Odvozování klíčů

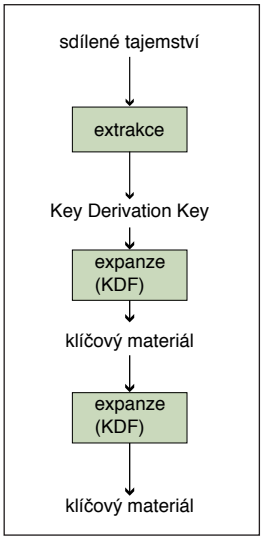
Jestliže dvě strany sdílejí určité společné tajemství, které se nazývá klíč, je možné pomocí moderní kryptografie z něho odvodit mnoho dalších klíčů pro různé účely. Ty se nazývají odvozené klíče a v internetových, počítačových a jiných normách jsou jich stovky. Kryptografie jako věda je zde proto, aby řekla, jak se to dělá bezpečně, a normy popíšou krok za krokem, jak to udělat v praxi. Před odvozováním klíčů v určité aplikaci bude nutné se prokousat několika normami, které se zcela jistě budou zdát zbytečně složité (nestačilo by třeba na klíč naxorovat konstantu nebo to celé zhašovat?) a možná i nepochopitelné. Ukažme si proto, jak se v nich orientovat, jaké jsou jejich hlavní principy, aby si jejich uživatel mohl říci, že je v souladu s normou pro odvozování klíčů. Pro rychlé dobrání se pointy bude třeba pracovat se stavebními bloky, které se na čtenáře začnou v normách postupně hrnout. Ale nakonec se ukáže, že to vůbec není tak hrozné, jak to vypadá.

Postačí dva nástroje

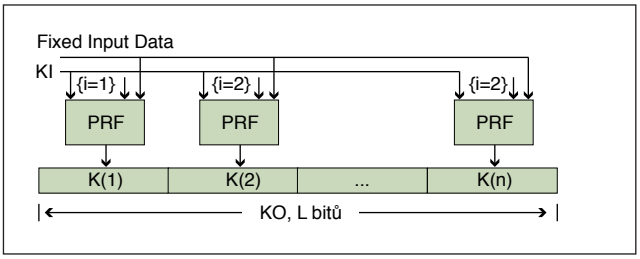
Přestože kryptografie je bohatá věda, je relativně chudá na základní nástroje. Při odvozování klíčů od nějakého sdíleného tajemství si lze v převážné většině norem vystačit s blokovou šifrou a hašovací funkcí. V moderních normách se konkrétně používá bloková šifra AES (ve starších normách DES a TripleDES) a hašovací funkce SHA-256 nebo SHA-512 (ve starších je to MD5 a SHA-1). S jejich pomocí se konstruují pseudonáhodné funkce – PRF, a z nich se vytvářejí funkce pro tvorbu klíčového materiálu (klíčů) – KDF. Teď je nutná určitá míra trpělivosti, neboť co to je PRF a KDF? Ale představme si, že to jsou funkce stejné jako AES nebo SHA-256, které mají nějaké vstupy a výstupy; pak je možné jít dále. Funkce PRF i KDF mají obecně dlouhý binární vstup i výstup, ale v praxi má PRF delší vstup a krátký výstup a u KDF je to obráceně. Proč je tomu tak, bude zřejmé za okamžik. Vstupem i výstupem jsou binární řetězce.

Zásady derivování klíčů

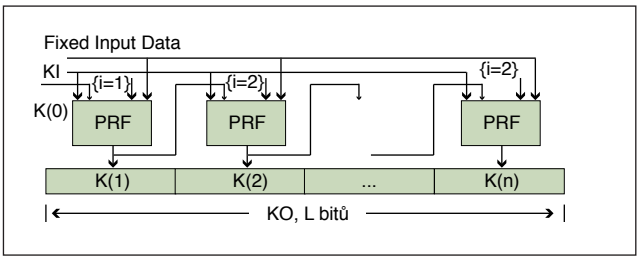
Pointa nebo zásada tvorby odvozených klíčů je ta, že by měly vznikat ve dvou fázích, viz *obr. 1*. V první fázi (která se nazývá extrakčně-expanzní) se ze sdíleného tajemství za použití první derivační funkce KDF vytvoří prvotní binární klíčový materiál (tzv. klíče pro derivaci klíčů). Poté se v druhé fázi tento materiál opět určitou funkcí KDF přetvoří v libovolně dlouhý seznam odvozených klíčů. Tím byl popsán princip zhruba deseti nejpoužívanějších norem, např. SSL/TLS, ANSI, SSH, IKE. Některé z nich fázi 1 neaplikují, a proto musely být předmětem specifického zkoumání, zda takovýto postup v daném konkrétním případě neohrožuje použití odvozených klíčů. Naštěstí pro osm nejpoužívanějších průmyslových norem (viz uvedené plus třeba normu pro Trusted Platform Module) udělal americký standardizační úřad NIST dobrou výjimku a práci, když posoudil jejich postupy a shledal je v pořádku, budou-li použity kvalitní nástroje (viz AES, SHA-256/512). Jsou to standardy American National Standard (ANS) X9.42-2001 (RFC 2631) a ANS X9.63-2001 (RFC 3278) řešící dvě oblasti PKC, Internet Key Exchange (IKE) (RFC 2409 a RFC 4306), Secure Shell (SSH): RFC 4253, Transport Layer Security (TLS) versions 1.0: RFC 2246, version 1.1: RFC 4346, The Secure Real-time Transport Protocol (SRTP, RFC 37110), User-based Security Model (USM) for Simple Network Management Protocol (SNMP, RFC 2574) a Trusted Platform Module (TPM).



Obr. 1 Postup odvozování klíčů



Obr. 2 KDF vytvořená z PRF v čítačovém módu



Obr. 3 KDF vytvořená z PRF ve zpětnovazebním módu

Píšete vlastní aplikaci s odvozováním klíčů?

Bude-li uživatel sám vytvářet klíče ve své aplikaci, nechť si vezme k ruce normy [1] a [2], které pro tyto účely vytvořil NIST. Dejme tomu, že je k dispozici hašovací funkce nebo bloková šifra a s její pomocí vytvořená funkce PRF (to bude ukázáno příště). Potom lze z PRF vytvořit KDF snadno podle *obr. 2* nebo *obr. 3*. Tuto funkci je pak možné použít podle *obr. 1* k vytváření samotných klíčů pro kryptografické algoritmy ochrany vlastních dat. Na obrázcích je vždy KI vstupní klíč a KO výstupní klíčový materiál. Použije-li se pro PRF bloková šifra, je KI klíčem blokové šifry, použije-li se HMAC, je KI klíčem konstrukce HMAC. Další vstupy do funkce PRF na obrázcích jsou vždy chápány jako datové vstupy pro blokovou šifru nebo HMAC. Obsahují čítač (i) a poté další pevná vstupní data (Fixed Input Data), která mohou obsahovat dosti libovolnou přídavnou informaci, jako je návěští (identifikátor typu použití klíče) nebo identifikátory komunikujících stran či náhodné řetězce (nonce), známé oběma komunikujícím stranám. Výstupem je řetězec téměř libovolné délky (KO), který se vytváří tolika voláními PRF, až je této délky dosaženo.

Použití klíčů

Výsledek (KO) je možné rozdělit (disjunktně!) na tolik klíčů, které jsou zapotřebí. Mohou být použity k libovolným účelům – jako inicializační vektory, jako šifrovací klíče, jako klíče pro zabezpečovací kódy, jako autentizační nonce apod. Jediným zákazem je, že KO nelze použít přímo jako proud hesla pro proudovou šifru.

V příštím pokračování budou dodefinovány PRF pomocí blokové šifry nebo hašovací funkce (HMAC).

Vlastimil Klíma,
vlastimil.klima@knzsro.cz

LITERATURA

[1] NIST Special Publication 800-108: Recommendation for Key Derivation Using Pseudo-random Functions (Revised). Computer Security Division, ITL, CS, October 2009.

[2] NIST Special Publication 800-135 (DRAFT): Recommendation for Existing Application-Specific Key Derivation Functions. Computer Security Division, ITL, CS, August 2010.