Slovenská technická univerzita
FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLÓGIÍ
Ilkovičova 3, 812 19 Bratislava

Vypracovaná ponuka na tému č.3:

Infraštruktúra PKI a vybavenie pre koncových používateľov

Odbor: Počítačové systémy a siete

Bc. Jozef Hamar
Bc. Martin Mačica
Bc. Peter Mulika
Bc. Tomáš Smolek
Bc. Radomír Škrib

4. októbra 2004

Obsah

1. Predstavenie tímu

Náš tím s názvom **Boli sme SI** sa skladá z týchto členov:

Bc. Jozef Hamár

Bc. Martin Mačica

Bc. Peter Mulinka

Bc. Tomáš Smolek

Bc. Radomír Škrib

Všetci členovia tímu sú študentmi inžinierskeho štúdia na FIIT STU v Bratislave v odbore Počítačové systémy a siete. V predchádzajúcom roku ukončili bakalárske štúdium v odbore Informatika, zameranie Softvérové Inžinierstvo.
Nasleduje predstavenie jednotlivých členov tímu. Uvádzame osobné skúsenosti členov, ktoré by mohli byť užitočné pri nadchádzajúcom projekte.

Bc. Tomáš Smolek:

Má bohaté skúsenosti s programovaním v C/C++, .NET/C#, HTML, Javascript, PHP, využívaní štýlov CSS a taktiež s používaním XML. Preferuje vývojové prostredia pre OS Microsoft Windows®, ale výborne ovláda aj prostredie UNIX/LINUX. Najväčšie skúsenosti má a preferuje vyvíjanie oknových aplikácií pod Windows vo Visual C++ 6 alebo Builder C++ 6. Už pol roka vyvíja softvér pre právnickú firmu, ktorý je zameraný na získavanie, spracovávanie a hromadnú tlač údajov. Má dokonalo zvládnutý dopytovací jazyk SQL, hlavne MSSQL a MySQL. Skúsenosti s SQL si prehĺbil v práci, kde vytáraný projekt bol závislý predovšetkým na databáze MSSQL, kde bolo potrebné často použiť zložitý dotaz na rôzne štatistické výstupy. Záverečná bakalárska práca bola zameraná na vytvorenie web stránky, ktorá bude podporovať rozvoj turistiky v určitom regióne. Pri tejto práci získal skúsenosti s MySQL, serverom Apache a vytáraním HTML stránok. Momentálne dokončuje ďalšiu stránku www.pozemky.sk, ktorá bude ponúkať realitným agentúram zverejňovať svoje inzeráty. Pracoval už na niekoľkých projektoch, na ktorých riešení sa zúčastňovalo viacero

ľudí, kde získal skúsenosti s prácou v tíme. Prínosom pre tím je jeho zodpovednosť, komunikatívnosť a skúsenosti s tvorbou používateľských rozhraní.

Vzťah k vybranej téme

V budúcnosti sa chce venovať sieťovým aplikáciám a rôznym metódam zabezpečenia dát, kde praktická znalosť v PKI bude veľmi prínosná. Jedná sa o vytvorenie web aplikácie s čim má veľké skúsenosti.

Bc. Radomír Škrib

Ovláda programovacie jazyky: C/C++, Java, Pascal, Lisp, Prolog. V rámci záverečného bakalárskeho projektu riešil problém zálohovania a obnovy databázy v prostredí Oracle. Popri štúdiu pracuje už piatym rokom v softvérovej firme zaoberajúcej sa vývojom informačných systémov. Vďaka tomu má bohaté skúsenosti s prácou v týme. Je expertom v dopytovacom jazyku SQL. Má praktické skúsenosti v nasledovných databázových prostrediach: Sybase, Oracle, MS SQL a MySQL. Preferuje vývoj aplikácií pod operačným systémom Windows vo vývojových prostrediach C++ Builder 5.0, Visual C++ 6 a J Builder 8.0.
Prínosom pre tím sú jeho mnohoročné skúsenosti získané na rozličných projektoch a skúsenosti s prácou v tíme.

Vzťah k vybranej téme

Danú tému si vybral hlavne kvôli jej aktuálnosti v tejto dobe, keďže elektronický styk používa denne stále viac a viac ľudí.

Bc. Jozef Hamár

Bakalárske štúdium ukončil obhájením bakalárskej prace z oblasti bezpečnosti v os. Linux. Momentálne študuje na Ústave počítačových systémov a sieti a výberom predmetov (Základy kryptológie, Bezpečnosť v Internete) sa špecializuje na bezpečnosť. V zvýšenej miere sa venuje počítačovým sieťam (na všetkých vrstvách RM OSI) a operačným systémom. Tieto znalosti uplatňuje už dlhší čas u jedného väčšieho slovenského ISP, kde ma na starosti zabezpečenie funkčnosti chrbticovej siete.

Aktívna znalosť anglického jazyka mu umožňuje bezproblémové štúdium anglických manuálov a textov. Z programovacích jazykov ovláda Pascal, C/C++, Shell scripting, HTML. Ma skúsenosti s vývojovými prostrediami Delphi, Kylix, Visual Studio.

V minulosti sa zúčastnil na niekoľkých tímových projektoch, takže práca v tíme mu nie je cudzia. Je komunikatívny a zodpovedný.

Vzťah k vybranej téme

Jeho vzťah k vybratej téme odráža aj to, že na predmete Bezpečnosť počítačových systémov si vybral tému "Infraštruktúra verejného kľúča (PKI)". V budúcnosti sa plánuje venovať bezpečnosti v oblasti komunikácie a počítačových sieťach.

Bc. Peter Mulinka

Dokonale ovláda programovacie jazyky assembler, pascal a C/C++, taktiež sa venuje aj skriptovacím jazykom PHP, bash, perl a javascript. SQL, HTML, CSS mu nerobia problém. V minulosti pracoval s databázovými systémami MySQL a PostgreSQL, pomocou ktorých vytvoril niekoľko projektov, či už školských alebo komerčných. Dlhú dobu sa venuje počítačovej grafike, hlavne programovaniu OpenGL v operačných systémoch Linux/UNIX a Windows. Počas bakalárskej práce pracoval na vizualizácii simulačného procesu generovania terénu, kde si osvojil dobré programátorské návyky extrémneho programovania a odskúšal metódy refaktoringu. Pri projektoch sa hlavne zameriava na výborný návrh systému. V súčasnej dobe sa zaoberá s administráciou vlastných linuxových serverov. Siete a bezpečnosť v nich sa stala novou oblasťou jeho štúdia. Skúsenosti s prácou v tíme nadobudol pri riešení projektov:

- www.bogotest.chytrak.cz (PHP, JavaScript, MySQL – návrh tabuliek)
- www.sacred-game.wz.cz (JavaScript, HTML, MySQL)

Vzťah k vybranej téme

V dnešnej dobe sú čoraz viac potrebný odborníci z oblasti bezpečnosti sietí a informačných systémov, PKI je jednou z neoddeliteľných častí tejto sféry. Využitím znalostí z tohto projektu zabezpečí vyššiu bezpečnosť v administrovaných systémoch, poprípade skvalitní služby vo vlastnej firme zaoberajúcou sa ISP.

Bc. Martin Mačica

Riešil viacero problémov programovacími jazykmi C, C++, niektoré zadania riešil a prezentoval netradične cez DHTML s použitím JavaScriptu. Má praktické skúsenosti s ASP na IIS spolu s MS SQL Serverom, ktoré získal ako pri práci v technickom tíme firmy Telenor Slovensko, s.r.o. , tak aj pri vývoji vlastnej web-stránky. Pri vypracovaní záverečného projektu sa zoznámil s nízkoúrovňovými knižnicami Xservera (XFree86) pod Linuxom. Pri vývoji web-stránok sa zameriava najmä na správny návrh databázovej časti, ako aj na client-side skriptovanie (oživenie) web prezentácii prostredníctvom JavaScript-u. Ukážky práce

- http://mam.noc.sk Vlastná web-prezentácia
- http://mam.noc.sk/dogs/default.html Chovateľská stanica Bos Grunniens

2. Analýza

2.1. Analýza súčasného stavu

V súčasnosti prebieha čoraz väčší, aj keď často iba prvotný, nárast popularity slova „bezpečnosť“. Jedna z tém, ktoré s tým súvisia, je PKI (Public Key Infrastructure - Systém Verejného Kľúča). Mnoho ľudí má však nedostatky či už v teoretickej, alebo praktickej časti tohto systému. Nie sú im jasné základné pojmy, princípy a vo väčšine prípadov ani použitie tohto systému. Aj keď sa systém PKI používa už niekoľko rokov v rôznych aplikáciách a jeho použitie je naozaj rozšírené, používatelia často ani nevedia, že ho používajú. Táto situácia sa zmenila so zavedením pojmu „Elektronický podpis“, či „Digitálny podpis“. Jeho implementácia na Slovensku však dlho stagnovala. Tento stav sa mierne zlepšuje od vzniku prvej slovenskej certifikačnej autority, avšak stále zaostáva za krajinami, kde sa elektronický podpis už dlhšiu dobu používa. Keďže ide o problematiku veľmi úzko prepojenú z oborom šifrovania a počítačov, môžeme predpokladať, že rozšírenie medzi masy je otázka budúcnosti. V súčasnosti sa predpokladá rozšírenie hlavne do podnikovej sféry a medzi ľudí aktívne využívajúcich počítačovú komunikáciu s potrebou efektívneho utajovania prenášaných dát.
V nasledujúcej kapitole vysvetlíme základne pojmy a princípy PKI

2.2. Úvod do PKI

2.2.1. Rozdelenie šifrovacích metód

Šifrovacie metódy rozdeľujeme v zásade na jednosmerné a obojsmerné. Jednosmerné šifrovanie nám neumožňuje neskoršie rozšifrovanie skrytého textu. Využitie nájde tam, kde nám stačí porovnať dva texty. Jednosmerné šifrovanie spravidla nepotrebuje žiadny kľúč. V praxi sa používajú algoritmy MD5 a SHA. Typická aplikácia je uchovávanie hesiel, ale aj takzvané otlačky dokumentov. Otlačok slúži na overenie integrity dokumentu, t.j., či bol dokument v prenosovom kanále modifikovaný, alebo nie. Na druhej strane obojsmerné šifrovanie nám umožňuje rozšifrovať šifrovaný text a prečítať pôvodnú správu. Tento systém sa používa pri prenose dát, pri ich uskladnení atď.

Obojsmerné šifrovanie možno ďalej rozdeliť na symetrické, asymetrické a hybridné. Pri symetrickom sa správa šifruje aj dešifruje rovnakým kľúčom. Táto metóda je rýchla

a zvykne sa jej hovoriť „Systém súkromného kľúča“. Naopak, pri asymetrickom šifrovaní je potrebné mať dva kľúče: súkromný a verejný. Vyznačujú sa tým, že správu zašifrovanú jedným kľúčom je možné rozšifrovať len kľúčom druhým. Tento systém sa nazýva „Systém verejného kľúča“. Používa sa na skôr na overenie identity subjektu. Hybridné šifrovanie spočíva v tom, že na začiatku komunikácie si subjekty pomocou pomalého asymetrického šifrovania vymenia kľúč pre symetrické šifrovanie a ďalej už šifrujú pomocou tohto kľúča.

2.2.2. Digitálny podpis

Digitálny podpis je vlastne otlačok dokumentu, ktorý je podpisovaný. Následne je tento otlačok zašifrovaný privátnym kľúčom podpisovateľa dokumentu. Tento systém má dve hlavné časti: v prvom rade ak niekto zmení daný dokument, tak nebude sedieť otlačok vygenerovaný pri podpisovaní. Druhá dôležitá časť je, že zašifrovaním otlačku sa súčasne zamedzí podvrhnutiu nového otlačku z modifikovaného dokumentu (tretej strane principiálne nič nebráni po modifikácii dokumentu vygenerovať aj nový otlačok) a súčasne je odosielateľ (osoba, ktorá podpísala dokument) jednoznačne určený, pretože danú správu ide rozšifrovať výlučne len jej verejným kľúčom.

Problém však nastáva pri vymieňaní verejných kľúčov. Nemáme totiž istotu, že obdržaný verejný kľúč patrí naozaj tomu, o kom to predpokladáme. Tento problém možno vyriešiť tak že nám daný verejný kľúč podpíše niekto, koho verejný kľúč už máme, a dôverujeme mu. Túto úlohu plnia certifikačné autority. Verejný kľuč podpísaný certifikačnou autoritou nazývame certifikát.

3. Špecifikácia

Infraštruktúra PKI a vybavenie pre koncových používateľov

Pre pedagogické účely vytvorte WEB aplikáciu demonštrujúcu princípy a činnosť PKI. Taktiež demonštrujte použitie certifikátov verejného kľúča na podpisovanie a overovanie podpisov elektronických dokumentov u koncových používateľov. Navrhnite a implantujte PKI a aplikáciu na podpisovanie a overenie podpisu elektronického dokumentu u koncového používateľa. Pri návrhu rešpektujte platné štandardy.

Našou úlohou bude vytvorenie web stránky, kde budeme názorne prezentovať princípy a činnosť Public Key infrastructure (PKI). Na stránke nájdeme základné informácie a vysvetlenie činnosti PKI a kryptografie. Taktiež bude na stránke prezentovaná činnosť PKI v praxi.

Ďalej sa budeme venovať témam s tým súvisiacimi, certifikáty verejného kľúča, a elektronický podpis. Na stránke budeme demonštrovať použitie certifikátov verejného kľúča na podpisovanie a overovanie podpisov elektronických dokumentov u koncových používateľov.

Ako posledný bod bude návrh a implementácia PKI a aplikácia slúžiaca na podpis a overenie elektronického dokumentu u koncového používateľa. Pri návrhu a implementácií budeme dodržiavať platné štandardy, zapísané v dokumentoch RFC2511, RFC2511,RFC2560, RFC2630,RFC2787, RFC2986, RFC3280, RFC3369, zákon NR SR č. 215/2002 Z.z. o elektronickom podpise a vyhlášku NBÚ k zákonu o elektronickom podpise č. 536 až 542/2002.

4. Predpokladané zdroje

V tejto kapitole sú zhrnuté predpokladané zdroje na vývoj a nasadenia systému.

4.1. Požiadavky na softvér

- Predpokladaný server Apache na podporu PHP
- Softvér na vývoj HTML
- OS Windows

4.2. Požiadavky na hardvér

- Štandardný osobný počítač na prezentáciu
- Na vývoj, postačujú počítače, ktoré sú v softvérovóm štúdiu.
- USB kľúč na uloženie privátneho kryptovacieho kľúča

5. Preferované poradie projektov

Tím uprednostňuje témy tímových projektov v nasledovnom poradí:

1. **Infraštruktúra PKI a vybavenie pre koncových používateľov**
2.
3.