombinaci spolu.

Internet Security Association and Key Management Protocol (ISAKMP)

Security Association (dále jen SA) obsahuje všechny relevantní informace pro potřebu vzájemně komunikujících systémů, aby mohly úspěšně používat IPSec protokoly, jako je AH nebo ESP. Například SA bude identifikovat užité šifrovací mechanismy, informace o klíčích a identifikaci zúčastěných stran. Obecně platí, že ISAKMP definuje množinu procedur pro autentizaci a komunikaci účastníků spojení, dále definuje způsob vytváření a řízení SA a techniky generování klíčů.

ISAKMP probíhá ve dvou fázích. V první fázi je ustavena tzv. „master secret", ze které budou následně odvozeny všechny šifrovací klíče pro ochranu uživatelských dat. V nejobecnějším případě je užito šifrování pomocí veřejných klíčů k ustavení ISAKMP bezpečného spojení mezi dvěma systémy a k vytvoření klíčů, které budou užity k ochraně ISAKMP zpráv.

První fáze je tedy zaměřena na ustavení bezpečného doprovodu pro následné ISAKMP zprávy mezi sebou. V druhé fázi komunikující systémy dohodnou bezpečné spojení a klíče (využití výsledků z první fáze), které budou chránit výměnu uživatelských dat.

Užití transport a tunnel mode

Jak je zřejmé z předchozího odstavce, AH a ESP mohou být užívány v transport nebo tunnel mode. Pro lepší objasnění těchto dvou variant spojení si ukážeme typické situace jejich využití.

Transport mode je obvykle užíván mezi dvěma koncovými body spojení. Například pokud je bezpečná komunikace požadována u všech elementů cesty mezi klientem a serverem, měl by klient a server užít IPSec transport mode. Naproti tomu *tunnel mode* je zpravidla užíván mezi dvěma stroji, pokud alespoň jeden z nich není koncovým bodem spojení.

Je-li například bezpečná komunikace požadována mezi dvěma firewally, které jsou umístěny mezi klientem a serverem, měly by firewally mezi sebou užívat IPSec tunnel mode. Nebo pokud je vzdálený host 1 volán ve své domácí síti, může požadovat bezpečnou cestu mezi sebou a vstupní bránou 1 do své domácí sítě. A naopak vzdálený host 2 a vstupní brána 1 mohou v této situaci užívat IPSec tunnel mode.

Jak je vidět, IPSec AH a EPS jsou protokoly podobné. Pokud ESP využívá autentizační funkce, tj. nějaké HMAC algoritmy (například HMAC-SHA), jsou užívány podobně jako u AH protokolu. Pro lepší rozlišení jejich funkcí jsou v následujícím textu stručně uvedeny některé rozdíly mezi těmito protokoly.

V transport mode chrání ESP autentizační funkce pouze originální IP Payload, ne však originální IP Header; oproti tomu AH protokol chrání originální IP Header i IP Payload.

V tunnel mode chrání ESP autentizace originální IP Header a IP Payload, ne však novou IP Header; oproti tomu AH chrání novou IP Header, originální IP Header a IP Payload.

Závěr

IPSec je množina vhodně navržených protokolů zajišťujících bezpečnou výměnu informací pomocí internetu. Vzhledem k důmyslně navržené architektuře můžeme očekávat využití těchto protokolů nejen v současnosti, ale i v budoucnosti. Musíme si však uvědomit, že pouhá implementace jednoho, byť sebelepšího protokolu nám nezajistí požadovanou ochranu privátních informací. Teprve vhodně navržená bezpečnostní politika, zahrnující například srovnání a popsání možností jednotlivých protokolů či standardů, otázku lidského faktoru aj., nám zajistí tolik požadovanou bezpečnost. Proto i v příštím článku si o trochu rozšíříme obzor svých obecných znalostí v oblasti bezpečnostní politiky.

Milan Pinte (pinte@kpv.zcu.cz)