Kdo jsem a co smím

Lidé umí jednotlivé osoby od sebe poměrně snadno rozeznat například podle vzhledu nebo hlasu. Počítače ale smysly nemají, a proto jim musíme svou identitu prokázat nějakou metodou autentizace.

Jakmile se počítači nebo počítačovému systému prokážeme, proběhne ještě autorizace, která definuje, co můžeme provádět.

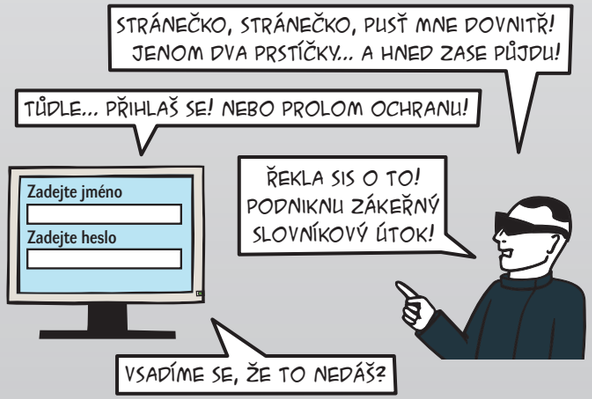
Elektronická identita (Kdo jsem...)

V reálném světě má každý člověk jednu fyzickou identitu, avšak v kybernetickém jich často používá několik.

Protože ale počítač nemá jinou možnost ověřit, kdo s ním pracuje, musíme mu svou identitu prokázat. K tomu slouží různé způsoby, tzv. metody autentizace.

- **Znalost tajné informace**
- **Vlastnictví předmětů nebo biometrických znaků**

Počítač ale již není schopen poznat, zda tajnou informaci zadal ten, komu patří, nebo ten, kdo ji pouze získal (ukradl).



Problematika hesel

Použití jména a hesla je nejrozšířenější způsob autentizace, protože je snadné, levné a uživatelé jsou na něj zvyklí. Heslo ale musí být zvoleno tak, aby odolalo různým způsobům kompromitace.

Je nutné si uvědomit, že ne všichni správci služeb jsou zodpovědní a proto heslo může uniknout. Z toho vyplývá požadavek na různá hesla do různých služeb.

Heslo může být uhodnuto tzv. hrubou silou, kdy se útočník zkouší přihlásit jako uživatel generovanými hesly. Čím delší a složitější heslo je, tím je menší pravděpodobnost, že bude úspěšně vygenerováno a vyzkoušeno.

V případě přihlašování on-line je zpravidla útočník omezen počtem pokusů za určitý čas, ale může se dostat k uloženým heslům v počítačovém systému. Naštěstí ta už dnes nikdo rozumný neukládá v čitelné podobě, ale zašifrovaná.

Pokud ale útočník nějak získá hesla v zašifrované podobě a uhodne typ použité šifry, může dále už bez omezení počtu pokusů generovat náhodná hesla, šifrovat je a porovnávat, zda šifra souhlasí s některou v seznamu. V případě, že ano, je velká pravděpodobnost, že bylo vygenerováno stejné heslo. Z toho vyplývá požadavek na délku a složitost.

Heslo k uživatelskému jménu by měl znát jen ten, komu uživatelské jméno patří, v opačném případě by se mohl k elektronické identitě s daným uživatelským jménem hlásit někdo jiný a počítač by tuto skutečnost neodhalil.

Kvalitní heslo by mělo být:

- **dlouhé** - alespoň 12 znaků, čím více, tím lépe.
- **složité** - použity kombinace různých skupin znaků, tj. malá písmena, velká písmena, číslice, interpunkce nebo další speciální znaky (středník, zavináč, lomítko). Nižší složitost je možno kompenzovat délkou.

- **jedinečné** - pro každou kombinaci přihlašovacích údajů (uživatelské jméno + heslo) musí být použito jiné heslo.
- **pravidelně měněné** - zvláště v těch případech, kde není použita dvoufázová autentizace. Interval změny by měl být přiměřený důležitosti hesla a dalším použitým prvkům zabezpečení. Obvykle tento interval určuje poskytovatel služby.

Autorizace (Co smím...)

Ne každý a vždy může v počítačovém systému provádět stejné akce. Například učitel může zapisovat známky do elektronické žákovské knížky, rodič a žák je ale mohou pouze číst.

Uživateli, který se přihlásí a projde tedy úspěšnou autentizací, musí být přiřazena příslušná oprávnění. Proběhne tzv. autorizace, která umožní tomuto uživateli provádět pouze takové činnosti, které mu přísluší.

V praxi je v každém počítačovém systému seznam uživatelů a jejich rolí. Tyto role nastavuje správce systému na základě potřeb vlastníka systému. Často jsou také role přidělovány na základě účasti v definované skupině. Systém po přihlášení uživatele zjistí, jaké role uživatel má, a přiřadí mu odpovídající oprávnění.

ROLE: STUDENT
- rozvrh
- zapisování na termíny
- odevzdávání prací...
- atd

ROLE: VYUČUJÍCÍ
- rozvrh
- vypisování termínů
- zadání prací...
- atd

Jsem leták ke školení IT bezpečnosti uživatelů sítě ZČU. Školení má 10 témat. Mě, ostatní letáky, brožury a prezentace najdete na https://bezpecnost.zcu.cz.

Naší almou mater je Západočeská univerzita v Plzni a na svět jsme přišly také díky podpoře Fondu rozvoje CESNET, z.s.p.o.