PŘIHLÁŠKA VYNÁLEZU

Zveřejněná podle §31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2015-473

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

G06F 21/00	(2013.01)
G06F 21/33	(2013.01)
G06F 21/31	(2013.01)
H04L 29/06	(2006.01)
H04L 9/32	(2006.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **07.07.2015**

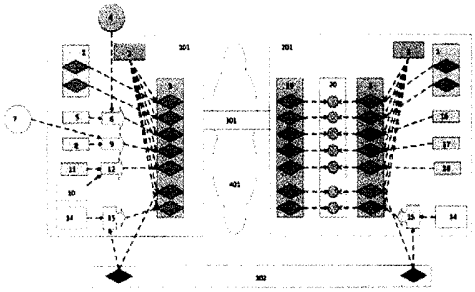
(40) Datum zveřejnění přihlášky vynálezu: **08.02.2017**

(Věstník č. 6/2017)

(71) Přihlašovatel:
ADUCID s.r.o., Brno - Přízřenice, CZ

(72) Původce:
Ing. Libor Neumann, CSc., Praha 5 - Lužiny, CZ
RNDr. Vlastimil Klíma, Praha 4, CZ

(74) Zástupce:
INVENTIA s. r. o., RNDr. Kateřina Hartvichová, Na Bělidle 3, 150 00 Praha 5



(54) Název přihlášky vynálezu:

Způsob zabezpečení autentizace při elektronické komunikaci

(57) Anotace:
Způsob zabezpečení autentizace při elektronické komunikaci mezi alespoň jedním klientským autentizačním prostředkem (101, 102, 103) a alespoň jedním serverovým autentizačním prostředkem (201), kdy se nejprve provede primární autentizace, při níž se vytvoří sekundární autentizační tajemství (2, 22, 23) sdílené klientským autentizačním prostředkem (101, 102, 103) a serverovým autentizačním prostředkem (201) a platné pouze pro danou autentizační transakci, a následně se toto sekundární autentizační tajemství (2, 22, 23) použije jako vstup kryptografické transformace prováděné klientským autentizačním prostředkem na každém elementu autentizačního vektoru odděleně za vytvoření prvního odvozeného autentizačního vektoru (3), přičemž autentizační vektor (AV) je uspořádaná množina elementů autentizačního vektoru (AVE(i)), přičemž první odvozený autentizační vektor (3) se přenese z klientského autentizačního prostředku (101, 102, 103) na serverový autentizační prostředek (201) a tam se vyhodnotí s pomocí sekundárního autentizačního tajemství (2, 22, 23).

CZ 2015 - 473 A3

Způsob zabezpečení autentizace při elektronické komunikaci

Oblast techniky

Vynález spadá do oblasti bezpečnosti informačních a komunikačních technologií. Vynález se týká ochrany prostředků, zejména zařízení používaných k autentizaci při lokální či vzdálené elektronické komunikaci, proti zneužití neoprávněnou osobou.

Dosavadní stav techniky

Existují prostředky používané k bezpečnému navazování chráněné elektronické komunikace (autentizace), které zajišťují různou úroveň bezpečnosti, tedy různou úroveň odolnosti proti zneužití neoprávněnou osobou. Pro zvýšení bezpečnosti se používají různé metody směřované vůči různým způsobům možného zneužití. Mezi hlavní rizika zneužití autentizačních prostředků používaných při elektronické komunikaci patří získání samotných prostředků či utajovaných informací, které tyto prostředky k autentizaci používají.

V praxi velmi rozšířený způsob autentizace pomocí zadání login jména a hesla uživatelem je velmi citlivý na to, když útočník nějakým způsobem získá informaci o zadávaném hesle. K tomu má řadu příležitostí např. sledovat funkci klávesnice, pomocí které uživatel heslo zadává, snímat komunikaci po datové síti, kterou se heslo přenáší, přečíst informace z databáze poskytovatele služby, pomocí které se hesla kontrolují, nebo od uživatele heslo podvodně získat (phishing).

K snížení rizik spojených se zneužitím autentizačního prostředku se používá více autentizačních faktorů. Útočníkovi pak nestačí prolomit jeden autentizační faktor, ale musí prolomit všechny použité autentizační faktory. Velmi známým v praxi rozšířeným dvoufaktorovým autentizačním prostředkem jsou čipové platební karty. Uživatel má kartu s čipem, která ke své funkci vyžaduje zadání PIN, tedy tajného čísla. Útočník musí získat jak platební kartu, tak uhádnout nebo jinak zjistit PIN, aby kartu mohl zneužít.

K snížení rizik spojených se zneužitím autentizačního prostředku se používají speciálně konstruovaná zařízení, která poskytují zvýšenou ochranu tajným informacím uloženým na

autentizačním prostředku, které jsou pro autentizaci používány. Tím se snižuje riziko, že se útočník zmocní těchto informací čtením z autentizačního předmětu (lokálním či vzdáleným). Jako příklad lze uvést specializované autentizační tokeny či kalkulátory nebo čipové karty či USB tokeny s vestavěným „chytrým" čipem (smart chip).

Zpravidla platí, že čím bezpečnější autentizační řešení je, tím je složitější a pro uživatele komplikovanější. Proto existují i řešení, která riskují možné kopírování tajných informací používaných k autentizaci útočníkem, protože tím snižují náklady na používání takových autentizačních prostředků a umožňují snížit uživatelskou složitost a nároky na speciální znalosti a dovednosti, které specializovaná zařízení vyžadují. Příkladem takového řešení je umístění autentizačního X.509 certifikátu (s privátním klíčem) na disk osobního počítače či na běžný USB paměťový token.

V praxi používaná řešení mají řadu nevýhod, které vedou buď k nízké bezpečnosti, tedy zvýšeným šancím útočníků na zneužití takových autentizačních prostředků nebo k drahým a uživatelsky komplikovaným řešením, které uživatelé nechtějí nebo neumí používat.

Mezi nevýhody stávajících řešení patří fakt, že způsob ochrany proti zneužití je pevně vestavěn do příslušného autentizačního prostředku a je využíván při použití autentizačního prostředku nezávisle na tom, jak vysoká bezpečnost je přiměřená konkrétnímu použití autentizačního prostředku v daném okamžiku. Autentizace je pak buď nedostatečně bezpečná v případech použití s vyššími nároky na bezpečnost, když zvítězí kritérium pohodlí pro klienta elektronické služby, nebo je obsluha autentizačního prostředku nepřiměřeně komplikovaná, v případě použití pro služby s běžnými nároky na bezpečnost, a použití takových prostředků není uživatelem akceptováno.

Mezi nevýhody takových řešení patří také to, že druhý a případně další faktor je vyhodnocován přímo autentizačním zařízením před zahájením vlastní autentizace. Zařízení může získat útočník a může nalézt způsoby, kterými obejde ochranné mechanizmy zařízení. Buď obejde nutnost druhý faktor použít, nebo získá dostatečný počet pokusů druhý faktor uhodnout, případně najde jiný způsob, jak informaci o druhém faktoru z autentizačního prostředku získat.

Kromě toho je uživatel nucen používat více různých autentizačních prostředků pro různé služby, což mu komplikuje život, snižuje celkovou bezpečnost používání elektronické komunikace a elektronických služeb a konečně i zvyšuje cenu.

Podstata vynálezu

Předkládaný vynález poskytuje způsob zabezpečení autentizace při elektronické komunikaci mezi alespoň jedním klientským autentizačním prostředkem a alespoň jedním serverovým autentizačním prostředkem, při němž se nejprve provede primární autentizace, při níž se vytvoří sekundární autentizační tajemství (SAS) sdílené klientským autentizačním prostředkem a serverovým autentizačním prostředkem a platné pouze pro danou autentizační transakci, a následně se toto sekundární autentizační tajemství použije jako vstup transformace, s výhodou kryptografické transformace, prováděné klientským autentizačním prostředkem na každém elementu autentizačního vektoru (AVE) odděleně za vytvoření elementů prvního odvozeného autentizačního vektoru (AVEP), přičemž autentizační vektor (AV) je uspořádaná množina elementů autentizačního vektoru (AVE(i)) a první odvozený autentizační vektor (AVP) je uspořádaná množina příslušných elementů odvozeného prvního autentizačního vektoru (AVEP(i)), která se přenese z klientského autentizačního prostředku na serverový autentizační prostředek a tam se vyhodnotí s pomocí sekundárního autentizačního tajemství.

S výhodou má klientský autentizační prostředek uloženy hodnoty elementů autentizačního vektoru a/nebo jsou do něj zadány uživatelem nebo získány z nosiče informací nebo z okolního prostředí před autentizační transakcí nebo v průběhu autentizační transakce a/nebo jsou před autentizační transakcí nebo v průběhu autentizační transakce získány z transformovaných hodnot elementů autentizačního vektoru (T-AVE(i)) s pomocí informací zadaných uživatelem nebo získaných z nosiče informací nebo z okolního prostředí, a serverový autentizační prostředek má uloženy referenční hodnoty elementů autentizačního vektoru (AVER(i)) nebo je před autentizační transakcí nebo v průběhu autentizační transakce získá z nosiče informací nebo z okolního prostředí.

Transformace může zahrnovat např. přičtení SAS, zřetězení s SAS, bitové manipulace s SAS, kryptografické transformace, atd.

Kryptografická transformace může být jednosměrná (např. funkce hash) nebo obousměrná (např. šifrování a dešifrování).

Element autentizačního vektoru (AVE – Authentication Vector Element) je autentizační prvek použitelný k dílčí autentizaci. Jednotlivé AVE jsou jednoznačně odlišeny svým indexem (i - index). Je zapisováno AVE(i). Příslušný AVE(i) je jednoznačně přiřazen účelu svého použití. Element autentizačního vektoru (AVE) může být použit k různým účelům, například k ověření dalšího autentizačního faktoru nebo k ochraně proti kopírování autentizačního tajemství. Jednotlivé elementy autentizačního vektoru jsou s výhodou vybrány ze skupiny zahrnující data z předcházejících autentizačních transakcí, o identifikaci klientského autentizačního prostředku, o lokálním autentizačním faktoru, o tajemství datového kanálu, atd.

Autentizační vektor (AV – Authentication Vector) je uspořádaná množina AVE(i). Počet a výběr AVE v konkrétním použití AV v konkrétní autentizační transakci může být jiný než v předchozí či následné autentizační transakci. Výběr AVE použitých v dané konkrétní autentizační transakci může být přímo či nepřímo řízen serverovým autentizačním prostředkem a to na základě požadavků zadaných, s výhodou on-line, cílovým systémem užívajícím autentizaci.

Referenční hodnota elementu autentizačního vektoru (AVER(i) - Authentication Vector Element Reference) je hodnota určená k ověření správnosti AVE(i). Je to hodnota vzniklá před ověřením AVE(i) způsobem, který je příslušný účelu AVE(i).

Element odvozeného autentizačního vektoru (AVEP(i) – Authentication Vector Element Product) je informace vzniklá transformací, s výhodou kryptografickou transformací, příslušného AVE(i) pomocí sekundárního autentizačního tajemství. Odvozený autentizační vektor AVP je uspořádaná množina AVEP(i).

Sekundární autentizační tajemství (SAS – Secondary Authentication Secret) je sdílené tajemství vzniklé a autentizované při primární autentizaci, např. pomocí primárního autentizačního tajemství. Jedná se o pseudonáhodnou utajenou informaci známou jen oběma

stranám, které se účastní autentizace, tj. klientskému autentizačnímu prostředku a serverovému autentizačnímu prostředku. SAS je platné jen po dobu autentizace (autentizačního procesu, autentizační transakce) a je vytvořeno tak, aby nebylo předvídatelné ani při znalosti primárního autentizačního tajemství. Postupy primární autentizace a postupy vytvoření sdíleného sekundárního autentizačního tajemství jsou v oboru známy.

V jednom provedení vynálezu se první odvozený autentizační vektor na serverovém autentizačním prostředku vyhodnotí tak, že v serverovém autentizačním prostředku se z referenčních hodnot elementů autentizačního vektoru uložených na serverovém autentizačním prostředku vytvoří druhý odvozený autentizační vektor tak, že se sekundární autentizační tajemství použije jako vstup kryptografické transformace prováděné serverovým autentizačním prostředkem na každém elementu autentizačního vektoru odděleně, a první a druhý odvozený autentizační vektor se porovnají.

V jiném provedení vynálezu se první odvozený autentizační vektor na serverovém autentizačním prostředku vyhodnotí tak, že v serverovém autentizačním prostředku se každý element prvního odvozeného autentizačního vektoru odděleně podrobí inverzní transformaci k transformaci použité klientským autentizačním prostředkem, a výsledek se vyhodnotí s použitím referenčních hodnot elementů autentizačního vektoru.

V jednom provedení vynálezu se při každé autentizační transakci použijí všechny elementy autentizačního vektoru.

V jiném provedení vynálezu se při různých autentizačních transakcích použijí jen některé elementy autentizačního vektoru, přičemž se informace o tom, které elementy autentizačního vektoru se použijí při dané autentizační transakci, předá ze serverového autentizačního prostředku na klientský autentizační prostředek v průběhu autentizační transakce. Tím se lze snadno přizpůsobit nárokům každé specifické autentizační transakce na bezpečnost.

Před použitím AV jsou určeny jednotlivé elementy autentizačního vektoru AVE(i), a to včetně účelu použití každého AVE(i). Určení AVE(i) je platné pro všechny další autentizace až do doby než je toto přiřazení změněno.

Před každou jednotlivou autentizační transakcí je možné určit, které konkrétní elementy autentizačního vektoru AVE(i) budou v této transakci použity a které nebudou. Tyto řídicí informace jsou předány serverovému autentizačnímu prostředku. V jednom výhodném provedení serverový autentizační prostředek na základě řídicí informace určí, které elementy autentizačního vektoru AVE(i) budou v autentizační transakci použity, předá tuto informaci klientskému autentizačnímu prostředku, a ten vytvoří první odvozený autentizační vektor s využitím pouze stanovených elementů AVE(i). Pokud klientský autentizační prostředek nemůže získat hodnotu některého elementu AVE(i), a tedy ani odpovídajícího elementu prvního odvozeného autentizačního vektoru AVEP(i), sdělí to serveru. Server pak informaci o chybějící hodnotě zahrne do vyhodnocení autentizace.

Prvním krokem dané autentizace je provedení primární autentizace, např. pomocí primárního autentizačního tajemství, a vytvoření sekundárního autentizačního tajemství SAS.

Aktuální řídicí informace určující, které konkrétní elementy autentizačního vektoru AVE(i) mají a které nemají být v této autentizaci použity, mohou být bezpečně přeneseny ze serverového autentizačního prostředku na klientský autentizační prostředek. K ochraně přenosu lze použít vytvořené SAS nebo informaci z něj odvozenou.

Klientský autentizační prostředek získá informace potřebné k naplnění účelu každého jednotlivého elementu autentizačního vektoru AVE(i), který má být použit. Tyto informace získá a zpracuje způsobem příslušným k účelu použití. Tím získá hodnoty všech elementů autentizačního vektoru AVE(i). Pomocí transformace vypočte klientský autentizační prostředek z každého elementu autentizačního vektoru AVE(i) a ze sekundárního autentizačního tajemství SAS jednotlivé elementy odvozeného autentizačního vektoru AVEP(i).

Všechny takto vypočtené elementy odvozeného autentizačního vektoru AVEP(i) jsou bezpečně přeneseny z klientského autentizačního prostředku na serverový autentizační prostředek jako první odvozený autentizační vektor. K ochraně přenosu lze použít sekundární autentizační tajemství SAS nebo informaci z něj odvozenou.

Podle účelu použití každého jednotlivého elementu autentizačního vektoru AVE(i) předá serverový autentizační prostředek přímo výsledek vyhodnocení každého v autentizaci použitého elementu autentizačního vektoru AVE(i) jako součást výsledku autentizace cílové aplikaci nebo provede jiné zpracování a další akce či činnosti.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je detekce zkopírování klientského autentizačního prostředku. K tomu je využito M elementů autentizačního vektoru. Tyto elementy označme AC-AVE(i) (AntiCopy Authentization Vector Element).

Každý z M elementů AC-AVE(i), kde i = 1 až M, je přiřazen jedné z předchozích provedených autentizací, a to s výhodou tak, že AC-AVE(1) je přiřazen bezprostředně předcházející autentizaci, AC-AVE(2) autentizaci která předcházela této autentizaci, AC-AVE(j) je přiřazen j-té předchozí autentizaci. Elementy AC-AVE(i) odpovídají informaci, která je jednoznačně přiřazena příslušné předchozí autentizační transakci a je známa pouze oběma stranám transakce.

Takovou informací může být s výhodou například SAS, nebo hodnota ze SAS kryptograficky odvozená, s výhodou pomocí jednosměrné kryptografické transformace. Každá autentizace je provedena tak, že vznikne autentizované SAS platné a známé jen v této autentizaci. Klientský i serverový autentizační prostředek mají v dané autentizaci k dispozici shodné SAS. Ze SAS pomocí kryptografické transformace (z bezpečnostních důvodů je výhodné použít jednosměrnou kryptografickou transformaci) vypočte klientský i serverový autentizační prostředek v průběhu autentizační transakce nezávisle novou hodnotu AC-AVE pro tuto autentizaci. Označme ji AC-AVE(0).

Klientský autentizační prostředek vytvoří ze dříve zapamatovaných hodnot AC-AVE(i), kde i = 1 až M, elementů odvozeného autentizačního vektoru AVEP(i) a předá je serverovému prostředku k vyhodnocení. K vytvoření elementů odvozeného autentizačního vektoru použije transformaci používající jako vstup SAS.

Klientský autentizační prostředek po výpočtu AC-AVE(0) posune dříve zaznamenané hodnoty AC-AVE(i) tak, že hodnotu AC-AVE(0) zaznamená jako AC-AVE(1), když hodnotu AC-AVE(1) přesunul na AC-AVE(2) atd. To znamená, že při každé provedené autentizaci se nově vypočtená hodnota AC-AVE(0) zařadí na začátek seznamu hodnot AC-AVE(i) a ostatní hodnoty se o jednu pozici přesunou směrem ke konci seznamu hodnot.

Serverový autentizační prostředek využije vypočtený AC-AVE(0) jako příslušnou referenční hodnotu složky autentizačního vektoru AC-AVER(0).

Serverový autentizační prostředek použije dříve zaznamenané hodnoty AC-AVER(i), kde i=1 až M, k ověření shody s hodnotami předanými k ověření klientským autentizačním prostředkem tak, že po posunu dříve zaznamenaných hodnot AC-AVER(i-1) na AC-AVER(i) vytvoří stejnou transformací, používající jako vstup SAS, elementy odvozeného

autentizačního vektoru a porovná je s hodnotami obdrženými od klientského autentizačního prostředku.

Serverový autentizační prostředek také zaznamená nově vypočtenou hodnotu AC-AVE(0) a při tom posune dříve zaznamenané hodnoty AC-AVER(i) tak, že hodnotu AC-AVE(0) zaznamená jako AC-AVER(1), když hodnotu AC-AVER(1) přesunul na AC-AVER(2) atd. To znamená, že při každé provedené autentizaci se nově vypočtená hodnota AC-AVE(0) se zařadí na začátek seznamu hodnot AC-AVER(i) a ostatní hodnoty se o jednu pozici přesunou směrem ke konci seznamu hodnot.

Vyhodnocení složek AC-AVEP(i), kde i=1 až M, je prováděno tak, aby se odlišily situace, kdy došlo k technickému problému na straně klientského či serverového autentizačního prostředku od situace, kdy došlo ke zkopírování dat z klientského autentizačního prostředku a jejich použití jiným klientským autentizačním prostředkem.

Vyhodnocení s výhodou rozlišuje následující situace:

- Všechny složky AC-AVE(i) jsou vyhodnoceny jako shodné s AC-AVER(i). To znamená, že nedošlo k technickému problému ani k použití kopie.
- Všechny složky AC-AVE(i) s výjimkou *n* bezprostředně sousedních složek na začátku seznamu jsou shodné s AC-AVER(i+/-n), tedy s referenčními složkami posunutými vpřed nebo vzad o *n* pozic. To znamená, že došlo k technickému problému při *n* po sobě následujících autentizacích buď na klientském, nebo serverovém autentizačním prostředku. Při vyhodnocení situace technického problému je k příslušným AC-AVER(i) poznamenáno, že taková situace byla vyhodnocena a tato informace je použita při následujících vyhodnoceních, kdy se hodnoty dostávají ze začátku seznamu.
- Pokud nastala jiná neshoda, tedy liší se jedna či více porovnávaných složek AC-AVE(i) od AC-AVER(i) jiným způsobem než odpovídá technické problému klientského nebo serverového autentizačního prostředku. To znamená, že byla provedena kopie autentizačního tajemství a ta byla alespoň jednou použita.

Při vyhodnocení existence a použití kopie autentizačního tajemství je tato skutečnost signalizována jako výstup prostředků ochrany autentizačních prostředků proti zneužití a může být použita k nápravným opatřením jako je zablokování autentizačních prostředků, vnucené odlišení kopie od originálu, atd.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je ověření lokálních autentizačních faktorů. Klientský autentizační prostředek získá

hodnotu lokálního autentizačního faktoru (LAF) z okolního prostředí a referenční hodnota elementu autentizačního vektoru LF-AVER(i) uložená na serverovém autentizačním prostředku je pak buď přímo lokální autentizační faktor, nebo informace z lokálního autentizačního faktoru odvozená, nebo referenční informace, přičemž je-li LF-AVER(i) referenční informace, je tato referenční informace na lokálním autentizačním faktoru nezávislá.

Lokální autentizační faktor (LAF) je informace získaná technickým vybavením klientského autentizačního prostředku z fyzického okolí tohoto prostředku, případně přímo od uživatele, za účelem ověření držení klientského autentizačního prostředku oprávněným uživatelem. Lokální autentizační faktor může být informace, která musí být uživatelem zadána (např. PIN, heslo), nebo informace získaná z jiného předmětu, který má vlastnit jen oprávněný uživatel (např. bezdrátové platební karty), rozpoznání biometrických znaků či biometrie chování oprávněného uživatele (např. sejmutí obrazu obličeje, otisku prstu, gesta, pravidelné zvyklosti), apod.

Pro ověření L lokálních autentizačních faktorů LAF je využito K elementů autentizačního vektoru, kde K >= L. Tyto elementy označme LF-AVE(i) (Local Factor Authentization Vector Element), kde i = 1 až K.

Počet ověřovaných LAF nemusí být vždy shodný, může být řízen požadavkem serverového autentizačního prostředku, na základě kterého je konkrétně určeno, zda a které LAF mají být v daném konkrétním případě získány technickým vybavením klientského autentizačního prostředku a mají být použity k ověření. Počet právě získaných LAF nemusí být vždy shodný s počtem ověřovaných LAF. Pro ověření lze použít také LAF získané v minulosti a zapamatované klientským autentizačním prostředkem v povolenou dobu, ve které je možné takový LAF znovu použít. Povolenou dobu je možné nastavit buď uživatelem klientského autentizačního prostředku, nebo může být součástí požadavku serverového autentizačního prostředku či může být vzdáleně konfigurována pomocí serverového autentizačního prostředku na klientském autentizačním prostředku.

V okamžiku kdy je příslušný LAF definován (inicializován), je provedena inicializace prostředků ověření LAF jak klientským autentizačním prostředkem, tak serverovým autentizačním prostředkem. Hodnota LF-AVE(i), tj. elementu získávaného klientským autentizačním prostředkem, příslušného k LAF, může být buď přímo LAF, nebo informace z LAF odvozená, nebo referenční informace transformovaná kryptografickou transformací, jejímž vstupem je LAF. Hodnota LF-AVER(i), tj. referenční hodnota uložená na serverovém

autentizačním prostředku, je pak v odpovídajících případech buď přímo LAF, nebo informace z LAF odvozená, nebo referenční informace. Je-li LF-AVER(i) referenční informace, je tato referenční informace na LAF nezávislá.

Ověření, že konkrétní LAF včetně hodnoty LF-AVE(i) produkované LAF přísluší oprávněnému uživateli, je možné provést při nebo po definování LAF (například organizačními prostředky, jako je například první zadání LAF před důvěryhodnou osobou, státním orgánem, nebo e-mailem).

V případě, že LF-AVER(i) je referenční informace nezávislá na LAF, je inicializace prostředků LF-AVE(i) prováděna na Klientském autentizačním prostředku takto:

- Je sejmut referenční LAF (např. proběhne první zadání a kontrola hesla, PIN, je použit příslušný identifikační předmět, je sejmut referenční obraz obličeje, otisku prstu). Výsledkem sejmutí referenčního LAF je referenční hodnota či soubor lokálních referenčních hodnot (označme LAF-RV(i) Local Authentication Factor Reference Value). Může jít o jednu či více hodnot.
- Zároveň je pseudonáhodně vytvořen příslušný počet odvozených referenčních hodnot elementu autentizačního vektoru LF-AVER(i) ze SAS.
- K sobě příslušné hodnoty LAF-RV(i) a LF-AVER(i) jsou použity jako vstup vhodné kryptografické transformace (například zašifrování LF-AVER(i) pomocí LAF-RV(i)). Výsledek kryptografické transformace je uložen na klientském autentizačním prostředku k dalšímu použití a není jinam přenášen. Označme tuto hodnotu jako T-AVE(i) (Transformed Authentication Vector Element).
- Zároveň je na serverovém autentizačním prostředku uložena příslušná referenční hodnota příslušného elementu autentizačního vektoru LF-AVER(i) vypočteného stejným způsobem ze SAS na Serverovém autentizačním prostředku.

Tento postup je aplikován na všechny hodnoty všech LAF, přičemž nemusí proběhnout pro všechny hodnoty, nebo pro všechny LAF, současně. Může jít o postupný proces, kde hodnoty či jednotlivé LAF, které byly inicializovány, mohou být využívány k ověření již před tím, než jsou inicializovány další hodnoty či další LAF.

Ověřování LAF(i) je pak prováděno takto:

- Technické vybavení klientského autentizačního prostředku získá LAF a vytvoří příslušnou hodnotu či hodnoty nebo je použit dříve získaný LAF a jeho zapamatovaná příslušná hodnota či hodnoty (označme LAF-VV(i) - Local Authentication Factor Verified Value).

- Dříve inicializovaná a zaznamenaná příslušná hodnota T-AVE(i) a verifikovaná hodnota LAF-VV(i) jsou vstupem inverzní kryptografické transformace použité při inicializaci (např. dešifrování T-AVE(i) pomocí LAF-VV(i)).
- Výstup inverzní kryptografické transformace je použit jako hodnota složky autentizačního vektoru LF-AVE(i). K ověření je použit mechanizmus ověření složky autentizačního vektoru popsaný dříve.

Tento mechanizmus je použit pro každou hodnotu každého LAF odděleně a je odděleně vyhodnocován.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je autentizace neautentizovaného datového kanálu. Pro tento účel stačí jediný element autentizačního vektoru AVE(i), může jich však být využito více.

Datový kanál vedoucí mezi klientskou částí a serverovou částí vytvoří interní tajemství používané k ochraně Datového kanálu (např. k šifrování a ochraně integrity přenášených dat).

Klientská strana Datového kanálu vytvoří pomocí jednosměrné transformace z interního tajemství Datového kanálu exportovatelné tajemství datového kanálu DCSE (Data Channel Secret Exporter).

Shodné exportovatelné tajemství datového kanálu vytvoří také serverová strana Datového kanálu.

Klientský autentizační prostředek získá DCSE od klientské strany Datového kanálu a Serverový autentizační prostředek získá DCSE od serverové strany Datového kanálu.

Klientský autentizační prostředek použije získaný DCSE jako element autentizačního vektoru AVE(i) a serverový autentizační prostředek použije získaný DCSE jako referenční hodnotu elementu autentizačního vektoru AVER(i) .

Příslušný element autentizačního vektoru je vyhodnocen dříve popsaným způsobem a tím dojde k autentizaci Datového kanálu sekundárním autentizační tajemství SAS, které bylo autentizováno (primárním) autentizačním tajemstvím.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je ověření klientského autentizačního prostředku (tedy ověření pravosti, identity zařízení, např. interních identifikačních dat), které je identifikováno jedním nebo několika identifikátory, pokud tyto identifikátory na jednotlivých kusech zařízení nejsou shodné. Označme identifikátor zařízení DI(i) (Device Identifier).

Použitím DI(i) jako LF-AVE(i) je možné ověřit, že použité zařízení je shodné jako bylo v době Inicializace prostředků LAF(i). Přitom je možné inicializaci DI(i) provést ihned při prvním použití Klientského autentizačního prostředku.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je vyloučení útočníka užitím datového kanálu. Pro tento účel stačí jediný element autentizačního vektoru AVE(i), je však možno jich použít více.
Pomocí Datového kanálu vedoucího mezi klientskou částí a serverovou částí je vytvořeno sekundární tajemství datového kanálu DCSS (Data Channel Secondary Secret). Tím může být například exportovatelné tajemství datového kanálu DCSE (Data Channel Secret Exporter) nebo Datovým kanálem přenesené tajemství DCTS (Data Channel Transported Secret).
Klientský autentizační prostředek získá DCSS od klientské strany Datového kanálu a serverový autentizační prostředek získá DCSS od serverové strany Datového kanálu.
Označme Veřejný klíč (primárního) autentizačního tajemství klientského autentizačního prostředku CPuK (Client PublicKey).
Klientský autentizační prostředek vypočte hodnotu tohoto elementu autentizačního vektoru AVE(i) pomocí jednosměrné transformace aplikované na dvojici CPuK a hodnotu DCSS získanou od klientské strany.
Serverový autentizační prostředek vypočte referenční hodnotu tohoto elementu autentizačního vektoru AVER(i) pomocí stejné jednosměrné transformace aplikované na dvojici CPuK a hodnotu DCSS získanou od serverové strany Datového kanálu. Serverový autentizační prostředek použije jemu známou hodnotu CPuK, kterou používá pro primární autentizaci klientského autentizačního prostředku.
Příslušný element autentizačního vektoru je vyhodnocen dříve popsaným způsobem a tím je vyloučen aktivní MITM (Man-In-The-Middle) útok na primární autentizaci, pokud je předpokládáno, že útočník není současně na Datovém kanále a mezi klientským a serverovým autentizačním prostředkem.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je vyloučení útočníka při použití repliky. V tomto provedení se používají dva klientské autentizační prostředky a jeden serverový autentizační prostředek a dvě provázaná tajemství K, PK. První klientský autentizační prostředek vytvoří náhodné tajemství PK a z něj odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K.

První klientský autentizační prostředek předá přímo tajemství PK druhému klientskému autentizačnímu prostředku.

Druhý klientský autentizační prostředek z předaného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K.

K vyloučení útočníka je dále potřeba ověřit ve správném pořadí pomocí klientského autentizačního prostředku, že serverový autentizační prostředek má k dispozici stejné tajemství K, resp. PK, a také ověřit pomocí serverového autentizačního prostředku, že klientský autentizační prostředek má k dispozici stejné tajemství K, resp. PK.

Při tom je využíváno jednosměrné závislosti mezi tajemstvími, tedy toho, že z PK lze vypočítat K, ale z K nelze vypočítat PK.

Pro vyloučení útočníka je potřeba nejprve ověřit tajemství K prvního klientského autentizačního prostředku serverovým autentizačním prostředkem, poté je potřeba ověřit tajemství PK druhého klientského autentizačního prostředku serverovým autentizačním prostředkem, poté tajemství K serverového autentizačního prostředku prvním klientským autentizačním prostředkem a nakonec tajemství PK serverového autentizačního prostředku druhým klientským autentizačním prostředkem.

Při tom je nejprve přeneseno tajemství K z druhého klientského autentizačního prostředku na serverový autentizační prostředek a později je přeneseno tajemství PK z prvního klientského autentizačního prostředku na serverový autentizační prostředek.

K ověření tajemství K a PK jsou používány dva elementy autentizačního vektoru AVE(k) a AVE(pk).

Při ověření serverovým autentizačním prostředkem je element odvozeného autentizačního vektoru (AVEP) vypočten klientským autentizačním prostředkem, a vyhodnocení porovnáním s referenční hodnotou elementu autentizačního vektoru (AVER), resp. její odvozenou informací, je prováděno serverovým autentizačním prostředkem.

Při ověření klientským autentizačním prostředkem je element odvozeného autentizačního vektoru (AVEP) vypočten serverovým autentizačním prostředkem, a vyhodnocení porovnáním s referenční hodnotou elementu autentizačního vektoru (AVER), resp. její odvozenou informací, je prováděno klientským autentizačním prostředkem.

Při tom je element odvozeného autentizačního vektoru (AVEP) vypočten z tajemství K resp. PK a tajemství K resp. PK je použito jako referenční hodnota elementu autentizačního vektoru (AVER).

Protože tajemství K a PK vypočetly oba klientské autentizační prostředky hned na začátku, je vyhodnocení klientským autentizačním prostředkem provedeno ihned po přijetí elementu odvozeného autentizačního vektoru (AVEP) od serveru.
Protože serverový autentizační prostředek nemá k dispozici tajemství K a PK v době, kdy dostal element odvozeného autentizačního vektoru (AVEP) od klientského autentizačního prostředku, je vyhodnocení provedeno později, až v okamžiku, kdy tajemství K a později tajemství PK je přeneseno na serverový autentizační prostředek.

V jednom výhodném provedení vynálezu se elementy autentizačního vektoru AVE(k) a AVE(pk) a referenční hodnoty elementu autentizačního vektoru (AVER) vypočtou pomocí jednosměrné transformace aplikované na dvojici Veřejný klíč (primárního) autentizačního tajemství klientského autentizačního prostředku CPuK a K resp. CPuK a PK.

V jednom výhodném provedení vynálezu se vytvoří tři provázaná tajemství PK, K a NK, kde NK je odvozené jednosměrnou kryptografickou funkcí např. hash z tajemství K.
Druhý klientský autentizační prostředek z předaného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K a toto tajemství K předá serverovému autentizačnímu prostředku.
Serverový autentizační prostředek z předaného tajemství K odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství NK a toto tajemství předá prvnímu klientskému autentizačnímu prostředku.
První klientský autentizační prostředek z vytvořeného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K a z něj NK a toto tajemství ověří tajemstvím NK, které obdržel od serverového autentizačního prostředku.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je vyloučení útočníka při vzniku identity. K tomuto účelu se používají dva serverové autentizační prostředky a jeden klientský autentizační prostředek a tři provázaná tajemství K, PK. První serverový autentizační prostředek vytvoří náhodné tajemství PK a z něj odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K.
První serverový autentizační prostředek předá přímo tajemství PK druhému serverovému autentizačnímu prostředku.

Druhý serverový autentizační prostředek z předaného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K.

K vyloučení útočníka je dále potřeba ověřit ve správném pořadí pomocí klientského autentizačního prostředku, že serverový autentizační prostředek má k dispozici stejné tajemství K resp. PK, a také ověřit pomocí serverového autentizačního prostředku, že klientský autentizační prostředek má k dispozici stejné tajemství K resp. PK.

Situace je analogická s ohledem na předmět vynálezu jako v předchozím provedení vynálezu s tím rozdílem, že při použití elementů autentizačního vektoru AVE(k) a AVE(pk) funkci serverového autentizačního prostředku přebírá klientský autentizační prostředek a naopak.

V jednom výhodném provedení vynálezu obsahuje autentizační vektor elementy, jejichž účelem je ověření modifikace aplikace škodlivým kódem (tj. ochrana proti malware).

Tyto elementy využívají funkci FAM1(x), kde x je parametr (výzva) a kde funkce FAM1(x) je parametrický podpis obrazu ověřované aplikace. Tato funkce spočítá kontrolní součet (např. hash, MAC) obrazu aplikace z trvalého úložiště a podepíše kontrolní součet spolu s výzvou (parametr x) privátním klíčem primární autentizace Klientského autentizačního prostředku.

Operační systém má k dispozici trvalou sadu párů klíčů nebo jediný pár klíčů asymetrické kryptografie, kde neexistuje funkčnost čtení privátního klíče. Existují jen vybrané operace s privátním klíčem nekompromitující privátní klíč a operace čtení veřejného klíče. Jeden pár klíčů přísluší buď celému operačnímu systému, nebo jednomu serverovému autentizačnímu prostředku.

Dále elementy využívají volitelně funkci FAM2(x) resp. FAM2(i, x), kde x je parametr (výzva) a i je index páru klíčů použitý v případě použití sady párů klíčů. Funkce FAM(x) resp. FAM(i, x) je parametrický podpis obrazu aplikace v operační paměti. Při zavedení kontrolovaného programu do paměti spočítá operační systém kontrolní součet (např. hash, MAC) zavedeného programu a podepíše kontrolní součet spolu s výzvou (parametr x) požadovaným privátním klíčem (parametr i). Výslednou hodnotu FAM(x) resp. FAM(i, x) předá jádro operačního systému jen tomu programu, který operační systém nastartoval a jehož kontrolní součet použil.

Dále elementy využívají volitelně funkci FS(x), resp. FS(i, x), kde x je parametr (výzva) a i je index páru klíčů použitý v případě použití sady párů klíčů. Funkce FS(x), resp. FS(i, x) je

parametrický podpis nezávislý na obrazu aplikace v operační paměti. Funkce podepíše výzvu (parametr x) požadovaným privátním klíčem (parametr i).

Pro ověření modifikace kódu aplikace jsou využity alespoň dva elementy autentizačního vektoru AVE(i), které označíme jako AM1, AM2, popřípadě další dva elementy AM3 a AM4.

Element autentizačního vektoru AM1 obsahuje kontrolní součet obrazu aplikace z trvalého úložiště např. z disku.

Element autentizačního vektoru AM2 obsahuje parametrický asymetrický podpis kontrolního součtu obrazu aplikace z trvalého úložiště podepsaný privátním klíčem primární autentizace klientského autentizačního prostředku FAM1(x). Parametrem x podpisu je derivát SAS.

Element autentizačního vektoru AM3 obsahuje parametrizovaný kontrolní součet obrazu aplikace v operační paměti podepsaný privátním klíčem operačního systému FAM2(x), resp. FAM2(i, x), kde x je derivát SAS a i je index přiřazený danému serverovému autentizačnímu prostředku.

Element autentizačního vektoru AM4 obsahuje podpis parametru podepsaný privátním klíčem operačního systému FS(x) resp. FS(i, x), kde x je derivát SAS a i je index přiřazený danému serverovému autentizačnímu prostředku.

Protože Serverový autentizační prostředek nemá prostředky pro vytvoření referenčního podpisu, ale jen prostředky pro kontrolu podpisu vytvořeného pomocí asymetrické kryptografie použité ve funkcích FAM1, FAM2 a FS, musejí být přeneseny elementy autentizačního vektoru AM2, AM3 a AM4 v nezměněné podobě z Klientského autentizačním prostředku na serverový autentizační prostředek a při tom ochráněny při přenosu. Proto se element odvozeného autentizačního vektoru (AVEP) vypočte klientským autentizačním prostředkem pro elementy AM2, AM3 a AM4 symetrickou kryptografickou transformací např. zašifrováním pomocí SAS.

Vyhodnocení elementů AM2, AM3 a AM4 Serverovým autentizačním prostředkem se provede metodami ověřování podpisu vytvořeného pomocí asymetrické kryptografie. K ověření jsou použity zrekonstruované hodnoty elementů AM2, AM3 a AM4 získané např. rozšifrováním pomocí SAS serverovým autentizačním prostředkem, příslušné veřejné klíče a referenční hodnoty kontrolních součtů a parametru x (derivát SAS).

V jednom výhodném provedení vynálezu se vytvoří tři provázaná tajemství PK, K a NK, kde NK je odvozené jednosměrnou kryptografickou funkcí např. hash z tajemství K.

Druhý serverový autentizační prostředek z předaného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K a toto tajemství K předá klientskému autentizačnímu prostředku.

Klientský autentizační prostředek z předaného tajemství K odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství NK a toto tajemství předá prvnímu serverovému autentizačnímu prostředku.

První serverový autentizační prostředek z vytvořeného tajemství PK odvodí jednosměrnou kryptografickou transformací, např. funkcí hash, tajemství K a z něj NK a toto tajemství ověří tajemstvím NK, které obdržel od klientského autentizačního prostředku.

Je zejména výhodné zkombinovat některá nebo všechna zde popsaná výhodná provedení dohromady. To je možné udělat vhodným přiřazením elementů autentizačního vektoru AVE(i) a použitím různých AVE(i) s různými účely.

Objasnění výkresů

Obr. 1 schematicky znázorňuje systém podle příkladu 1.

Obr. 2 schematicky znázorňuje systém popsaný v příkladu 2.

Příklady provedení vynálezu

Příklad 1

Příklad použití konkrétního přiřazení Elementů autentizačního vektoru AVE(i) a jejich použití. Popisovaný systém je schematicky znázorněn na obr. 1.

Prvních M Elementů autentizačního vektoru AVE(1) až AVE(M) je použito k ochraně proti kopírování, Element autentizačního vektoru AVE(M+1) je použit k ověření Uživatelem zadávaného lokálního faktoru (např. PIN či NFC platební karta), Element autentizačního vektoru AVE(M+2) je použit k ověření místního lokálního faktoru (např. WiFi hot spot), Element autentizačního vektoru AVE(M+3) k ověření Klientského autentizačního prostředku (např. ověření interních identifikačních dat Klientského autentizačního prostředku), Element autentizačního vektoru AVE(M+4) k autentizaci datového kanálu, Element autentizačního vektoru AVE(M+5) k vyloučení útočníka užitím datového kanálu.

V případě vytváření repliky nebo v případě vzniku identity je Element autentizačního vektoru AVE(M+6) a Element autentizačního vektoru AVE(M+7) použit k dalšímu vyloučení útočníka.

Nejprve proběhne primární autentizace mezi Klientským autentizačním prostředkem 101 a Serverovým autentizačním prostředkem 201, je vytvořen Autentizovaný kanál 301 přes Nezabezpečenou síť 401 mezi Klientským autentizačním prostředkem 101 a Serverovým autentizačním prostředkem 201, a také je vytvořeno Sekundární autentizační tajemství 2 (SAS), které má k dispozici Klientský autentizační prostředek 101 a také Serverový autentizační prostředek 201.

Prvních M Elementů autentizačního vektoru AVE(1) až AVE(M) používá M hodnot AC-AVE(i) 1 uložených v Klientském autentizačním prostředku 101. Z hodnot AC-AVE(i) 1 je za použití Sekundárního autentizačního tajemství 2 (SAS) Klientského autentizačního prostředku 101 vypočteno M hodnot elementů odvozeného autentizačního vektoru 3 AVEP(i) Klientského autentizačního prostředku 101.

Po zadání Lokálního faktoru 4 uživatelem je zadaná hodnota použita k rozšifrování Transformované referenční hodnoty 5 lokálního faktoru 4 T-AVE(1). Rozšifrovaná hodnota 6 osobního faktoru je použita jako Element autentizačního vektoru AVE(M+1), to znamená, že z Rozšifrované hodnoty 6 osobního faktoru 4 je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+1) Klientského autentizačního prostředku 101.

Po zjištění hodnoty místního Lokálního faktoru 7 ze zařízení v blízkosti Klientského autentizačního prostředku 101 je zjištěná hodnota použita k rozšifrování Transformované referenční hodnoty 8 místního lokálního faktoru 7 T-AVE (2). Rozšifrovaná hodnota 9 osobního faktoru 7 je použita jako Element autentizačního vektoru AVE(M+2), to znamená, že z Rozšifrované hodnoty 9 lokálního faktoru 7 je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+2) Klientského autentizačního prostředku 101.

Interní identifikační data 10 Klientského autentizačního prostředku 101, např. výrobní číslo, MAC adresa síťového rozhraní, jsou použita k rozšifrování Transformované referenční hodnoty 11 lokálního faktoru zařízení T-AVE(3). Rozšifrovaná hodnota 12 lokálního faktoru zařízení je použita jako Element autentizačního vektoru AVE(M+3), to znamená, že z Rozšifrované hodnoty 12 lokálního faktoru zařízení je za použití Sekundárního

autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+3) Klientského autentizačního prostředku 101.

Neautentizovaný datový kanál 302 vytvořil na obou svých koncích Exportovatelné tajemství 13 datového kanálu DCSE. Exportovatelné tajemství 13 datového kanálu DCSE přenesené do Klientského autentizačního prostředku 101 je použito jako Element autentizačního vektoru AVE(M+4), to znamená, že z Exportovatelného tajemství 13 datového kanálu DCSE je za použití Sekundárního autentizační tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+4) Klientského autentizačního prostředku 101.

Z Exportovatelného tajemství 13 datového kanálu DCSE přenesené do Klientského autentizačního prostředku 101 a Veřejného klíče (primárního) autentizačního tajemství 14 Klientského autentizačního prostředku 101 CPuK je vypočtena jednosměrnou kryptografickou transformací (např. hash) Odvozená hodnota 15. Odvozená hodnota 15 je použita jako Element autentizačního vektoru AVE(M+5), to znamená, že z výsledku jednosměrné kryptografické transformace aplikované na Exportovatelné tajemství 13 datového kanálu DCSE a Veřejný klíč (primárního) autentizačního tajemství 14 Klientského autentizačního prostředku 101 CPuK je za použití Sekundárního autentizační tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+5) Klientského autentizačního prostředku 101.

Tím je na Klientském autentizačním prostředku 101 k dispozici celý odvozený autentizační vektor AVP.

Serverový autentizační prostředek 201 využije M hodnot AC-AVE(i) 1 uložených v Serverovém autentizačním prostředku 201 jako příslušné referenční hodnoty složky autentizačního vektoru AC-AVER(i). Z hodnot AC-AVE(i) 1 je za použití Sekundárního autentizačního tajemství 2 (SAS) Serverového autentizačního prostředku 201 vypočteno M hodnot Elementu odvozeného autentizačního vektoru 3 AVEP(i) na Serverovém autentizačním prostředku 201.

Serverový autentizační prostředek 201 využije Referenční hodnotu 16 lokálního faktoru LAF-RV(1) jako Element autentizačního vektoru AVE(M+1), to znamená, že z Referenční hodnoty 16 lokálního faktoru LAF-RV(1) je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+1) na Serverovém autentizačním prostředku 201.

Serverový autentizační prostředek 201 využije Referenční hodnotu 17 lokálního faktoru LAF-RV(2) jako Element autentizačního vektoru AVE(M+2), to znamená, že z Referenční hodnoty 17 lokálního faktoru LAF-RV(2) je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+2) na Serverovém autentizačním prostředku 201.

Serverový autentizační prostředek 201 využije Referenční hodnotu 18 lokálního faktoru zařízení LAF-RV(3) jako Element autentizačního vektoru AVE(M+3), to znamená, že z Referenční hodnoty 18 lokálního faktoru zařízení LAF-RV(3) je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+3) na Serverovém autentizačním prostředku 201.

Exportovatelné tajemství 13 datového kanálu DCSE přenesené do Serverového autentizačního prostředku 201 je použito jako Element autentizačního vektoru AVE(M+4), to znamená, že z Exportovatelného tajemství 13 datového kanálu DCSE je za použití Sekundárního autentizačního tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+4) na Serverovém autentizačním prostředku 201.

Z Exportovatelného tajemství 13 datového kanálu DCSE přeneseného do Serverového autentizačního prostředku 201 a Veřejného klíče (primárního) autentizačního tajemství 14 Klientského autentizačního prostředku CPuK je vypočtena jednosměrnou kryptografickou transformací (např. hash) Odvozená hodnota 15. Odvozená hodnota 15 je použita jako Element autentizačního vektoru AVE(M+5), to znamená, že z výsledku jednosměrné kryptografické transformace aplikované na Exportovatelné tajemství 13 datového kanálu DCSE a Veřejný klíč (primárního) autentizačního tajemství 14 Klientského autentizačního prostředku CPuK je za použití Sekundárního autentizační tajemství 2 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+5) na Serverovém autentizačním prostředku 201.

Tím je na Serverovém autentizačním prostředku 201 k dispozici celý Odvozený autentizační vektor 3 AVP (Authentization Vector Product).

Pomocí dříve vzniklého Autentizovaného kanálu 301 přes Nezabezpečenou síť 401 mezi Klientským autentizačním prostředkem 101 a Serverovým autentizačním prostředkem 201 je přenesen celý Odvozený autentizační vektor 3 AVP z Klientského autentizačního prostředku 101 na Serverový autentizační prostředek 201 a tam je použit jako Vstupní vektor 19.

Každý jednotlivý element Vstupního vektoru 19 je porovnán s příslušným Elementem odvozeného autentizačního vektoru 3 vytvořeného na Serverovém autentizačním prostředku

201. V případě shody je do příslušného elementu Vektoru výsledků 20 vyznačeno pozitivní vyhodnocení a v případě neshody je vyznačeno negativní vyhodnocení.
Vektor výsledků 20 je dále zpracován Serverovým autentizačním prostředkem 201 nebo je předán Serverovým autentizačním prostředkem 201 k dalšímu zpracování jiným systémům.

Příklad 2

Příklad použití k dalšímu vyloučení útočníka při vytváření repliky. Popisovaný systém je schematicky znázorněn na Obr. 2.

V tomto příkladu je popsáno využití Elementu autentizačního vektoru AVE(M+6) a Elementu autentizačního vektoru AVE(M+7) k dalšímu vyloučení útočníka. Popisovaný systém je schematicky znázorněn na obr. 2. Z důvodu přehlednosti popisu nejsou popisovány ostatní Elementy autentizačního vektoru AVE. Příklad způsobu použití ostatních Elementů autentizačního vektoru AVE(i) je uveden v Příkladu 1.

Nejprve proběhne primární autentizace mezi prvním Klientským autentizačním prostředkem 102 a Serverovým autentizačním prostředkem 201, je vytvořen první Autentizovaný kanál 301 přes Nezabezpečenou síť 401 mezi prvním Klientským autentizačním prostředkem 102 a Serverovým autentizačním prostředkem 201, a také je vytvořeno první Sekundární autentizační tajemství 22 SAS, které má k dispozici první Klientský autentizační prostředek 102 a také Serverový autentizační prostředek 201.
První Klientský autentizační prostředek 102 vygeneruje Tajemství PK 24. Tajemství PK 24 předá přímo druhému Klientskému autentizačním prostředku 103.
První Klientský autentizační prostředek 102 vypočte z Tajemství PK 24 pomocí jednosměrné kryptografické transformace, např. hash, Tajemství K 25. Také druhý Klientský autentizační prostředek 103 vypočte z Tajemství PK 24 pomocí asymetrické kryptografické transformace Tajemství K 25. V tomto okamžiku mají oba Klientské autentizační prostředky 102, 103 k dispozici stejnou dvojici tajemství a to Tajemství PK 24 a Tajemství K 25.
Také proběhne primární autentizace mezi druhým Klientským autentizačním prostředkem 103 a Serverovým autentizačním prostředkem 201, je vytvořen druhý Autentizovaný kanál 303 přes Nezabezpečenou síť 401 mezi druhým Klientským autentizačním prostředkem 103 a Serverovým autentizačním prostředkem 201, a také je vytvořeno druhé Sekundární

autentizační tajemství 23 (SAS), které má k dispozici druhý Klientský autentizační prostředek 102 a také Serverový autentizační prostředek 201.

První Klientský autentizační prostředek 102 využije Tajemství K 25 jako Element autentizačního vektoru AVE(M+6), to znamená, že z Tajemství K 25 je za použití prvního Sekundárního autentizačního tajemství 22 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+6) prvního Klientského autentizačního prostředku 102.

Pomocí dříve vzniklého prvního Autentizovaného kanálu 301 přes Nezabezpečenou síť 401 mezi prvním Klientským autentizačním prostředkem 102 a Serverovým autentizačním prostředkem 201 je přenesen Odvozený autentizační vektor 3 AVP z prvního Klientského autentizačního prostředku 102 na Serverový autentizační prostředek 201 a tam je použit jako první Vstupní vektor 32. První Vstupní vektor 32 je uložen do doby, až bude Serverový autentizační prostředek 201 mít k dispozici Tajemství K 25.

Druhý Klientský autentizační prostředek 103 využije Tajemství PK 24 jako Element autentizačního vektoru AVE(M+7), to znamená, že z Tajemství PK 24 je za použití druhého Sekundárního autentizačního tajemství 23 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+7) druhého Klientského autentizačního prostředku 103.

Pomocí dříve vzniklého druhého Autentizovaného kanálu 303 přes Nezabezpečenou síť 401 mezi druhým Klientským autentizačním prostředkem 103 a Serverovým autentizačním prostředkem 201 je přenesen Odvozený autentizační vektor 3 AVP a také Tajemství K 25 z druhého Klientského autentizačního prostředku 103 na Serverový autentizační prostředek 201 a tam je použit jako druhý Vstupní vektor 33. Druhý Vstupní vektor 33 je uložen do doby, až bude Serverový autentizační prostředek 201 mít k dispozici Tajemství PK 24.

V tomto okamžiku má Serverový autentizační prostředek 201 k dispozici Tajemství K 25. To využije k vyhodnocení Elementu autentizačního vektoru AVE(M+6), to znamená, že z Tajemství K 25 je za použití prvního Sekundárního autentizační tajemství 22 (SAS) vypočtena hodnota Elementu odvozeného prvního autentizačního vektoru 42 AVEP(M+6). Tato hodnota je porovnána s dříve zaznamenanou hodnotou prvního Vstupního vektoru 32.

Serverový autentizační prostředek 201 použije také Tajemství K 25 k ověření Elementu autentizačního vektoru AVE(M+6) v obráceném směru, to znamená, že z Tajemství K 25 je za použití prvního Sekundárního autentizačního tajemství 22 (SAS) vypočtena hodnota Elementu odvozeného prvního autentizačního vektoru 52 AVEP(M+6).

První Klientský autentizační prostředek 102 využije Tajemství K 25 jako Element autentizačního vektoru AVE(M+6), to znamená, že z Tajemství K 25 je za použití prvního Sekundárního autentizačního tajemství 22 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+6) na prvním Klientském autentizačním prostředku 102.

Pomocí dříve vzniklého prvního Autentizovaného kanálu 301 přes Nezabezpečenou síť 401 mezi prvním Klientským autentizačním prostředkem 102 a Serverovým autentizačním prostředkem 201 je přenesen Odvozený autentizační vektor 52 AVP ze Serverového autentizačního prostředku 201 na první Klientský autentizační prostředek 102 a tam je použit jako Vstupní vektor 31 prvního Klientského autentizačního prostředku 102.

V případě shody Elementu odvozeného autentizačního vektoru 3 AVEP(M+6) na prvním Klientském autentizačním prostředku 102 a příslušné položky Vstupního vektoru 31 je mimo jiné ověřeno, že druhý Klientský autentizační prostředek 103 a Serverový autentizační prostředek 201 mají k dispozici správnou hodnotu Tajemství K 25.

Proto pomocí dříve vzniklého prvního Autentizovaného kanálu 301 přes Nezabezpečenou síť 401 mezi prvním Klientským autentizačním prostředkem 102 a Serverovým autentizačním prostředkem 201 je přeneseno Tajemství PK 24 z prvního Klientského autentizačního prostředku 102 na Serverový autentizační prostředek 201.

V tomto okamžiku má Serverový autentizační prostředek 201 k dispozici Tajemství PK 24. To využije k vyhodnocení Elementu autentizačního vektoru AVE(M+7), to znamená, že z Tajemství PK 24 je za použití druhého Sekundárního autentizační tajemství 23 (SAS) vypočtena hodnota Elementu odvozeného druhého autentizačního vektoru 43 AVEP(M+6). Tato hodnota je porovnána s dříve zaznamenanou hodnotou druhého Vstupního vektoru 33. Serverový autentizační prostředek 201 použije také Tajemství PK 24 k ověření Elementu autentizačního vektoru AVE(M+7) v obráceném směru, to znamená, že z Tajemství PK 24 je za použití druhého Sekundárního autentizačního tajemství 23 (SAS) vypočtena hodnota Elementu odvozeného druhého autentizačního vektoru 53 AVEP(M+7).

Druhý Klientský autentizační prostředek 103 využije Tajemství PK 24 jako Element autentizačního vektoru AVE(M+7), to znamená, že z Tajemství PK 24 je za použití druhého Sekundárního autentizačního tajemství 23 (SAS) vypočtena hodnota Elementu odvozeného autentizačního vektoru 3 AVEP(M+7) na druhém Klientském autentizačním prostředku 103.

Pomocí dříve vzniklého druhého Autentizovaného kanálu 303 přes Nezabezpečenou síť 401 mezi druhým Klientským autentizačním prostředkem 103 a Serverovým autentizačním prostředkem 201 je přenesen Odvozený druhý autentizační vektor 53 AVP ze Serverového

autentizačního prostředku 201 na druhý Klientský autentizační prostředek 103 a tam je použit jako Vstupní vektor 31 druhého Klientského autentizačního prostředku 103.

V případě shody Elementu odvozeného autentizačního vektoru 3 AVEP(M+7) na druhém Klientském autentizačním prostředku 103 a příslušné položky Vstupního vektoru 31 je mimo jiné ověřeno, že první Klientský autentizační prostředek 102 a Serverový autentizační prostředek 201 mají k dispozici správnou hodnotu Tajemství PK 24.

V takovém případě je eliminována možnost přítomnosti útočníka na jednom z obou Autentizovaných kanálů tj. na prvním Autentizovaném kanálu 301 resp. na druhém Autentizovaném kanálu 303.

PATENTOVÉ NÁROKY

1. Způsob zabezpečení autentizace při elektronické komunikaci mezi alespoň jedním klientským autentizačním prostředkem (101, 102, 103) a alespoň jedním serverovým autentizačním prostředkem (201), vyznačující se tím, že se nejprve provede primární autentizace, při níž se vytvoří sekundární autentizační tajemství (2, 22, 23) sdílené klientským autentizačním prostředkem (101, 102, 103) a serverovým autentizačním prostředkem (201) a platné pouze pro danou autentizační transakci, a následně se toto sekundární autentizační tajemství (2, 22, 23) použije jako vstup transformace, s výhodou kryptografické transformace, prováděné klientským autentizačním prostředkem (101, 102, 103) na každém elementu autentizačního vektoru odděleně za vytvoření elementu prvního odvozeného autentizačního vektoru (3), přičemž autentizační vektor je uspořádaná množina elementů autentizačního vektoru (AVE(i)), přičemž první odvozený autentizační vektor (3) se přenese z klientského autentizačního prostředku (101, 102, 103) na serverový autentizační prostředek (201) a tam se vyhodnotí s pomocí sekundárního autentizačního tajemství (2, 22, 23).

2. Způsob podle nároku 1, vyznačený tím, že klientský autentizační prostředek (101, 102, 103) má uloženy hodnoty elementů autentizačního vektoru nebo jsou do něj zadány uživatelem nebo získány z nosiče informací nebo z okolního prostředí před autentizační transakcí nebo v průběhu autentizační transakce nebo jsou před autentizační transakcí nebo v průběhu autentizační transakce získány z transformovaných hodnot (5, 8, 11) elementů autentizačního vektoru (T-AVE(i)) s pomocí informací zadaných uživatelem nebo získaných z nosiče informací nebo z okolního prostředí, a serverový autentizační prostředek (201) má uloženy referenční hodnoty (16, 17, 18) elementů autentizačního vektoru (AVER(i)) nebo je před autentizační transakcí nebo v průběhu autentizační transakce získá z nosiče informací nebo z okolního prostředí.

3. Způsob podle nároku 1 nebo 2, vyznačený tím, že v serverovém autentizačním prostředku se z referenčních hodnot elementů autentizačního vektoru vytvoří druhý odvozený autentizační vektor (3) tak, že se sekundární autentizační tajemství (2, 22, 23) použije jako vstup transformace prováděné serverovým autentizačním prostředkem (201) na každém elementu autentizačního vektoru odděleně, a první a druhý odvozený autentizační vektor (3) se porovnají.

4. Způsob podle nároku 1 nebo 2, vyznačený tím, že v serverovém autentizačním prostředku se každý element prvního odvozeného autentizačního vektoru (3) odděleně podrobí inverzní transformaci k transformaci použité klientským autentizačním prostředkem (101, 102, 103), a výsledek se vyhodnotí s použitím referenčních hodnot elementů autentizačního vektoru (3).

5. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije více (M) elementů (1) autentizačního vektoru AC-AVE(i), kde i = 1 až M, jejichž účelem je detekce zkopírování klientského autentizačního prostředku (101, 102, 103), přičemž každý z elementů AC-AVE(i) (1) je přiřazen jedné z předchozích provedených autentizací, s výhodou je odvozen ze sekundárního autentizačního tajemství (2, 22, 23) příslušného této předchozí provedené autentizaci.

6. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je ověření lokálních autentizačních faktorů (4, 7), přičemž klientský autentizační prostředek (101, 102, 103) získá hodnotu lokálního autentizačního faktoru (4, 7) z okolního prostředí a referenční hodnota (16, 17, 18) elementu autentizačního vektoru LF-AVER(i) uložená na serverovém autentizačním prostředku je pak buď přímo lokální autentizační faktor (4, 7), nebo informace z lokálního autentizačního faktoru odvozená, nebo referenční informace, přičemž je-li LF-AVER(i) referenční informace, je tato referenční informace na lokálním autentizačním faktoru (4, 7) nezávislá.

7. Způsob podle nároku 6, vyznačující se tím, že LF-AVER(i) je referenční informace, přičemž se inicializace příslušného elementu autentizačního vektoru provede tak, že se sejme referenční lokální autentizační faktor, tím se získá referenční hodnota LAF-RV(i), následně se pseudonáhodně vytvoří referenční informace elementu autentizačního vektoru LF-AVER(i) z autentizovaného sdíleného tajemství, s výhodou sekundárního autentizačního tajemství (2, 22, 23), a na k sobě příslušné hodnoty LAF-RV(i) a LF-AVER(i) se aplikuje kryptografická transformace, s výhodou zašifrování LF-AVER(i) pomocí LAF-RV(i), načež se výsledek této kryptografické transformace uloží na klientském autentizačním prostředku (101, 102, 103) k dalšímu použití a nepřenáší se jinam, přičemž zároveň se na serverovém autentizačním prostředku (201) uloží referenční informace elementu autentizačního vektoru LF-AVER(i)

vypočtená stejným způsobem z autentizovaného sdíleného tajemství, s výhodou sekundárního autentizačního tajemství (2, 22, 23), na serverovém autentizačním prostředku (201).

8. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je autentizace neautentizovaného datového kanálu, přičemž tento element se vytvoří tak, že klientská strana Datového kanálu vytvoří pomocí jednosměrné transformace z interního tajemství Datového kanálu exportovatelné tajemství (13) datového kanálu DCSE a shodné exportovatelné tajemství (13) datového kanálu vytvoří také serverová strana Datového kanálu, přičemž klientský autentizační prostředek (101, 102, 103) použije získaný DCSE (13) jako element autentizačního vektoru AVE(i) a serverový autentizační prostředek (201) použije získaný DCSE (13) jako referenční hodnotu elementu autentizačního vektoru AVER(i).

9. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je ověření klientského autentizačního prostředku (101, 102, 103), přičemž tímto elementem je identifikátor zařízení DI(i), který se použije jako lokální autentizační faktor.

10. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je vyloučení útočníka užitím datového kanálu, přičemž tento element se vytvoří tak, že pomocí Datového kanálu vedoucího mezi klientskou částí a serverovou částí se vytvoří sekundární tajemství datového kanálu DCSS, přičemž klientský autentizační prostředek (101, 102, 103) vypočte hodnotu elementu autentizačního vektoru AVE(i) pomocí jednosměrné kryptografické transformace aplikované na dvojici Veřejný klíč autentizačního tajemství CPuK a hodnotu DCSS získanou od klientské strany, a serverový autentizační prostředek (201) vypočte referenční hodnotu tohoto elementu autentizačního vektoru AVER(i) pomocí stejné jednosměrné transformace aplikované na dvojici CPuK a hodnotu DCSS získanou od serverové strany Datového kanálu.

11. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je vyloučení útočníka při použití repliky, přičemž se použijí dva klientské autentizační prostředky (102, 103) a jeden serverový autentizační prostředek (201) a dvě provázaná tajemství K (25), PK (24), přičemž první

klientský autentizační prostředek (102) vytvoří náhodné tajemství PK (24) a z něj odvodí jednosměrnou kryptografickou funkcí tajemství K (25); první klientský autentizační prostředek (102) předá přímo tajemství PK (24) druhému klientskému autentizačnímu prostředku (103); druhý klientský autentizační prostředek (103) z předaného tajemství PK (24) odvodí jednosměrnou kryptografickou transformací tajemství K (25); a následně se ověří tajemství K (25) prvního klientského autentizačního prostředku (102) serverovým autentizačním prostředkem (201), poté se ověří tajemství PK (24) druhého klientského autentizačního prostředku (103) serverovým autentizačním prostředkem (201), poté se ověří tajemství K (25) serverového autentizačního prostředku (201) prvním klientským autentizačním prostředkem (102) a nakonec se ověří tajemství PK (24) serverového autentizačního prostředku (201) druhým klientským autentizačním prostředkem (103).

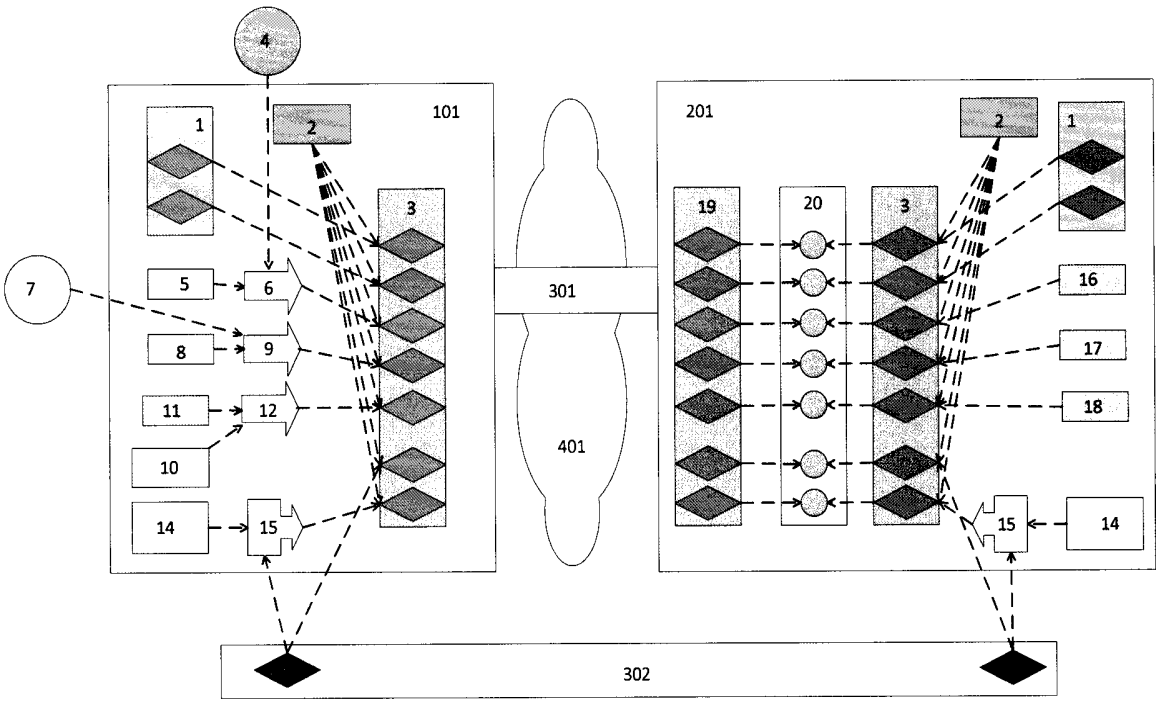
12. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použije alespoň jeden element autentizačního vektoru, jehož účelem je vyloučení útočníka při vzniku identity, přičemž se použijí dva serverové autentizační prostředky a jeden klientský autentizační prostředek (101, 102, 103) a dvě provázaná tajemství K (25), PK (24), přičemž první serverový autentizační prostředek (201) vytvoří náhodné tajemství PK (24) a z něj odvodí jednosměrnou kryptografickou transformací tajemství K (25); první serverový autentizační prostředek (201) předá přímo tajemství PK (24) druhému serverovému autentizačnímu prostředku (201); druhý serverový autentizační prostředek (201) z předaného tajemství PK (24) odvodí jednosměrnou kryptografickou transformací tajemství K (25); a následně se ověří tajemství K (25) prvního serverového autentizačního prostředku (201) klientským autentizačním prostředkem (101, 102, 103), poté se ověří tajemství PK (24) druhého serverového autentizačního prostředku (201) klientským autentizačním prostředkem (101, 102, 103), poté se ověří tajemství K (25) klientského autentizačního prostředku (101, 102, 103) prvním serverovým autentizačním prostředkem (201) a nakonec se ověří tajemství PK (24) klientského autentizačního prostředku (101, 102, 103) druhým serverovým autentizačním prostředkem (201).

13. Způsob podle kteréhokoliv z předcházejících nároků, vyznačující se tím, že se použijí elementy autentizačního vektoru, jejichž účelem je ověření modifikace aplikace škodlivým kódem, přičemž tyto elementy využívají funkci FAM1(x), kde x je parametr a kde funkce FAM1(x) je parametrický podpis obrazu ověřované aplikace, přičemž operační systém má

volitelně k dispozici trvalou sadu párů klíčů nebo jediný pár klíčů asymetrické kryptografie, kde neexistuje funkčnost čtení privátního klíče, existují jen vybrané operace s privátním klíčem nekompromitující privátní klíč a operace čtení veřejného klíče, přičemž jeden pár klíčů přísluší buď celému operačnímu systému nebo jednomu serverovému autentizačnímu prostředku (201), přičemž dále elementy autentizačního vektoru využívají volitelně funkci FAM2(x) resp. FAM2(i, x), kde x je parametr a i je index páru klíčů použitý v případě použití sady párů klíčů, a funkce FAM(x) resp. FAM(i, x) je parametrický podpis obrazu aplikace v operační paměti, a dále elementy autentizačního vektoru využívají volitelně funkci FS(x), resp. FS(i, x), kde x je parametr a i je index páru klíčů použitý v případě použití sady párů klíčů, a funkce FS(x), resp. FS(i, x) je parametrický podpis nezávislý na obrazu aplikace v operační paměti, a přičemž se pro ověření modifikace aplikace škodlivým kódem se použijí alespoň dva elementy autentizačního vektoru AM1, AM2, popřípadě další dva elementy AM3 a AM4, kde element autentizačního vektoru AM1 obsahuje kontrolní součet obrazu aplikace z trvalého úložiště, element autentizačního vektoru AM2 obsahuje parametrický asymetrický podpis kontrolního součtu obrazu aplikace z trvalého úložiště podepsaný privátním klíčem primární autentizace klientského autentizačního prostředku (101, 102, 103) AM1(x), kde parametrem x podpisu je derivát sekundárního autentizačního tajemství (2, 22, 23), element autentizačního vektoru AM3 obsahuje parametrizovaný kontrolní součet obrazu aplikace v operační paměti podepsaný privátním klíčem operačního systému FAM2(x), resp. FAM2(i, x), kde x je derivát sekundárního autentizačního tajemství (2, 22, 23) a i je index přiřazený danému serverovému autentizačnímu prostředku (201), a element autentizačního vektoru AM4 obsahuje podpis parametru podepsaný privátním klíčem operačního systému FS(x) resp. FS(i, x), kde x je derivát sekundárního autentizačního tajemství (2, 22, 23) a i je index přiřazený danému serverovému autentizačnímu prostředku (201), přičemž elementy prvního odvozeného autentizačního vektoru (2) příslušné elementům AM2, AM3, AM4 se vypočtou symetrickou kryptografickou transformací.

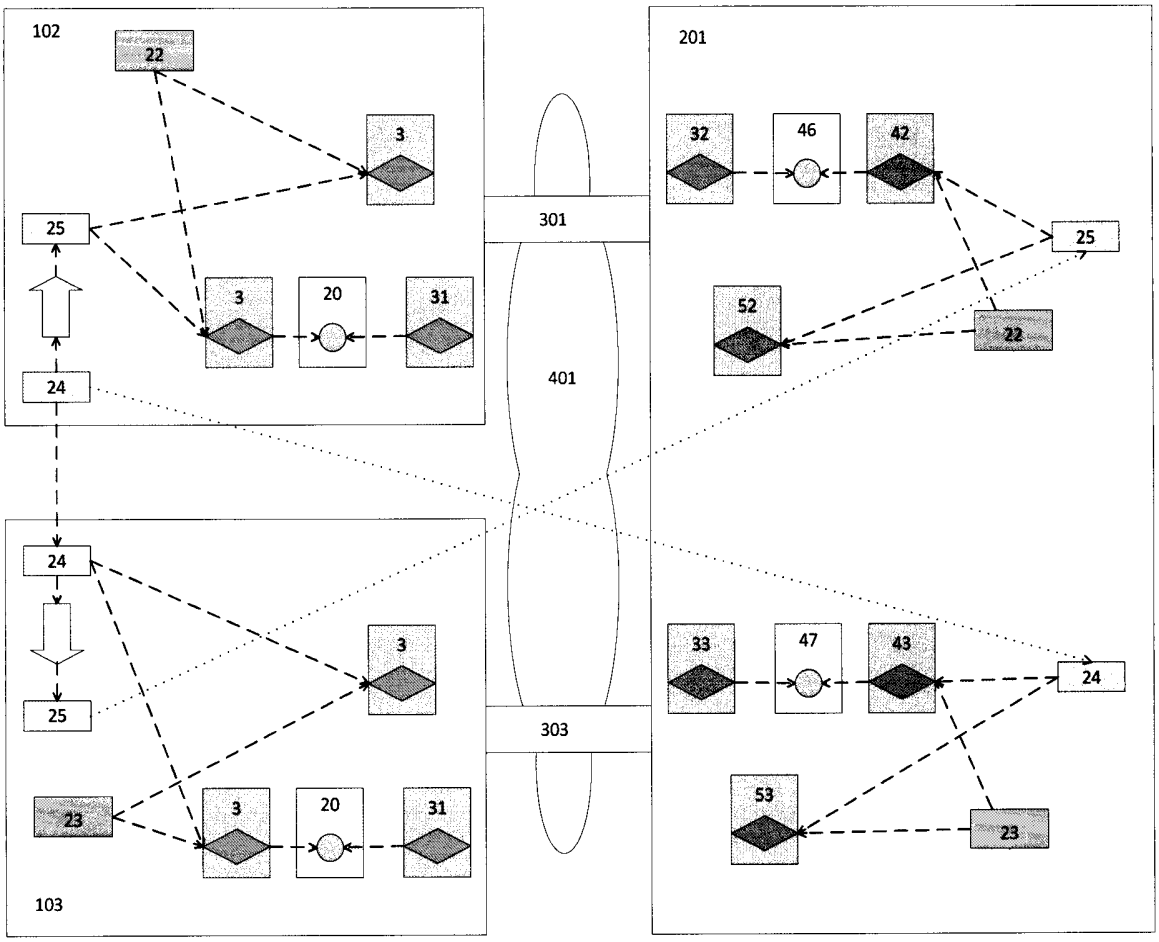
PV 2015-473
07.07.15

Obr.1



07.07.15

Obr.2


102
22
3
25
3
20
31
24
301
401
303
201
32
46
42
25
52
22
24
3
25
23
3
20
31
103
33
47
43
24
53
23