BEZ – BI-SPOL-8

Infrastruktura veřejného klíče, distribuce klíčů, digitální podpis. Certifikáty, certifikační autority. Kryptograficky bezpečné generátory náhodných čísel.

Obsah

1 Infrastruktura veřejného klíče

Jedná o specifikaci technických a organizačních opatření pro vydávání, správu, používání a odvolávání klíčů a certifikátů.

2 Distribuce klíčů

Při distribuci veřejného klíče hrozí podvrhnutí prostřednictvím útoku man-in-the-middle. Jedná se o útok, kde komunikace probíhá přes prostředníka, který zaměňuje předávané klíče za své, a tím může číst obsah jednotlivých zpráv.

Z tohoto důvodu vzniklo několik způsobů, které tuto situaci řeší.

3 Techniky distribuce VK

3.1 Zveřejnění VK

- VK je zaslán individuálně nebo hromadně v rámci skupiny
- vystaví se na internet, dá se do emailu, atd…
- je to rychlé a jednoduché, ale není odolné proti podvržení

3.2 Veřejně dostupný adresář

- vyšší stupeň bezpečnosti
- distribuci zabezpečuje důvěryhodná autorita, která odpovídá za obsah a je správcem adresáře
- bezpečná registrace (osobně a nebo přes zabezpečenou komunikaci)
- položky jsou v adresáři ukládány jako dvojice [jméno ; VK]
- problém může nastat ve chvíli, kdy se odhalí SK patřící správci

3.3 Autorita pro VK

- autorita vykonává činnost správce adresáře
- podmínkou je, že každý účastnk zná VK autority
- každý účastník musí komunikovat s autoritou

3.4 Certifikace veřejného klíče

- jedná se o distribuci VK, bez kontaktu s třetím důvěryhodným subjektem
- vyžaduje se certifikát a certifikační autorita

4 Certifikát

Jedná se o strukturu, která obsahuje:

- VK držitele certifikátu
- ID držitele certifikátu
- T doba platnosti certifikátu

Tato struktura je podepsána soukromým klíčem certifikační autority. Každý účastník může verifikovat obsah certifikátu pomocí veřejného klíče certifikační autority.

4.1 Řetězec certifikátů

- posloupnost certifikátů uživatele až ke kořenovému CA
- uživatel nemusí věřit CA, stačí pouze ověřit jeden, ne nutně kořenový, certifikát
- certifikát je platný $\Leftrightarrow$ platné všechny certifikáty v řetězci certifikátu
- pokud existuje více CA pro různé okruhy lidí, vznikají oddělené stromy certifikátů
- v případě existence více stromů certifikátů, pomocí křížové certifikace, jednotlivé CA si navzájem podepíší certifikáty

5 Digitální podpis

Digitální podpis je obvykle formou asymetrického kryptografického schématu. VS slouží k podepsání a VK k ověření.
Musí splňovat následující vlastnosti:

- nezfalšovatelnost - podpis se nedá napodobit jiným subjektem než podepisujícím
- ověřitelnost - příjemce dokumentu musí být schopen ověřit, že podpis je platný
- integrita - podepsaná zpráve se nedá změnit, aniž by se zneplatnil podpis
- nepopíratelnost - podepisující nesmí mít později možnost popřít, že dokument podepsal

Digitální podpisi se dělí na:

- přímé - předají si podpis dvě strany mezi sebou (problém s popíratelností)
- verifikované - využívá důvěryhodnou třetí stranu, která ověřuje podpisy všech zpráv

6 Kryptograficky bezpečné generátory náhodných čísel

Náhodné číslo - čislo vygenerované procesem, který má nepředpovídatelný výsledek a jehož průběh nelze přesně reprodukovat. Tomuto procesu říkáme generátor náhodných čísel.

Od náhodných posloupností očekáváme dobré statistické vlastnosti:

- rovnoměrné rozdělení - všechny hodnoty jsou generovány stejnou pravděpodobností
- jednotlivé generované hodnoty jsou nezávislé - není mezi nimi žádná korelace

6.1 Pseudonáhodné generátory

Jedná se o algoritmicky generovaná "náhodná" čísla. Generátory potřebují náhodný a tajný seed.

Kryptograficky bezpečný PRNG musí splňovat:

- next-bit test: pokud se zná prvních n bitů náhodné posloupnost, nesmí existovat algoritmus, který v polynomiálním čase dokáže předpovědět další bit, s pravděpodobnstí větsí jak 1/2.
- state compromise: i když je znám vnitřní stav generátoru, nelze zpětně zrekonstruovat dosavadní vygenerovanou posloupnost. Navíc, pokud do generátoru za běhu vstupuje entropie, nemělo by být možné ze znalosti stavu předpovědět stav v dalších iteracích.

6.2 Blum-Blum-Shub

Jedná se o PRNG, který by měl být kryptograficky bezpečný.

$$x_{n+1} = x_{n-1}^2 mod m$$

- x_0 je definováno seedem a musí být větší 1 (jinak by nefungovalo to umocňování)
- modul m = q*r, kde q i r jsou prvočísla
- pro q i r musí platit, že q/r = 3 (mod 4)
- při znalosti x0 lze dopočítat pomocí rovnice jakýkoliv člen, proto musí zůstat utajen
- pokud x_{n+1} vyjde sudé, jde na výstup 0, jinak 1