(Ne)popiratelnost digitálních podpisů

Tomáš Rosa, trosa@ebanka.cz
divize Informační bezpečnost

Cíl přednášky

1. Ukázat specifické problémy spojené se zajišťováním nepopiratelnosti digitálních podpisů.
2. Nabídnout inspiraci pro řešení problémů (1) přechodem od klasických ke kvantovým schématům.

Jazyková vsuvka

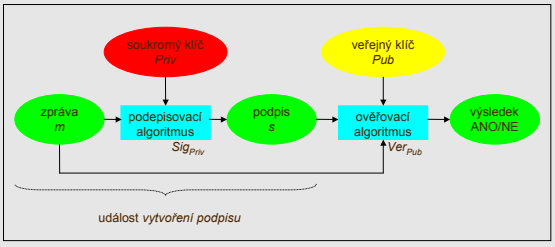
- **důkaz**, -u m
  - **(log.) zdůvodnění pravdivosti nebo nepravdivosti určitého výroku**
  - **(práv.) prostředek potvrzující zjištěné skutečnosti**

[kol. autorů: *Slovník spisovné češtiny pro školu a veřejnost*, Academia, Praha 2001]

Nepopiratelnost

- **Cíl:** Nezávislá třetí strana je schopna rozhodovat spory o tom, zda se nějaká událost stala či nestala.
- **Prostředek:** Důvěryhodný digitální důkaz, token.
- **Nástroj:** Digitální podpis autorizující důkaz (token).

Událost vytvoření podpisu



Meze striktně logických důkazů

- Triviálně lze ukázat, že
  - $\{s \leftarrow Sig_{Priv}(m)\} \Rightarrow \{Ver_{Pub}(m, s) = \text{ANO}\}$
- My bychom však rádi ukázali, že také
  - $\{Ver_{Pub}(m, s) = \text{ANO}\} \Rightarrow \{s \leftarrow^{(!)} Sig_{Priv}(m)\}$
  - zde jsme odkázáni na heuristiku... (viz ovšem rozdílné chápání *logického* a *právního* důkazu)

Příklad

- Buď $Sig_{Priv}(m)$ podepisovací operace schématu RSA.
- Potom $Sig_{Priv}(m) = [\psi(h(m))]^d \bmod N$, kde $Priv = (N, d)$ je privátní klíč, h je hašovací funkce a ψ je formátovací transformace.
  - Buď $\psi(h(m))$ = 00 01 FF…FF 00 ($ID_h \,||\, h(m)$), kde ID_h je identifikátor použité hašovací funkce.
  - Viz PKCS#1, metoda EMSA-PKCS1-v1_5.

Příklad (pokračování)

- Buď $\{Ver_{Pub}(m, s) = \text{ANO}\} \Rightarrow \{s \leftarrow^{(!)} Sig_{Priv}(m)\}$.
- Tedy $\{Ver_{Pub}(m, s) = \text{ANO}\} \Rightarrow \{s \leftarrow^{(!)} [\psi(h(m))]^d \bmod N\}$.
- **Pro běžné zprávy je toto sporný výrok.**
- (BÚNO) Buď h = SHA-1. Délka $h(m)$ je pevná a činí 160 bitů.
- Na množině všech zpráv délky 161 bitů tak musí existovat dvojice (m, m') taková, že $h(m) = h(m')$ a $m \neq m'$.
- Odtud $Sig_{Priv}(m) = Sig_{Priv}(m') = s$.
- Takže $\{Ver_{Pub}(m, s) = \text{ANO}\}$ neimplikuje $\{s \leftarrow^{(!)} [\psi(h(m))]^d \bmod N\}$. Mohlo totiž proběhnout pouze **$\{s \leftarrow [\psi(h(m'))]^d \bmod N\}$, kde $h(m) = h(m')$**.

Jak z toho ven?

- *Prokazatelná nepopiratelnost* je velmi obtížně dosažitelná.
  - Cílem by bylo formálně vyloučit útoky nebo alespoň najít jejich meze. **(možné uplatnění pro QC)**
- *Prokazatelná nepopiratelnost* není nutná pro aplikaci práva.
  - Využití principu **reductio ad absurdum**.

Kde je slabé místo

- Jiný hodnověrný popis události vysvětlující, proč:
- A) neproběhlo
  - $s \leftarrow Sig_{Priv}(m)$
- B) (a přesto) platí
  - $Ver_{Pub}(m, s)$ = ANO
- Hodnověrnost vylučující reductio ad absurdum.

eBanka

Zdroje alternativního vysvětlení

- Kolize hašovacích funkcí
  - Neproběhlo $s \leftarrow Sig_{Priv}(m_1)$, ale $s \leftarrow Sig_{Priv}(m_2)$, kde $h(m_1) = h(m_2)$, ale $m_1 \neq m_2$.
- Vnitřní kolize podpisových schémat
  - Obdobný efekt jako kolize hašovacích funkcí.
- Kolize klíčů
  - Neproběhlo $s \leftarrow Sig_{Priv_1}(m)$, ale $s \leftarrow Sig_{Priv_2}(m)$, kde $Priv_1 \neq Priv_2$.
- Sémantické kolize
  - Zpráva se má dekódovat jako $\varphi_2(m)$, nikoliv jako $\varphi_1(m)$, kde $\varphi_1 \neq \varphi_2$.

eBanka

Novinka: Nalezeny kolize MD5!

- Celosvětově široce rozšířená funkce.
  - I přes řadu výhrad dodnes nasazována v nových aplikacích.
- CRYPTO 2004, srpen t.r., St. Barbara, USA.
  - Nalezeny bloky M, N takové, že MD5(M || N) = MD5($M + \Delta$ || $N - \Delta$), kde M, N, $\Delta \in \mathbf{Z}_{2^{32}}^{16}$.
  - Podrobněji $\varphi(\varphi(IV, M), N) = \varphi(\varphi(IV, M + \Delta), N - \Delta)$, kde φ je kompresní funkce schématu MD5.
  - Metoda hledání M, N pracuje pro libovolnou hodnotu IV.
- Funkce MD5 v podpisových schématech končí.

eBanka

Sémantická kolize - příklad

eBanka

Mentální hra

1. Čím může útočník náš důkaz zpochybnit?
2. Uvěří mu nezávislý soud?
3. Máme hodnověrný protiargument?
4. Uvěří nám nezávislý soud?
5. …

eBanka

Závěrem

- Novum informatiky - ***digitální důkaz***.
  - Prostředek k zajištění nepopiratelnosti.
  - Důvěryhodnost určena konstrukcí.
- Přirozený nástroj – ***digitální podpis***.
  - Nepopiratelnost je další, nový rozměr digitálního podpisu, nikoliv jeho automatická vlastnost.
- Striktně logický přístup selhává, nutno adoptovat „právní logiku“.
- Co na to kvantová kryptografie…?
  - **Nabídne prokazatelnou nepopiratelnost?**

eBanka

Další zdroje

- Archiv výzkumu, článků a přednášek autora
  - http://crypto.hyperlink.cz
- Stránky Dr. Vlastimila Klímy nejen o kolizích MD5
  - http://cryptography.hyperlink.cz/2004/kolize_hash.htm
- Manažerská verze příspěvku
  - Rosa, T.: *Nepopiratelnost digitálních podpisů*, DSM 5/2004
- Originální zpráva o prolomení MD5
  - Wang, X., Feng, D., Lai, X., and Yu, H.: *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, CRYPTO 2004 Rump Session, IACR ePrint archive 2004/199, eprint.iacr.org
- Logika v právním myšlení
  - Knapp, V., Gerloch, A.: *Logika v právním myšlení*, Eurolex Bohemia, Praha 2001

eBanka

eBanka

Děkuji za pozornost

Tomáš Rosa, trosa@ebanka.cz