Identifikace uživatele Informačním systémem

Jan Čapek
Ústav systémového inženýrství a informatiky, FES, Univerzita Pardubice

Anotation

Within presented article is discussed problem of user identification by information system. Some approach is mentioned from many possibillities such as PKI method and method of combination password and way of the password writing. As the evaluation method is used fuzzy numbers with Tagaki-Sugeno rules.

1. Úvod

Během posledního desetiletí jsme svědky hlubokého proniknutí ICT (informačních a komunikačních technologií) do každodenního života.

Uživatele ICT můžeme rozdělit do několika skupin, podle druhu technologie, kterou používají. Vyloučíme-li mobilní technologie jako mobilní telefony a PDA (Personal Digital Assistant) z důvodů obtížnosti implementovat níže uvedené návrhy řešení, zůstanou nám k dispozici jako široce používané představitelé ICT počítače.

Počítače jsou používány buď izolovaně jednotlivými uživateli nebo skupinou uživatelů a nebo jsou zapojeny do různých druhů sítí. Z dalšího uvažování vylučme individuální uživatele nebo skupinu individuálních uživatelů, které mají většinou stejná práva a počítač používají izolovaně a nebo jej připojují do globální sítě – Internetu.

Dále se zaměřme na uživatele resp. na skupinu uživatelů, kteří mají počítač spojený do různých typů podnikové sítě (Intranet), která je z hlediska těchto uživatelů spravována informačním systémem (IS) podniku.

Bezpečnost IS podniku je většinou řešena dvojím způsobem.

1) Prostorovým oddělením počítačů od veřejnosti, tím je myšleno, že většinou jsou počítače umístěny v kancelářích podniků (úřadů), kam by neměl mít nepovolaný přístup.

2) Používáním hesel.

O této problematice je popsáno mnoho papíru, namátkou uvádím [1], [2]. Lze vyjmenovat obecně známé závěry, že bezpečnost přístupů do systému roste s délkou použitého hesla a s použitím náhodně zvolených znaků zahrnujících kromě velkých a malých písmen čísla a další znaky jako závorky, uvozovky, atd. Tato hesla zvláště když svoji délkou přesahují deset znaků jsou však obtížně zapamatovatelná, což vede většinou k porušování základních pravidel bezpečnosti.

V některých firmách se vůbec hesla nepoužívají nebo se dlouhou dobu nemění, takže se IS stává nedůvěryhodným ba přímo pro obhospodařovaná data nebezpečným.

V příspěvku nebude probírána problematika ochrany IS před narušitelem přicházejícím po globální síti.

2. Formulace problému

Pro větší firmu, která používá více počítačů, které mohou být sdíleny větším počtem uživatelů než povolí operační systém počítače nastává problém identifikace oprávněného uživatele informačním systémem.

Tedy problémem je povolit nebo zamítnout přístup do informačního systému podniku oprávněnému uživateli, z kteréhokoliv počítače zapojeného do IS podniku. Tento problém lze rozšířit i na distribuovaný podnik, tj. podnik který má více pracovišť územně oddělených a spojených přes globální síť.

3. Řešení problému

Způsob identifikace osob běžně prováděných na úřadech je založen na předložení občanského průkazu (OP), kde hlavním identifikačním prvkem je fotografie obličeje dané osoby. Bohužel současné technologie rozpoznávání neumožňují rozeznat podle analogové fotografie danou osobu pomocí počítače. Je tedy nutné použít jinou metodu. Nabízí se přímo použít obdobu občanského průkazu a sice čipovou kartu [3], [4]. Čipová karta patří mezi tzv. „Chytré karty" a může obsahovat více údajů než OP a údaje, které IS může rozpoznat a tak umožnit přístup předložiteli čipové karty. Zde si musíme všimnout posledních slov tj. systém vybavený čtečkou čipové karty umožňuje přístup do systému předložiteli karty tj. vlastně jen čipové kartě. Ověření totožnosti zde odpadá, je to jen kontrola systému versus čipová karta, kdokoliv kdo předloží čipovou kartu může do systému vstoupit.

3.1. PKI technologie

Další způsob může být založen na využití technologie PKI (Public Key Infrastructure), kterou chápeme jako soubor serverů, certifikačních autorit, registračních autorit (RA), adresářů a aplikací, které organizacím umožňují elektronicky modelovat důvěru. Tento systém zahrnuje funkce na uchovávání a správu nainstalovaných certifikátů.

Základní funkce PKI je:

- vydávání certifikátů k veřejným klíčům
- odvolávání platnosti certifikátů
- vytváření a zveřejňování seznamu certifikátů
- vytváření a zveřejňování zneplatnělých certifikátů v seznamu CRL (Certificate Revocation List)
- správa klíčů po dobu jejich platnosti (životního cyklu)

PKI je založen na funkci certifikačních autorit (CA), které provedou identifikaci žadatele o dvojici soukromý a veřejný klíč. Identifikace spočívá v osobní návštěvě žadatele CA, prokázání se dostupnými dokumenty (OP, rodný list, atd.). Poté CA přidělí žadateli soukromý klíč a veřejný klíč žadatele a ručí zato, že veřejný klíč žadatele patří danému žadateli.

Certifikát je digitální dokument v normalizovaném datovém formátu, který svazuje veřejný klíč s osobou, aplikací nebo službou.

Certifikát vytváří důvěryhodná třetí strana, certifikační autorita (CA) a certifikát stvrzuje svým digitálním podpisem. Tento digitální podpis generuje prostřednictvím svého privátního klíče.

Veřejný klíč CA je k všeobecné disposici. Digitálním podpisem ověřuje CA pravost a integritu certifikátu.

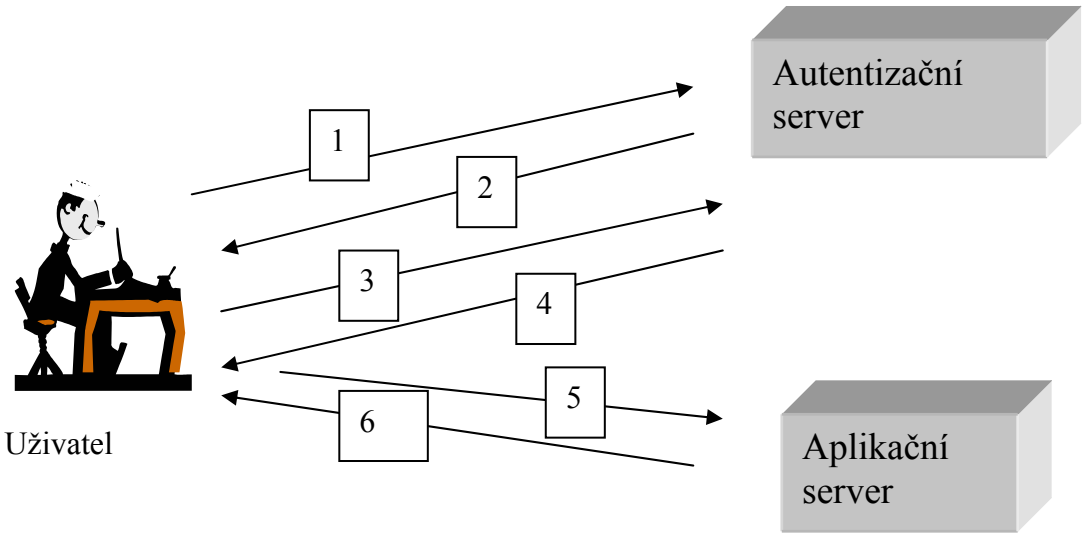
Formát certifikátu je popsán normou RFC2459 a doporučením ITU X.509.

Certifikát je datová struktura popsaná v jazyce ASN.1 a pro přenos je kódovaná podle specifikace DER (Distinguished Encoding Rules). Obsahuje zejména:

- sériové číslo certifikátu
- identifikace algoritmu
- název algoritmu asymetrického

- název jednocestného algoritmu
- délka klíče
- identifikace vydavatele certifikátu (CA)
- platnost certifikátu (od - do)
- identifikace vlastníka certifikátu (jméno, adresa, zaměstnavatel, e-mail adresa .....)
- veřejný klíč, pro který je certifikát vydán
- digitální podpis CA

Jedna z aplikací PKI systému je autentizační systém Kerberos. Obr. 1.



Obr. 1: Systém Kerberos

Uživatel si otevírá relaci na své pracovní stanici – přihlašovací jméno → proces pro otevření relace. Tento proces (přihlašovací klient), předá (1) přihlašovací jméno uživatele autentizačnímu serveru uživatelů AS. AS vyhledá v databázi Kerbera uživatelovo heslo, z něho vygeneruje tajný klíč a tímto klíčem zašifruje počáteční pověřovací listiny (TGT, Ticket Granting Ticket) vracené klientovi (2) (Přihlašovací klient TGT přijme a vyžádá si od uživatele zadání hesla (3). Z hesla vygeneruje stejným postupem jako AS tajný klíč (4). Pokud tímto klíčem úspěšně dešifruje dodané TGT, uživatel je oprávněný se přihlásit (5)(6) (otevřít si relaci) – udal správné heslo – V TGT je uvedena specifikace serveru TGS (Ticket Granting Server) autentizujícího přístup ke službám Uživatel vlastnící úspěšně dešifrované TGT je oprávněn po TGS požadovat pověřovací listiny.

3.2. Kombinace Hesla a biometrické metody

Avšak i PKI systém je po odcizení hesla prolomitelný. Zřejmě výhodné bude v dalším uvážit použití nezcizitelných identifikačních znaků vlastních každé osobě. Tyto znaky jsou předmětem tzv. biometrických metod, které předpokládají ve většině případů použití speciálních přístrojů. Předpokládejme dále, že ze širokého rejstříku biometrických metod využijeme dynamiku psaní hesla. Zkombinujeme tedy heslo jako takové se způsobem psaní hesla na klávesnici počítače [5]. Běžně používané metody identifikace způsobu psaní hesla na klávesnici postupují podle následujícího schematu:

1. Uživatel napíše na klávesnici několikrát heslo.
2. Sledují se doby stisku klávesy a nebo doba mezi stiskem následující klávesy, případně obě doby.
3. Spočte se průměr jednotlivých dob pro dané heslo a vytvoří se časový vzor hesla.
4. Nově přijaté heslo se porovnává s tímto časovým vzorem.

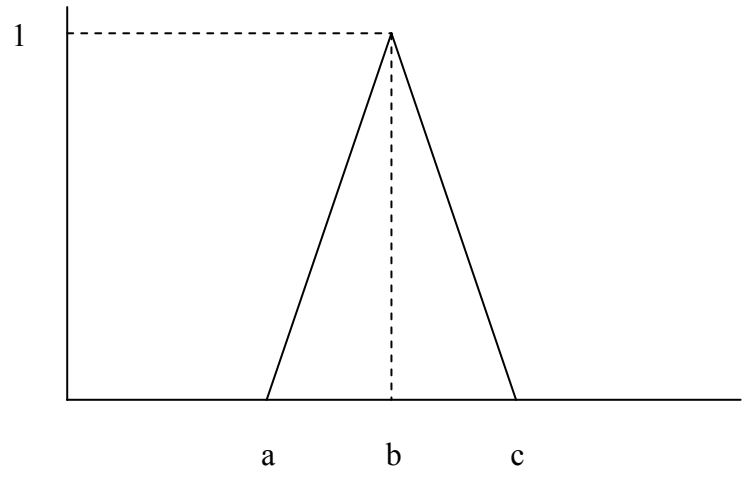
Porovnání spočívá v určení rozdílu jednotlivých nově přijatých časů vůči vzoru. Pokud nepřekračují dohodnutou hranici, je uživateli povolen přístup do systému. Pro určení rozdílu vzoru a přijatého hesla se používají různé metriky (např. Eukleidovská, Manhatanská atd.) Zajímavým řešením je použití fuzzy čísel.

3.3 Fuzzy čísla

Fuzzy čísla jsou speciální fuzzy množiny v množině reálných čísel a intuitivně reprezentují nepřesné hodnoty, které můžeme slovně charakterizovat jako „asi 3“ atd. [6]. Nejpoužívanějším typem fuzzy čísel jsou tzv. trojúhelníková fuzzy čísla, jejichž funkce příslušnosti tvoří trojúhelník. Obecný předpis trojúhelníkového fuzzy čísla je následující:

$$M(x,a,b,c) = \begin{cases} 0 & x < a \text{ , nebo } , x > c \\ \dfrac{x-a}{b-a} & a \le x \le b \\ \dfrac{c-x}{c-b} & b \le x \le c \\ 1 & x = b \end{cases}$$

kde a,b,c jsou parametry znázorněné na obr. 2. Zpravidla parametry a,c jsou symetricky umístěny okolo parametru b. Funkce příslušnosti tvoří tedy rovnoramenný trojúhelník.



Obr. 2: Funkce příslušnosti trojúhelníkového fuzzy čísla

V tomto případě jednotlivé doby stisku klávesy a nebo doby mezi stiskem kláves tvoří jednotlivá fuzzy čísla. Nepočítáme zde průměr a vzdálenost tohoto průměru od časového vzoru, ale na vyhodnocování použijeme upravená Tagaki-Sugeno pravidla. Dostaneme podle délky hesla různě velkou množinu pravidel např. ve tvaru:

P_1 = Jestliže X_1 je M_1 , X_2 je M_2 .... . X_n je M_n Pak 1
P_2 = Jestliže Y_1 je T_1 , Y_2 je T_2 .. ..Y_n je T_n Pak 1

kde X je doba stisku klávesy u hesla a M je příslušné fuzzy číslo časového vzoru, a Y je doba mezi stiskem kláves a T je příslušné fuzzy číslo časového vzoru. Platnost pravidel pak určí platnost hesla a povolí uživateli vstup do systému.

4. Závěr

V předloženém článku byla načrtnuta problematika identifikace uživatele informačním systémem, který dosud jednoznačným a levným způsobem řešen není. Jako možné řešení je zde naznačeno využití fuzzy čísel s Tagaki-Sugeno pravidly pro vyhodnocení dynamiky psaní hesla na klávesnici. Je možné tuto metodu zkombinovat i s PKI metodou. Při kombinaci různých metod však musíme mít na zřeteli, že kombinujeme jak silné stránky jednotlivých metod tak i jejich slabé stránky, to může mít za následek, že výsledná metoda nepřekročí nejslabší článek metod vstupujících do kombinace a že tak vlastně nedosáhneme kýženého výsledku.

5. Literatura:

[1] Hanáček P., Staudek J.: Bezpečnost Informačních systémů – met. příručka zabezpečení produktů a systémů budovaných na bázi IT. Úřad pro inf. syst. Praha 2000.

[2] Klein D.: A survey of and improves to password security. Unix security workshop II USENTUA soc. 1990.

[3] Trampuš M., Ciglarič M., a kol.: Uporaba pametnih kartic za varno hranjenje dokumentov. In. Proceeding of the 6th International Multiconference Inteligent and Copmuter Systems, Complex System in E-Business. 13-17th of October 2003, Ljubljana Slovenia.

[4] Proimadis A., Telonis P., a kol.: Access Authentication with Smart Card over Internet: A case study in E-commerce. In. WSEAS Transactions on Information Science and Applications. Issue 5, Vol. 1 November 2004, pp.1400 – 1405. ISSN 1790-0832

[5] Hub M.: Strategie výběru identifikačních znaků ve vícefaktorové autentizaci. In. E+M pp 147-150, Liberec 2003. ISSN 1212-3609.

[6] Novák V.: Základy fuzzy modelování. BEN Praha 2000. ISBN 80-7300-009-1

Recenzoval: doc. Ing. Peter Fabián, CSc., Fakulta riadenia a informatiky, Žilinská univerzita v Žilině