Kompatibilní a kvalitní kryptografické nástroje

Článek by se také mohl jmenovat kryptografie v moderních měřicích přístrojích a ve smart grids, neboť následující sdělení platí zejména pro moderní elektroměry a jiné přístroje ve smart grids.

Jak se chránit

Už jste se dostali do situace, kdy je třeba předat e-mail nebo soubor, nebo dokonce obsah DVD elektronicky a je nutné jeho obsah skrýt před nepovolanými zvědavci? Jistě ano. A jak jste to řešili? Já mnohokrát, a mám pro to osvědčený nástroj, program, který je zdarma volně dostupný a rozšířený po celém světě a především funguje v operačních systémech Windows i Unix/Linux (bohužel ne na macu, kde je k němu nutná určitá konverze). Komunikuji s ním po celém světě a jediné, co musím, je ustavit si šifrovací klíč s příjemcem. To lze při vzájemném setkání, což se téměř vždy uskuteční, nebo jinými komunikačními kanály než tím, kterým si předáváme zašifrovaná data. Ve stejné situaci se nalézá americký státní aparát, který potřebuje mezi úřady, mezi různými domácími firmami nebo zahraničními dodavateli či vojenskými misemi a místním prostředím apod. předávat informace. Tuhle nesourodou datovou výměnu na území a mimo území USA nelze mít pod takovou kontrolou jako vládní linky ve Washingtonu. NSA proto ustavila kryptografické nástroje typu B, které považuje za bezpečné, jež ale na rozdíl od nástrojů A musí z uvedených důvodů interoperability zveřejnit. Úřad pro standardizaci NIST zase zřídil validační program, který hodnotí, zda určitý software, čipová karta nebo hardwarové zařízení splňují požadavky na to, aby mohly chránit citlivé informace, a vydal tudíž normu (FIPS 140-2, 3). Proto státní správa, spojenci a dodavatelé mohou tyto prostředky, certifikované NIST podle FIPS 140-2/3 nebo jiných norem, používat, neboť je zaručena jejich bezpečnost. Aby byly kompatibilní i na úrovni používaných kryptografických ochran, je naprosto nezbytné, aby používaly stejné kryptografické algoritmy sady B.

Základní kryptografické algoritmy

Časem se ustálily tyto základní kryptografické nástroje: symetrický šifrovací algoritmus, hašovací algoritmus, algoritmus digitálního podpisu a algoritmus výměny klíčů. Mají mnoho podob a variant a realizací, a právě proto musel být vybrán vždy jen jeden reprezentant do základní čtveřice, která tvoří tzv. sadu B u NSA. Sada B nejsou outsideři, neboť mohou chránit i informace stupně TAJNÉ, rozdíl je ten, že algoritmy A jsou utajené. Sada B má velmi vysoký stupeň důvěry NSA, neboť kdyby se někdo ve světě byť jen otřel o jejich kvalitu, měla by NSA parádní mezinárodní ostudu.

Sada B

Algoritmem pro šifrování v sadě B je algoritmus AES-128 a AES-256, hašovací funkcí SHA-256 a SHA-384, digitální podpis zajišťuje ECDSA nad eliptickou křivkou ECC GF(p) pro prvočíslo P-256 nebo P-384 (krátce ECDSA-P-256 nebo 384) a klíče mění ECDH nad ECC s P-256 nebo P-384 (krátce ECDH-P-256 nebo 384). Do stupně TAJNÉ včetně je možné používat AES se 128bitovým klíčem, SHA-256, ECDSA-P-256, ECDH-P-256. Pro přechodové období, kdy se zcela přejde na eliptické křivky, je možné (ještě tento rok) používat DH-2048, DSA-2048 a RSA-2048. Do stupně PŘÍSNĚ TAJNÉ včetně je možné používat AES s 256bitovým klíčem, SHA-384, ECDSA-P-384, ECDH-P-384. Bezpečnost algoritmů ukazuje *tabulka 1*, přičemž sada B začíná na bezpečnosti 128 bitů.

Tabulka 1 Bezpečnost jednotlivých kryptografických nástrojů

Dosažená bezpečnost v bitech	Symetrický šifrovací algoritmus	Hašovací algoritmus	Počet bitů veřejného modulu RSA, DSA	Počet bitů veřejného modulu DH	Počet bitů prvočísla veřejné křivky ECC pro ECDSA	Počet bitů prvočísla veřejné křivky ECC pro ECDH
80	DES	SHA-1	1024	1024	160	160
112	2Key-3DES	SHA-224	2048	2048	224	224
128	AES-128	SHA-256	3072	3072	256	256
192	AES-192	SHA-384	7680	7680	384	384
256	AES-256	SHA-512	15 360	15 360	512	512

Kompatibilita módů a algoritmů

Jestliže se řekne, že dva prostředky používají stejný algoritmus šifrování, zdaleka to neznamená, že jsou kompatibilní. Důležité je např., jak odvozují klíč (pomocí tzv. KDF – key derivation function) a jak vlastně tím algoritmem šifrují. Týž algoritmus lze využít různými způsoby, což je opět standardizováno jako tzv. módy činnosti. Pro algoritmus AES jsou např. určeny módy ECB, OFB, CFB, CBC, GCM, MAC-CBC apod. Pro algoritmus ECDH je napsána příručka NSA o 33 stranách, jak tento algoritmus realizovat, ačkoliv se může zdát, že je to vzorec, který má jeden výklad. Realizovat ECDH je natolik variabilní a složité, že je zcela nemožné, aby se domluvily dva prostředky realizující tentýž algoritmus s týmiž parametry a klíči bez úzké spolupráce vývojářů (viz např. zmíněná příručka Suite B Implementer's Guide to NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography). Shoda v algoritmu je základní podmínkou interoperability, neboť ve skutečnosti je to jen shoda v názvu algoritmu. Shodu v implementacích mají zajistit specifické normy, např. pro internetové použití je to šest norem:

- IPsec using the IKE or IKEv2: Suite B Cryptography for IPsec, RFC 4869.
- Suite B for TLS, RFC 5430.
- TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES GCM.
- S/MIME: Suite B in S/MIME, RFC 5008.
- SSH: AES Galois Counter Mode for the Secure Shell Transport Layer Protocol, draft-igoe-secsh-aes-gcm-02.txt.
- IPsec: NIST Special Publication 500-267, A Profile for IPv6 in the U.S. Government – Version 1.0.

Porovnání složitosti (síly) jednotlivých nástrojů je uvedeno v *tabulce 1*, která je zpracována podle NIST Special Publication 800-57, Recommendation for Key Management.

Závěr

Vše, o čem je zde psáno, plně platí pro moderní elektroměry a zařízení, která se budou používat ve smart grids. Nejdále v interoperabilitě jsou USA, kde již existují normy pro tuto oblast. Nejnověji, právě v době psaní článku, vydala skupina The Smart Grid Interoperability normu DRAFT NISTIR 7628: Smart Grid Cyber Security Strategy and Requirements. Kryptografická interoperabilita je stanovena velmi konkrétně a ani nepřekvapí, že je to právě na úrovni 128 bitů představené sady B kryptografických nástrojů NSA.

Vlastimil Klíma, nezávislý kryptolog,
v.klima@volny.cz

LITERATURA

[1] Archiv autora a článků kryptologie pro praxi: http://cryptography.hyperlink.cz.