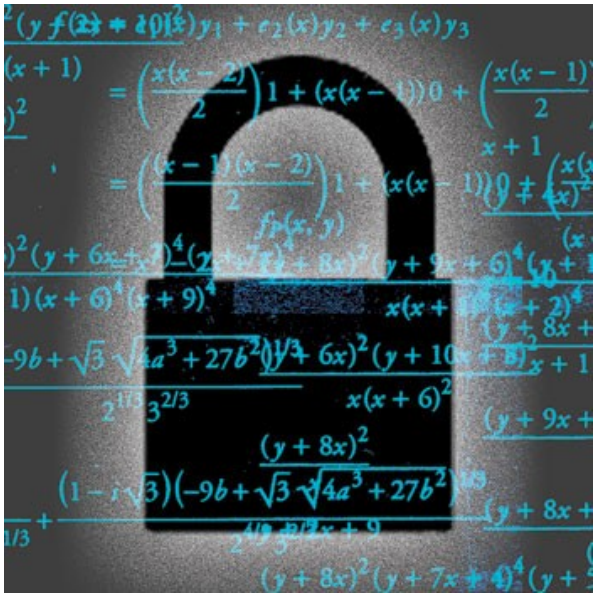
# Kryptografie a bezpečnost

# Kryptografie

- věda zabývající se zajištěním utajené a důvěryhodné komunikace – tedy tvorbou šifer pro lepší zabezpečení nás na síti



# Proč kryptografie?

- Stále větší část našich dat je na síti
- Prostřednictvím internetu děláme i důležité úkony (el. Podpis, žádosti o práci, platby…)
- Kryptografie na síti je stejně logická jako to, že zamykáme svoje domy nebo auta
- S kryptografií se setkáváme každý den, i když si to ani neuvědomujeme -> třeba při přihlašování do IS MU

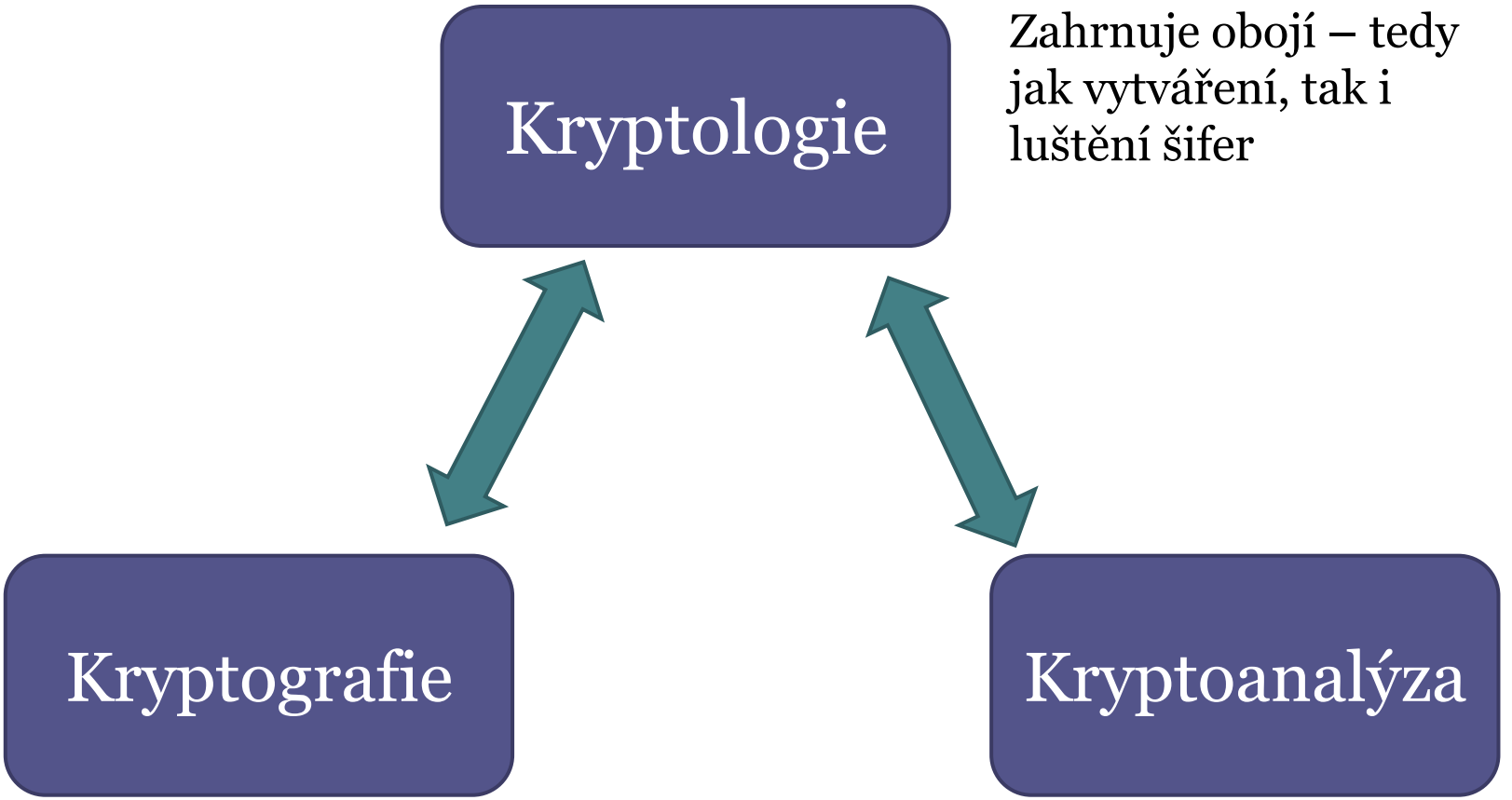
# Něco z historie

- Lidé šifrovali svoji komunikaci již od starověku
- Šifrovali se rozkazy pro vojska, deníky politiků, depeše diplomatů…
- Kryptografie nebyla tedy vědou spojenou s IT, ale obecně s šifrováním zpráv

**Skytalé** - šifrování, který se skládá z válce a na něm navinutém pergamenu na kterém je napsaný vzkaz. Používali je Řekové, kteří ji využívali během válek.

**Enigma** - šifrovací stroj používaný za války německou armádou

# Kryptografie vs. Kryptoanalýza



# Cíle kryptografie

- zabezpečit komunikaci citlivých dat mezi uživatelem a internetovou službou
- zajistit důvěryhodnost komunikace mezi uživateli (např. email)
- autorizace závažných úkolů (ebanking, el. obchody, …)
- omezit přístup k určitým službám jen pro určené jedince (zabezpečená wi-fi)

# Časté omyly uživatelů

- „V tom e-mailu stejně nemám nic co by stálo za to ukrást.“ – chyba. Stačí i to, že znají vaše e-mailové heslo, které může být stejné/podobné jako heslo k e-bankingu, pracovním datům a podobně
- „Jaká je pravděpodobnost, že se to stane zrovna mě?“ – docela slušná. Data o uživatelích dnes kradou často autonomní programy. Pokud odhalí že máte slabé zabezpečení zaměří se na vás.
- I když vy sami nejste pro hackera zajímavý, může z vašich dat získat informace třeba o vašem zaměstnavateli

# Co tedy napomáhá k naší ochraně?

- Dobré heslo
- Certifikační systém
- Šifrované spojení
- Zdravá paranoia ☺

# Autentizace

- … je ověření identity uživatele, který se pokouší přihlásit do služby, systému apod. (od slova autentický)

## Autentizace – jak se provádí?

❖podle toho, co uživatel zná (zná správnou kombinaci uživatelského označení a hesla nebo PIN)

❖podle toho, co uživatel má (nějaký technický prostředek, který uživatel vlastní – hardwarový klíč, smart card, privátní klíč apod.)

❖podle toho, čím uživatel je (uživatel má biometrické vlastnosti, které lze prověřit – otisk prstu, snímek oční duhovky či sítnice apod.)

❖podle toho, co uživatel umí (umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz)

# Heslo – vaše osobní šifra

# Co je to „dobré heslo“

- …je takové, co půjde špatně odhalit ☺
- 1) Heslo by se neměl tvořit nějaký snadno dohádatelný údaj o uživateli. – tedy ne vaše jméno, jména vašich dětí apod.
- 2) Mělo by být dostatečně dlouhé – čím delší tím déle trvá jeho odhalení. S každým dalším znakem se násobí časová  délka nutná k jeho odhalení
- 3) Mělo by obsahovat velká a malá písmena, čísla a speciální znaky (@, ?). Nejdůležitější je ale jeho délka

# Jak s heslem zacházet

- hesla k důležitým službám (ebanking, IS, email, ...) nesmí být stejná
- heslo nikdy nikomu nesdělujte
- důležitá hesla neukládejte v prohlížeči, ani je nikam nezapisujte
- po zadání hesla na nedůvěryhodném stroji (např. na cestách) jej při nejbližší příležitosti změňte

Klikni zde

Něco více o heslech

# Útoky na hesla

- **Sociální inženýrství** - patří mezi nejúčinnější metody útoků . Útočník se snaží zjistit buď přímo zjistit heslo, nebo informace, které ho k heslu dovedou. Prostě se vás zeptá. Druhá varianta je zjistit si základní informace o daném člověku a potom zkusit zmiňované jméno partnera, dětí, dalších rodinných příslušníků, nebo domácích zvířat.

- **Odchycení hesla-** používají se například keyloggery (programy pro snímání stisknutých kláves na klávesnici).

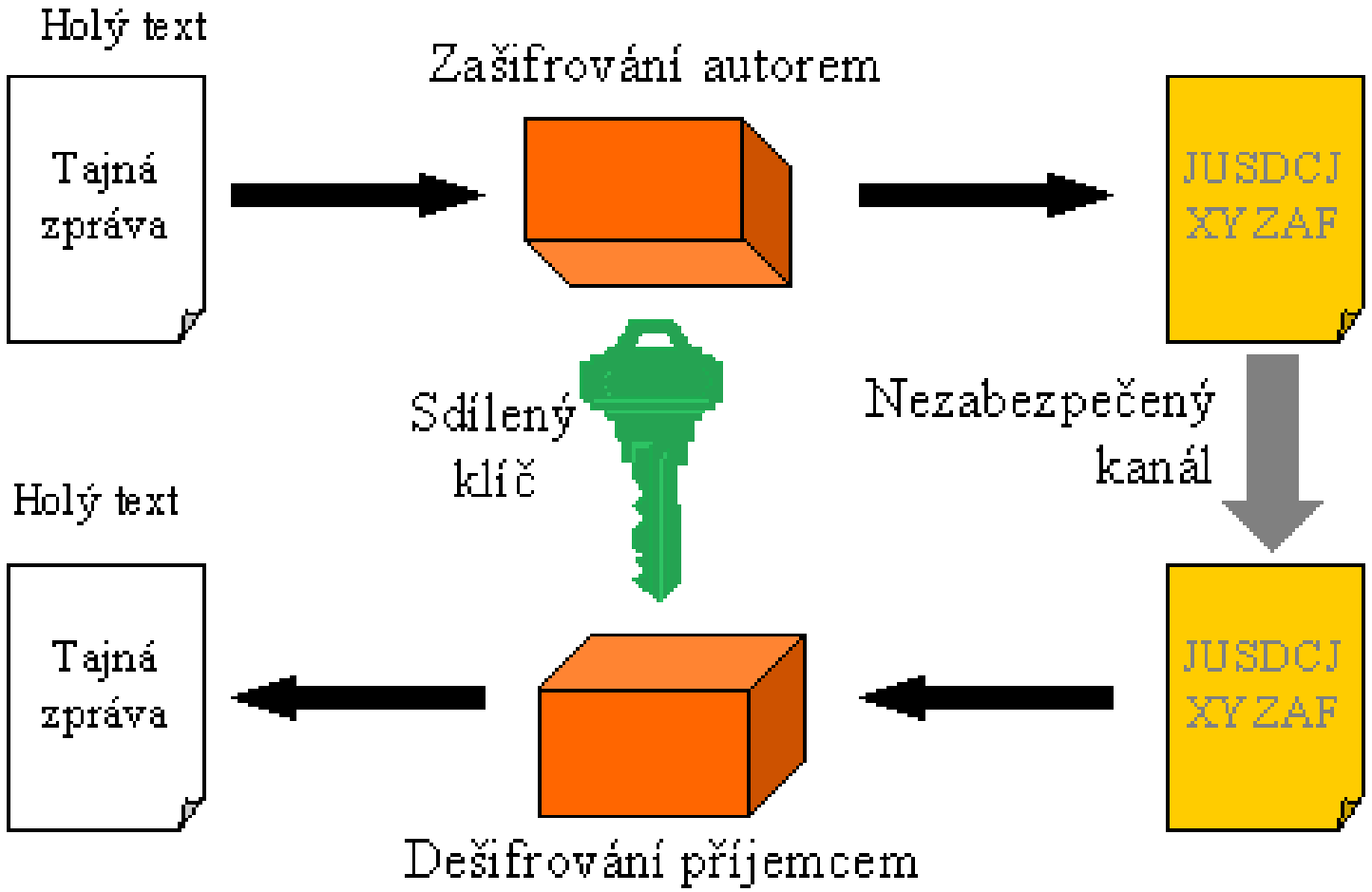
- **Slovníkový útok -** Útočník má slovník slov daného jazyka a zkouší zadat jako heslo jednotlivá slova z tohoto slovníku. Nezadává ručně, ale automaticky pomocí počítačového programu. Takovým způsobem pak může vyzkoušet mnoho hesel za sekundu.

- **Útok hrubou silou -** Nejprimitivnější varianta útoku, útočník zkouší postupně zadávat všechny kombinace, například: aaa, aab, aac, aad,...

# Symetrická kryptografie

- Funguje na jednodušším principu než asymetrická
- Odesilatel  i příjemce zprávy mají ten stejný klíč k zašifrování i rozšifrování – typicky heslo
- **Příklad:** Posíláte symetricky zašifrovaná data vašemu známému. Jako heslo si určíte „heslo123“ , které mu předtím řeknete. Vy toto heslo použijete na zašifrování dat on toto stejné heslo použije na rozšifrování dat a převedení zašifrovaných dat zpět do podoby běžného textu. Je to v principu stejné jako když má více lidí stejný klíč k jedněm dveřím

# Symetrické šifrování



# Symetrická kryptografie

- Výhody:
- Jednodušší na výpočetní výkon – symetrická šifra je vytvořena velice rychle
- Nevýhody:
- Nutnost předání soukromého klíče druhé straně

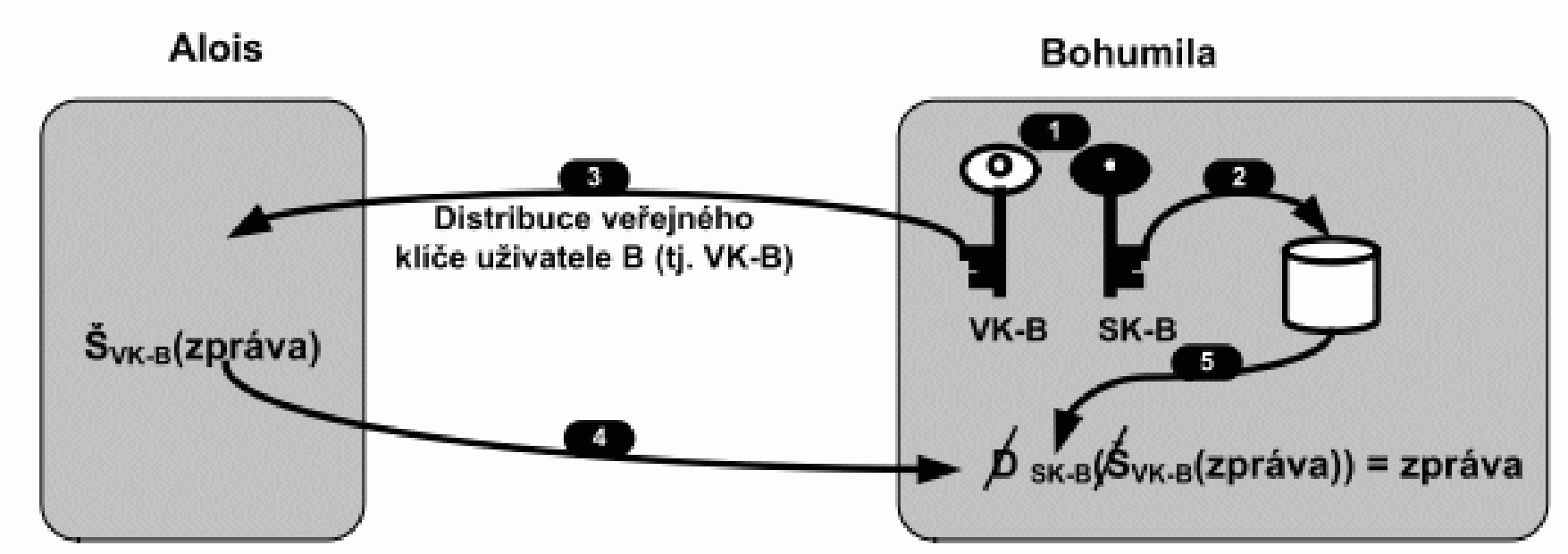
# Asymetrická kryptografie

- Tyto šifry nepoužívají jeden tajný šifrovací klíč sdílený mezi odesilatelem a příjemcem, ale vždy se používá **pár šifrovacích klíčů**. Jeden klíč **pro šifrování** a **druhý pro dešifrování**. U digitálního podpisu pak uvedeme, že operace šifrování a dešifrování jsou u některých šifer zaměnitelné, proto u asymetrických šifer nemluvíme o šifrovacím a dešifrovacím klíči, ale o **veřejném a soukromém klíči**.

# Asymetrická kryptografie

- Bohumila, tj. příjemce zprávy, si musí vygenerovat dvojici klíčů: **veřejný klíč** (VK-B) a **soukromý klíč** (SK-B).
- Bohumila si uloží svůj soukromý klíč do důvěryhodného úložiště klíčů. Např. na disk, na čipovou kartu atd. **Soukromý klíč je aktivem Bohumily, které si musí střežit.**
- Bohumila distribuuje svůj veřejný klíč (VK-B) **do celého světa**. Klidně může svůj veřejný klíč poslat Aloisovi po slídivém Cyrilovi.
- Alois po obdržení veřejného klíče Bohumily šifruje zprávu Bohumile jejím veřejným klíčem (VK-B).
- Bohumila (příjemce) dešifruje přijatou šifrovanou zprávu svým soukromým klíčem (SK-B) a získá původní zprávu.

# Asymetrická kryptografie




- Základní vlastností šifrování na bázi asymetrických algoritmů je skutečnost, že je relativně jednoduché za využití veřejného klíče šifrovat text, ale na základě znalosti veřejného klíče a veřejným klíčem šifrované zprávy je velice obtížné získat původní zprávu.

# Elektronický podpis

- Vychází z principů asymetrického šifrování

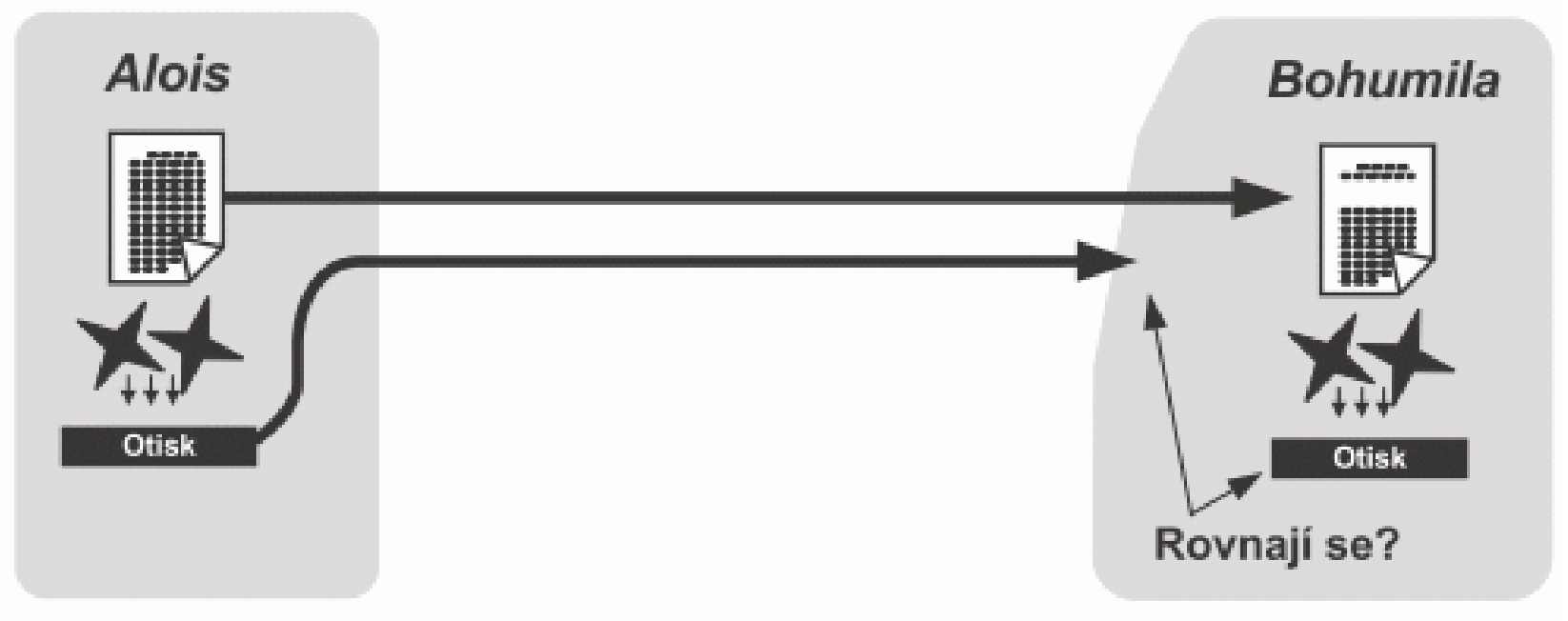
- El. podpis je potvrzení, že zpráva byla vytvořena daným autorem
- realizován pomocí asymetrické kryptografie:
  - pomocí soukromého klíče je k dané zprávě vytvořen podpis
  - příslušný veřejný klíč umožňuje ověřit pravost podpisu

# Hash – kontrolní výpočet


- Krátký **otisk** textu (zprávy, hesla) vytvořený jednocestnou funkcí. Pro daný text je hash jednoznačně daný, nelze z něj ale zrekonstruovat žádné informace o původním textu

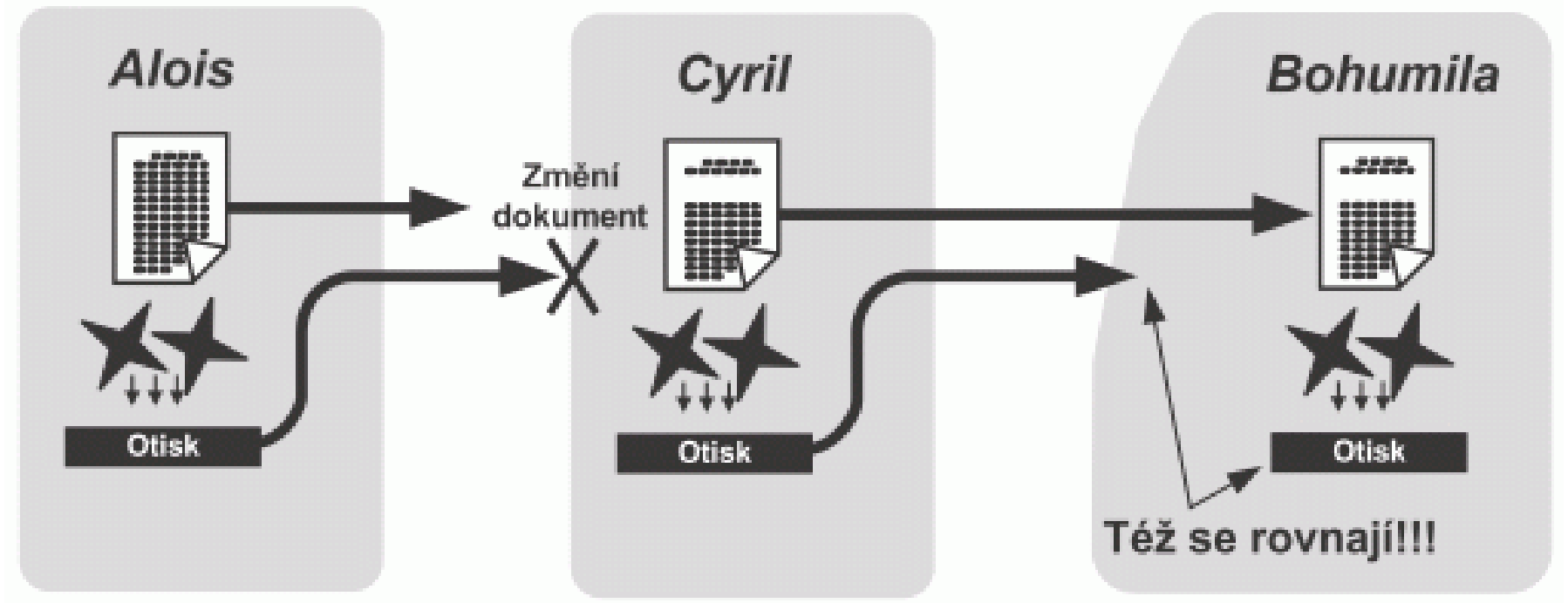
- …. ale lze jej použít pro kontrolu přijaté zprávy, že nebyla cestou změněna

# Hash – jak funguje?




- Alois posílá zprávu Bohumile. Spolu s ní odešle hash. Bohumila, poté co přijme zprávu, spočte otisk (hash) z přijaté zprávy a porovná svůj výsledek s otiskem ze zápatí přijaté zprávy (tj. s otiskem spočteným Aloisem). Pokud jsou oba otisky shodné, zpráva nebyla cestou změněna.

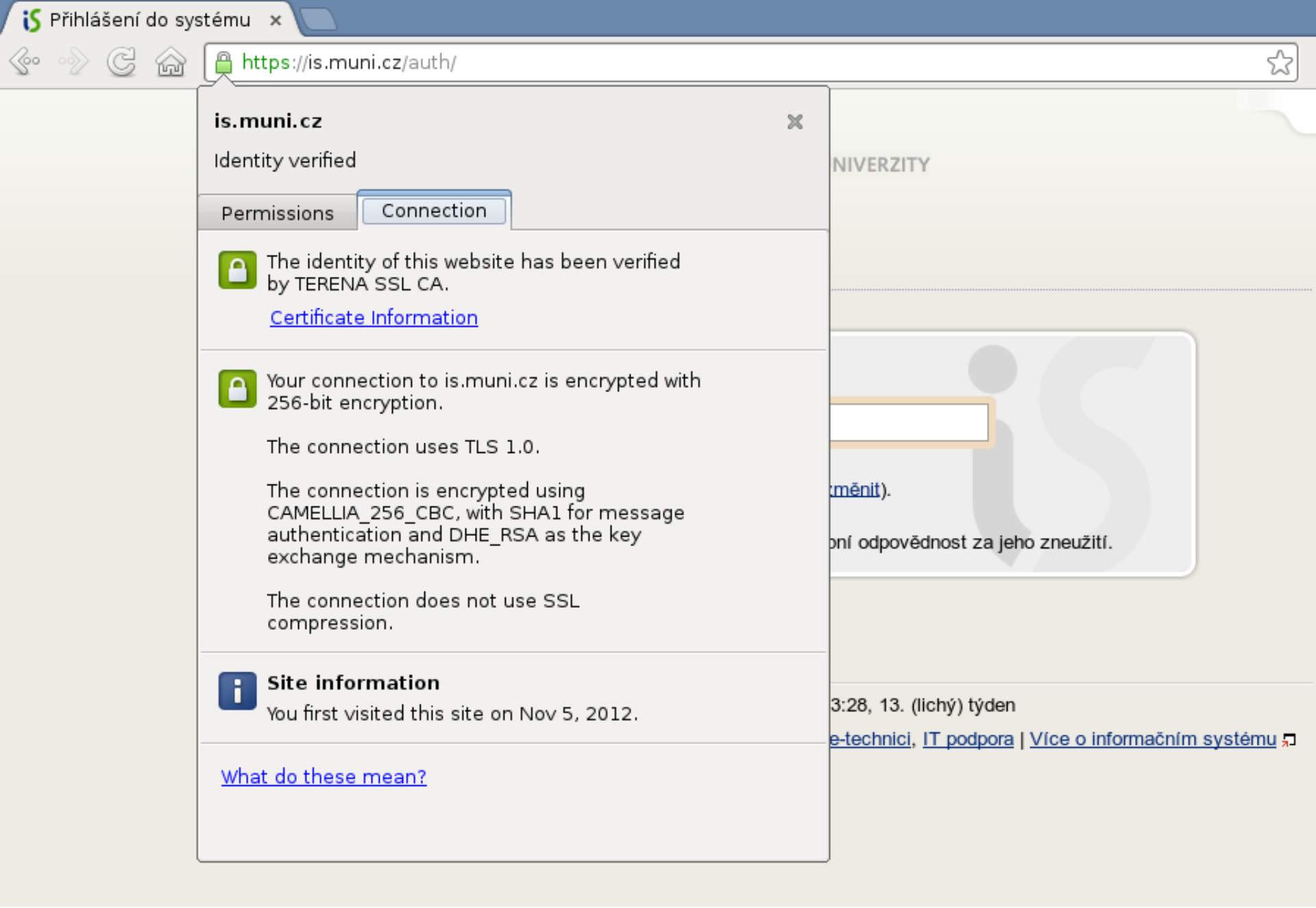
# Hash – jak funguje?



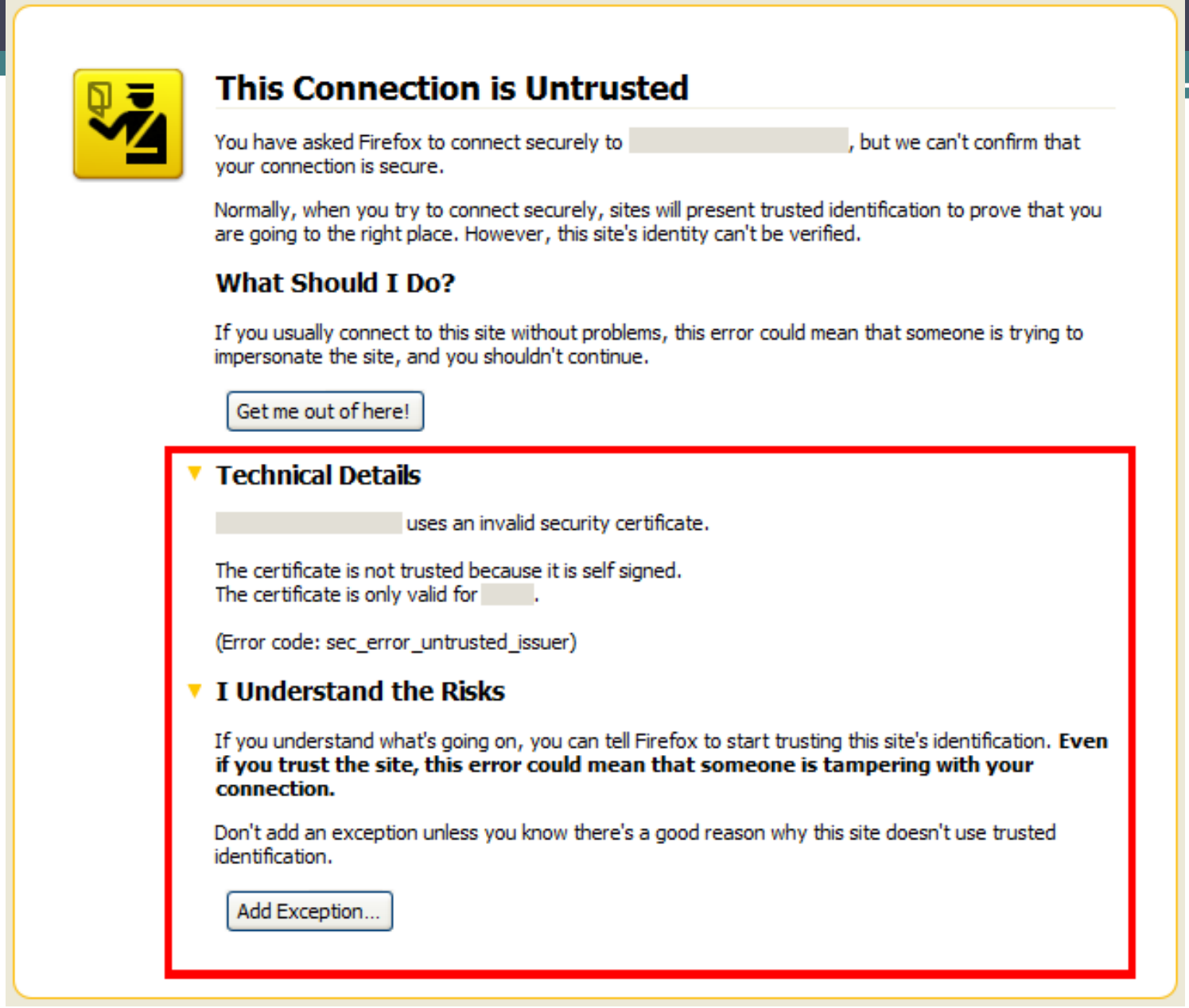

- Zprávu odchytí (a tím pozmění) slídil Cyril. Zpráva dojde (pozměněná) Bohumile. Tím že došlo ke změně zprávy, tak už nejde zpětně dopočítat hash, Bohumila tedy ví, že zpráva byla po cestě změněna.

# Certifikace pomocí https

- Nástavba běžného http protokolu, který není šifrován
- U https jsou využívány certifikáty důvěryhodnosti, které vydává nějaká velká certifikační autorita
- Dnešní prohlížeče s certifikáty umí běžně pracovat a pokud web žádnou certifikaci nemá (nebo ji jen předstírá) snaží se vás většinou varovat




- Certifikát v Google Chrome



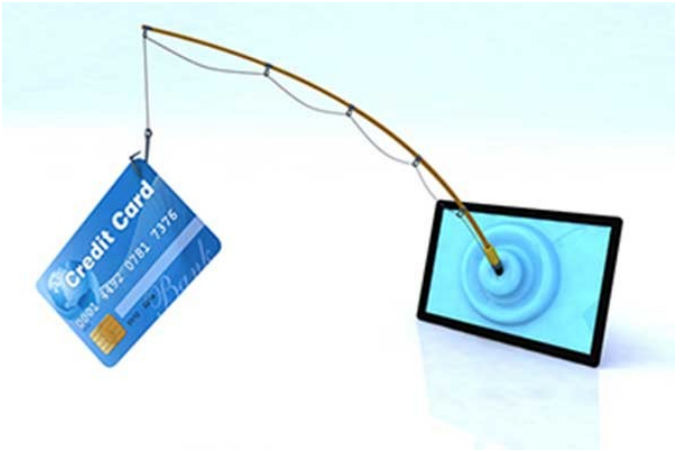

- Odhalení nedůvěryhodného certifikátu

# Některé formy útoku

- **Phising** – podvržené stránky a zahrávání si s psychologií uživatele
- **Útoky na hesla** – různé metody jak odhalit vaše heslo. Viz. kapitola o heslech
- **Odposlech bezdrátové komunikace**
- **Malware** – různé druhy škodlivého softwaru, které mohou získat vaše hesla, nebo přímo data

# Psychologie v útoku - phishing

- *Only amateurs attack machines; professionals target people.*
  - *— Bruce Schneier*



# Phishing

- Pro útočníka je jednodušší využít neopatrnosti cíle (vás) a jeho oklamání, než složitě nabourávat šifrované stroje

- Evolučně jsme si vytvořili poznávací mechanismy, proti podvodům z očí do očí, teď se musíme naučit mechanismy pro odhalení podvodů skrze monitor.

# Phishing – jak funguje


- Vytvoření návnady  (falešná stránka vaší banky)
- Rozeslání e-mailů uživatelům (výzva ke změně hesla, kontrole údajů…)
- Uložení vašich údajů u útočníka
- …poté proběhne standardní přihlášení do běžné služby, aby se nevytvořilo podezření


THE NIGERIAN PRINCE NEEDS MY HELP?
I'LL GET MOM'S CREDIT CARD!

# Šifrování wifi vs. odposlech

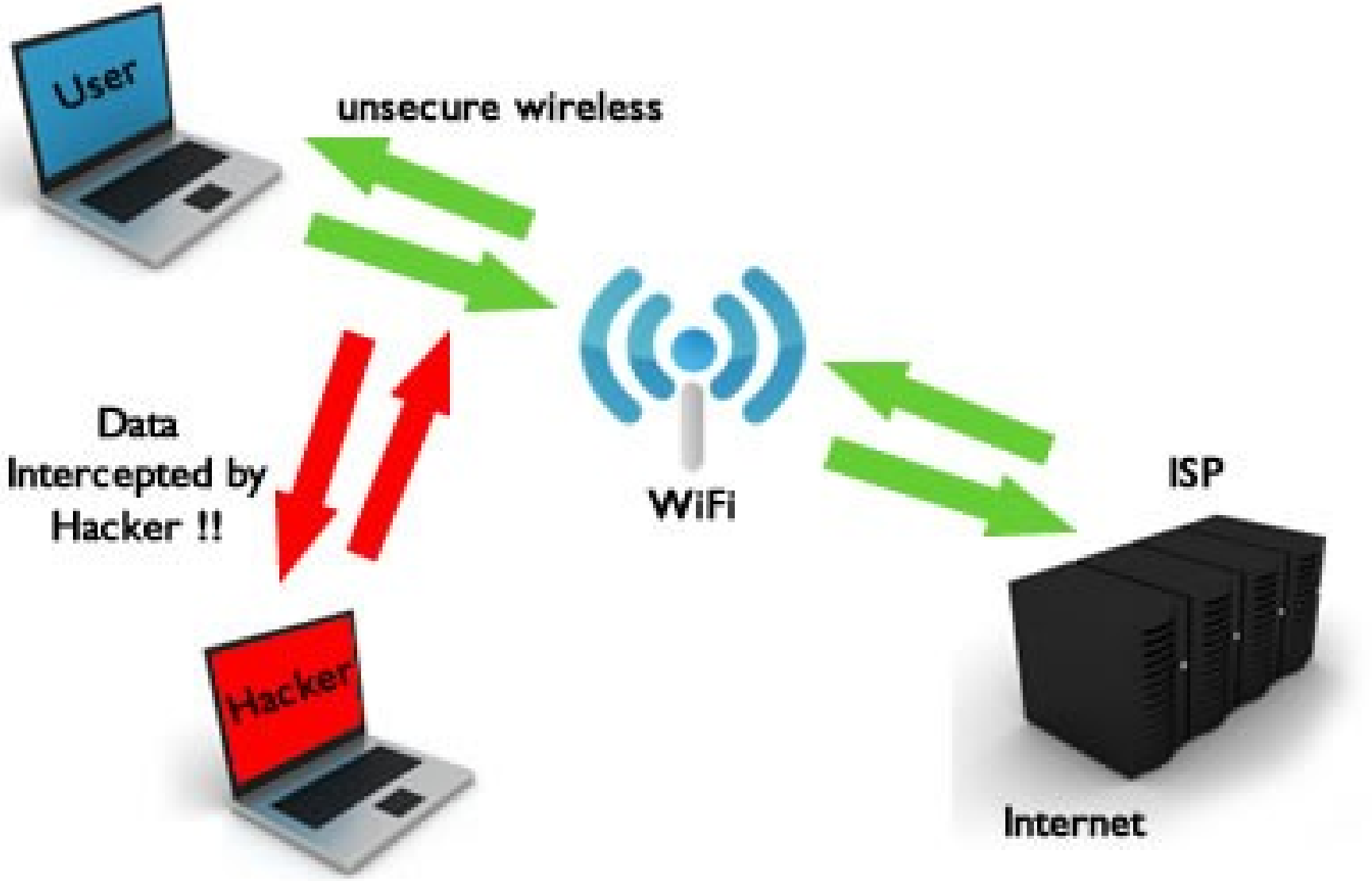
- Na rozdíl od pevné (drátové) sítě nelze fyzicky omezit přístup k bezdrátové síti. U wifi není možné zjistit, zda probíhající komunikaci někdo nesleduje (a nenahrává). Z těchto důvodů se zavádí autentizace (přihlašování) při připojení síti a šifrování provozu přihlášených uživatelů

- Pozor tedy na wifi zdarma! ☺

# Útok na wifi

- **Odposlech**
- není možné jeho aktivitu zjistit
- v případě nešifrované (nebo slabě šifrované — WEP) vidí veškerou komunikaci vedenou mimo zabezpečené protokoly (např. https)
- může sledovat například osobní údaje, stahované dokumenty a další data putující sítí, které mu umožní vést přímé útoky: vydávání se za uživatele (krádež identity), získání přístupu přes fingovanou ztrátu hesla a pod.

- **Ofenzivní útočník**
- v případě slabého šifrování může získat klíč pro vstup do sítě (WEP)
- může získat přístup k nastavení přípojného bodu (a využít jej např. ke sledování aktivity na síti)
- po získání přístupu do sítě útočit na jednotlivé počítače (i tak jednoduše, jako vyhledávání nevědomky sdílených složek)
- vytvořit volně přístupný přípojný bod, na kterém bude sledovat veškerou komunikaci


User
unsecure wireless
Data
Intercepted by
Hacker !!
WiFi
ISP
Hacker
Internet

# Jak se tedy bránit?

- **jako uživatel**
  - nepřipojujte se k nedůvěryhodným přípojným bodům
  - používejte zabezpečený protokol https
  - mějte zapnutý firewall
- **při nastavení domácí sítě**
  - změňte výchozí hodnoty pro název sítě a heslo pro administraci
  - vyberte šifrování provozu pomocí WPA (WPA-2), **WEP varianta je dnes již považována za slabou**
  - zvolte dostatečně silné heslo (viz výše)

# Malware

- = škodlivý software, jehož účelem je poškození, nebo infiltrace počítačového systému

- Řadí se sem různé viry, trojské koně, keylogery, atp.

- Pomocí malwaru je možné:
  - Získávat data a údaje z postiženého PC (třeba hesla, soukromá data…)
  - Použít ovládnutý počítač k nelegální aktivitě (rozesílání dalších virů, útokům na velké cíle…)

# Některé druhy malwaru

- Trojský kůň – vydává se za užitečný SW, po instalaci uživatelem provádí svoji pravou funkci
- Keylogger – program který snímá stisknuté klávesy (odposlech hesel)
- Adware – méně škodlivý, způsobuje časté zahlcování reklamou

# Rady na závěr

- Buďte paranoidní ! Pomáhá to ☺
- Nepodceňujte svoji významnost !
- Když nevíte nechte si poradit od vašeho správce sítě!
- Vždycky někdo někde poslouchá !

# Zdroje


- http://prf-czv.osu.cz/nabidka/seminar/data/Kryptografie.pdf
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c05.pdf
- http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/mzka.png
- http://frakira.fi.muni.cz/~izaak/PBIT/Kryptografie_a_bezpe%C4%8Dnost.html
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf
- http://www.flops.cz/zaklady-sifrovani-symetricka-a-asymetricka-kryptografie
- http://cs.wikipedia.org/wiki/Autentizace
- http://www.guardmyip.com/images/wireless_security1.jpg

- DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.