



Nepopiratelnost digitálních podpisů

Tomáš Rosa, trosa@ebanka.cz
divize Informační bezpečnost

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]



2



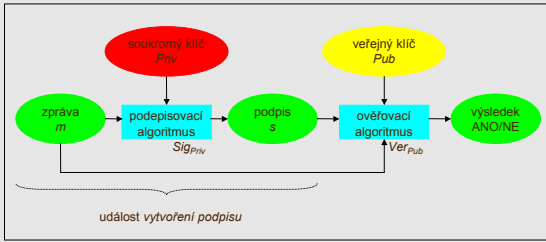
Nepopiratelnost

- **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).



3

Událost vytvoření podpisu



Meze striktně logických důkazů



- Triviálně lze ukázat, že
 - $[s \leftarrow \text{Sig}_{Priv}(m)] \Rightarrow [\text{Ver}_{Pub}(m, s) = \text{ANO}]$
- My však potřebujeme ukázat, že také
 - $[\text{Ver}_{Pub}(m, s) = \text{ANO}] \Rightarrow [s \leftarrow^{(!)} \text{Sig}_{Priv}(m)]$
 - zde jsme odkázáni na heuristiku... (viz ovšem rozdílné chápání logického a právního důkazu)



Kde je slabé místo

- Jiný hodnověrný popis inkriminované události, který vysvětlí, proč:
 - A) neproběhlo
 - $[s \leftarrow \text{Sig}_{Priv}(m)]$
 - B) (a přesto) platí
 - $[\text{Ver}_{Pub}(m, s) = \text{ANO}]$
- Alternativní vysvětlení

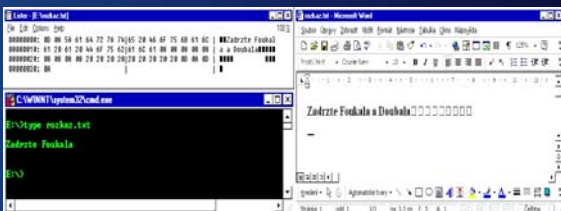
Zdroje alternativního vysvětlení

- Kolize hašovacích funkcí
 - Neproběhlo [$s \leftarrow \text{Sig}_{\text{Priv}_1}(m_1)$], ale [$s \leftarrow \text{Sig}_{\text{Priv}_2}(m_2)$], 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 [$s \leftarrow \text{Sig}_{\text{Priv}_1}(m)$], ale [$s \leftarrow \text{Sig}_{\text{Priv}_2}(m)$], kde $\text{Priv}_1 \neq \text{Priv}_2$.
- Sémantické kolize
 - Zpráva se má dekodovat jako $\varphi_2(m)$, nikoliv jako $\varphi_1(m)$, kde $\varphi_1 \neq \varphi_2$.

Novinka: Nalezeny kolize MD5!

- Celosvětově široce rozšířená funkce.
 - I přes řadu výhrad dodnes nasazována v nových aplikacích.
- Kolize předvedeny v srpnu 2004 na konferenci CRYPTO 2004 v St. Barbaře, USA.
 - Nalezeny bloky M, N takové, že $\text{MD5}(M \parallel N) = \text{MD5}(M \Delta \parallel N - \Delta)$, kde $M, N, \Delta \in \mathbb{Z}_{2^{32}}^{16}$.
 - Metoda hledání M, N pracuje pro různé hodnoty IV .
- Funkce MD5 v podpisových schématech končí.

Sémantická kolize - příklad





Závěrem

- Novum informatiky - **digitální důkaz**.
 - Prostředek k zajištění nepopíratelnosti.
 - Důvěryhodnost určena konstrukcí.
- Přirozený nástroj – **digitální podpis**.
 - Ne každá konstrukce vede k nepopíratelnosti.
 - Nepopíratelnost je další, nový rozměr digitálního podpisu, nikoliv jeho automatická vlastnost.
 - Stejně jako ostatní aspekty informační bezpečnosti, i nepopíratelnost musí být kontinuálně řízena.





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.: *Nepopíratelnost 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





Děkuji za
pozornost



Tomáš Rosa, trosa@ebanka.cz
