Kryptologie pro praxi – protokol D-H

Jak jsme se již zmínili v předchozích dílech, používají se v současné době asymetrické šifry [1] prakticky výhradně v rámci takzvaných hybridních šifrovacích schémat. Zde je otevřený text nejprve zašifrován některou ze symetrických metod [2], kde je ochráněn takzvaným dočasným symetrickým klíčem, který je generován náhodně pro každou novou zprávu. Tento dočasný symetrický klíč je poté sám zašifrován pomocí zvolené asymetrické šifry a v tomto tvaru je přiložen k šifrovému textu zprávy. Důvodem pro takové uspořádání je mimo jiné podstatně vyšší rychlost symetrických metod v porovnání s asymetrickými. Připomeňme také, že asymetrická kryptografie tento trend reflektuje tím, že vytváří speciální druhy schémat právě pro účely bezpečného ustavení dočasného sdíleného symetrického klíče mezi komunikujícími stranami [1]. K nejpoužívanějším schématům takového typu patří i Diffieho-Hellmanův protokol dohody na klíči (zkráceně D-H) [4], [5] a [6], kterému se budeme nyní věnovat.

Klíče a transformace

Předpokládejme, že uživatel A chce společně s uživatelem B používat protokol D-H. V rámci inicializace svých instancí se oba uživatelé nejprve shodnou na veřejných parametrech (*p, g*), kde *p* je prvočíslo *g* je generátor grupy $\boldsymbol{Z}_p^*$. Každý z nich si dále zvolí svůj privátní klíč x_A, respektive x_B jako celé číslo z intervalu <1, *p*–2> a spočítá k němu svůj veřejný klíč $y_A=g^{x_A} \bmod p$, respektive $y_B=g^{x_B} \bmod p$. V okamžiku, kdy si A chce dohodnout s B symetrický klíč, tak si oba nejprve důvěryhodným způsobem sdělí své veřejné klíče. Toto sdělení může samozřejmě probíhat veřejně přístupným kanálem, avšak musí být zajištěna autenticita jednotlivých klíčů. V praxi se proto nejčastěji používá výměna veřejných klíčů prostřednictvím jejich certifikátů. Zdůrazněme, že autenticita těchto veřejných klíčů je zde zásadním předpokladem bezpečnosti, neboť eliminuje triviální útoky typu man-in-the-middle (útočník C vystupuje jako B vzhledem k A a zároveň na druhou stranu jako A vzhledem k B; A i B si přitom myslí, že komunikují jen spolu a roli prostředníka C nezaregistrují). Na základě znalosti veřejného klíče y_B, provede A výpočet $K_A=y_B^{x_A} \bmod p$. Obdobně B vypočte $K_B=y_A^{x_B} \bmod p$. Lze snadno ověřit, že platí $K_A=K_B=K$. Hodnota *K* je nyní sdíleným tajemstvím mezi A a B (útočník tuto hodnotu s pouhou znalostí veřejných parametrů a klíčů nedokáže spočítat), z něhož se dále vhodným definovaným způsobem odvodí symetrický šifrovací klíč [5]. Kromě hodnoty *K* do tohoto procesu (využívajícího hašovací funkce) obvykle vstupují ještě nějaké náhodné diversifikační hodnoty, které si oba uživatelé vymění na začátku dohody. Cílem těchto diversifikátorů je zabránit útokům založeným na opakovaném přenosu zachycené zprávy, atp.

Ephemeral D-H

Vezmeme-li v úvahu, že první popis protokolu D-H spatřil světlo světa v roce 1976 (tj. ještě o dva roky dříve než RSA), nelze se příliš divit tomu, že cestou do současnosti prošel řadou úprav a rozšíření, a že dnes je vlastně přesnější hovořit o celé *rodině* protokolů D-H. Za jednu z podstatnějších modifikací lze považovat takzvanou dočasnou (doslovně *prchavou* – anglicky *ephemeral*) variantu, která dnes tvoří hlavní způsob použití protokolu D-H. Jejím cílem je odstranit zřejmý nedostatek základní definice, kdy komunikující uživatelé musí sdílet stejné veřejné parametry (*p, g*). Zkušenosti s využíváním takového sdílení u (EC)DSA, kde toto lze principiálně také provádět [3], jasně ukazují, že uživatelé preferují vlastní, nezávislou volbu veřejných parametrů. To by v případě výše uvedeného protokolu ovšem znamenalo, že pro komunikaci na množině s *n* partnery by v systému mohlo naráz koexistovat až $n(n–1)$ veřejných klíčů, respektive jejich certifikátů. Asymetrické systémy přitom právě usilují o to, aby certifikátů bylo asymptoticky jen $\boldsymbol{O}(n)$. To je silným impulzem, aby nebylo trváno na podmínce, že oba uživatelé při dohodě používají certifikovaný veřejný klíč. V této úpravě se rozdělují role odesílatele a příjemce zprávy, přičemž pouze příjemce používá certifikovaný (tj. „pevný“) veřejný klíč. Odesílatel si svůj privátní a tím i veřejný klíč volí vždy ad hoc na základě parametrů (*p, g*) z certifikátu příjemce. Po ustanovení sdíleného tajemství *K* je možné (a záhodné) tyto dočasné klíče na straně odesílatele bezpečně smazat. Celá úprava se nedotýká nijak podstatně vztahů uvedených výše. Stačí si jen pod hodnotou x_A představit dočasně vygenerované náhodné číslo z příslušného intervalu. S ohledem na útoky man-in-the-middle je nyní nutné počítat s tím, že zde pouze odesílatel má určitou jistotu, že komunikuje se správným příjemcem. Pokud je nutné, aby obdobnou jistotu získal i příjemce (v původní verzi byla tato důvěra symetrická), musí k tomu odesílatel použít jiné prostředky, například může své zprávy digitálně podepisovat, atp. V praxi toto obvykle nepředstavuje žádné zásadní omezení, je jen třeba na tento fakt pamatovat a ošetřit ho s ohledem na požadovanou bezpečnost.

Bezpečnost (EC) D-H

Podobně jako v případě DSA je teoretická bezpečnost protokolu D-H opírána o problém diskrétního logaritmu. Standardně schéma D-H pracuje na multiplikativní grupě $\boldsymbol{Z}_p^*$, pro $p>2^{1023}$, avšak i zde je možný přechod k aditivní grupě bodů rovinné eliptické křivky. Takovým přenesením potom vzniká schéma EC D-H. Dodejme, že podobně jako u DSA se o tomto přechodu dosud uvažuje převážně v teoretické rovině. Existuje ovšem určitý mezikrok, který se v řadě systémů používá už teď (mj. je doporučován v [5]). Toto bezpečnostní rozšíření spočívá v tom, že místo celé grupy $\boldsymbol{Z}_p^*$ se využívá pouze nějaká její podgrupa $\boldsymbol{Q}$ prvočíselného řádu *q*. Pro velikost *q* přitom požadujeme alespoň $q>2^{159}$, čili *q* je nejméně 160bitové číslo. Veřejnými parametry schématu je potom trojice (*p, q, g*), kde *g* je generátorem $\boldsymbol{Q}$, tj. řád *g* je *q*, nikoliv *p*–1. Popis generování veřejných parametrů a detaily používání upraveného protokolu jsou rozebrány v [5] a není přitom náhodou, že uvedený postup vychází z generování veřejných parametrů DSA. Technicky vzato se totiž protokol D-H popsaným mezikrokem posunujeme právě na úroveň DSA – jedná se o totožný trik, jakým se DSA mj. odlišuje od schématu ElGamal (tomu se budeme věnovat v dalším dílu). Zatímco rozšíření na EC D-H je zatím skutečně spíše luxus, tak právě uvedenou modifikaci je velmi vhodné nasadit už dnes. Umožní nám totiž například i eliminaci informací vynášených prostřednictvím postranních kanálů, zejména chybových. Dodržením kontrol na integritu veřejných parametrů a veřejného klíče protistrany doporučených v [5] tak můžeme v řadě případů doslova uniknout čím dál tím více agresivnějším metodám moderní kryptoanalýzy. V tomto ohledu je nanejvýš žádoucí provést i revizi všech starších implementací (dokončených před rokem 2001 a dříve).

Vlastimil Klíma, Tomáš Rosa,
klima@lec.cz, trosa@ebanka.cz

LITERATURA

[1] Kryptologie pro praxi (3) , ST č. 8/2003
[2] Kryptologie pro praxi (2), ST č. 7/2003
[3] Kryptologie pro praxi – DSA, ECDSA, ST č. 4/2004
[4] PKCS#3: Diffie-Hellman Key-Agreement Standard
[5] Rescorla, E.: RFC 2631 - Diffie-Hellman Key Agreement Method
[6] Archivy http://cryptography.hyperlink.cz a http://crypto.hyperlink.cz