Oponentský posudek doktorské práce

Autor doktorské práce: *Ing. Rudolf Vohnout*
Téma doktorské práce: ***Řešení integrity digitálního archivu pomocí relativní časové autentizace***

Oponent doktorské práce: *Doc. Ing. Cyril Klimeš, CSc.*
Ostravská univerzita Ostrava

Téma práce a splnění cíle

Problematika archivace elektronických dokumentů je úzce spojena s řešením jejich zabezpečení a integrity z pohledu dlouhodobé archivace a podmínek platné legislativy. Předložená disertační práce se zabývá právě návrhem a tvorbou univerzálního systémového řešení vedoucího k zajištění nepopiratelnosti svěřených, archivem spravovaných objektů.

Disertační práce vychází z platné legislativy ČR a dalších zemí především EU, analyzuje již existující projekty dlouhodobé archivace a respektuje doporučené formáty archivovaných dokumentů.

Práce je pojata jak analyticky, tak návrhově a experimentálně, což vede k dosažení stanovených cílů a jsou v ní diskutována i vhodná témata na pokračování výzkumu v této oblasti.

Vzhledem k výše uvedeným skutečnostem se jedná o téma velmi aktuální a dynamicky se rozvíjející s možností přímé aplikace v konkrétních institucích. Práce má teoreticko-metodologický charakter s praktickými výstupy.

Přínos v oblasti poznání

Za přínos v oblasti poznání považuji využití funkce DSSC pro dlouhodobou archivaci elektronických dokumentů a navržení obecného identifikátoru datové struktury bez využití hashovací funkce.

Přínos ve společenské praxi

Přínos ve společenské praxi lze spatřovat v implementaci autorem navrženého způsobu zajištění integrity archivovaných objektů do systémových návrhů a koncepce dlouhodobých archivů.

Formální úprava, publikace

Doktorandská disertační práce je členěna do 10 základních popisných kapitol a 6 kapitol doplňujících práci o použitou literaturu, seznamy zkratek, obrázků, tabulek, vzorců a jednou přílohou. Disertační práce obsahuje celkem 133 stran. Práce je psána přehledně a pečlivě.

V seznamu literatury v kapitole 11 jsem dohledal 4 vlastní publikace autora a není tedy zřejmá celková publikační činnost autora.

Dotazy a připomínky

V disertační práci je problematické vymezení některých pojmů a jejich používání. Konkrétně, v abstraktu je uvedeno „Návrhová pasáž se věnuje tvorbě univerzálního systémového řešení vedoucího k zajištění nepopiratelnosti svěřených, archivem spravovaných, objektů“. Následně v kapitole 2.2 je poté uvedeno vymezení pojmů, převážně bez odkazů na zdroj, což lze chápat, že se jedná o vlastní vymezení a definice. Zde je definována např. „Autenticita“ jako synonymum ke slovům pravost, původnost či hodnověrnost. Následně v podkapitole 2.2.1 je vymezen pojem „Integrita“ kde je zdůrazněno že „… tento pojem ovšem neřeší autenticitu (pravdivost, hodnověrnost) obsažené informace.“ Tato vymezení pojmů jsou v rozporu se závěry disertační práce. Konkrétně v kapitole 10. Závěr je na str. 114 na konci druhého odstavce uvedeno „Z tohoto přehledu jednoznačně vyplynulo, že všechny tyto metody využívají rozdílným způsobem hashovacích funkcí jako prostředek, jenž zajišťuje autenticitu daného objektu.“ Následně na str. 115 ve druhém odstavci je uvedeno „Model záměny zabezpečovacího prvku implementuje výstupy z DSCC pro včasnou detekci výskytu kolize použité hashovací funkce (s tím souvisejícím zpochybnění její bezpečnosti).“ Z těchto závěrů však vyplývá, že integritu a autenticitu nelze oddělovat. Z tohoto pohledu v práci nejsou řešeny operace s archivy typu „migrace“ a „emulace“, kde často dochází ke ztrátě integrity. Podle mého názoru autor, definuje integritu z pohledu změny či smazání dokumentu či pravosti dokumentu (zda se jedná stejný dokument, který byl vložen). Doporučuji, aby autor tyto pojmy při obhajobě vyjasnil.

Dále považuji za vhodné, aby autor vysvětlil závěr uvedený na str. 115 v prvním odstavci „V analytické části práce bylo zjištěno, že v oblasti bezpečnosti dlouhodobé archivace elektronických dokumentů (archivovaných objektů), resp. její podmnožině zabývající se integritou archivu jako systémového celku, neřeší všechny autorovi známé přístupy fakt nutné změny hashovacího algoritmu v čase. Závěry z analytické části práce pomohly stanovit obecný výchozí rámec pro tvorbu systému zabezpečení dlouhodobě archivovaného digitálního objektu a vedly tak je splnění prvního dílčího cíle práce.“

Doporučuji, aby při obhajobě autor vysvětlil, proč se nezabýval použitím PKI infrastruktur (CRL, časová razítka, atd.), dále SGML (standard pro metadata) a UNICITRAL (United Nations Commission on International Trade Law - zákonné požadavky).

Určitý problém práce vidím v používání pojmů hashovací funkce a hlavně pak nekonfliktní hashovací funkce. Autor používá DSSC, jako datovou strukturu která umožňuje automatickou analýzu bezpečnosti vybraných kryptografických algoritmů v daném časovém okamžiku nebo k určitému datu. Problém je v návrhu autora, že bude používat alespoň dvě bezkolizní hashovací funkce. Pro provedení experimentu přitom autor navrhuje takové funkce, kdy řada z nich má krátké klíče, některé funkce jsou prokázány jako nebezpečné a není vhodné je nasazovat (jsou již nalezeny způsoby kolize). Není také v této souvislosti poukázáno na špatnou implementace, či slabou algoritmizaci.

V souvislosti s uvedením přínosů doktorské disertační práce na str. 109 doporučuji, aby autor objasnil své tvrzení o teoretickém (vědeckém) přínosu: „Obohacení počítačové vědy o systém zaručující bezpečnost libovolného datového objektu bez jeho přímého ovlivnění slábnutím kryptografických algoritmů“. Toto tvrzení je v kontrastu se zjištěním z praxe, že krátké klíče, vadné funkce, špatné implementace funkcí, špatné implementace algoritmů vždy ovlivní bezpečnost.

Dále doporučuji vysvětlit i druhý teoretický přínos „Přispění do badatelské domény počítačové bezpečnosti mechanismem jednoznačné identifikace dokumentu s vyloučením závislosti na hashovacích funkcích“ a to jednak v kontextu použití hashovacích funkcí autorem (velká část práce je zaměřena hashovací funkce a aplikace dokonce podporují jen vybrané hashovací funkce) a také v kontextu s podkapitolou 6.2.2, kde jsou uvedeny Parametry identifikátoru. Zde je uvedeno, že budou nezávislé na hashovací funkci, přičemž

aplikaci, kterou autor navrhuje je ale naprosto závislá na podporovaných funkcích. Navržená nezávislá funkce výtahu zprávy je v podstatě náhradou hashovací funkce, ale nebyla podrobena kryptoanalýze, což považuji za jistou slabinu. Jak je zajištěno, že vzniklá datová věta nemůže být pozměněna?

V této souvislosti doporučuji vysvětlit, zda „bezkolizní hashovací funkce“ definovaná na str. 86 v posledním odstavci splňuje bezkoliznost prvního řádu (kdy pro dvě rozdílné zprávy nelze nalézt stejnou hashovací funkci), nebo druhého řádu (kdy pro jednu hashovací funkci není možno nalézt dva rozdílné vzory). Obecně bezkolizní hashovací funkce neexistuje, je však závislá na výpočetních schopnostech a z tohoto pohledu doporučuji tento pojem vysvětlit.

Závěr

Předložená práce Ing. Rudolfa Vohnouta splňuje požadavky kladené na doktorskou disertační práci a to jak z pohledu teoreticko - metodologické úrovně, tak ve využitelnosti v praxi. Práce obsahuje původní výsledky.

Doporučuji předloženou disertační práci k obhajobě před příslušnou komisí a rovněž doporučuji, aby na základě úspěšné obhajoby byla panu Ing. Rudolfu Vohnoutovi udělena vědecká hodnost Ph.D. v oboru Informatika.

V Ostravě 4.8.2014 Doc. Ing. Cyril Klimeš, CSc.