Ochrana dat a Smart metering

Rozvoj sítí chytrých měřicích přístrojů a systémů dodávky a odběru vody, plynu, tepla a elektřiny nabírá na intenzitě. I když v ČR jsme na samém začátku vize jak by to mělo fungovat, začínají se nasazovat první chytré měřicí přístroje v pilotních projektech typu AMM (automatic meter management). Měří spotřebu daného média (energie nebo něčeho jiného), ale mají i inteligenci k provádění operací, které mohou obdržet od dodavatele. V každém případě se jedná o oboustrannou komunikaci. Pro jednoduchost hovořme jen o chytrých elektroměrech. V době psaní článku vrcholila příprava evropské konference o chytrém měření v Londýně (9.–10. července.). V příštím roce bude tato „šňůra“ v Evropě pokračovat a jedna ze tří konferencí bude v dubnu v Praze. V USA tuto oblast stát, reprezentovaný NISTem a stimulovaný přímo prezidentovým rozhodnutím, dosti podporuje. NIST tím, že vydává standardy, které vytváří prostředí pro interoperabilitu a tím i konkurenci v dodávkách chytrých měřidel, domácích systémů, návazných služeb apod. Na okraj poznamenejme, že v USA už také mají za sebou první útoky na rozvodné sítě, řízené počítači a z dalších mají obavu.

Obr. 1 Chytrý měřicí přístroj

Bezpečnost chytrých sítí

Během několika let bude i u nás několik milionů domácností (a časem jistě všechny) používat chytré elektroměry. Budou primárně hlásit spotřebu, vysílat alarmy, když zjistí porušení nějakých bezpečnostních pojistek, přijímat příkaz na vypnutí elektřiny nebo přechod na jiný tarif apod. Jistě je tu hrozba černého odběru elektřiny tím, že útočník zmanipuluje data vysílaná elektroměrem. Může také zmanipulovat data vysílaná z tzv. koncentrátoru, což je většinou nějaký počítač umístěný v rozvodné stanici. Koncentrátor může předávat data od všech elektroměrů, které má k sobě připojeny, i od rozvodné stanice. Další hrozba je ze strany útočníka v centrále, kde se sbíhají data ze všech koncentrátorů. Odtud lze také masově korigovat chování jednotlivých eleletroměrů (prostřednictvím koncentrátorů). Útočník může být kdekoli, nejlépe v centrále nebo na komunikačním kanálu, který z centrály vede příslušnou komunikaci s koncentrátory. Tím, že zařízení jsou schopna přijímat příkazy, je možné z centrály vypnout elektroměry ve všech domácnostech a podnicích. To může být užitečným nástrojem v havarijních situacích nebo při černém odběru nebo u neplatičů, ale nemělo by to být umožněno pro zábavu hackerům. Škody, které by mohly tímto vzniknout, jsou totiž velmi vysoké. Pokud systém řízení chytrých měřidel nebude postaven dobře koncepčně, může být obnova normálního stavu značně časově i finančně náročná a škody nedozírné. Představme si sci-fi, že se útočník dostane k možnosti si hrát se sítí tím, že se napojí na komunikační kanál z centrály. Co když je elektroměr tak technicky nedokonale vyrobený, že ho útočník zahltí příkazy natolik, že se „neuchladí“ a spálí se? Nebo ho dostane do stavu deadlocku díky nějaké chybě v programu? Raději ponechme sci-fi a předpokládejme „jen“, že útočník vypne několik milionů elektroměrů. Aby toto a jiné útoky nebyly možné, musíme na komunikačních kanálech centrála – koncentrátory – elektroměry zajistit autentizaci a neporušenost příkazů „shora“ i autentičnost a neporušenost dat předávaných „zdola“. Dostáváme se k tomu, že síť elektroměrů, koncentrátorů a centrály se z „hloupé sítě“ minulosti stává sítí kryptografických zařízení, které zajišťují službu autentizace (ev. i šifrování). To je ovšem předěl, na který nejsou výrobci připraveni, ani cenově, ani organizačně. Nyní výrobci poznají, že šifrování (autentizace, elektronické podpisy) není žádná technická otázka výběru algoritmů, ale zejména a hlavně klíčové hospodářství, tj. organizační a technický problém, jak plnit, měnit a ochránit klíče k nim. To ostatní je vůči tomu opravdu prkotina.

Ověření příkazů z centrály

Jaké kryptologické mechanismy použít? Pochopitelně, že první volba padne na kryptografii s veřejným klíčem (PKC), kde bychom mohli u elektroměrů mít pouze veřejný klíč centrály (nemusíme ho utajovat) a pomocí něj ověřovat pravost a neporušenost příkazů centrály. Ověření pravosti příkazu je však pro elektroměr náročná výpočetní operace i při použití těch nejefektivnějších metod (například malý veřejný exponent RSA). Tyto operace nezvládnou běžné mikroprocesory používané v současných elektroměrech, které se dostatečně potí jen vlastním sběrem dat. Je tedy nutná změna technologie a jejich vybavení výkonnějšími procesory. Jak výkonnými, záleží na tom, který typ kryptografie použijeme.

Ověření dat z elektroměru

Pokud chceme ověřit pravost a neporušenost dat, vysílaných z elektroměru, musíme v elektroměru držet buď privátní podpisový klíč pro daný systém PKC nebo tajnou hodnotu klíče pro klasický symetrický systém. V obou případech bude elekroměr muset obsahovat nějakou tajnou informaci, a bude se muset řešit otázka, kdy a kdo tam tuto informaci bude plnit a jakým fyzickým způsobem bude chráněna. Z elektroměru se stává šifrátor. To, co brání využití asymetrické kryptografie v elektroměrech, je také použitý komunikační kanál (zejména PLC), který je poruchový. Proto se preferuje přenos co nejkratších velmi úsporných paketů dat oběma směry. Z tohoto důvodu bude často použita symetrická kryptografie, například AES, kde jsou bloky dat o velikosti 128 bitů. Navíc se v centrále sbíhá velké množství těchto komunikací a je nutno je zde rychle odšifrovat nebo ověřit jejich digitální podpis.

Lidová tvořivost

Nelze očekávat, že by firmy, které dosud vyvíjely měřicí přístroje, měly své kryptology, a tak v mnohých chytrých měřidlech nalezneme celou škálu „pašáckých“ kryptografických metod. Připomeňme, že pašákem nazýváme v tomto seriálu toho, kdo všemu rozumí a hned „jde na věc“. Právě díky takovým řešením bude často možné pouze sedět na komunikačním kanálu a měnit data, posílaná elektroměrům, neboť „pašáci“ se obvykle dopouští dvou chyb: za prvé používají techniky na něco jiného než jsou určeny (například šifrování k autentizaci) nebo způsobem, který je v daném kontextu nepřijatelný (například heslo vygenerované pomocí AES naxorují na paket). Otevřený text paketu, čili příkaz elektroměru, lze pak změnit „přes šifrový text“, aniž by útočník znal klíč AES nebo produkované heslo. Takové případy nastanou a lze je těžko napravovat. Lidová tvořivost může nastat i o úroveň výše, tj. v koncentrátorech a centrále, ale to je zcela jiná problematika, neboť se jedná o jiné prostředí s nesrovnatelně lepšími možnostmi k ochraně než má měřicí přístroj.

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

LITERATURA

[1] http://cryptography.hyperlink.cz