Kryptologie pro praxi – tipy a triky

Řešení problému doplňování u blokových šifer

V *ST 11* [1] jsme si uvedli nejpoužívanější blokové šifry a v *ST 9* [2] nejznámější způsoby jejich použití, tzv. operační módy. Při použití blokových šifer automaticky předpokládáme, že máme k dispozici celé *N*bajtové bloky (vstupního) otevřeného textu. Musíme však umět vyřešit i situaci, kdy otevřený text (například soubor dat) končí několika bajty, nedávajícími celý *N*bajtový blok. Na tuto situaci pamatuje norma PKCS#5, která říká, že chybějících *b* bajtů se má (pouze u posledního bloku) nahradit *b* bajty s hodnotou *b*. Příjemce si pak u posledního bloku přečte poslední bajt – dejme tomu, že má hodnotu 3 – a odstraní 3 bajty s hodnotou 3. Problém nastává, pokud na konci nejsou 3 bajty s hodnotou 3. V tomto případě zcela jistě nastala na komunikačním kanálu chyba a v důsledku toho příjemce neví, kolik bajtů otevřeného textu je v posledním bloku platných. Obvykle protistraně vydá chybové hlášení a ve většině protokolů čeká na zopakování bloku. Ve *ST 3* [3] jsme ukázali, že toto chybové hlášení vytváří tzv. postranní kanál, prostřednictvím něhož může útočník, aktivně působící na komunikačním kanálu, nakonec vyluštit celý otevřený text. Na obranu proti tomu byly navrženy jiné metody doplňování, například na konferenci USENIX [4]. Jako jedno z nejúčinnějších opatření se jevilo doplnit všechny zbývající bajty stejnou (libovolnou) hodnotou, odlišnou od posledního platného bajtu. Tato metoda byla nazvána ABYT-PAD (Arbitrary Byte Padding). Rozhodně je to lepší metoda, než původní, ale vzápětí nato jsme na konferenci NATO SPI [6] ukázali, že i to může za určitých okolností vést k luštění celého otevřeného textu (jedná se o celou třídu tzv. TLV neboli Tag-Length-Value formátů a protokolů). A tak jedinou prakticky používanou obranou proti uvedeným útokům postranními kanály je doplnění původní zprávy kryptografickým zabezpečovacím kódem, a to buď na otevřeném textu (tj. šifruje se zpráva a její zabezpečovací kód) nebo na šifrovém textu (šifruje se zpráva a za ní následuje zabezpečení, vypočítané ze šifrového textu). V prvním případě musíme být ještě dost opatrní, abychom například časovým postranním kanálem nedali najevo jaká chyba nastala tím, že bychom reagovali příliš brzo – pak bychom tím řekli to, co jsme chtěli skrýt, tzn. že chyba nastala v doplňku zprávy, protože ke kontrole zabezpečovacího kódu jsme se ještě v tak krátkém čase nemohli dostat. Jednou z metod tvorby zabezpečovacího kódu je technika MAC (Message Authentication Code), o ní jsme psali v *ST 9*, nebo technika HMAC (klíčový hašový autentizační kód zprávy), využívající hašovací funkce, o ní se zmíníme příště. Pokud si připomeneme problém doplňování u asymetrických šifer (rozebírali jsme to v *ST 10*), pak vidíme, že je vlastně stejně závažný u symetrických i u asymetrických šifer. Ukázali jsme, že u obou typů šifer může zanedbání řešení této na první pohled nevýznamné banality vést k prolomení celého jinak dokonalého systému.

Tabulka 1 Kradení šifrového textu

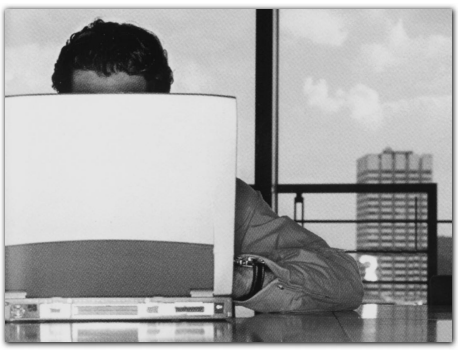
A – zašifrování posledních dvou bloků:
$\check{S}T_{n-1}=E_K(OT_{n-1} \text{ xor } \check{S}T_{n-2})$,
rozdělíme blok $\check{S}T_{n-1}$ na prvních b bajtů a zbytek: $[\check{S}T_{n-1}]_b \,||\, [\check{S}T_{n-1}]_{n-b}$
$\check{S}T_n = E_K(([OT_n]_b \text{ xor } [\check{S}T_{n-1}]_b) \,||\, \text{zbylých n–b bajtů } [\check{S}T_{n-1}]_{n-b})$
vysílá se šifrový text ... $[\check{S}T_{n-1}]_b$, $\check{S}T_n$,
B – odšifrování posledních dvou bloků:
$D_K(\check{S}T_n) = ([OT_n]_b \text{ xor } [\check{S}T_{n-1}]_b \,||\, \text{n–b bajtů } [\check{S}T_{n-1}]_{n-b})$
z první části pomocí $[\check{S}T_{n-1}]_b$ určíme $[OT_n]_b$, z druhé části $[\check{S}T_{n-1}]_{n-b}$,
sestavením získáme celý blok $\check{S}T_{n-1}$ a odtud dopočítáme $OT_{n-1} = D_K(\check{S}T_{n-1}) \text{ xor } \check{S}T_{n-2}$

Kradení šifrového textu

Za určitých okolností se lze vyhnout doplňování posledního bloku a použít tzv. kradení šifrového textu (Ciphertext stealing). Je to velmi hezká technika, umožňující použít blokovou šifru v módu CBC k zašifrování posledního neúplného (*b*bajtového) bloku otevřeného textu $[OT_n]_b$ bez nárůstu počtu bajtů šifrového textu. Zašifrování a odšifrování probíhá podle vztahů v *tabulce 1*.

Náhodná čísla

Dalším detailem, který musíme řešit v kryptografických protokolech (např. SSL/TLS), při použití blokového i proudového šifrování i šířeji v počítačové praxi, je častá potřeba náhodných čísel. Například jsou to inicializační hodnoty, náhodné symetrické klíče všeobecně (například klíče na sezení), doplňky pro formátování vstupů u schémat digitálních podpisů a asymetrických šifer, hodnoty výzev pro protokoly typu challenge-response apod. Protože v praxi nebývá k dispozici kvalitní hardwarový generátor šumu (RNG), často se používají zdroje, které jsou v daném systému k dispozici, jako je systémový generátor náhodných čísel nebo nějaká funkce systémového času. V mnoha systémech mohou být tyto náhražky přípustné, pro důležité kryptografické hodnoty je ovšem nelze doporučit (například pro generování symetrických nebo asymetrických klíčů apod.). U hardwarových generátorů je vhodné, abychom prověřili jejich kvalitu náročnými statistickými testy při výrobě a průběžnými testy při použití. Jedná se o tzv. go/no-go testy, které zjišťují, zda v průběhu života generátoru nedošlo k jeho poškození. Může se jednat o přerušení spoje nebo jen o dočasné silné tepelné nebo elektromagnetické působení okolí na generátor, které by mohlo způsobit dočasné generování pravidelné posloupnosti. Tyto testy jsou popsány například v normě FIPS PUB 140-1 (viz [5], novelizace FIPS-PUB 140-2). Další normy, které se týkají problematiky náhodnosti, jsou například ANSI X9.17 (pseudonáhodný generátor na bázi DES), FIPS PUB 186-2 (obsahuje pseudonáhodný generátor na bázi hašovací funkce nebo DES) nebo internetová norma RFC 1750, obsahující tipy a triky pro výběr



RNG. Ke generování vhodných zdrojových posloupností můžeme, jak je vidět, použít kromě blokových a proudových šifer i hašovací funkce. O nich bude pojednávat další pokračování.

Generování prvočísel

Na závěr ještě drobná poznámka. Při generování klíčů pro asymetrické šifry se setkáme s požadavky generovat náhodná prvočísla s určitými vlastnostmi, nejčastěji je to požadavek na jejich délku, tj. pro nějaké *n* (například 512) generovat *n*bitové prvočíslo. V tomto případě se nejprve vygeneruje *n*bitová náhodná počáteční (lichá) hodnota (tzv. seed) a testuje se, zda je prvočíslem. Pokud ne, seed se zvýší o 2 nebo jinou vhodnou konstantu a test se opakuje, dokud není prvočíslo nalezeno. Nejznámějšími testy prvočíselnosti jsou Fermatův a Miler-Rabinův test. Jedná se o pravděpodobnostní testy, ale pravděpodobnost, že označí složené číslo za prvočís-

lo klesá exponenciálně s počtem provedených iterací testů.

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

LITERATURA

[1] Kryptologie pro praxi (6) , Sdělovací technika č. 11, s. 16, 2003.

[2] Kryptologie pro praxi (4), Sdělovací technika č. 9, s. 16, 2003.

[3] Vybrané aspekty moderní kryptoanalýzy, Sdělovací technika č. 3, s. 3 -7, 2003.

[4] Black, J., and Urtubia, H.: Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption, In Proc. of 11th USENIX Security Symposium, San Francisco 2002, pp. 327-338.

[5] Stránka amerického standardizačního úřadu NIST: http://csrc.nist.gov

[6] Klíma, V., and Rosa, T.: Side Channel Attacks on CBC Encrypted Messages in the PKCS#7 Format, Security and Protection of Information 2003, 2nd International Scientific Conference, NATO PfP/PWP - CATE, Brno, Czech Republic, 28.4.-30.4.2003, dostupné na Cryptology ePrint Archive, http://eprint.ia.cr.org/2003/098.pdf

[7] Archiv převážně českých článků o kryptologii a bezpečnosti je přístupný přes osobní stránky autorů: http://cryptography.hyperlink.cz nebo http://crypto.hyperlink.cz

Operační zesilovače pro digitální věk

Při návrhu současných vložených (embedded) řídicích systémů je často třeba analyzovat parametry, které jsou běžné v analogovém světě. Přestože řídicí povely jsou doménou digitálního světa, jsou většinou ovlivněny tím, co se odehrává ve světě analogovém. Převod analogového signálu na digitální hodnotu se významně zjednodušil, když množství samostatných AD převodníků nahradily výkonné mikrokontroléry, jichž jsou tyto převodníky integrální součástí. Analogový signál však často není v podobě, kterou je možno přímo převést na digitální hodnotu.

Řada senzorů, které měří parametry, jako jsou teplota nebo tlak, generují signály, které nejsou vhodné pro konverzi. Signál je buď příliš slabý pro převod nebo obsahuje vysokofrekvenční šum, který vnáší falešné informace do digitální hodnoty v průběhu převodu. Pro zesílení signálu a aktivní filtraci vysokofrekvenčních složek se proto často používají operační zesilovače.

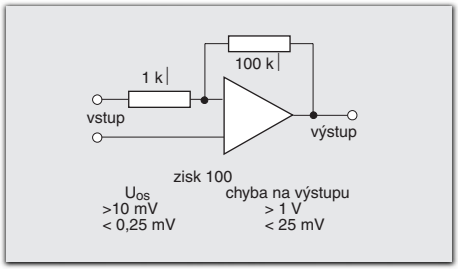
Mnohé operační zesilovače mají poměrně velký vstupní klidový proud a ofset a pokud jim nevěnujeme pozornost, vnášejí v uvedených aplikacích významnou chybu. Musíme proto používat další dodateční součástky, abychom tyto jevy eliminovali. Řešením může být použití nové generace operačních zesilovačů s nízkým ofsetem, která je navržena pro použití v digitálních systémech. Ceny těchto nových operačních zesilovačů se přitom pohybují pod cenovou úrovní přesných operačních zesilovačů používaných v minulosti.

Jak můžeme vidět na obr. 1, typická aplikace se zesílením 100 může ztratit hodně z rozsahu výstupních napětí právě díky chybovému napětí způsobenému ofsetem. V tomto konkrétním případě se jedná o nevyužitých 20 % při 5 V napájení. V případě nižších napájecích napětí je situace ještě horší, při napájení 3 V ztrácíme více než 33 % výstupního napětí.

V stejném obrázku je znázorněn i případ, kdy operační zesilovač má ofset 0,25 mV. Výsledkem je chybové napětí na výstupu pouze 25 mV, tj. pouze 0,5 % rozsahu výstupního napětí při napájení 5 V.

V konfiguraci invertujícího zesilovače pokles napětí na vstupním odporu způsobený klidovým proudem může způsobit chybu na výstupu. Návrhář proto musí věnovat pozornost tomu, aby hodnota odporu nebyla příliš vysoká. Tuto situaci lze zcela eliminovat použijeme-li operační zesilovač s velmi malým klidovým proudem.

Firma Microchip Technology takové operační zesilovače nabízí. Jedná se o rodinu tvořenou typy MCP606 (jeden zesilovač), MCP607 (dvojice), MCP608 (jeden zesilovač s výběrem čipu) a MCP609 (čtveřice). Tyto zesilovače pracují s jedním napájecím napětím v rozsahu od 2,5 do 5,5 V, který je obvyklý v systémech s mikrokontroléry a signálovými procesory. Další nároky na napájení jsou reprezentovány klidovým proudem pouhých 20 mA na jeden zesilovač. Zesilovače jsou ideální pro aplikace v dnešních bateriově napájených zařízeních.



Obr. 1 Vliv klidového vstupního proudu a offsetu na činnost operačního zesilovače

Vezmeme-li navíc v úvahu nízký vstupní klidový proud (IB < 1 pA) a malý ofset (Uos <250 mV) a fakt, že tyto součástky poskytují stabilní jednotkový zisk, vyhneme se spoustě komplikovaných úvah při návrhu zařízení, což umožní jejich rychlejší uvedení na trh.

Tam, kde jsou požadovány zesilovače s vyšším součinem zisku a šířky pásma (Gain BandWidth Product, GBWP=10 MHz) nabízí Microchip typy MCP6021 (jeden zesilovač), MCP6022 (dvojice), MCP6023 (jeden zesilovač s výběrem čipu) a MC6024 (čtveřice), které disponují rovněž nízkým vstupním klidovým proudem (IB < 1 pA) a malým offsetem (Uos <500 mV).

Řada MCP602X reprezentuje operační zesilovače kategorie rail-to-rail (se vstupním a výstupním napětím pohybujícím v rozsahu napájecího napětí), které nabízejí návrhářům nákladově příznivou cestu zvýšení provozní doby a výkonu bateriově napájených systémů a aplikací v oblasti zpracování nf signálů, telekomunikací, měřicích a lékařských přístrojů. Operační zesilovače nabízejí využití plného rozsahu napájecích napětí od 5,5 do 2, V na vstupu i na výstupu. Nabízené typy MCP6021 (jeden zesilovač), MCP6022 (dvojice) a MCP6024 (čtveřice) vyhovují průmyslovým standardům uspořádání vývodů pouzder PDIP, SOIC a TSSOP. Tyto zesilovače je možné, díky stabilitě jednotkového zesílení s GBWP=10 MHz, nízkému šumu (8,7 nV/rtHz) a maximálnímu klidovému napájecímu proudu IQ=1,35 mA , používat bez nákladných stabilizačních obvodů. Malý ofset eliminuje potřebu dalších externích součástek, přičemž umožňuje udržet nízkou spotřebu, minimalizovat prostor na desce plošných spojů, náklady i dobu pro uvedení na trh. Operační zesilovače řady MCP602X jsou ideální pro řízení AD převodníků, buffering v DA převodnících a pro aplikace snímání čárového kódu.

Je ironií, že vznik těchto zesilovačů umožnilo digitální řízení – využití energeticky nezávislých (non-volatile) pamětí pro uložení regulačních odchylek, které slouží ke kompenzaci ofsetu zesilovače při dalším provozu. Vzhledem k tomu, že tyto kompenzační hodnoty jsou uloženy až při konečném testu operačního zesilovače, jsou jimi kompenzovány i efekty, které může mít kompletace obvodu na výsledný ofset.

Dosud používané nastavovací postupy vyžadují nákladní laserové zařízení a je možné je provádět pouze na úrovni polovodičové desky (wafer). Použití energeticky nezávislých pamětí umožňuje kompenzaci na úrovni finálního produktu, a to s vysokou přesností a bez potřeby nákladného laserového nastavovacího zařízení. Digitální řídicí obvody tak slouží k většímu uplatnění analogových obvodů na trhu, což je příznivě vnímáno návrháři digitálních systémů.

K dispozici je stále větší množství analogových produktů, které mají na paměti požadavky návrhářů digitálních systémů. Svět zůstane analogový i přes jednoznačný trend digitalizace řídicích systémů. Proto se snaží výrobci nabídnout cesty jak tento rozpor překlenout a vyhovět požadavkům digitálního věku.

Art Eck, product marketing manager Microchip technology Inc. www.microchip.com