Konference o AES

Bitva o trůn

Přípravy nového šifrovacího standardu pro začátek třetího tisíciletí (Advanced Encryption Standard, AES) jsou v plném proudu. Na jaře vyvrcholily konferencí amerického standardizačního úřadu NIST, jenž sezval do Říma všech 15 týmů, které navrhly své kandidátské algoritmy, k všeobecné diskusi (pranici). Kdo zvítězil a kdo utrpěl šrámy, se dozvíte v tomto článku.

Konference se konala 22. – 23. března a přinesla velmi zajímavé výsledky. Jsou důležité pro rozvoj kryptologie jako vědy, protože přinesly mnoho nových pohledů a metod kryptografie a kryptoanalýzy, ale pravděpodobně z mnoha hledisek ovlivní i **bezpečnostní praxi**. Hlavním cílem sice bylo vybrat šifrovací algoritmus, ale hodně času se věnovalo i implementačním a aplikačním aspektům – vždyť algoritmy budou použity v řadě bezpečnostních zařízení pro ochranu senzitivních informací.
Protože si NIST uvědomuje velký význam **čipových karet** jako bezpečnostního nástroje, patřila k důležitým tématům rovněž rychlost a bezpečná aplikace různých algoritmů právě v čipových kartách. Byly také zvažovány mnohé útoky na čipové karty („timing attack“, „power analysis“, „differential power analysis“) a konkrétně byl prezentován reálný útok odhalující tajný šifrovací klíč algoritmu *Twofish* na základě energetické spotřeby čipové karty. Takovému útoku bohužel nemohou odolat ani někteří další kandidáti a na konferenci poté zavládla skepse, zda je vůbec možné se proti této hrozbě efektivně bránit. Jakékoliv naděje na postup do dalšího kola ztratily algoritmy *MAGENTA, Frog a LOKI97*. Skolily je teoretické slabiny, přestože praktická realizace útoků by byla velmi drahá. Konference však také ukázala, kteří kandidáti mají naději na úspěch největší.

Časový plán přijetí standardu

Shrňme si, jak probíhal a bude probíhat celý proces výběru nového šifrovacího standardu. AES by měl nahradit svého předchůdce DES pro ochranu vládních citlivých (ale neutajovaných) informací a měl by platit v letech 2000 – 2030:

- 2. 1. 97 – vypsání výběrového řízení (viz Chip 4/97, str. 20);
- 15. 4. 97 – pracovní konference o definici požadavků na AES;
- 8. 9. 97 – NIST vydal oficiální dokument obsahující náležitosti pro podání návrhu nového algoritmu (viz Chip 11/97, str. 44);
- 20. 8. 98 – pracovní konference (AES1), kde bylo představeno 15 přihlášených algoritmů (viz Chip 12/98, str. 170) a zahájeno 1. kolo technické analýzy AES (tzv. Round 1);
- 22. 3. 99 – druhá pracovní konference o kandidátech na AES (AES2);
- 15. 4. 99 – ukončení připomínek ke kandidátům;
- 15. 5. 99 – uzávěrka všech doplňků a malých změn, které chtějí učinit autoři algoritmů (po diskusích na AES2 a dalších veřejných připomínkách);
- den X uprostřed léta 1999 – NIST oznámí finalisty (očekává se asi pět kandidátů);
- den X + 1 měsíc – začíná 2. kolo technické analýzy, autoři algoritmů mohou aktualizovat programové kódy, které odevzdali v prvním kole;
- 15. 1. 2000 – uzávěrka příspěvků pro konferenci AES3;
- 10. 4. 2000 – konference AES3 v New Yorku, kde budou všechny finální algoritmy podrobeny závěrečné veřejné analýze;
- 15. 5. 2000 – uzavření všech komentářů k finalistům;
- v srpnu 2000 oznámí NIST vítězný algoritmus (není to sice pravděpodobné, ale NIST si ponechává teoretickou možnost vyhlásit i více vítězů!).

Tabulka 1: Kandidáti na AES v prvním kole.

Kandidát AES	Přihlášen kým			Odpověď na otázku „Měl by NIST tento algoritmus vybrat do 2.kola ?“						Neoficiální hodnocení pořadí
Jméno algoritmu	Autoři	Firma	Stát	Žádná	Ano	Nevím	Ne	Celkem odpovědí	Hodnota „ANO - NE“	
Rijndael	Joan Daemen, Vincent Rijmen		Belgie	7	77	19	1	104	76	1
RC6		RSA Laboratories	USA	4	79	15	6	104	73	2
Twofish	Bruce Schneier, John Kelsey, Dough Whiting, David Wagner, Chris Hall, Niels Ferguson		USA	9	64	28	3	104	61	3
MARS		IBM	USA	5	58	35	6	104	52	4
Serpent	Ross Anderson, Eli Biham, Lars Knudsen		UK, Izrael, Norsko	6	52	39	7	104	45	5
E2		Nippon Telegraph and Telephone Corporation	Japonsko	11	27	53	13	104	14	6
CAST-256		Entrust Technologies, Inc.	Kanada	12	16	58	18	104	-2	7
SAFER+		Cylink Corporation		13	20	47	24	104	-4	8
DFC		Centre National pour la Recherche Scientifique - Ecole Normale Superieure	Francie	12	22	43	27	104	-5	9
Crypton		Future Systems, Inc.	Korea	14	16	43	31	104	-15	10
DEAL	Richard Outerbridge, Lars Knudsen		Kanada, Norsko	10	1	22	71	104	-70	11
HPC	Rich Schroeppel		USA	12	1	13	78	104	-77	12
MAGENTA		Deutsche Telecom AG	Německo	9	1	10	84	104	-83	13
Frog		TecApro International S.A.	Jižní Afrika	11	1	6	86	104	-85	14
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry		Austrálie	10	1	7	86	104	-85	15

Zajímavosti z konference

Na konferenci přijelo přes 180 účastníků z 23 zemí. Všech 28 oficiálních příspěvků bylo zveřejněno a stále jsou k dispozici na internetu (viz infotipy). Všechny kandidáty vidíte v tabulce 1 i se jmény autorů, jejich firem a se státní příslušností. Kromě oficiálních analytických příspěvků, které ukazovaly kladné a zá-

porné vlastnosti jednotlivých algoritmů, vystoupilo ve volné diskusi (tzv. Rump Session) téměř 20 dalších účastníků.
Nejočekávanější byl příspěvek M. Smida z NIST. Prezentoval kryptoanalyticko-statistické testy a **srovnání rychlostí algoritmů**. Rychlostní testy se ukázaly jako velmi diskutabilní, přestože bylo definováno prostředí i všechny testovací parametry. To si NIST uvědomoval také, a proto M. Smid prezentoval další dva nezávislé pohledy.

	Příprava klíče				Zašifrování		Odšifrování		Průměrná rychlost za šifrování a odšifrování			
	NIST		Gladman		NIST	Gladman	NIST	Gladman	NIST		Gladman	
Jméno algoritmu	hodinové cykly	pořadí	hodinové cykly	pořadí	hodinové cykly	hodinové cykly	hodinové cykly	hodinové cykly	Mbit/s	pořadí	Mbit/s	pořadí
CAST-256	10098	9	4333	7	2169	633	2171	634	12	9	40	6
Crypton	620(693)	1	531(1369)	2	579	474	664	474	41	1	54	5
DFC	13726	10	7166	8	3491	1203	3505	1244	7	10	21	9
E2	3667	4	9473	10	1523	687	1509	691	17	6	37	7
MARS	5481	5	4316	6	807	369	733	376	33	3	69	3
RC6	2272	2	1632	3	636	270	621	226	41	2	103	1
Rijndael	6787(7467)	6	305(1389)	1	809	374	832	352	31	4	71	2
SAFER+	3049	3	4278	5	2095	1722	2092	1709	12	8	15	10
Serpent	6953	7	2402	4	1629	952	1561	914	16	7	27	8
Twofish	9724	8	8414	9	973	376	965	374	26	5	68	4
DES											27	

"Poznámky:
a) v závorce je čas v případě odšifrování, pokud se podstatně liší od zašifrování (jednoho bloku dat)
b) uvedené časy jsou pro referenční počítač, u NIST je uveden lepší čas ze dvou měření (BC, MSVC)
c) při použití nulové šifry trvá u NIST příprava klíče 292 hodinových cyklů (vstupě-výstupní rámce)
d) DES se zde uvádí pro srovnání"

Tabulka 2: Rychlostní charakteristiky kandidátů na AES.

Nejhůře přitom dopadly rychlostní testy v jazyce Java, protože moderní algoritmy (kryptograficky nejzajímavější, a tedy žhaví kandidáti) jsou v Javě mnohem pomalejší – některé z nich dokonce pomalejší než DES! Vysvětlení je nasnadě, neboť 32bitové operace, psané přímo „na tělo" současným mikroprocesorům, efektivně „překroutit" do instrukcí virtuálního počítače (JVM) není snadné.
O tom, jakou váhu mají rychlosti na určitých platformách, se vedly na konferenci i na internetu nekonečné diskuse – zdá se, že rychlosti mají velký význam, ale nebudou určujícím faktorem. Statistické testy NIST a další dva testovací programové balíky (CRYPT-XB a DIEHARD) neodhalily podle NIST žádnou zvláštní anomálii. (To se ale celkem očekávalo, protože každý si podobné testy určitě před přihlášením provedl.)
Velmi bolavým místem však zůstaly autorské, patentové a licenční otázky. U vítězného algoritmu je sice zaručeno, že autoři souhlasí s jeho absolutně volnou a bezplatnou šiřitelností, ale vznikla otázka, zda poražení nebudou chtít vítězi a NIST znepříjemňovat život svými případnými autorskými nebo patentovými nároky na vítězný algoritmus.
Zajímavá byla i dobrovolná anonymní anketa, v níž byla účastníkům položena otázka, zda by NIST měl vybrat daný algoritmus jako kandidáta do dalšího kola. Zúčastnilo se jí 104 respondentů – z jejich odpovědí v tabulce 1 je patrné, že pět posledních algoritmů zřejmě nemá žádnou šanci projít.

Jak rychlá bude nová šifra?

Rychlost algoritmu je pochopitelně závislá na způsobu implementace, operačním systému, typu kompilátoru a kromě toho také na metodě měření, včetně toho, co se měří a v jakém rámci. U *blokových* šifer jsou samozřejmě podstatné čas zašifrování jednoho bloku dat (zde 128 bitů), čas odšifrování jednoho bloku dat (nemusí být totožný s předchozím!), ale také čas potřebný k přípravě klíče pro zašifrování a čas na přípravu klíče pro odšifrování (různé časy u algoritmů Crypton a Rijndael). To vše pochopitelně v operační paměti počítače.
V tabulce 2 vidíte tyto údaje pro 10 algoritmů, které mají šanci na přežití. NIST měřil časy na tzv. referenční platformě a s programy (v ANSI C), které dodali s jednotným rozhraním sami autoři. Bohužel do měřených časů se započítávaly i některé operace vlastního testovacího programu NIST. Tak například generování klíče pro zašifrování u nulového algoritmu (tj. algoritmu, kde vstup = výstup) trvalo 292 namísto očekávaných 0 cyklů. Na druhé straně tyto „přívažky" byly pro všechny stejné a toto měření svoji logiku má. Stejně tak má logiku měřit čistý čas těchto operací, a proto NIST zveřejnil výsledky testování Briana Gladmana (bez I/O operací testovacího programu, bez přehazování pořadí vstupních a výstupních bajtů, s vlastní implementací jednotlivých algoritmů), které jsou považovány za reprezentativní (viz infotipy).
Referenční platformou NIST bylo PC Pentium Pro 200 MHz s 64 MB RAM a s Windows 95, překladačem Borland C++ 5.0. NIST také provedl testy na referenční platformě s překladačem MS VC++ 6.0 a v tabulce 2 je vždy uveden lepší z obou časů. V závorce jsou dále uvedeny časy pro případ odšifrování (u algoritmů Crypton a Rijndael při generování klíče), pokud se významně liší od časů pro zašifrování.

Java převrací výsledky

S ohledem na předpokládané použití AES v čipových kartách provedl NIST i testy v jazyce Java (JDK 1.16, technika překladu „Just in Time"). Měřily se časy vytvoření klíče, zašifrování a odšifrování, ale i velikost statické paměti pro program a velikost dynamicky použité paměti při tvorbě klíče a při šifrování. Výsledky, jak už bylo naznačeno, nedopadly pro Javu právě lichotivě...

Závěr

Konference přinesla nesmírné množství poznatků. U řady algoritmů byly zjištěny teoretické nebo praktické slabiny, a proto vypadávají z dalšího kola posuzování. Pokud vás zajímají další podrobnosti, zejména o úspěšných útocích na jednotlivé šifry, najdete je na přiloženém Chip CD 7/99 v rubrice *Co nebylo v Chipu* pod názvem „Z konference o AES". Uvidíte tam i grafické znázornění, jak rychlost šifrování ovlivní použitý procesor, a také výsledky měření algoritmů zapsaných v jazyce Java.
NIST v nejbližší době určí finalisty a na ně se pak soustředí ohromná pozornost. Doufejme, že přitom budou všechny dobré i špatné vlastnosti kandidátů odhaleny, abychom nejlepšímu z nich mohli ochranu citlivých dat svěřit.

VLASTIMIL KLÍMA (*VKLIMA@DECROS.CZ*)

infotipy

Všechny komentáře a připomínky zaslané NIST v 1. kole posuzování:
http://csrc.nist.gov/encryption/aes/round1/pubcmnts.htm
Domovská stránka AES obsahující všechny události a odkazy na další relevantní stránky (například projekt Ceasar ap.):
http://csrc.nist.gov/encryption/aes/aes_home.htm
Rychlostní testy kandidátů AES od Briana Gladmana:
http://www.seven77.demon.uk/aes.htm