Inovace bakalářského studijního oboru Aplikovaná chemie

http://aplchem.upol.cz

CZ.1.07/2.2.00/15.0247

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Internet a zdroje

Bezpečnost na Internetu

Petr Jakubec

Tomáš Zelený

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
OKRESNÍ HOSPODÁŘSKÁ KOMORA OLOMOUC
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Inovace bakalářského studijního oboru Aplikovaná chemie

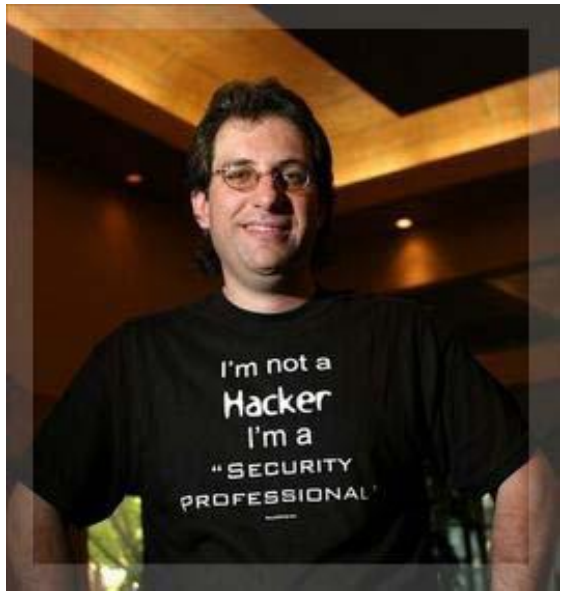
Základní typy útoků

1. network packet sniffers – neautorizovaný odposlech paketů
2. IP spoofing – paket, který obsahuje zfalšované informace (předstírá, že pochází odjinud, než doopravdy) – předvoj DoS útoku
3. útoky na hesla (Password Attacks) – trójský kůň, IP spoofing, dictionary program, sociální inženýrství atd.
4. útoky z cílem přenést citlivé interní informace z interních zdrojů k neautorizovaným externím zdrojům s cílem zneužití těchto informací
5. neutorizované vstupy do komunikačního kanálu, tzv. útoky "Man-in-the-Middle„
6. útoky na síťové služby s cílem způsobit jejich nedostupnost, tzv. útoky DoS (Denial of Service) a DDoS (Distributed Denial of Service)

Sociální inženýrství

Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace

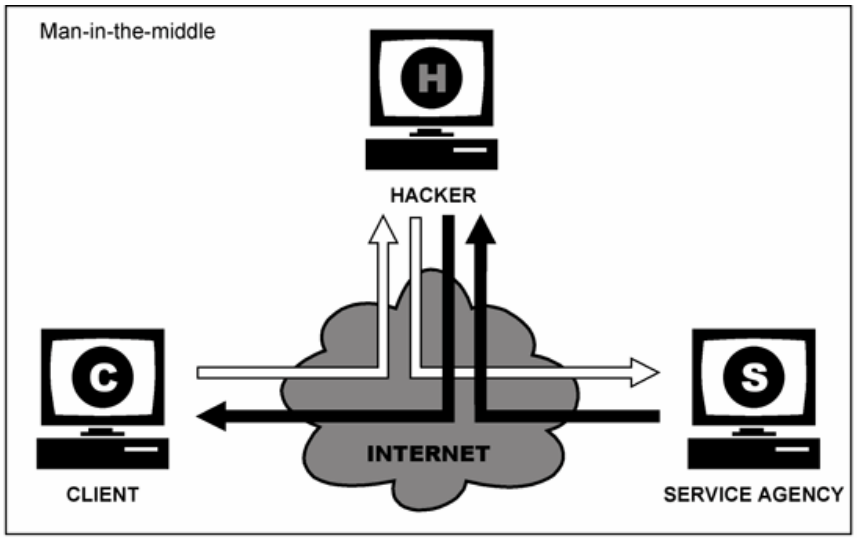
- **Techniky sociálního inženýrství:**
  - **Pretexting**
    - využívání vymyšleného scénáře → skloubení lži s kouskem pravdivé informace získané dříve (datum narození, rodné číslo, jméno šéfa)
  - **Phishing**
    - internetový podvod (př. snaha získat přístup k bankovním účtům)
  - **IVR (telefonní phishing)** → falešné hlasové automaty
  - **Baiting** → trojské koně reálného světa (zanechání infikovaných médií: CD, Flash disků na „vhodném místě“)



Kevin David Mitnick (* 6. října 1963)

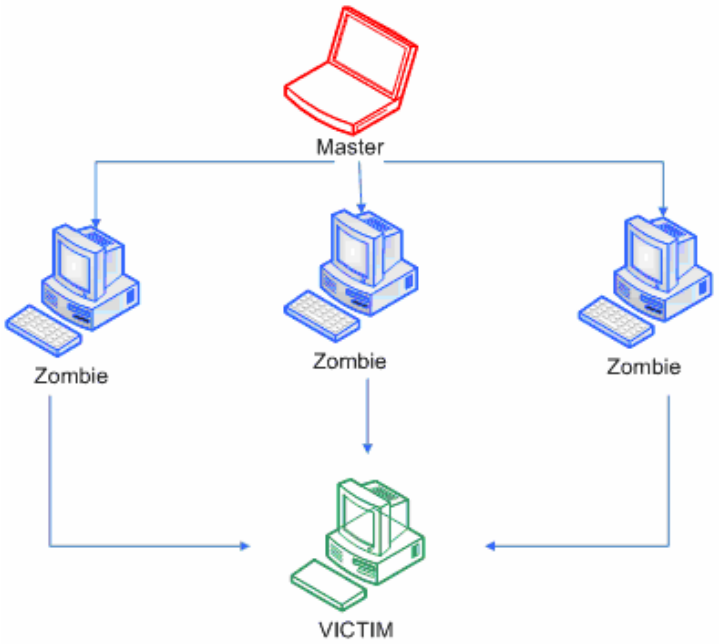
Útoky Man-in-the-Middle

- **Man in the middle** (člověk uprostřed) → odposlouchávání komunikace mezi účastníky tak, že se útočník stane aktivním prostředníkem
- **Řešení problému:**
  - vzájemnou výměnou veřejných klíčů jiným, bezpečným kanálem
  - ověřením získaných veřejných klíčů jiným bezpečným kanálem, nejlépe pomocí jejich otisku
  - ověřením klíčů pomocí elektronického podpisu pomocí certifikační autority nebo sítě důvěry
  - **Kvantová kryptografie** – propletenost a polarizace fotonů



Útoky DoS (1. část)

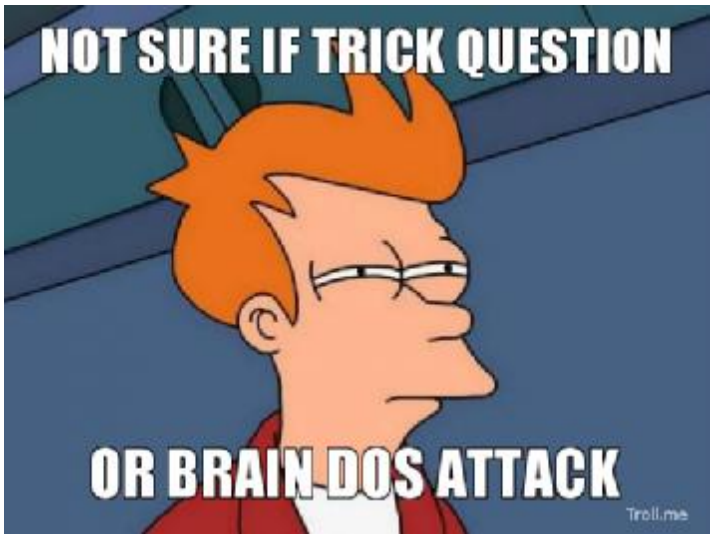
- **DoS** (**D**enial **o**f **S**ervice) – technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele
- Projevy útoku:
  - zaplavení provozu na síti náhodnými daty které zabraňují protékání skutečných dat
  - Zabránění nebo přerušení konkrétnímu uživateli v přístupu ke službě
  - Narušení konfiguračního nastavení
  - Extrémnímu zatížení CPU cílového serveru
  - Pád samotného operačního systému



Útoky DoS (2. část)

Typy útoku

- **ICMP floods**
  - **Smurf attack** – chyba v kofiguraci systému → rozeslání paketů všem počítačům zapojených v síti přes Broadcast adresu
  - **Ping-flood** – zahlcení cílového počítače žádostmi o ping odezvu
- **Teardrop útok**
  - zaslání IP fragmentu s překrývajícím se příliš velkým nákladem dat na cílový počítač
- **Peer-to-peer útok** – využití masivního zástupu lidí na P2P sítích (zneužití bugu v klientu `DC`)



Jak se bránit?

1. **Používat aktuální antivir, antispyware, firewall**
2. **Pravidelně aktualizovat používaný operační systém** a užívané programy (zejména prohlížeče a jejich pluginy. `Flash, Java`)
3. **Používat bezpečné heslo**
4. Kontrolovat u podezřelých stránek jejich skutečnou adresu v řádku prohlížeče
5. Neotvírat neznámé či podezřelé soubory, programy nebo přílohy poštovních zpráv
6. **K citlivým službám se připojovat pouze z vlastního počítače** a nikdy přes neznámou wifi nebo z internetové kavárny




Jak se bránit? (2. část)

7. **U internetového bankovnictví se řádně odhlašovat ze služby**
8. K zabezpečení e-mailové komunikace používat vhodné programy jako `PGP`, `GnuGP`
9. Pamatovat že smazaná data nejsou na disku ve skutečnosti smazána, ale pouze označena k přepsání
10. **Pravidelně zálohovat důležitá data**
11. V sociálních sítích využívat co nejméně aplikací třetích stran (her, kvízů atp.)
12. **Uvažovat, které informace o sobě internetu poskytujete**

Antiviry

Virus = typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama

Další info → Igiho stránka o virech: `www.viry.cz`

Program	kategorie hodnocení		
	ochrana	oprava	použití
BitDefender: Internet Security Suite 2011	6,0	4,0	5,5
BullGuard: Internet Security 10.0	5,5	2,0	3,5
F-Secure: Internet Security 2011	5,5	4,5	5,5
Kaspersky: Internet Security 2011	5,5	4,5	4,0
Symantec: Norton Internet Security 2011	5,5	5,0	4,5
AVG: Internet Security 10.0	5,0	4,0	4,5
G Data: Internet Security 2011	5,0	4,0	5,0
Panda: Internet Security 2011	5,0	4,5	4,5
Webroot: Internet Security Complete 7.0	4,5	5,0	3,0
Avira: Premium Security Suite 10.0	4,0	3,5	4,0

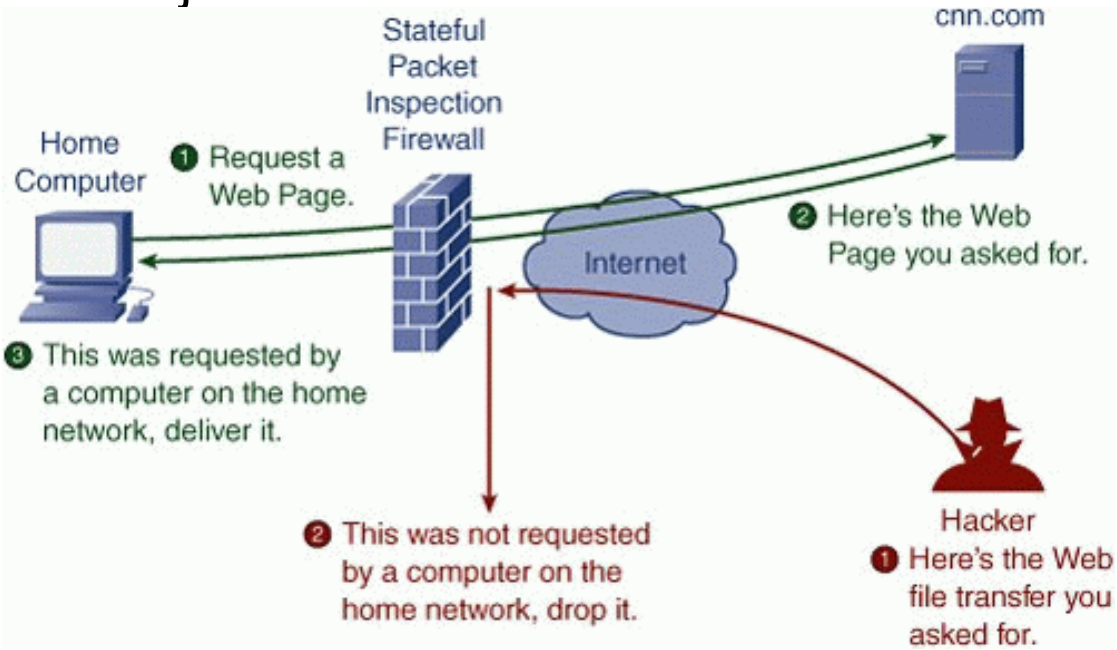
Test antiviru 2011 (společnost AV-Test GmbH; `www.av-test.org`)

Firewall

- síťové zařízení/aplikace, sloužící k řízení a zabezpečení síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
- **Zjednodušeně:** kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje

Rozdělení firewallů:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS



Firewall – podrobněji

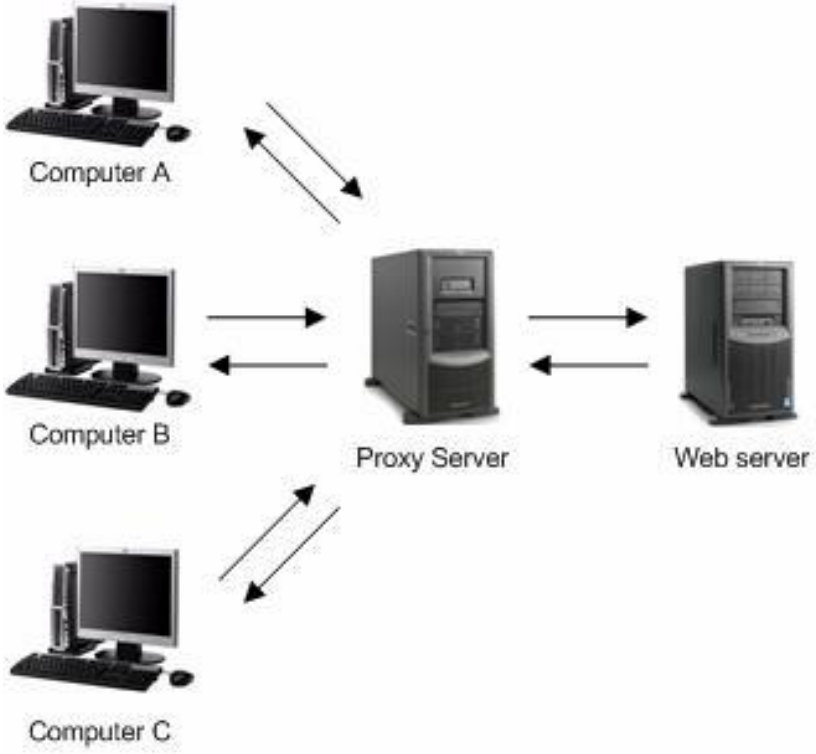
Paketové filtry: Nejjednodušší a nejstarší forma firewallování

- pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket
- **Výhoda:** vysoká rychlost zpracování (vysokorychlostní přenosy velkých množství dat)

Aplikační brány (Proxy firewally):

- **Průběh komunikace →**

klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi



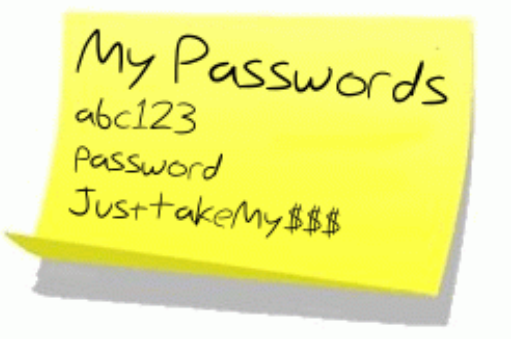
Firewall – podrobněji 2

Stavové paketové filtry:

- kontrola jako u paketových filtrů + ukládaní informací o povolených spojeních → usnadnění rozhodnutí zda pakety pustit nebo ne
- Výhody:
  - urychlení zpracování paketů již povolených spojení
  - nastavení směru navazování spojení → firewall sám povolí odpovědní pakety
  - Vysoká rychlost, relativně solidní úroveň zabezpečení (je horší než u Aplikační brány), jednoduchá konfigurace
- Příklady:
  - Komerční: Cisco PIX, Cisco IOS Firewall
  - Free: `iptables` v linuxovém jádře a `ipfw` v *BSD

Bezpečné heslo

- **Nevhodná volba hesla:**
  - vlastní jméno či jméno někoho z rodiny, jméno psa, milenky apod.
  - rodné číslo či datum narození
  - č. domu, adresa, telefonní číslo...
  - heslo, 1234...
- **Délka hesla:** minimálně 8 znaků (nejlépe 14+)
- **Kvalita hesla:** kombinace písmen, čísel a znaků
  - Heslo skládající se z 15 náhodných písmen a číslic je přibližně 33 tisíckrát bezpečnější než heslo tvořené 8 znaky z celé klávesnice



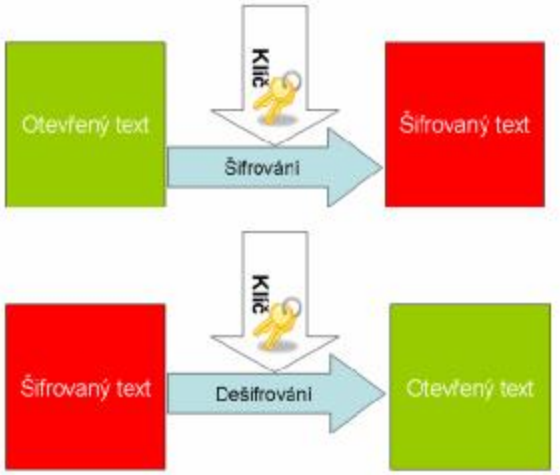
Použité znaky \ Délka hesla		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	**10 000** 2 minuty	**100 000** 16 minut	**1 000 000** 3 hodiny	**10 000 000** 1 den	**100 000 000** 11 dní
a-z; 0-9	36 znaků	**7311616** 5 hodin	**380204032** 7 dní	**2×10^9** 8 měsíců	**8×10^{10}** 25 let	**3×10^{12}** 900 let
a-z; A-Z; 0-9	62 znaků	**14776336** 2 dny	**916132832** 3 měsíce	**5×10^{10}** 18 let	**4×10^{12}** 1000 let	**2×10^{14}** 70 000 let
a-z; A-Z; 0-9; ščáéě… ;@#$^*?!…	85 znaků	**52200625** 6 dní	**443705312** 1 rok	**3×10^{11}** 120 let	**3×10^{13}** 10 000 let	**3×10^{15}** 800 000 let

Základy šifrování

Symetrická kryptografie

→ šifrovací algoritmus používá k šifrování i dešifrování jediný klíč

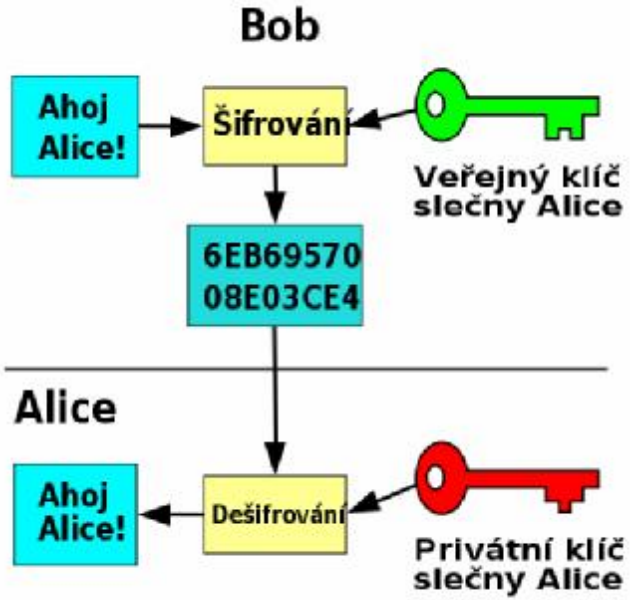
- Výhoda: nízká výpočetní náročnost
- Nevýhoda: nutnost sdílení tajného klíče
- Rozdělení:
  - Blokové šifry → rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost (AES, Blowfish, DES atd.)
  - Proudové šifry → zpracovávají otevřený text po jednotlivých bitech (FISH, RC4)



Základy šifrování

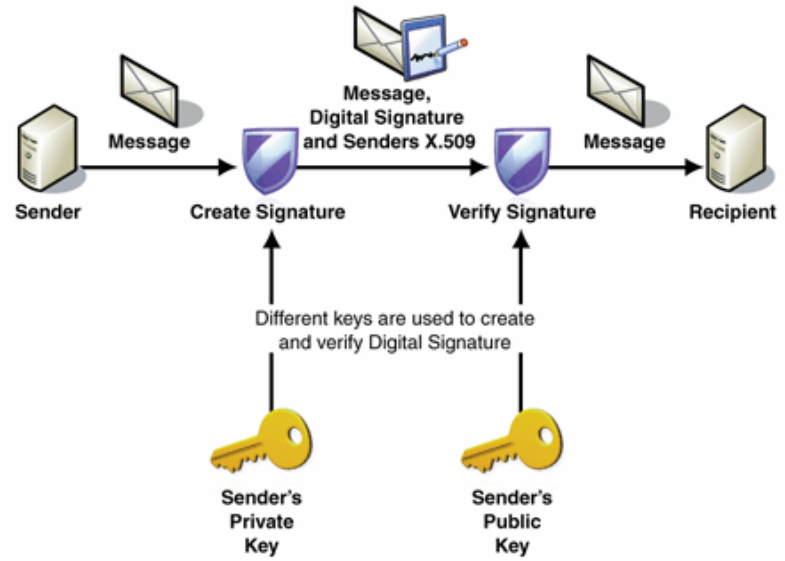
Asymetrická kryptografie

- pro šifrování a dešifrování používají odlišné klíče (využití i u elektronického podpisu)
- Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče:
  - šifrovací klíč je veřejný, majitel klíče ho volně uveřejní
  - dešifrovací klíč je soukromý, majitel jej drží v tajnosti
- Mechanismy funkce
  - Asymetrická kryptografie je založena na tzv. jednocestných funkcích → operace, které lze snadno provést pouze v jednom směru
  - ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup (např. násobení)
  - rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný



Digitální podpis

- Elektronický podpis jsou elektronické identifikační údaje autora (odesílatele), které jsou připojené k elektronického dokumentu
- Zaručený elektronický podpis dokumentu zajišťuje:
  - autenticitu – lze ověřit původnost (identitu subjektu, kterému patří elektronický podpis)
  - integritu – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není úmyslně či neúmyslně poškozen
  - nepopiratelnost – autor nemůže tvrdit, že podepsaný elektronický dokument nevytvořil (např. nemůže se zříct vytvoření a odeslání výhružného dopisu)
  - může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu



evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
OKRESNÍ HOSPODÁŘSKÁ KOMORA OLOMOUC
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Inovace bakalářského studijního oboru Aplikovaná chemie