

(Ne)popiratelnost digitálních podpisů

Tomáš Rosa

trosa@ebanka.cz

crypto.hyperlink.cz



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]

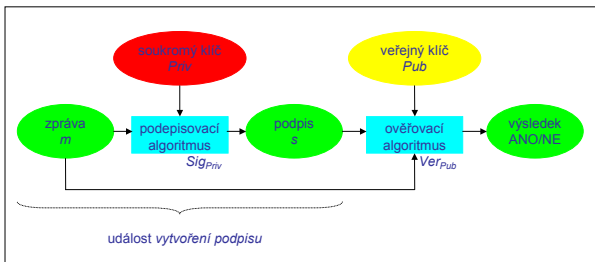


Nepopiratelnost

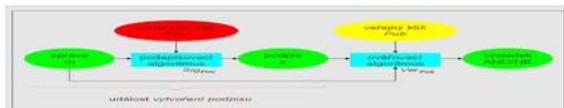
- Cíl
 - Nezávislá třetí strana je schopna rozhodovat spory o tom, zda se nějaká událost stala či nestala.
- Prostředek
 - Důvěryhodný digitální důkaz (nosič nazýváme token, *srov. informace vs. data*).
- Nástroj
 - Digitální podpis autorizující token.



Událost vytvoření podpisu



Meze striktně logických důkazů



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

Příklad

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

Příklad - pokračování

- Bud' $\{Ver_{pub}(m, s) = ANO\} \Rightarrow \{s \leftarrow^{(1)} Sig_{priv}(m)\}$.
- Tedy $\{Ver_{pub}(m, s) = ANO\} \Rightarrow \{s \leftarrow^{(1)} [\psi(h(m))]^d \bmod N\}$.
- **Pro běžné zprávy je toto sporný výrok.**
- (BÚNO) Bud' $h = \text{SHA-1}$. 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 $\{Ver_{pub}(m, s) = ANO\}$ neimplikuje $\{s \leftarrow^{(1)} [\psi(h(m))]^d \bmod N\}$. Mohlo totiž proběhnout pouze $\{s \leftarrow [\psi(h(m'))]^d \bmod N\}$, kde $h(m) = h(m')$.



Jak z toho ven?

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



Reductio ad absurdum

- zhruba řečeno...

- ...z pohledu matematické logiky
- Výrok Q je prohlášen za platný tehdy, když z platnosti $\text{neg}(Q)$ plyne nějaký absurdní výrok P .
 - Důležité: P nemusí být sporný výrok ve smyslu matematické logiky.
 - Pojem absurdní můžeme též chápat jako „velmi nepravděpodobný“.



Jisté slabiny zůstávají

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



Zdroje alternativního vysvětlení

- Kolize hašovacích funkcí
 - Neproběhlo $s \leftarrow \text{Sig}_{\text{Priv}}(m_1)$, ale $s \leftarrow \text{Sig}_{\text{Priv}}(m_2)$, 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 $s \leftarrow \text{Sig}_{\text{Priv}_1}(m)$, 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 $\varphi_1 \neq \varphi_2$.

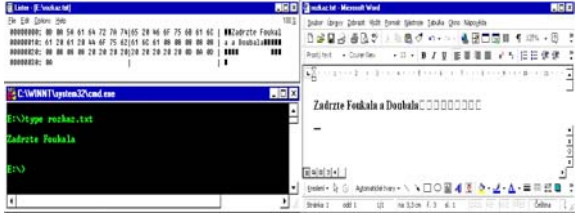


Pozor!

- Útočníkem na nepopiratelnost může být sám oprávněný majitel podepisovacího klíče...
- Pohov!



Sémantická kolize



Mentální hra (pozor, způsobuje nespavost)

1. Čím může útočník náš důkaz zpochybnit?
2. Uvěří mu nezávislý soud?
3. Máme hodnověrný protiargument?
4. Uvěří nám nezávislý soud?
5. Čím může útočník náš argument zpochybnit?
6.

Závěr

- Novum informatiky – **digitální důkaz**.
 - Prostředek k zajištění nepopíratelnosti.
 - Důvěryhodnost určena konstrukcí.
- Přirozený nástroj – **digitální podpis**.
 - Nepopíratelnost 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 nepopíratelnost?*

Děkuji za pozornost...