Open presentation

Miroslav Ludvík
Security Consultant

miroslav@ludvik.cz

Metody útoků

- Technické
- Trash Engineering – beztrestnost
- Social Engineering - Evropa vs. USA
- Agregace databází – příklad z Kalifornie

Útoky na switchovaném ethernetu

- **Nejdříve trocha historie**

  Ethernet

  - koaxiální kabeláž
  - strukturovaná kabeláž (HUB)
  - strukturovaná kabeláž (SWITCH)
  - strukturovaná kabeláž (SWITCH s možností 802.1x)

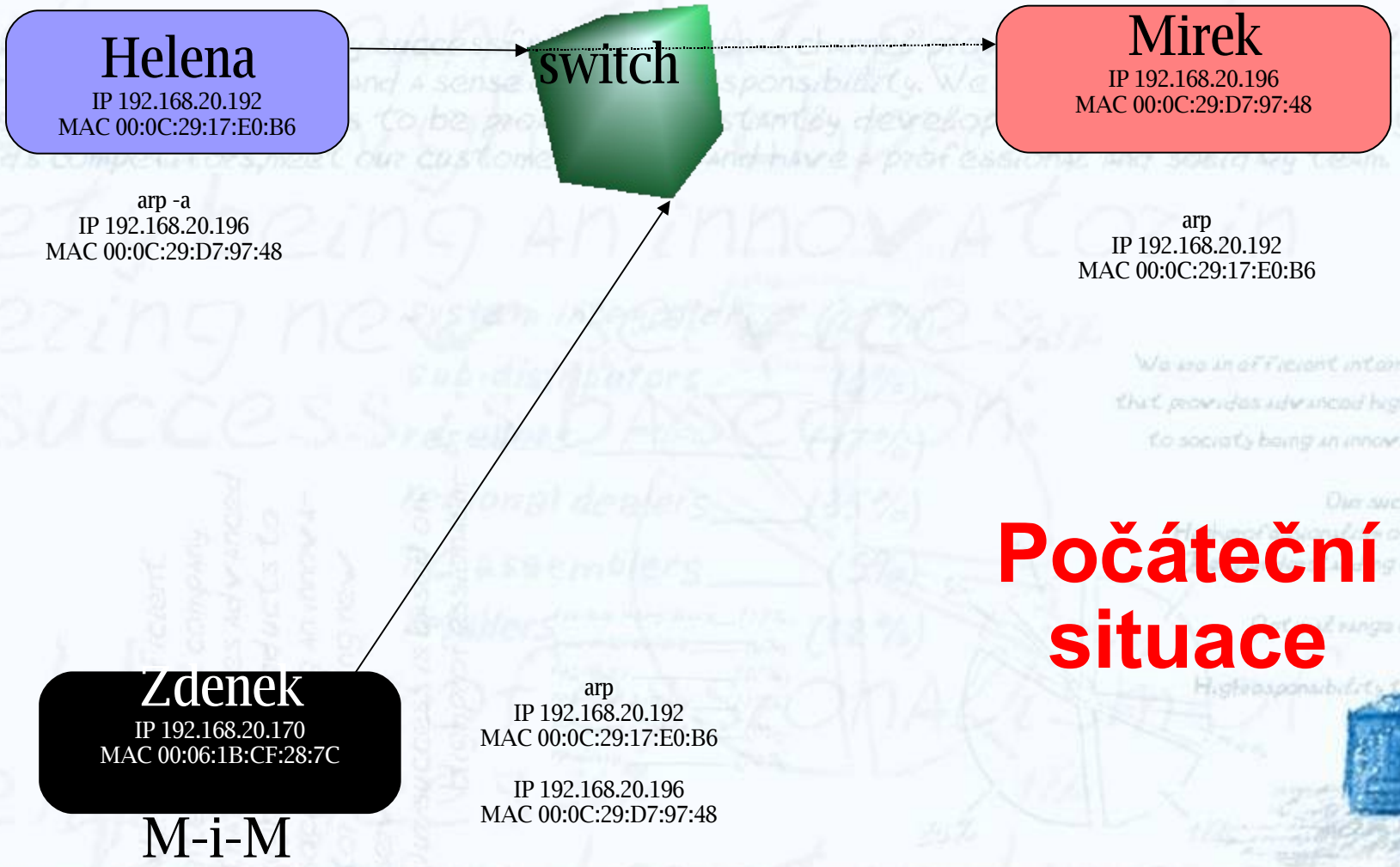
Útoky na switchovaném ethernetu

- **Zbořme mýty**

  Existuje mnoho mýtů v oblasti bezpečnosti. Jeden z nich praví, že na switchovaném ethernetu není možné odposlouchávat, neboť traffic jde jen do portu, kde je adresát.

  Nyní si v praktické ukázce předvedeme ten nejjednodušší, ale velmi účinný způsob založený na špatné implementaci protokolu arp.

Útoky na switchovaném ethernetu

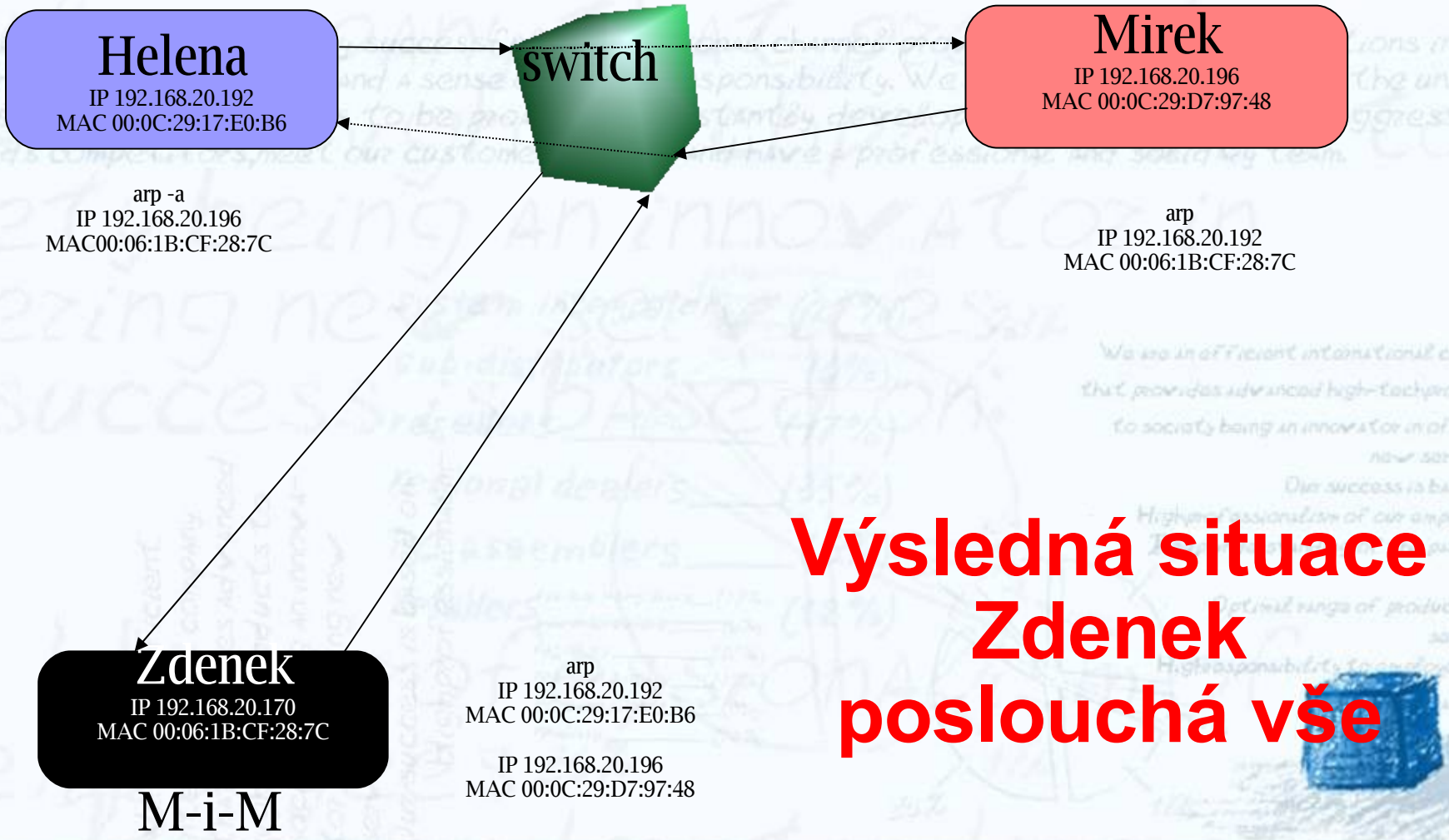


Počáteční situace

Útoky na switchovaném ethernetu

Zdenkovy nekalé aktivity

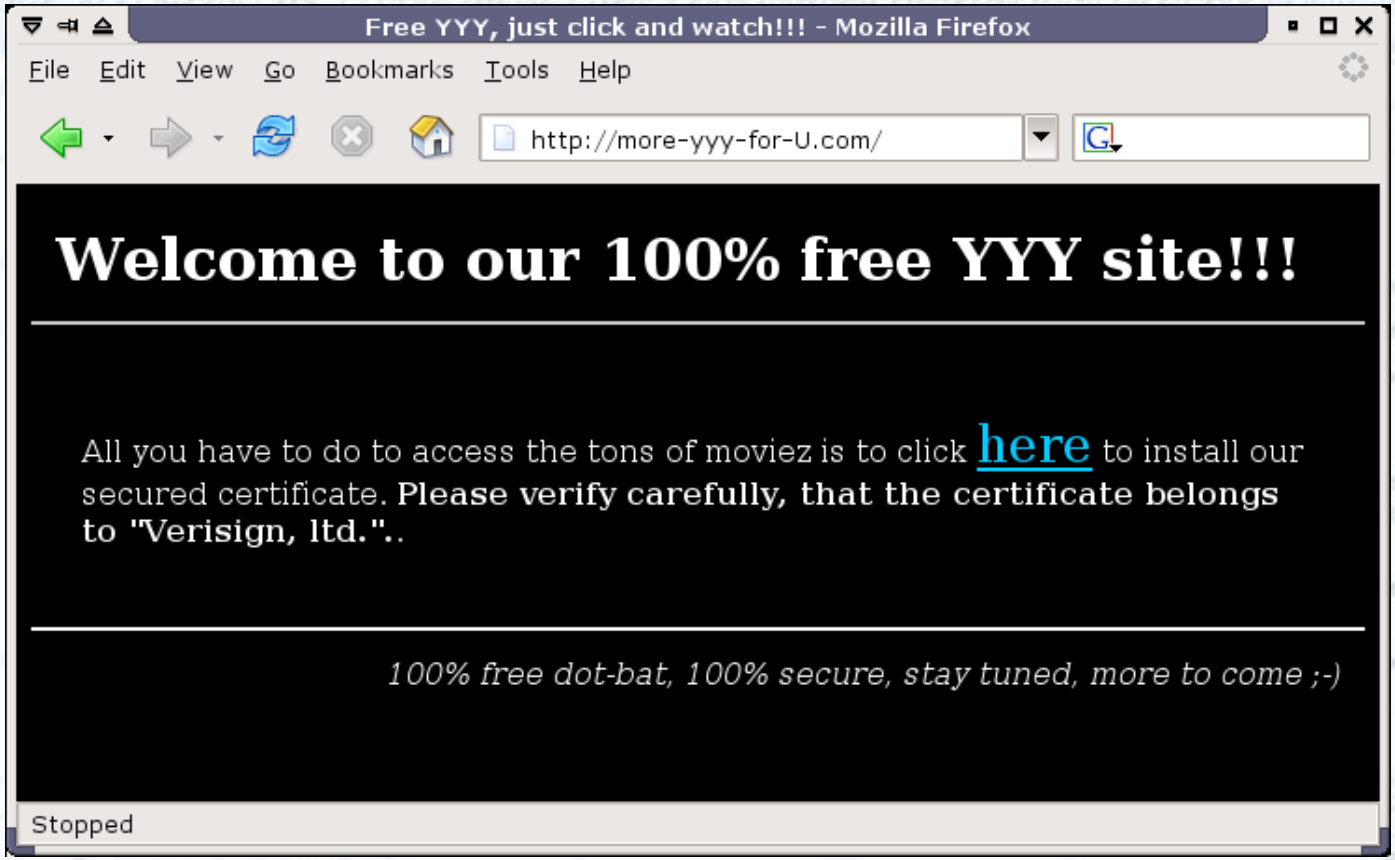
Útoky na switchovaném ethernetu



Výsledná situace
Zdenek
poslouchá vše

Útoky na šifrované spojení

Praktická ukázka útoku

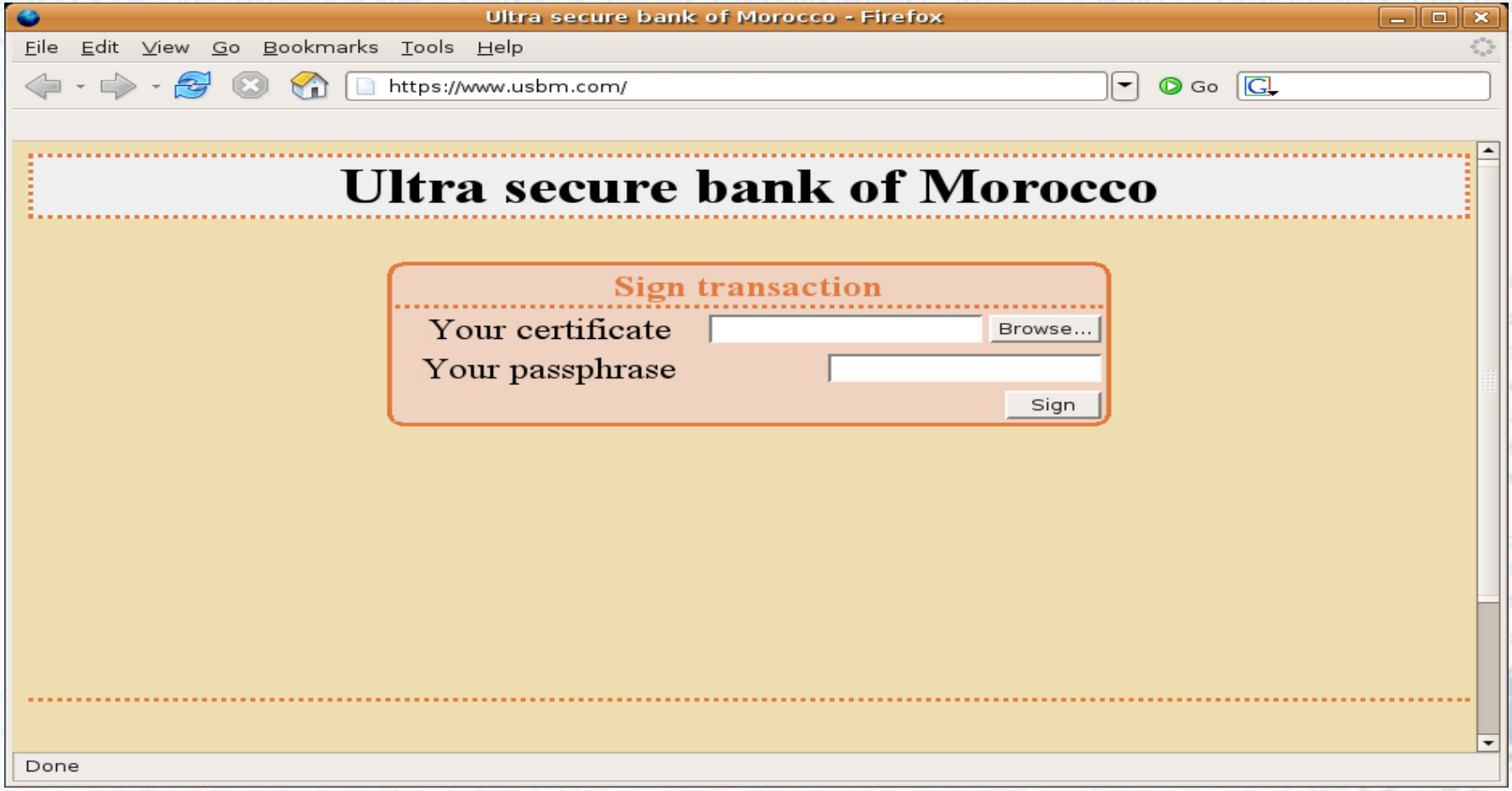


Útoky na šifrované spojení

Praktická ukázka útoku

Útoky na šifrované spojení

Praktická ukázka útoku



Útoky na šifrované spojení

Důvěryhodnost a autentizace

- Více vrstev
- IPSec
- DNSSec
- Telefonické a jiné ověření

Kryptografie

Často opomíjená fakta

Bezpečnost
- podmíněná
- nepodmíněná

Kryptografie

Často opomíjená fakta

Podceňování skutečné situace

Často opomíjená fakta

Současná situace

1994 - Peter Shor nalezl efektivní algoritmy pro kvantový počítač .

Současná kapacita je 7 qubitů a vrcholem bylo rozložení čísla **15** na prvočísla. :)

Pro reálné použitá na “louskání” současných šifer je třeba kapacita v řádu tisíců qubitů.

Nám známé technologie končí na cca 20 qubitech.

Často opomíjená fakta

2007 oznámila společnost D-Wave vytvoření prvního komerčně dostupného počítače obsahujícího **16 qubitů.**

2008 společnost D-Wave předpokládá, že bude mít k dispozici komerčně dostupný počítač obsahující 1000 qubitů !!!

Závěr:

Nová kryptografická primitiva musí být založena na nebodmíněně bezpečných úlohách. Nejlépe na fyzikálních zákonech. Doba, kdy to bude opravdu nutné se velmi rychle blíží.

Jedno z řešení

Kvantová mechanika

Zatím asi nejúplnější pohled na fungování světa
Vhodný kandidát pro kriptografické aplikace
Fyzika malých částic
Masivní paraelismus (umožňuje rychlé počítání)

Základní vlastnosti kvantové mechaniky

Qubit – kvantový bit
pro oblast kvantové kryptografie se užívají fotony
Neznámý kvantový stav NEJDE kopírovat „non cloning theorem“

Druhý úder bezpečnosti

Princip podepisování zpráv

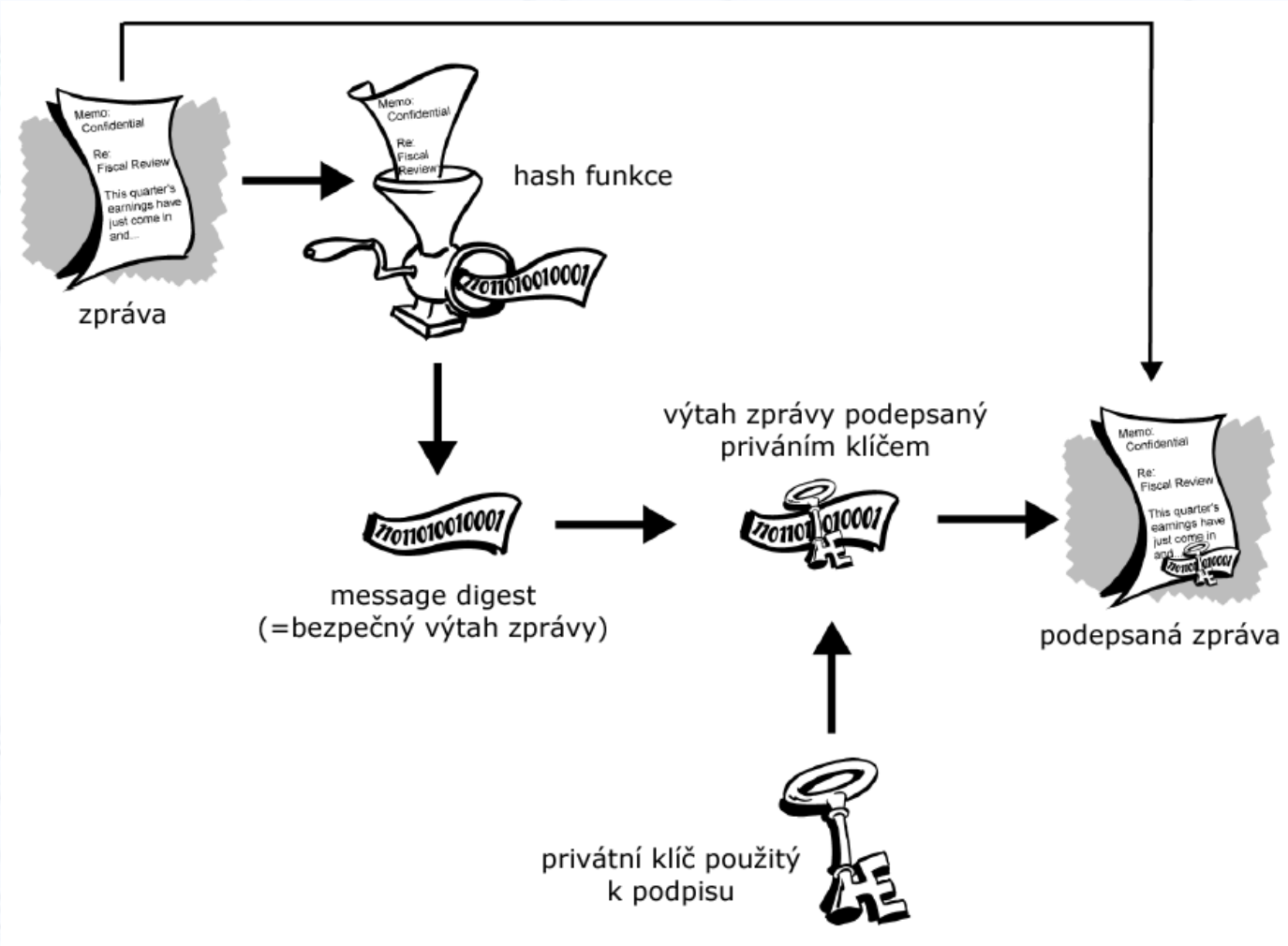
Nepodepisujeme zprávu, ale její hash.

Nejpoužívanější algoritmy pro vytvoření HASHe, jsou MD5 a SHA-1.

MD5 bohužel výrazně převládá.

Oba zmíněné algoritmy jsou kryptograficky prolomeny.

Druhý úder bezpečnosti



Druhý úder bezpečnosti

A co na to naše legislativa

Soud by se nespokojil s „matematickým světem“ a hledal by i jiné důkazy. Právníci tuto situaci mají o mnoho jednodušší, neboť používají pojem, kterému se říká „projev vůle“

Děkuji za pozornost