Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 812 19 Bratislava

Infraštruktúra PKI a vybavenie pre koncových používateľov

Tímový Projekt

Reakcia na posudok dokumentu „Analýza, špecifikácia a hrubý návrh

Reakciu vypracovali:
Tím číslo 4 PSS:
Bc. Peter Mulinka
Bc. Radovan Škríb
Bc. Martin Mačica
Bc. Jozef Hamar
Bc. Tomáš Smolek

Posudok vypracovali:
Tím číslo 2 PSS:
Bc. Vladimir Balaš
Bc. Martin Kerni
Bc. Štefan Novák
Bc. Peter Prochádzka
Bc. Ján Olbert
Bc. Pavol Skočík

Rok: 2004 / 2005
Vedúci projektu: Doc. Ing. Ladislav Hudec, Csc.

1 Úvod

Tento dokument vznikol ako reakcia na posudok tímu číslo 2, v ktorom posudzovali našu odovzdanú dokumentáciu. Odovzdaná bola v prvom kontrolnom bode v zimnom semestri, týkala sa iba analýzy. Konkurenčný tým hodnotil našu prácu ako analýzu a hrubý návrh. Hrubý návrh však nebol uvedený v dokumente vzhľadom na to, že výsledkom zimného semestra mala byť analýza PKI a jej zjednodušená verzia prístupná na internete ako webová stránka, ktorá by bola vhodná aj pre laika.

V úvode konkurenčný tím poznamenáva, že náš prístup k analýze PKI je „laxný“. Toto tvrdenie označujeme za subjektívny názor vzhľadom na to, že v našej analýze sme opísali všetky aspekty aj zákutia algoritmov a zaužívaných spôsobov či noriem PKI relevantných pre nasledujúcu prácu na tímovom projekte.

V nasledujúcich kapitolách sa pokúsime vyvrátiť alebo opraviť tvrdenia tímu číslo 2, avšak niektoré kritické aspekty posudku sú opodstatnené. Posudok sa použije v budúcnosti ako nápomocný dokument k tvorbe analýzy.

2 Formálna stránka dokumentu

Posudok konkurenčného tímu nás upozornil na niekoľko gramatických ako aj formálnych chýb. Jednou z nich boli viaceré slovníky pojmov vo vybraných kapitolách, neobsahovali vysvetlenia daných pojmov. Do dokumentu boli zaradené náhodou, mali sa vyskytovať iba na konci v kapitole 7, kde sú pojmy aj vysvetlené. Ďalej sa spomína v posudku zlé zarovnanie kapitol 3.4 až 4 smerom doprava, táto informácia nie je pravdivá. Zmena riadkovania v 7. kapitole bola spravená za účelom lepšej prehľadnosti kľúčových slov a ich definícií.

Väčšina ostatných formálnych chýb ako nejednotné štýly, nesprávne zalomenie textu, nevhodné číslovanie strán v sekcii obsahu, rovnaké čísla obrázkov na strane 10 a 11 sú ojedinelé chyby, ktoré sa už viac v dokumente neobjavujú, ale aj tak sú dôležité pre budúcu opravu dokumentu. Za hlavnú príčinu množstva formálnych chýb v dokumente označujeme nedostatok času potrebného pre prácu na tímovom projekte.

3 Obsahová stránka dokumentu

Ako sa už skorej spomenulo, konkurenčný tím vychádzal zo všeobecného zadania, teda že odovzdaný dokument nutne musí obsahovať hrubý návrh, avšak akýkoľvek návrh webovej stránky vysvetľujúcej PKI by bola už jej implementácia. Totiž návrh informatívnej webovej stránky nie je tak zložitý ako návrh nejakého veľkého informačného systému, preto pre jej vytvorenie bude použitý model rýchleho prototypovania. Pre doplnenie: model rýchleho prototypovania sa vyznačuje slabou viditeľnosťou celého procesu. Návrh a implementáciu samotného softvéru na podpisovanie sme nechali na letný semester.

V posudku sa viac krát nachádza kritika obsahu analýzy. Náš tím sa v nej snažil dokumentovať tie procesy, ktoré budú potrebné pre prácu v nadchádzajúcom letnom semestri vzhľadom na ponuku. Procesy označené ako „slabo zdokumentované“ boli z tohto hľadiska označené za okrajové.

3.1 Kapitola 1 – Predslov

Citát „Súkromný kľúč je iba jeden a je naším výlučným vlastníctvom, kým verejný kľúč môžeme poskytnúť viacerým osobám, s ktorými sme v elektronickom styku“ pre konkurenčný tím navodzuje pocit, že pre jeden súkromný kľúč existuje viacero verejných kľúčov. Tento „pocit“ je čisto subjektívny a ich osobný, keďže v citáte sa verejný kľúč spomína v jednotnom čísle, v množnom čísle sú iba osoby, ktorým ho môžeme poskytnúť.

3.2 Kapitola 2

V praxi sa používajú viac ako 2 algoritmy na výpočet „hešu“, to je pravda, proti tomuto tvrdeniu sa nedá namietať a v kapitole 2.2 ani netvrdíme opak, iba že najčastejšie používané sú práve 2.

Sto percentná bezpečnosť neexistuje. Nad týmto tvrdením by mohol pouvažovať konkurenčný tím miesto upínania sa na informačné zákony, takéto názory vedú ku kompromitácii systému. Síce je pravda, že jednosmerné funkcie sú nereverzibilné, ale z ich súčtu je možné vyčítať mnoho a pri dostatočnom počte informácií sa dá pôvodný text aspoň

uhádnuť. Svedčia o tom aj posledné pokusy s hešovacími funkciami MD5, MD4 a niektorými ďalšími, kde sa za pomoci nie veľkého výpočtového výkonu a v reálnom čase podarilo nájsť k jednému kontrolnému súčtu viacero pôvodných textov. Išlo o rádovo sekundy až 2 hodiny. Uvádzam adresu na článok, kde je možné nájsť viac informácii (http://www.root.cz/clanek/2368).

Samotný kontrolný súčet nám nezaručuje integritu správy, ale za použitia napríklad symetrického podpisu, ktorý je opisovaný tesne pred tvrdením „Kontrolný súčet nám zaručuje integritu správy...“, nám tú integritu zaručí.

Zdieľanie problémov elektronického podpisu a asymetrického šifrovania je na začiatku kapitoly 2.7 len zdôraznené pre konzistenciu nasledujúceho textu, autori túto skutočnosť dokonale chápu.

3.3 Kapitola 3

Možno nie každému je jasné prečo je autentifikácia taká dôležitá pre PKI, ale treba si uvedomiť, že bez nej by nebol riešiteľný problém ako napríklad oprávnené zrušenie privátneho kľúča pri jeho strate (jednorázové heslo).

Tvrdenie „...kde jednocestný algoritmus je založený na symetrickej šifre“ je pritvrdé označovať ako logickú chybu, skôr ako preklep (symetrický - ***a***symetrický). Vzhľadom na častejší výskyt správneho použitia slovného spojenia „jednocestná funkcia“, autori jeho význam chápu.

Za ostatné pripomienky ku kapitole 3 ďakujeme konkurenčnému tímu, boli na mieste a pomohli k uceleniu tejto kapitoly.

3.4 Kapitola 4

Vysvetlenie hierarchickej štruktúry v tejto kapitole nepopiera fakt že nemusí byť čisto stromová, dokonca ho táto kapitola aj uvádza.

Pri kompromitácii privátneho kľúča CA sa nikde v texte nespomína ukončenie existencie samotnej CA, píše sa iba o katastrofe pre samotnú existenciu CA. Postreh konkurenčného tímu sa neviaže k odovzdanému dokumentu.

Kapitola 4.4.1, všetky body algoritmu overovania si verejných kľúčov sú v správnom poradí a v správnom znení až na bod 5, kde New Yorkský smerovač mal byť vlastne Pražský. Tento preklep spôsobil viac nedorozumení na strane posudzovateľov. Veríme že jeho opravením sa problémy vyriešily.

V kontexte kapitoly 4.5 nieje nikde spomínaná žiadna nedôverihodnosť certifikátu národnej CA a ani certifikátu spoločnosti Microsoft. Upozornenie o tom, že zoznam CTL (Certificate Trusted List) je volitelný chýba, avšak miesto toho podobná myšlienka vyplýva z kontextu vety „Musíme si dávať pozor, aby nami používaný internetový prehliadač obsahoval iba dôveryhodné certifikáty“.

V kapitole 4.7 správne upozornili autori posudku na chýbajúcu možnosť úložiska privátneho kľúča CA – HSM modul.

3.5 Kapitola 5

Tvrdenie že norma X.509 vznikla v roku 1988 a v roku 1993 bola aktualizovaná na verziu 2 nehovorí nič o jej frekvencii používania na internete, akurát že v roku 1988 nebola dokonale navrhnutá a že ju bolo treba v roku 1993 opraviť aby ju bolo možné využívať. Ďalej fakt, že táto norma je iba doporučením ITU (International Telecomunication Standard) a doteraz nebola štandardizovaná hovorí sám za seba. Každá spoločnosť používa vlastnú verziu tohto štandardu, napríklad IETF PKI používa verziu 3. Netscape a Microsoft používajú toto doporučenie, avšak medzi sebou ich certifikáty pre SSL vo web serveroch a browseroch nemusia byť kompatibilné.

Malá frekvencia využívania privátneho kľúča CA nemení nič na fakte, že ak jej privátny kľúč bude skompromitovaný všetky certifikáty podpísané danou CA stratia dôverihodnosť. Preto bezpečnostný dôvod skrátenia doby platnosti certifikátu CA je namieste.

Tvrdenie že platnosť certifikátu CA by mala vypršať až po poslednom ňou vydanom certifikáte len ozrejmuje dôvod, že prečo sa podriadené certifikáty vydané danou CA vydávajú s maximálnou dobou platnosti rovnou s dobou platnosti certifikátu CA.

V kapitole 5.4 je ponúknuté presne také isté riešenie problému kompromitovaného certifikátu ako v posudku. Nieje potrebné ho opakovať.

Kapitola 5.7 v dokumente neexistuje, autori asi mysleli kapitolu 5.6.

3.6 Kapitola 6 – Použitá literatúra

Spomenuté neplatné linky linky naozaj nefungujú.

3.7 Porovnanie s ponukou tímu

Ako bolo už vyššie spomenuté, ponuka sa vsťahovala na obidva semestre, teda zimný aj letný. Odovzdaná analýza v zimnom semestri mala za úlohu zanalyzovať PKI a nie možnosti softvéru v letnom semestri. Prezentačná WWW stránka bude výsledkom analýzy.

4 Záver

Konkurenčný tím celkovo hodnotil vytvorenú analýzu ako slabú po obsahovej stránke. Avšak v celom posudku nespomenuli ani jednu konkrétnu kapitolu, ktorá chýba analýze a naozaj tam nebola. Niekoľko krát spomenuli absenciu hrubého návrhu, ktorý sa v dokumente v skutku nenachádza. Dôvod k jeho absencii je ten, že podľa ponuky a zadania sme si rozdelili prácu na dve oddelené časti, analýzu a výslednú prezentačnú stránku na zimný semester a návrh a implementáciu aplikácie umožňujúcej podpisovanie/overovanie dokumentov na letný semester. Veľa chýb označených konkurenčným tímom ako „logické chyby“ boli iba nedorozumeniami poprípade vysvetlením si kontextu po vlastnom.

Dúfame, že po uverejnení reakcie na posudok sa veľké množstvo nedorozumení zo strany posudzovateľov zredukuje. Za nájdené nedostatky v dokumentácii či už formálne alebo obsahové ďakujeme tímu číslo 2, pokúsime sa ich vyvarovať pri našej nasledujúcej práci.