UŽIVATELSKÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Jaromír Ocelka, Jaroslav Měcháček

ÚVT MU v Brně, Botanická 68a, 602 00 Brno, ČR
E-mail: ocelka@ics.muni.cz, mechacek@ics.muni.cz

Abstrakt

S rozmachem informačních systémů nabývá na významu bezpečná komunikace laických uživatelů. Přístup z internetových kaváren je jedním z příkladů nebezpečných terminálů. V podobných prostředích je nutné použití hesla kombinovat s dalšími bezpečnostními opatřeními. V případě IS univerzity, který používá celá akademická obec, je nutné zvolit levné, ale ještě dostatečně bezpečné řešení. Součástí příspěvku je popis implementace *uživatelské IP bezpečnosti* na Masarykově univerzitě v Brně.

Úvod

Masarykova univerzita v Brně začala v roce 2000 vyvíjet intranetový systém INET, který mimo jiné začal zpřístupňovat akademické obci informace z personálních, mzdových a ekonomických databází. Každý zaměstnanec MU tedy může pomocí www prohlížeče překontrolovat například svůj stav dovolené, pracovní zařazení včetně platové třídy a stupně, prohlédnout si svůj výplatní lístek, … Vedoucí grantů mají přístup k ekonomickým sestavám. Uživatelé však začali projevovat obavy o zabezpečení celého systému a případný jednoduchý průnik do systému například díky „utroušení lístku s heslem“. Ony obavy nebyly ani tak o ekonomické přehledy grantů s částkami i několika miliónů Kč, ale především o výplatní lístky. V rámci řešení výzkumného záměru ÚVT MU tedy získal prioritu problém snížení bezpečnostních rizik (na straně klienta).

Bezpečnostní rizika www intranetu

Odcizení citlivých údajů je možné v zásadě na třech místech. Pomocí klientského počítače, prolomením se na server nebo odposlechnutím na přenosové trase mezi klientem a serverem. Přenosovou trasu lze zabezpečit šifrováním – například hojně využívaným SSL. Server s daty je nutné mít pod zámkem, aby se zabránilo fyzickému vniknutí útočníka, dále je nutné zakázat všechny nepoužívané protokoly – nejlépe ponechat pouze https (v případě www) – a pravidelně aktualizovat použitý software bezpečnostními záplatami. Největší problém v zabezpečení představuje uživatel (varianta první), neboť klientský počítač se může nacházet i mimo akademickou půdu (například internetové kavárně) – tedy je obecně nedůvěryhodný. Odcizení informací na klientské straně je možné dvojím způsobem: získáním z lokálních souborů či přímo z paměti uživatelova počítače, nebo při znalosti autentizačního slova (viz například úvod) vydáváním se za uživatele.

Nejjednodušší způsob, jak získat autentizační kód, často nabízí samotný uživatel: má kód zapsán na „lístečku“; kód je odhalitelný hrubou silou slovníkovým útokem; uživatel přistupuje z počítače vybaveného trojským koněm. Pouze druhá varianta je detekovatelná v systému univerzity a lze jí zabránit kontrolou triviálních/slovníkových hesel v kombinaci s blokováním podezřelých neúspěšných pokusů o přihlášení (různé loginy z jedné IP adresy, …).

Z výše uvedeného vyplývá, že obava o data je zcela oprávněná, avšak za případné odcizení citlivých informací si z valné většiny mohou uživatelé sami. Informační systém musí tedy být zabezpečen tak, aby snížil riziko i v případě, že dojde k odhalení autentizačního slova uživatele.

Proměnlivý autentizační kód

Přistupují-li uživatelé pomocí nestatického autentizačního kódu – tj. posloupnosti bytů, které mohou být v různých časových okamžicích různé, je útok do systému ztížen. Na konstrukci autentizačního kódu se může podílet i server. V případě www serverů a nejběžnější *basic autentizace* je však heslo uživatele posíláno při každém www požadavku, takže není obecně možné splnit podmínku různosti autentizačního slova v různých bodech na časové ose. Tento typ autentizace je možné nahradit *formulářovou autentizací*, kdy je heslo serveru posláno pouze jednou (při úvodní autentizaci v rámci jedné session) a další komunikace (www požadavky) je již většinou ověřována pomocí cookies. V tomto případě můžeme cookies chápat jako nové heslo vygenerované na základě času a identity uživatele. V případě trojského koně na uživatelově počítači nám ovšem nepomohou ani cookies, neboť každou novou session je nutné započít vždy stejným heslem.

Pravděpodobnost odcizení dat se zvyšuje s délkou časového intervalu, po který heslo platí. Požadavek na nové heslo každý půlrok je možné ještě prosadit, avšak délka tohoto intervalu je vzhledem k požadované bezpečnosti příliš dlouhá. Čím kratší interval (kratší změna), tím větší riziko, že si obyčejní uživatelé budou hesla psát na „lístečky“.

Výše uvedená rizika může eliminovat jednoúčelové zařízení generující autentizační kódy, jejichž platnost je časově omezena. Výhodou oproti cookies je, že iniciální vygenerování kódů probíhá na zařízení, které je prosto trojských koní, neboť je jednoúčelové, a také že se pro započetí další session nepoužívá stejný autentizační kód.

Největším nebezpečím je uživatel

Nyní se dostává na řadu opět obyčejný uživatel. V celkovém řešení bezpečnosti informačního systému musíme dosáhnout největšího počtu uživatelů, kteří mají svůj autentizační kód uložen na nezcizitelném místě (například mozek)[1]. Další požadavkem musí být možnost změnit autentizační kód při zjištění, že byl odhalen. V případě jednoúčelových zařízení generujících autentizační kód jsou pro odcizení informací velice nebezpeční ti uživatelé, kteří si na zařízení poznamenají jméno svého účtu, PIN zařízení, … Ztrátu či odcizení by měli uživatelé okamžitě hlásit správci systému, avšak statistiky jistě vykazují něco jiného. Navíc například autentizační kalkulátor není řešením realizovatelným na akademické půdě vzhledem k ceně a rozsáhlosti akademické obce.

Vstupní body

Jak již bylo zmíněno, uživatel může do informačního systému přistupovat z různých zařízeních různé důvěryhodnosti. Nejvíce důvěryhodná jsou univerzitní zařízení, méně důvěryhodné je domácí zařízení uživatele a například v internetové kavárně uživatel vůbec nemá jistotu, zda je jím zadaný autentizační kód v bezpečí. Samozřejmě lze namítnout, že má systém být přístupný pouze z univerzitních zařízení. Takováto směrnice by však v dnešní

[1] Uvedenou podmínku splňuje také autentizační metoda na základě biometrie. Kód získaný biometrií se však musí převést do počítače (v případě www prohlížeče), kde už může číhat trojský kůň.

době neuspěla, neboť některé informace chce mít například akademický pracovník přístupné i na různých konferencích. Současné informační systémy většinou nereflektují vstupní body a zpřístupňují uživateli vždy všechny aplikace. A to je potenciální bezpečnostní riziko.

Rozlišení, o jaký vstupní bod se v případě uživatelovy autentizace jedná, můžeme zajistit definováním sady různých autentizačních kódů pro různé typy aplikací (pro zpřístupnění výplatního lístku bude mít uživatel jiné heslo než pro informace o aktuálním obsazení počítačové studovny apod.). Toto řešení má výhodu, že uživatel má přístupné aplikace odkudkoliv a je na jeho důvěře ve vstupní bod, které aplikace navštíví a tedy jaké informace poskytne například potenciálnímu trojskému koni. Zřejmou nevýhodou je více autentizačních kódů a tím i zvýšená pravděpodobnost jejich „svěření lístečku".

Další možností, jak určit míru bezpečnost vstupního bodu vůči informačnímu systému, je její stanovení podle identity vstupního bodu klientského přístroje: systém při přístupu uživatele ověří, zda je vstupní bod definován jako důvěryhodný vzhledem k přistupované aplikaci.

Funkci rozhodující o vpuštění či nevpuštění můžeme definovat jako zobrazení z prvků kartézského součinu množiny všech uživatelů s množinou všech aplikací a množinou všech vstupních bodů na dvouprvkovou množinou {vpustit, nevpustit}. Množinu všech uživatelů má každý autentizovaný informační systém známu, stejně tak množinu všech aplikací. Jelikož předpokládáme, že vstupní zařízení budou k informačnímu systému přistupovat protokolem TCP/IP, lze vstupní bod identifikovat pomocí ethernetové adresy, IP adresy nebo jména. Pro identifikaci aktuální „polohy" uživatele je nevhodnější IP adresa – ethernetová adresa neumožňuje jednoduché definice skupin, je zjistitelná pouze v lokální síti a navíc se změní v případě výměny síťové karty (například z důvodů poruchy), jméno počítače zvětšuje bezpečnostní riziko, neboť útočníkovi stačí úspěšný útok na příslušný DNS server.

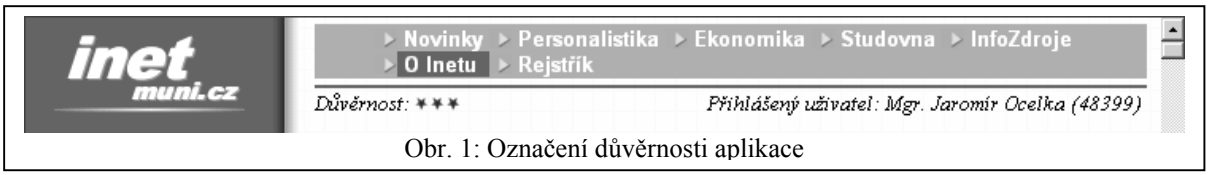
Uživatelská IP bezpečnost na MU

Jak již bylo zmíněno v úvodu, provozuje MU v Brně intranetový systém INET, který nabízí akademické obci univerzity řadu aplikací různé důvěrnosti. Vedle výplatní pásky, či ekonomických přehledů zakázek jsou k dispozici informace o aktuálním obsazení počítačové studovny, fotografie autentizované osoby apod. Spektrum zveřejňovaných informací je široké a bylo nutné minimalizovat obavy uživatelů o bezpečnost citlivých osobních informací. Tedy jinak řečeno, ochránit uživatele před sebou samým.

Při implementaci uživatelské IP bezpečnosti v INETu byla zvolena varianta *jednoho přístupového hesla* s možností definice *množiny vstupních bodů* (pomocí IP adres) různé bezpečnosti. V definici množin vstupních bodů může být použito expanzních znaků `*` a `?`. Jednotlivé aplikace jsou podle stupně důvěrnosti dat, se kterými pracují, rozděleny administrátorem do těchto čtyř kategorií/úrovní (čím nižší kód úrovně, tím důvěrnější data):

- 0 – Konfigurace IP adres
- 10 – Citlivá data
- 20 – Osobní data
- 30 – Veřejná data (v rámci MU)

Úrovně důvěrnosti jsou v záhlaví stránek aplikací označeny heslem „Důvěrnost:" (viz obr. 1) a počtem hvězdiček: *** pro konfiguraci IP adres, ** pro citlivá data a * pro osobní data (aplikace obsahující data veřejná v rámci MU se nijak neoznačují).

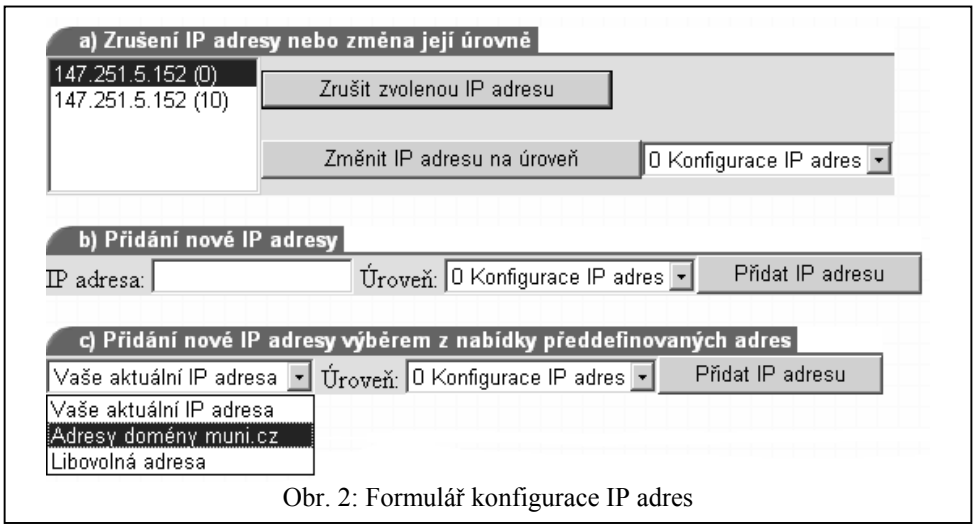


Obr. 1: Označení důvěrnosti aplikace

Každému uživateli je k dispozici aplikace pro vlastní konfiguraci uživatelské IP bezpečnosti a pouze tato jediná aplikace je označena kódem důvěrnosti 0. V počáteční konfiguraci není nastavena žádná bezpečnost, ale na tento (nedobrý a nedoporučitelný!) stav upozorňuje varování: *Uživatelská IP-bezpečnost je neaktivní, protože není nastavena žádná IP adresa úrovně 0 !!!*, které se červeně vypisuje v záhlaví konfigurační aplikace.
Pro přiřazování IP adres k úrovním důvěrnosti platí tato pravidla:

1. Je-li určitá IP adresa (skupina IP adres) přiřazena k úrovni důvěrnosti s kódem N, lze ze zařízení s touto identifikací přistupovat i k aplikacím, jejichž kód důvěrnosti je >N.
2. Není-li k úrovni důvěrnosti s kódem **0** přiřazena žádná IP adresa, jsou všechny IP adresy strojů, z nichž uživatel k aplikacím přistupuje, považovány za adresy s kódem úrovně 0, tj. uživatelská IP bezpečnost není aktivní a uživatel může k libovolné aplikaci přistupovat odkudkoli.
3. Je-li uživatelská IP-bezpečnost aktivní a má-li uživatel nastaveny IP adresy pouze pro některé úrovně důvěrnosti, jsou všechny IP adresy, které neodpovídají tomuto nastavení, chápány jako adresy úrovně N+1, kde N je maximální nastavená úroveň. Tedy ze vstupních bodů s IP adresami, které nejsou nastaveny pro žádnou úroveň důvěrnosti, lze přistupovat pouze k nejméně citlivým aplikacím.

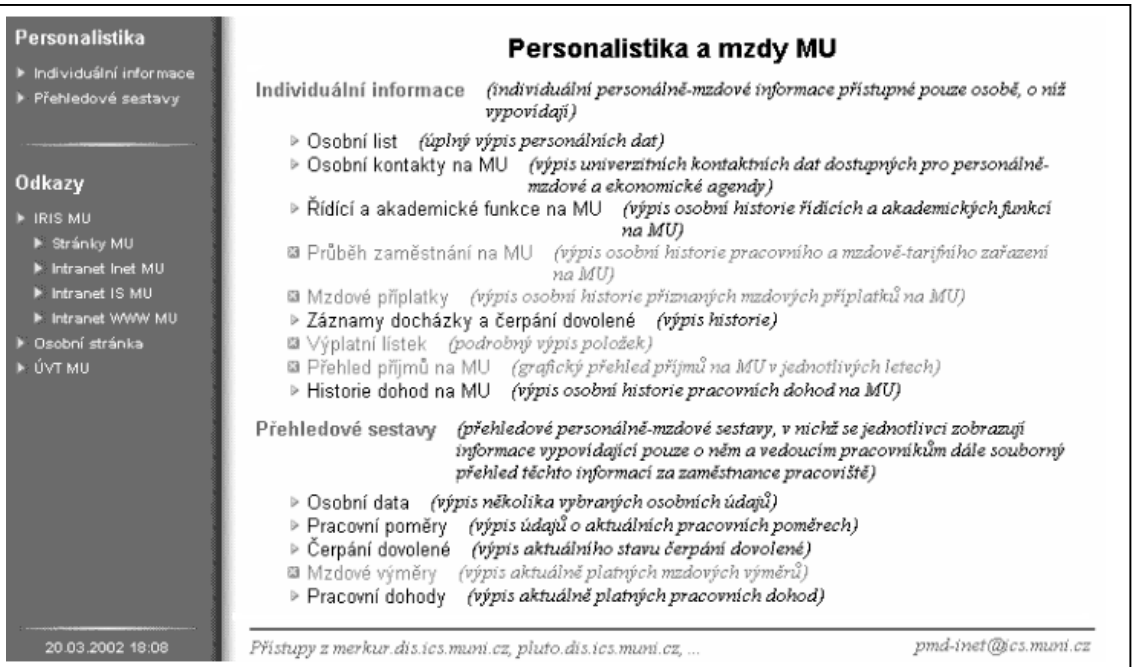
K zadávání IP adres slouží uživateli formulář (viz obr. 2), ve kterém má pro snazší zadávání k dispozici IP adresu aktuálního přístupového bodu a také regulární výraz popisující všechna zařízení z domény muni.cz.



Obr. 2: Formulář konfigurace IP adres

Uživateli je doporučováno nastavení, kde kódům důvěrnosti 0 a 10 přiřadí pouze svou pracovní stanici a kódu důvěrnosti 20 přidělí adresy vstupních bodů s IP adresami MU.

Nabídka aplikací v systému INET je uzpůsobena vstupnímu bodu a uživatel má zřetelně označeny aplikace (viz obr. 3), k nimž díky tomuto bodu nemá přístup. Jelikož má každá



Obr. 3: Nabídka aplikací omezená dle IP bezpečnosti

aplikace své URL, je nutné neopomenout zabezpečit případy, kdy uživatel nepřistoupí pomocí nabídky, ale zapíše URL aplikace přímo do adresního řádku www prohlížeče.
Vlastní uživatelská IP bezpečnost je ještě doplněna o aplikaci, která uživateli zobrazí všechny dvojice IP adres a jmen počítačů, z nichž přistupoval, doplněné o čas posledního přístupu. Všechny aplikace systému navíc v zápatí obsahují seznam posledních dvou přístupových bodů (viz obr. 3).

Závěr

Uživatelskou IP bezpečnost v intranetovém systému INET na Masarykově univerzitě v Brně si od jejího zveřejnění v říjnu 2001 nastavilo 13% návštěvníků této aplikace. Z těchto si nakonfigurovalo cca 80% na úroveň s kódem důvěrnosti 0 a 10 pouze svou pracovní stanici. Od zprovoznění se neozval žádný uživatel obávající se o bezpečnost svých informaci. Ovšem na druhé straně se provozovatelé INETu přesvědčili, že asi vždy budou existovat lidé, kteří jsou v dobré víře schopni poslat své heslo nezakryptovaně e-mailem.