Aplikovaná kryptografie

Applied Cryptography je název slavné knihy, která vyšla v roce 1995 z pera do té doby téměř neznámého Bruce Schneiera. Kniha se stala bestsellerem a její autor celebritou. Sám autor se za tu dobu hodně změnil a změnil se i svět okolo nás, počítačový svět i spotřební elektronika. Změnila se aplikovaná kryptografie, uživatelé jsou pohodlnější a výrobci více šetří. Hlavní počítačové bezpečnostní problémy, které před patnácti lety popsal Matt Blaze v doslovu k této přelomové knize, zůstaly stejné. Podívejme se na některé z nich.

NSA

Never Say Anything (NSA) má stále stejné heslo „V Boha věříme, vše ostatní monitorujeme“, ale z „brzdy kryptologického pokroku“ se stala jeho pomocníkem. Mnozí pochopili, že ne vše mohou od NSA slyšet, ale důvěra v ni vzrostla. Otevřela se veřejnosti a participuje na obecných problémech počítačové bezpečnosti. Pomáhá národnímu úřadu pro standardizaci (NIST). Jeho počítačová laboratoř je mezinárodní oporou bezpečnostního průmyslu v celé šíři od spotřební elektroniky, přes identifikační systémy, elektroměry, tzv. chytré sítě až po klasickou síťovou bezpečnost. Bohužel problémů přibývá, takže ne vše je vyřešeno do patřičné hloubky a v předstihu. A navíc, uživatele to většinou nezajímá a výrobci implementují jen to, co musí v rámci konkurenčního boje.

Měření bezpečnosti

Měření bezpečnosti je nadále velký sen. Sice vznikly mezinárodní bezpečnostní normy (např. Common Criteria), ale i ony bezpečnost známkují „stupněm důvěry“. Bezpečnost je blíže pocitu než číslu.

Bankomaty

Bankomaty technicky odpovídají útočníkům z doby před dvaceti lety a už neposkytují adekvátní bezpečnost. K inovaci se nikdo nechystá, neboť škody způsobené podvody jsou malé ve srovnání s investicí do technologické změny obrovského mezinárodního systému.

Software

Před patnácti lety byla tendence říkat, že „open SW“ je bezpečnější. Dnes se od toho ustupuje, protože to sice obecně je pravda, ale je to stejně málo platné. I v otevřených systémech bylo nalezeno příliš mnoho chyb na to, aby tuto tezi někdo příliš proklamoval jako rozhodující výhodu. Software, který k něčemu je, bývá velmi složitý, se stovkami tisíc řádků. Nikdo na světě nemůže garantovat, že je bez chyby a bez „zadních vrátek“, ať je otevřený nebo ne. Neúmyslná zadní vrátka byla nalezena v jádrech otevřených i uzavřených operačních systémů. Každý den lze sledovat nová odhalení a opravy chyb. Je s podivem, že kybernetická válka se projevuje tak málo, když téměř každý počítač je zranitelný. Tipuji, že stále platí prohlášení ředitele odboru počítačové kriminality FBI: „Dejte mi deset schopných hackerů a srazím tuto Zemi na kolena.“

DOS útoky

U mnoha systémů je vyžadována anonymita, čili tyto systémy musí reagovat na anonymní podněty. To umožňuje zahltit je nesmyslnými požadavky. Pokud na počátku nebude autentizace, nemůže se snížit riziko DOS útoku. Kryptografie umí vyřešit skrytí identity a přitom provést autentizaci.

Kam ukrýt tajemství

Kryptografie umí chránit velké objemy dat malými klíči (stovky bitů), které je však třeba někam ukrýt. Když budou ukryty, nelze s nimi pracovat. Když budou otevřeny systému, budou i otevřena vrátka k útoku na ně. Řešením je všechny operace s klíčem dělat přímo v předmětu s klíčem, ale často je tím degradován výkon systému.

Generátory náhodných znaků

Toto je věčné téma, stejně jako téma passwordů. Překvapením byla možnost degradovat náhodný generátor v bankomatu vysíláním určité nosné frekvence, na níž se generátor zamkne. Obvykle je nekvalitní sám o sobě nebo je špatně používán. Pořízení kvalitního generátoru je kupodivu velmi drahé (protože o ně není zájem), takže se využívají zdroje entropie běžně dostupné v daném výpočetním prostředí, a to není nejlepší. Kryptografie a teorie informace umějí zjistit entropii zdroje a poskytnout kvalitní náhodný řetězec potřebné délky. Lenost je příčinou nevyužití současných kryptografických možností.

Slabá hesla a nevhodné používání

Většina hesel je slabých a podlehne slovníkovému útoku. Druhým nešvarem je opakované užití stejného silného hesla i v nedůvěryhodném systému. Situace se zhoršila, passwordů na jednoho uživatele přibylo tolik, že není možné si je pamatovat. Kryptografie umí tento problém triviálně řešit, ale toto řešení vede k problému, kam ukrýt tajemství megapasswordu chránícího všechny ostatní.

Nerealizovaná důvěra

V počítačovém systému uživatel věří, že když s ním pracuje, program zajišťuje to, co má, např. důvěrnost a integritu cesty, kterou putuje password, klíč, data apod. Mnohdy tomu tak není a uživatel je systému vydán napospas. Každý systém může být napaden nebo upraven anebo prostě jen nevykonávat přesně to, co se od něj očekává. Stejně tak jako problém „kam ukrýt tajemství“ vzniká problém „kde najít důvěryhodné prostředí“ nebo „kam ukrýt důvěryhodné prostředí“.

Křehká propojenost

Je s podivem, že internet stále funguje velmi dobře. Stačí neopatrnost na některých místech, útok na servery DNS a všechno se může změnit. Je to křehké prostředí, a přesto ho denně zatěžujeme novými službami, povinnostmi a zařízeními. Internet byl tvořen s cílem dostupnosti, nikoliv bezpečnosti! A přesto po internetu běží citlivé služby, jako je bankovnictví. Na několika místech se po internetu řídí i elektroměry a zanedlouho sem vstoupí chytré městské sítě, dopravní signalizace, kamery, osvětlení, řízení domácností na dálku a nové masově využívané služby. Tyto služby musí mít kvalitní koncová zařízení. Například elektroměry budou podle nových norem muset realizovat kvalitní sadu algoritmů B od NSA, jak jsme o tom psali v minulém čísle ST. Budeme potřebovat internet cílený na bezpečnost, který by zajistil nejen opravdovou dostupnost, ale i integritu, auditovatelnost a takovou míru anonymity, aby umožnila dohledatelnost viníků a soukromí řádným uživatelům. Kryptografie má mnoho nástrojů pro taková budoucí řešení.

Neodpovídající analýza rizik

Analýza rizik může podchytit jen rizika, která analytici znají. Naproti tomu útočníci využijí to, co jim poskytuje realita. Průnik těchto dvou světů není velký, protože ti první jsou více abstraktní, zatímco ti druzí až příliš konkrétní. Kryptografie zde pomůže, ale rizika neodstraňuje, pouze je přesouvá jinam a snižuje.

Těžkopádnost bezpečnosti

Jestliže má bezpečnost fungovat, musí být transparentní a „přítulná“ k uživateli. To je obtížná úloha pro návrháře. Často jsou ochrany buď jednoduché, ale neúčinné, nebo trpí těžkopádností, kterou uživatelé za každou cenu obcházejí.

Bezpečnost na posledním místě

V tomto směru se svět za patnáct let malinko změnil, ale bylo by tomu tak, kdyby světové obchodní centrum stálo stále na svém místě? Svět je takový, že nejprve se musí stát neštěstí a pak následují bezpečnostní opatření (často i nesmyslná).

Vlastimil Klíma, v.klima@volny.cz