(73) Majiteľ: Veliký Dušan, Ing., Púchov - Horné Kočkovce, SK;

(72) Pôvodca: Zborun Igor, Ing., Žilina, SK;

(74) Zástupca: Labudík Miroslav, Ing., Kysucké Nové Mesto, SK;

(54) Názov: Spôsob šifrovania dát podľa identity v dôveryhodnej šifrovačnej autorite

(57) Anotácia:
Podstatou šifrovania dát podľa identity v dôveryhodnej šifrovačnej autorite je, že odosielateľ správy na analýzu identity zadá v perifériom zariadení indexy a identifikátorov identity odosielateľa a prijímateľov správy v určitej dôveryhodnej šifrovačnej autorite a po overení identity symetricky zašifruje správu, príčom jej symetrický šifrovací klúč sa pripojuje k jednotlivým indexom a identifikátorom identity prijímateľov a odosielateľa správy, ktoré sa odnošia na asymetrické zašifrovanie v tejto dôveryhodnej šifrovačnej autorite podľa indexov a identifikátorov identity odosielateľa a prijímateľov správy. Potom sa asymetricky zašifrovaný symetrický šifrovací klúč s identifikátorom dôveryhodnej šifrovačnej autority pripojuje k symetricky zašifrovaným dátam vo forme metabázy na zaslanie pre prijímateľov správy.
Oblastí techniky

Technické riešenie sa týka jednoduchého technického spôsobu šifrovania dát podľa identity v dôveryhodnej šifrovacej autorite na účely ich ochrany pred zneužitím nepovolanou osobou, najmä v oblasti technických informačných a telekomunikačných technológií.

Doterajší stav techniky

V oblasti informačných a telekomunikačných technológií sa na účely ochrany dát pred zneužitím používa symetrické, asymmetrické šifrovanie alebo kombinácia symetrického a asymmetrického šifrovania. Šifrovanie dát už nie je len záležitosťou veľkých a stredných firiem alebo vládných inštitúcií, ale čoraz viac aj menších firiem, domácností a súkromných osôb. Rozsiahle využívanie výpočetnej techniky vedie vo svojich dôsledkoch k stále sa zväčšujúcemu objemu pracovaných a ukladaných informácií. Rastie objem prenášaných, elektronických dát, či už prostredníctvom internetu či iných prenosových prostriedkov. Vznáša zraniteľnosť týchto dát. Šifrovanie dát je spôsob zmeny dát tak, aby sa účinne zamezilo neautORIZovaným osobám k prístupu do dát, ako sú napríklad súkromné alebo dôverné dokumenty, fotografie, komunikácia, heslá, rôzne prihlasovacie údaje a iné citlivé súbory, prípadne ním možno chrániť napr. elektronicke bankovníctvo alebo dátu posielané internetom. Šifrovanie dát zamedzi, že sa k pravému nedostane po ceste ďalšia osoba alebo medzi prístup k týmto dátam pri kradeže fyzického zariadenia napríklad (Notebooku, mobilu, USB flash disku, externých diskov, DVD a pod.). Ide teda o proces, keď sa z čitateľných dát, napr. textu, pomocou šifrovačного algoritmu a šifrovačnego kľúča sa vytvorila zašifrované dát, napr. textu.


Podstata technického riešenia

Uvedené nedostatky v podstatnej miere odstraňuje spôsob šifrovania dát podľa identity v dôležitnejšíš fince technického riešenia. Podstatou technického riešenia je, že odosielateľ správy na analýzu identity zadá v periférnom zariadení indexy a identifikačné identity odosielateľa a prijímateľa správy v určitej dôležitnejšíš fince technického riešenia. Po overení identity symetricky zašifruje správu, pričom jej symetricky šifrovacie kľúče sa pripojí k jednotlivým indexom a identifikátorom identity prijímateľa a odosielateľa správy, ktoré sa odosielá na asymetrické zašifrovanie v tejto dôležitnejšíš fince technického riešenia podľa indexov a identifikátorov identity odosielateľa a prijímateľa správy. Následne sa asymetricky zašifrované symetricky šifrovacie kľúče s identifikátorom dôležitnejšíš fince technického riešenia správy pripojia u odosielateľa a symetricky zašifrovaným dátom vo forme metafázy na zaslanie pre prijímateľov správy.

Spôsob šifrovania dát podľa identity v dôležitnejšíš fince technického riešenia spája vyhody symetrického a asymetrického šifrovania a prípadné ho integrované existujúcich systémov šifrovania dát podľa identity s existujúcimi systémami symetrického šifrovania a existujúcimi systémami správy ident. Zároveň spracováva dát na účely poskytnutia bezpečného dátového kontajnera, umožňujúceho jednoduché a bezpečné zdieľanie informácií, bez použitia napr. hesiel a certifikátov. Riešenie umožňuje pri zais- tení veľké bezpečnosti asymetricky šifrovaných prenášaných dát podstatné menšie časové náročnosti šifrovania a s podstatne menším objemom zašifrovaných dát v periférnom zariadení odosielateľa ako iba pri asymetricky zašifrovaných dátach bez nutnej následnej distribúcie a správy verejného kľúča u prijímateľov správy. Takto šifrované dátá využívajú u odosielateľa len periférne zariadenie s beznovou kapacitou a rýchlo- sfou i bežné dátovo priepustnú spájajúci sieť.

Príklady uskutočnenia

Pred šifrovaním odosielateľ správy pod heslom verifikované zaregistrované v dôležitnejšíš fince technického riešenia, napr. vzdialene na serveriho prevádzkovateľa určiteho internetového portálu alebo na firemnom serveri, prípadne v uspešnom operátora a pod., svoj identifikátor, t. j. napr. e-mailovú adresu, telefónne číslo, číslo občianskeho preukazu, odtlačok prsta a pod., pod príslušným indexom identity, napr. svojim menom, heslom a pod. Při šifrovaní správy odosielateľ právom na analýzu identity v svojom periférnom zariadení indexy a identifikátor identity odosielateľa a prijímateľa správy v odosielateľom zaregistrované periférnejšíš fince technického riešenia autorite. Po overení identity sa získaným spôsobom na pokyn dôležitnejšíš fince technického riešenia odosielateľa automaticky symetricky zašifruje správa, pričom jej symetricky šifrovacie kľúče sa pripojia k jednotlivým indexom a identifikátorom identity prijímateľa a odosielateľa správy, ktoré sa napíšu získaným spôsobom odosielajú na asymetrické zašifrovanie v tejto dôležitnejšíš fince technického riešenia autorite podľa indexov a identifikátorov identity odosielateľa a prijímateľa správy. Následne sa na pokyn dôležitnejšíš fince technického riešenia autorite dôležitnejšíš fince technického riešenia autority prijímateľa správy a podľa identity odosielateľa a symetricky zašifrovaným dátom vo forme metafázy na zaslanie pre prijímateľov správy.


Priemyselná využiteľnosť

Spôsob šifrovania dát podľa identity v dôležitnejšíš fince technického riešenia autorite je určený na šifrovanie a dešifrovanie dát najmä v oblasti technických informačných a telekomunikačných technológií a ochranné dátu pred zneužívaním vo firmách, vládnych a úradných inštitúciách, domácnostiach a na ochranu súkromnej korešpondencie osob.
NÁROKY NA OCHRANU

Spôsob šifrovania dát podľa identity v dôveryhodnej šifrovacej autorite, vyznačujúci sa tým, že odosielateľ správy na analýzu identity zadá v perifériom zariadení indexy a identifikátor identity odosielateľa a prijímateľov správy v určitej dôveryhodnej šifrovacej autorite a po overení identity symetricky zašifruje správu, pričom jej symetrický šifrovací klúč sa pripojí k jednotlivým indexom a identifikátorm identity prijímateľov a odosielateľa správy, ktoré sa odošlú na asymetrické zašifrovanie v tejto dôveryhodnej šifrovacej autorite podľa indexov a identifikátorov identity odosielateľa a prijímateľov správy, pričom sa asymetricky zašifrovaný symetrický šifrovací klúč s identifikátorom dôveryhodnej šifrovacej autority pripojí u odosielateľa k symetricky zašifrovaným dátam vo forme metabázy na zaslanie pre prijímateľov správy.

Koniec dokumentu