**Патент США 8,683,593**

**Mahaffey 25 березня 2014**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Аналіз даних для мобільного пристрою за допомогою сервера

**Реферат**

Мобільний пристрій порівнює прийняті дані з даними, що зберігаються в базі даних. У разі відсутності позитивного збігу, дані надходять на сервер для порівняння їх сервером. На основі порівняння, проведеного сервером, мобільний пристрій отримує або не отримує дозвіл на обробку даних.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Автор винаходу: Mahaffey; Kevin Patrick** (Сан-Франциско, Каліфорнія)

**Заявник: Ім'я Місто Штат Країна Тип**

**Lookout, Inc.** Сан Франциско, Каліфорнія США

**Початковий власник патенту: Lookout, Inc.** (Сан Франциско, Каліфорнія)

**Серійний номер: 42109684**

**Номер заявки: 13 / 742,173**

**Заявлений: 15 cічня 2013**

**Попередні публікації**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Кодове позначення документа Дата публікації**

US 20130133071 A1 23 травня 2013

**Пов'язані патентні документи США**

<Td <td = "" style = "color: rgb (0, 0, 0); font-family: 'Times New Roman'; font-size: medium; font-style: normal; font-variant: normal; font -weight: normal; letter-spacing: normal; line-height: normal; orphans: auto; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 1; word -spacing: 0px; -webkit-text-stroke-width: 0px; "> </ td <> <td <td =" "style =" color: rgb (0, 0, 0); font-family: 'Times New Roman '; font-size: medium; font-style: normal; font-variant: normal; font-weight: normal; letter-spacing: normal; line-height: normal; orphans: auto; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 1; word-spacing: 0px; -webkit-text-stroke-width: 0px; "> </ td <> <td <td = "" style = "color: rgb (0, 0, 0); font-family: 'Times New Roman'; font-size: medium; font-style: normal; font-variant: normal; font-weight: normal ; letter-spacing: normal; line-height: normal; orphans: auto; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 1; word-spacing: 0px; -webkit-text-stroke-width: 0px; "> </ td <>

**Номер заявки Дата подачі Номер патенту Дата публікації**

13333654 Грудень 21,2011 8381303

12255621 Січень 31, 2012 8108933

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Чинний клас США:** 726/23; 709/203; 726/24; 726/25; 726/3

**Чинний клас CPC:** G06F 21/564 (20130101); G06F 21/562 (20130101); H04W 12/08 (20130101); G06F 21/577 (20130101); G06F 2221/034 (20130101); H04L 63/1433 (20130101)

**Чинний міжнародний клас:** H04L 29/06 (20060101); G06F 7/04 (20060101); G06F 15/16 (20060101); G06F 17/30 (20060101)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Протипоставлені матеріали**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Патентні документи США**

3416032 Грудень 1968 Jahns і ін.

4553257 Листопад 1985 Mori і ін.

5319776 Червень 1994 Hile і ін.

5574775 Листопад 1996 Miller, II і ін.

5715518 Лютий 1998 Barrere і ін.

6185689 Лютий 2001 Todd і ін.

6269456 Липень 2001 Hodges і ін.

6272353 Серпень 2001 Dicker і ін.

6301668 Жовтень 2001 Gleichauf і ін.

6453345 Вересень 2002 Trcka і ін.

6529143 Березень 2003 Mikkola і ін.

6696941 Лютий 2004 Baker і ін.

6792543 Вересень 2004 Pak і ін.

6892225 Травень 2005 Tu і ін.

6907530 Червень 2005 Wang

6959184 Жовтень 2005 Byers і ін.

7020895 Березень 2006 Albrecht

7023383 Квітень 2006 Stilp і ін.

7069589 Червень 2006 Schmall і ін.

7096368 Серпень 2006 Kouznetsov і ін.

7123933 Жовтень 2006 Poor і ін.

7127455 Жовтень 2006 Carson і ін.

7159237 Січень 2007 Schneier і ін.

7171690 Січень 2007 Kouznetsov і ін.

7178166 Лютий 2007 Taylor і ін.

7181252 Лютий 2007 Komsi

7210168 Квітень 2007 Hursey і ін.

7228566 Червень 2007 Caceres і ін.

7236598 Червень 2007 Sheymov і ін.

7237264 Червень 2007 Graham і ін.

7266810 Вересень 2007 Karkare і ін.

7290276 Жовтень 2007 Ogata

7304570 Грудень 2007 Thomas і ін.

7305245 Грудень 2007 Alizadeh-Shabdiz і ін.

7308256 Грудень 2007 Morota і ін.

7308712 Грудень 2007 Banzhof

7325249 Січень 2008 Sutton і ін.

7356835 Квітень 2008 Gancarcik і ін.

7376969 Травень 2008 Njemanze і ін.

7386297 Червень 2008 An

7392043 Червень 2008 Kouznetsov і ін.

7392543 Червень 2008 Szor

7397424 Липень 2008 Houri

7397434 Липень 2008 Mun і ін.

7401359 Липень 2008 Gartside і ін.

7403762 Липень 2008 Morgan і ін.

7414988 Август 2008 Jones і ін.

7415270 Август 2008 Wilhelmsson і ін.

7415536 Август 2008 Nakazawa

7433694 Жовтень 2008 Morgan і ін.

7467206 Грудень 2008 Moore і ін.

7471954 Грудень 2008 Brachet і ін.

7472422 Грудень 2008 Agbabian

7474897 Січень 2009 Morgan і ін.

7493127 Лютий 2009 Morgan і ін.

7502620 Березень 2009 Morgan і ін.

7515578 Квітень 2009 Alizadeh-Shabdiz

7525541 Квітень 2009 Chun та ін.

7551579 Червень 2009 Alizadeh-Shabdiz

7551929 Червень 2009 Alizadeh-Shabdiz

7634800 Грудень 2009 Ide і ін.

7685132 Березень 2010 Hyman

7696923 Квітень 2010 Houri

7768963 Серпень 2010 Alizadeh-Shabdiz

7769396 Серпень 2010 Alizadeh-Shabdiz і ін.

7774637 Серпень 2010 Beddoe і ін.

7783281 Серпень 2010 Cook і ін.

7809353 Жовтень 2010 Brown і ін.

7809366 Жовтень 2010 Rao і ін.

7818017 Жовтень 2010 Alizadeh-Shabdiz і ін.

7835754 Листопад 2010 Alizadeh-Shabdiz і ін.

7856234 Грудень 2010 Alizadeh-Shabdiz і ін.

7856373 Грудень 2010 Ullah

7861303 Грудень 2010 Kouznetsov і ін.

7907966 Березень 2011 Mammen

7916661 Березень 2011 Alizadeh-Shabdiz і ін.

7991854 Серпень 2011 Bahl

7999742 Серпень 2011 Alizadeh-Shabdiz і ін.

8014788 Вересень 2011 Alizadeh-Shabdiz і ін.

8019357 Вересень 2011 Alizadeh-Shabdiz і ін.

8031657 Жовтень 2011 Jones і ін.

8037203 Жовтень 2011 Accapadi і ін.

8054219 Листопад 2011 Alizadeh-Shabdiz

8087082 Грудень 2011 Bloch і ін.

8089398 Січень 2012 Alizadeh-Shabdiz

8089399 Січень 2012 Alizadeh-Shabdiz

8090386 Січень 2012 Alizadeh-Shabdiz

8108555 Січень 2012 Awadallah і ін.

8121617 Лютий 2012 LaGrotta і ін.

8126456 Лютий 2012 Lotter і ін.

8127358 Лютий 2012 Lee

8135395 Березень 2012 Cassett і ін.

8195196 Червень 2012 Haran і ін.

8259568 Вересень 2012 Laudermilch і ін.

8261351 Вересень 2012 Thornewell і ін.

8266288 Вересень 2012 Banerjee і ін.

8266324 Вересень 2012 Baratakke і ін.

8346860 Січень 2013 Berg та ін.

8356080 Січень 2013 Luna та ін.

8364785 Січень 2013 Plamondon

8370580 Лютий 2013 Mobarak і ін.

8370933 Лютий 2013 Buckler

8401521 Березень 2013 Bennett і ін.

8447856 Травень 2013 Drako

8463915 Червень 2013 Kim

8484332 Липень 2013 Bush і ін.

8504775 Серпень 2013 Plamondon

2001/0044339 Листопад 2001 Cordero і ін.

2002/0042886 Квітень 2002 Lahti і ін.

2002/0087483 Липень 2002 Harif

2002/0108058 Серпень 2002 Iwamura

2002/0183060 Грудень 2002 Ko та ін.

2002/0191018 Грудень 2002 Broussard

2003/0028803 Лютий 2003 Bunker і ін.

2003/0046134 Березень 2003 Frolick і ін.

2003/0079145 Квітень 2003 Kouznetsov і ін.

2003/0115485 Червень 2003 Milliken і ін.

2003/0120951 Червень 2003 Gartside і ін.

2003/0131148 Липень 2003 Kelley і ін.

2004/0022258 Лютий 2004 Tsukada і ін.

2004/0025042 Лютий 2004 Kouznetsov і ін.

2004/0133624 Липень 2004 Park

2004/0158741 Серпень 2004 Schneider

2004/0185900 Вересень 2004 McElveen

2004/0209608 Жовтень 2004 Kouznetsov і ін.

2004/0225887 Листопад 2004 O'Neil і ін.

2004/0259532 Грудень 2004 Isomaki і ін.

2005/0010821 Січень 2005 Cooper і ін.

2005/0015443 Січень 2005 Levine і ін.

2005/0074106 Квітень 2005 Orlamunder і ін.

2005/0076246 Квітень 2005 Singhal

2005/0091308 Квітень 2005 Bookman і ін.

2005/0125779 Червень 2005 Kelley і ін.

2005/0130627 Червень 2005 Calmels і ін.

2005/0138395 Червень 2005 Benco і ін.

2005/0138413 Червень 2005 Lippmann і ін.

2005/0138450 Червень 2005 Hsieh

2005/0154796 Липень 2005 Forsyth

2005/0186954 Серпень 2005 Kenney

2005/0197099 Вересень 2005 Nehushtan

2005/0221800 Жовтень 2005 Jackson і ін.

2005/0227669 Жовтень 2005 Haparnas

2005/0237970 Жовтень 2005 Inoue

2005/0240999 Жовтень 2005 Rubin та ін.

2005/0254654 Листопад 2005 Rockwell та ін.

2005/0278777 Грудень 2005 Loza

2005/0282533 Грудень 2005 Draluk і ін.

2006/0026283 Лютий 2006 Trueba

2006/0073820 Квітень 2006 Craswell і ін.

2006/0075388 Квітень 2006 Kelley і ін.

2006/0080680 Квітень 2006 Anwar і ін.

2006/0095454 Травень 2006 Shankar і ін.

2006/0101518 Травень 2006 Schumaker і ін.

2006/0130145 Червень 2006 Choi і ін.

2006/0150238 Липень 2006 D'Agostino

2006/0150256 Липень 2006 Fanton і ін.

2006/0179485 Серпень 2006 Longsine і ін.

2006/0217115 Вересень 2006 Cassett і ін.

2006/0218482 Вересень 2006 Ralston і ін.

2006/0224742 Жовтень 2006 Shahbazi

2006/0236325 Жовтень 2006 Rao і ін.

2006/0253205 Листопад 2006 Gardiner

2006/0253584 Листопад 2006 Dixon та ін.

2006/0272011 Листопад 2006 Ide і ін.

2006/0277408 Грудень 2006 Bhat і ін.

2006/0294582 Грудень 2006 Linsley-Hood і ін.

2007/0005327 Січень 2007 Ferris

2007/0011319 Січень 2007 Mcclure і ін.

2007/0015519 Січень 2007 Casey

2007/0016953 Січень 2007 Morris і ін.

2007/0016955 Січень 2007 Goldberg і ін.

2007/0021112 Січень 2007 Byrne і ін.

2007/0028095 Лютий 2007 Allen і ін.

2007/0028303 Лютий 2007 Brennan

2007/0028304 Лютий 2007 Brennan

2007/0038677 Лютий 2007 Reasor і ін.

2007/0050471 Березень 2007 Patel і ін.

2007/0086476 Квітень 2007 Iglesias і ін.

2007/0089165 Квітень 2007 Wei і ін.

2007/0090954 Квітень 2007 Mahaffey

2007/0154014 Липень 2007 Aissi і ін.

2007/0174472 Липень 2007 Kulakowski

2007/0174490 Липень 2007 Choi і ін.

2007/0186282 Серпень 2007 Jenkins

2007/0190995 Серпень 2007 Wang і ін.

2007/0214504 Вересень 2007 Milani Comparetti і ін.

2007/0220608 Вересень 2007 Lahti і ін.

2007/0240217 Жовтень 2007 Tuvell і ін.

2007/0240218 Жовтень 2007 Tuvell і ін.

2007/0240221 Жовтень 2007 Tuvell і ін.

2007/0240222 Жовтня 2007 Tuvell і ін.

2007/0248047 Жовтень 2007 Shorty і ін.

2007/0250627 Жовтень 2007 May і ін.

2007/0253377 Листопад 2007 Janneteau і ін.

2007/0293263 Грудень 2007 Eslambolchi і ін.

2007/0297610 Грудень 2007 Chen та ін.

2008/0028470 Січень 2008 Remington і ін.

2008/0046369 Лютий 2008 Wood

2008/0046557 Лютий 2008 Cheng

2008/0047007 Лютий 2008 Satkunanathan і ін.

2008/0049653 Лютий 2008 Demirhan і ін.

2008/0065507 Березень 2008 Morrison і ін.

2008/0070495 Березень 2008 Stricklen і ін.

2008/0072329 Березень 2008 Herschaft і ін.

2008/0086773 Квітень 2008 Tuvell і ін.

2008/0086776 Квітень 2008 Tuvell і ін.

2008/0109871 Травень 2008 Jacobs

2008/0127171 Травень 2008 Tarassov

2008/0127179 Травень 2008 Moss і ін.

2008/0127334 Травень 2008 Gassoway

2008/0127336 Травень 2008 Sun і ін.

2008/0132218 Червень 2008 Samson і ін.

2008/0134281 Червень 2008 Shinde і ін.

2008/0140767 Червень 2008 Rao і ін.

2008/0148381 Червень 2008 Aaron

2008/0172746 Липень 2008 Lotter і ін.

2008/0178294 Липень 2008 Hu і ін.

2008/0181116 Липень 2008 Kavanaugh і ін.

2008/0186162 Серпень 2008 Rajan і ін.

2008/0196104 Серпень 2008 Tuvell і ін.

2008/0200160 Серпень 2008 Fitzpatrick і ін.

2008/0208950 Серпень 2008 Kim та ін.

2008/0209557 Серпень 2008 Herley і ін.

2008/0235801 Вересень 2008 Soderberg і ін.

2008/0276111 Листопад 2008 Jacoby і ін.

2008/0293396 Листопад 2008 Barnes і ін.

2008/0307243 Грудень 2008 Lee

2008/0318562 Грудень 2008 Featherstone і ін.

2009/0172227 Липень 2009 Taylor і ін.

2009/0199298 Серпень 2009 Miliefsky

2009/0205016 Серпень 2009 Milas

2009/0205047 Серпень 2009 Podjarny

2009/0248623 Жовтень 2009 Adelman і ін.

2009/0292487 Листопад 2009 Duncan і ін.

2009/0293125 Листопад 2009 Szor

2010/0019731 Січень 2010 Connolly і ін.

2010/0041946 Лютий 2010 Anderson і ін.

2010/0064341 Березень 2010 Aldera

2010/0088398 Квітень 2010 Plamondon

2010/0097494 Квітень 2010 Gum і ін.

2010/0100591 Квітень 2010 Burgess і ін.

2010/0100939 Квітень 2010 Burgess і ін.

2010/0100959 Квітень 2010 Mahaffey

2010/0100963 Квітень 2010 Mahaffey і ін.

2010/0100964 Квітень 2010 Burgess і ін.

2010/0154032 Червень 2010 Ollmann

2010/0210240 Серпень 2010 Mahaffey і ін.

2010/0240419 Вересень 2010 Horino

2010/0313270 Грудень 2010 Kim та ін.

2010/0317324 Грудень 2010 Brown і ін.

2010/0332593 Грудень 2010 Barash і ін.

2011/0047033 Лютий 2011 Mahaffey і ін.

2011/0047594 Лютий 2011 Mahaffey і ін.

2011/0047597 Лютий 2011 Barton і ін.

2011/0047620 Лютий 2011 Mahaffey і ін.

2011/0119765 Травень 2011 Burgess і ін.

2011/0145920 Червень 2011 Burgess і ін.

2011/0171923 Липень 2011 Daly і ін.

2011/0241872 Жовтень 2011 Mahaffey

2011/0296510 Грудень 2011 Hatlelid і ін.

2012/0042382 Лютий 2012 Mahaffey

2012/0060222 Березень 2012 Burgess і ін.

2012/0072569 Березень 2012 Xu

2012/0084836 Квітень 2012 Mahaffey і ін.

2012/0084864 Квітень 2012 Burgess і ін.

2012/0096555 Квітень 2012 Mahaffey

2012/0110174 Травень 2012 Mahaffey і ін.

2012/0124239 Травень 2012 Shribman і ін.

2012/0159636 Червень 2012 Pandya і ін.

2012/0179801 Липень 2012 Luna та ін ..

2012/0179814 Липень 2012 Swildens і ін.

2012/0188064 Липень 2012 Mahaffey і ін.

2012/0196571 Серпень 2012 Grkov і ін.

2012/0215938 Серпень 2012 Fletcher і ін.

2012/0233695 Вересень 2012 Mahaffey і ін.

2012/0259954 Жовтень 2012 McCarthy і ін.

2012/0278467 Листопад 2012 Schneider

2012/0303735 Листопад 2012 Raciborski і ін.

2012/0317153 Грудень 2012 Parthasarathy і ін.

2012/0317233 Грудень 2012 Redpath

2012/0317370 Грудень 2012 Luna

2012/0324076 Грудень 2012 Zerr і ін.

2012/0324094 Грудень 2012 Wyatt і ін.

2012/0324259 Грудень 2012 Aasheim і ін.

2012/0324568 Грудень 2012 Wyatt і ін.

2013/0013775 Січень 2013 Baumback і ін.

2013/0019311 Січень 2013 Swildens і ін.

2013/0023209 Січень 2013 Fisher і ін.

2013/0041946 Лютий 2013 Joel та ін.

2013/0041974 Лютий 2013 Luna та ін.

2013/0047034 Лютий 2013 Salomon і ін.

2013/0054796 Лютий 2013 Baumback і ін.

2013/0067054 Березень 2013 Pulleyn і ін.

2013/0086682 Квітень 2013 Mahaffey і ін.

Первинний Екзаменатор: Чан; Син-Хан

Повірений, Агент або Фірма: Dergosits & ТОО Ной

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Прецедентні тексти**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перехресне посилання на споріднені заявки

Справжня заявка є продовженням заявки на патент США № 13/333654, під назвою "СИСТЕМА І МЕТОДИ ЗАПОБІГАННЯ АТАК ПО", поданої 21 грудня 2011 року, яка є продовженням заявки на патент США № 12/255621, під назвою "СИСТЕМА І МЕТОДИ ЗАПОБІГАННЯ АТАК ПО ", поданої 21 жовтня 2008 року, і пов'язана з наступною патентної заявки США № 12/255635 під назвою" СТАН БЕЗПЕКИ і ВІДОБРАЖЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ", тепер патент США. № 8060936, заявка США № 12/255632, під назвою "ПЛАТФОРМА ЗАХИСТУ МОБІЛЬНОГО ПРИСТРОЇ", тепер патент США. №8087067, заявка на патент США № 12/255626, під назвою "СИСТЕМА І СПОСОБИ ДЛЯ крос-платформний СИСТЕМИ МОБІЛЬНОГО ЗАБЕЗПЕЧЕННЯ", тепер патент США №8099472 і патентній заявці США № 12/255614, під назвою "СИСТЕМА І СПОСОБИ МОНІТОРИНГУ ТА АНАЛІЗУ КІЛЬКОХ ІНТЕРФЕЙСІВ І БЕЗЛІЧІ ПРОТОКОЛІВ ", тепер патент США №8051480. Всі заявки включені в даний опис як посилання.

**Заявка**

**Формула винаходу:**

1. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, метод, що включає: процес, коли пристрій мобільного зв'язку приймає дані, створює хеш-ідентифікатор для даних, порівнює хеш дані ідентифікатора з базою даних відомих безпечних даних з базою даних, отриманих від сервера і зберігаються на пристрої мобільного зв'язку і не отримує позитивного збіги, отримавши хеш дані код на сервері, в якому отримання хеш даних ідентифікатора являеться сигналом від пристрою мобільного зв'язку, про те що аналіз даних за допомогою компонента безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; на сервері, з використанням відомого компоненту не безпеки, порівнюючи отримані хеш дані ідентифікатора з базою даних, що зберігаються в пам'яті, пов'язаної з сервером, що містить хеш-ідентифікатори, відомих не безпечних даних; і, якщо хеш дані порівняння ідентифікатора з відомими компонентами небезпечно покажуть позитивне збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

2. Спосіб за пунктом 1, являє собою наступне: якщо порівняння ідентифікатора хеш-даних на сервері компонентом відомою небезпеки не покаже позитивного збігу, то на сервері, за допомогою вирішального компонента, проводиться аналіз ідентифікатором хеш-даних для визначення безпеки або шкідливості даних; якщо вирішальний компонент на сервері визначає за допомогою аналізу, що дані безпечні, посилає команду від сервера на пристрій мобільного зв'язку на дозвіл обробки даних пристроєм мобільного зв'язку; і якщо вирішальний компонент на сервері визначає за допомогою аналізу, що дані, є шкідливими, він відправляє команду від сервера на пристрій мобільного звязку на відхилення обробки даних пристроєм мобільного зв'язку.

3. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того, як мобільний пристрій зв'язку приймає дані, і створює хеш ідентифікатор для даних, отримавши ідентифікатор хеш-даних на сервері, в якому отримання хеш-даних ідентифікатора являє собою сигнал від пристрою мобільного зв'язку, про те що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; потім, на сервері, з використанням компонент відомою не безпеки порівнюються отримані хеш дані ідентифікатора з базою даних, що зберігається в пам'яті, пов'язаної з сервером, що містить хеш-ідентифікатори, відомих не безпечних даних; якщо порівняння хеш даних ідентифікатора проведених компонентом відомою не безпеки покаже позитивне збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку; якщо порівняння хеш даних ідентифікатора на сервері проведених компонентом невідомої безпеки не покаже позитивний збіг, тоді на сервері використовуючи відомий компонент безпеки проводиться порівняння отриманих хеш даних ідентифікатора з базою даних ідентифікатора відомих безпечних даних зберігаються в пам'яті пов'язаної з сервером; на сервері, якщо порівняння проведене компонентом відомої безпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; якщо порівняння проведене компонентом відомої безпеки не покаже позитивного збігу, на сервері, за допомогою вирішального компонента, проводиться аналіз даних, з метою визначення безпеки або шкідливості даних; якщо аналіз, проведений відомим вирішальним компонентом на сервері визначає, що дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо аналіз проведений відомим вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

4. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того, як мобільний пристрій зв'язку приймає дані, і створює хеш ідентифікатор для даних, використовуючи компонент відомою небезпеки, порівнює отриманий хеш дані ідентифікатора з базою даних, що зберігаються в пам'яті мобільного пристрою зв'язку, що містить хеш-ідентифікатори, відомих небезпечних даних, отримуючи хеш-дані код на сервері, де отримання даних хеш ідентифікатора являє собою сигнал від пристрою мобільного зв'язку , про те що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; якщо порівняння хеш даних ідентифікатора проведених компонентом відомою небезпеки не покаже позитивний збіг, тоді на сервері використовуючи компонент відомої безпеки проводиться порівняння отриманих хеш даних ідентифікатора з базою даних ідентифікатора відомих безпечних даних зберігаються в пам'яті пов'язаної з сервером; на сервері, якщо порівняння проведене компонентом відомої безпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; якщо порівняння проведене компонентом відомої безпеки не покаже позитивного збігу, на сервері, за допомогою вирішального компонента, проводиться аналіз даних, з метою визначення безпеки або шкідливості даних; якщо аналіз, проведений відомим вирішальним компонентом на сервері визначає, що дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо аналіз, проведений відомим вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

5. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: коли мобільний пристрій зв'язку приймає дані, застосовуючи відомий логічний компонент до даних з метою порівняння характеристик даних з базою даних компонента відомої безпеки, бази даних отриманої від сервера для визначення безпеки даних і не показує позитивного збігу, отримуючи дані від пристрою мобільного зв'язку на сервері, де отримання даних є сигналом від пристрою мобільного зв'язку, про те, що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; на сервері з використанням логічного компонента невідомої безпеки по відношенню до прийнятих даними для порівняння характеристик даних з базою даних компонента відомою не безпеки для визначення безпеки або шкідливості даних; і якщо логічний компонент відомою не безпеки покаже, що отримані дані є шкідливими, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

6. Спосіб за пунктом 5, являє собою наступне: якщо логічний компонент відомою не безпеки не покаже, що отримані дані є шкідливими, на сервері, за допомогою вирішального компонента, проводиться аналіз отриманих даних, з метою визначення безпеки або шкідливості даних; якщо аналіз, проведений вирішальним компонентом на сервері визначає, що дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо аналіз, проведений відомим вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

7.На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того як мобільний пристрій зв'язку отримує дані, приймаючи дані на сервер, де отримання даних є сигналом від пристрою мобільного зв'язку, про те що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; на сервері з використанням логічного компонента відомої безпеки по відношенню до даних для визначення безпеки даних; на сервері, якщо визначення логічним компонентом відомої безпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; на сервері якщо визначення логічним компонентом відомої безпеки не покаже позитивного збіги, на сервері, з використанням вирішального компонента, проводиться аналіз отриманих даних, з метою визначення безпеки або шкідливості даних; якщо аналіз проведений вирішальним компонентом на сервері визначає, що отримані дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо аналіз, проведений відомим вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

8. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того як мобільний пристрій зв'язку отримує дані, приймаючи дані на сервер, де отримання даних є сигналом від пристрою мобільного зв'язку, про те що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; на сервері з використанням логічного компонента відомої безпеки по відношенню до даних для визначення безпеки даних; на сервері, якщо визначення логічним компонентом відомої безпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; якщо визначення логічним компонентом відомої безпеки не покаже позитивного збігу, на сервері, з використанням логічного компонента відомою не безпеки визначається безпеку або шкідливість даних; і якщо визначення, проведене логічним компонентом відомою не безпеки визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

9. На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того як мобільний пристрій зв'язку отримує дані, приймаючи дані на сервер, де отримання даних є сигналом від пристрою мобільного зв'язку, про те що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; на сервері з використанням логічного компонента відомою не безпеки по відношенню до даних для визначення шкідливості даних; якщо визначення компонентом відомою небезпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку; якщо визначення компонентом відомою небезпеки не покаже позитивного збігу на сервері, з використанням логічного компонента відомої безпеки визначається безпеку даних; на сервері, якщо визначення проведене компонентом відомої безпеки покаже позитивного збіги, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку. Якщо визначення проведене компонентом відомої безпеки не покаже позитивного збіги, на сервері, з використанням вирішального логічного компонента проводиться аналіз даних, з метою визначення безпеки або шкідливості даних; якщо визначення проведений вирішальним компонентом на сервері визначає, що отримані дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо визначення, проведене відомим вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

10.На сервері, що має мережевий інтерфейс для прийому і передачі даних з / на пристрій мобільного зв'язку, що має компоненти програмного забезпечення для обробки та аналізу даних, спосіб, є наступною: після того як мобільний пристрій зв'язку отримує дані, і застосовує логічний компонент відомої небезпечно для визначення шкідливості даних, приймаючи дані на сервер, де отримання даних є сигналом від пристрою мобільного зв'язку, про те, що аналіз даних проводиться компонентом безпеки пристрою мобільного зв'язку не дав можливості розпізнати дані, як безпечні або шкідливі; якщо визначення компонентом відомою не безпеки на пристрої мобільного зв'язку з цим не покаже позитивний збіг, на сервері, використовується логічний компонент відомої безпеки для визначення безпеки даних; якщо визначення проведене компонентом відомої безпеки покаже позитивний збіг, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; якщо визначення проведене компонентом відомої безпеки не покаже позитивного збіги, на сервері, з використанням вирішального логічного компонента проводиться аналіз даних, з метою визначення безпеки або шкідливості даних; якщо визначення проведений вирішальним компонентом на сервері визначає, що дані безпечні, відправляється команда від сервера на пристрій мобільного зв'язку, на дозвіл обробки даних пристроєм мобільного зв'язку; і, якщо визначення, проведене вирішальним компонентом на сервері визначає, що дані шкідливі, відправляється команда від сервера на пристрій мобільного зв'язку, на відхилення обробки даних пристроєм мобільного зв'язку.

**Опис**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Область**

Винахід стосується в цілому захисту інформації, зокрема, для запобігання та виявлення атак на пристрої мобільного зв'язку.

**Вступ**

Існує безліч способів для захисту комп'ютерних систем від шкідливого впливу вірусів, шкідливих програм, рекламного ПЗ, експлойтів і інших комп'ютерних забруднювачів (також відомих під загальною назвою "атак"). Стаціонарні комп'ютери, ноутбуки і серверні комп'ютери використовують численні антивіруси, мережі та аналогічні продукти, спрямовані на захист програмного забезпечення, здатні виявляти загрози для безпеки, такі як експлойти, віруси і шкідливі програми. Виявлення відомих вірусів і шкідливих програм часто включає в себе ідентифікацію характеристик програмних кодів або визначення відомих вірусів і шкідливих програм, зберігаючи характеристики цих кодів або визначень в базі даних на комп'ютері, і порівнюючи дані з цими характеристиками або визначеннями для того, щоб визначити, чи містять дані віруси або шкідливі ПО. Виявлення раніше невідомих вірусів і шкідливого ПО, може часто включає в себе аналіз даних за певними характеристиками або емулювання виконання даних, з метою визначення, що вони будуть робити, якщо дозволити їм працювати на хост-системі. Виявлення нових атак є питанням поновлення бази описів вірусів або бази вірусних сигнатур на комп'ютері або зміни правил, пов'язаних з невідомою системою виявлення вірусів / шкідливих програм. Це можливо, тому що комп'ютери мають апаратну, програмну і ресурсну пам'ять для зберігання і управління великими базами даних вірусних сигнатур, а також процесорні ресурси для виконання складних аналізів і емулювання середовища виконання. Виявлення експлойтів або інших атак, які можуть поставити під загрозу безпеку комп'ютера через мережу часто включає в себе ідентифікацію сигнатури відомих експлойтів або атак, що зберігаються в базі даних сигнатур на комп'ютері, який захищений, і порівнюючи дані по мережі з цими сигнатурами, з метою визначення змісту можливої ​​загрози для безпеки в данних.Также як і сигнатури вірусів і шкідливих програм, сигнатури мережевих атак можуть оновлюватися з метою виявлення нових загроз для безпеки. Як уже згадувалося раніше, така система стає можливою завдяки тому, що комп'ютери мають обчислювальні ресурси і ресурси зберігання, які дають можливість управляти великими базами даних сигнатур атак і порівнювати мережеві дані з багатьма сигнатурами до їх прояву.

Мобільні пристрої зв'язку не володіють такою ж потужністю, як комп'ютери, хоча вони часто розробляються для забезпечення деяких з тих же функціональних можливостей, які мають комп'ютери в портативної формі. Для того, щоб забезпечити ці функціональні можливості, в пристроях мобільного зв'язку часто збережені мобільні або портативні версії операційних систем стаціонарних комп'ютерів чи системних архітектур, такі як Windows, Mobile.RTM., Apple OS X iPhone.TM. або Java.RTM.ME. В результаті, деякі атаки спрямовані на традиційні комп'ютери можу бути легко переведені або модифіковані, для можливості нанесення шкоди пристрою мобільного зв'язку. Крім того, кількість і типи атак, спеціально спрямованих на платформу пристроїв мобільного зв'язку зростає.

При виявлення атак на пристрій мобільного зв'язку виникають проблеми, які не зустрічаються на традиційних комп'ютерних платформах. Як уже згадувалося раніше, пристроїв мобільного зв'язку не вистачає тих апаратних і програмних ресурсів, а також ресурсів пам'яті, які є у традиційного комп'ютера. Таким чином, зберігання великих баз даних сигнатур на пристрої мобільного зв'язку не представляється можливим, і запуск складних систем аналізу занадто перевантажує пам'ять, акумулятор і процесор пристрою. Інші рішення в області безпеки виявилися безуспішними в області розпізнавання атак, спеціально спрямованих на пристрої мобільного зв'язку, так як пристрої мобільного зв'язку надають функціональні можливості, яких немає на традиційних комп'ютерах. Наприклад, пристрій мобільного зв'язку може бути піддано атаці через мережеві дані, файли або виконувані файли, отримані через різні мережеві інтерфейси, такі як Bluetooth, Wi-Fi, ІЧ-порт або стільникові мережі.

Відсутність надійних антивірусних програм і попереджувальних заходів проти атак пристроїв мобільного зв'язку має серйозні наслідки для безпеки. Мобільні пристрої є частиною критичної інфраструктури: так як люди залежать від таких пристроїв в питанні зв'язку, передачі і прийому даних, а також доступу в Інтернет і веб-сайтів, і питання безпеки цих пристроїв стає все більш важливим. Якщо вони не захищені, значна частина мобільних пристроїв можуть піддаватися злочинним або кібер-терористичним актам, які можуть порушити нормальне функціонування як торгівлі, так і уряду. Фахівець у даній галузі може легко підірвати життєво важливі комунікації, використовуючи пристрій мобільного зв'язку, для злому нібито захищених серверів, які зберігають конфіденційну інформацію, крадіжки грошей з допомогою мобільних платіжних механізмів або виконання безлічі інших шкідливих і мерзенних актів.

Саме тому необхідний спосіб для запобігання атак і захисту пристроїв мобільного зв'язку без шкоди для функціонування пристрою.

**КОРОТКИЙ ОПИС РИСУНКІВ**

Винахід проілюстровано як приклад, і не обмеження в постатях додаються креслень, на яких однакові посилальні позиції вказують на однакові елементи, і на яких:

Рис. 1 являє собою приблизну блок-схему, яка зображує один варіант здійснення даного винаходу.

На рис. 2 показана приблизна схема послідовності етапів здійснення даного винаходу.

На рис. 3 показана приблизна схема послідовності етапів здійснення даного винаходу.

**ДЕТАЛЬНИЙ ОПИС**

Винахід являє собою систему і спосіб оцінки даних на пристрої мобільного зв'язку, для визначення наявності можливої ​​загрози для безпеки. В одному з варіантів здійснення даний винахід забезпечує пристрій мобільного зв'язку, механізмом для відхилення даних, який відразу визначаються як шкідливі, і для забезпечення можливості отримання даних, які визнані безпечними. Крім того, даний винахід дає можливість пристрою мобільного зв'язку, оцінити дані, які не відразу зізнаються безпечними або шкідливими. Винахід функціонує на пристрої мобільного зв'язку, незважаючи ні на апаратні, програмні ресурси, а також ресурси пам'яті, що містяться на пристрої. Використовуваний в описі вираз "мобільного зв'язку" може ставитися до мобільного телефону, слухавці, смартфону, КПК тощо. Пристрій мобільного зв'язку в першу чергу може бути використано для голосового зв'язку, але також може бути обладнано для прийому і передачі даних, в тому числі електронної пошти, текстових повідомлень, відео та інших даних. Ці дані можуть бути отримані у вигляді пакетів або потоків.

Слід розуміти, що даний винахід може бути реалізовано різними способами, в тому числі у вигляді процесу, пристрої, системи, способи, або машиночитаемого носія, такого як машинозчитувана носія інформації, що містить команди комп'ютерних програм або комп'ютерної мережі, в якому команди комп'ютерних програм передаються через оптичні або електронні канали зв'язку. Додатки, програми або зчитуються комп'ютером команди можуть згадуватися як компоненти або модулі. Додатки можуть приймати форму програмного забезпечення, яке використовується на комп'ютері загального призначення або може бути жорстко закодірованона апаратному рівні. В даному описі ці реалізації, або будь-які інші форми, які винахід може приймати, можуть називатися способами виконання. Загалом, порядок етапів описаних процесів, може бути змінений в рамках цього винаходу.

**А. Архітектура системи**

В одному з варіантів здійснення даний винахід включає в себе, щонайменше, три програмних резидентних компонента на пристрої мобільного зв'язку. Як показано на рис. 1, перший компонент 107 може бути використаний для розпізнавання даних, які є безпечними, або "відомими безпечними." Другий компонент 106 може бути використаний для розпізнавання даних, які є шкідливими, або "відома не безпечними". Третій компонент 105 є вирішальним компонентом, який може бути використаний для оцінки даних, які не є ні відомими безпечними, ні відомими невірними. Кожен з цих компонентів буде більш докладно обговорюватися нижче.

Необхідно пам'ятати, що як зазначено в цьому документі, дані можуть включати в себе мережеві дані, файли, що виконуються і невиконувані додатки, електронну пошту та інші типи об'єктів, які можуть бути передані або прийняті пристроєм мобільного зв'язку. Пристрої мобільного зв'язку, як правило, передають і приймають дані через один або кілька мережних інтерфейсів, включаючи Bluetooth, WiFi, ІК-порт, радіоприймачі тощо.

Аналогічним чином, дані можуть бути суміщені в уровневом протоколі передачі даних або наборі протоколів, таких як TCP / IP, HTTP, Bluetooth, тощо.

 Для того щоб оцінити рівень загрози безпеки даних, може бути необхідно ідентифікувати або розібрати один або кілька протоколів, використовуваних для поєднання даних. Це може бути здійснено за допомогою такої системи, як та, що описана в знаходиться на розгляді патентній заявці США № 12/255614, під назвою "Система і спосіб моніторингу та аналізу декількох інтерфейсів і декількох протоколів", патент США. №8051480, який включений в даний опис у вигляді посилання повним опису матеріалів даної заявки.

Крім того, необхідно розуміти, що дані можуть відрізнятися за розміром і складності в залежності від їх джерела, призначення і мети. Може бути важко проаналізувати отримані об'єкти даних в цілому; Тому для того, щоб оптимізувати використання ресурсів на платформі пристрої мобільного зв'язку, даний винахід може застосовувати функції хешування або алгоритми хешування по відношенню до отриманих даних. Алгоритм гешування перетворює дані в ідентифікатор фіксованої довжини для полегшення оцінки. Застосування хеш-функції може бути виконано за допомогою будь-якого з компонентів системи, як показано на рис. 1, або в якості альтернативи, можуть бути просто виконані самою системою.

Потім хешировать дані можуть бути спрямовані деяким або всім трьом компонентам для категоризації та подальших дій, якщо це необхідно. Наприклад, компонент відомої безпеки 107 може мати доступ або може об'єднаний з зберігається базою даних відомих безпечних хеш ідентифікаторів. Як обговорювалося раніше, база даних може бути сховищем даних або зведенням відомих безпечних хеш ідентифікаторів, або може бути логічною схемою, яка забезпечує порівняння хеш-ідентифікаторів з відомими безпечними даними. Коли дані проаналізовані за допомогою пристрою мобільного зв'язку, вони можуть бути швидко хешування і порівняні з цієї збереженої базою даних за допомогою компонента відомої безпеки. Ця база даних може включати в себе ідентифікатори даних, які були проаналізовані раніше і були визнані безпечними, які беруть свій початок з надійного джерела, або просто зізнаються безпечними на основі їх характеристик. Це може включати в себе вивчення структури, впливу на наступні події, передбачуваний джерело, призначення даних і т.д. Якщо є збіг з відомої безпечної базою даних хеш-ідентифікатора, то дані можуть бути класифіковані як відомо безпечні, і в такому випадку подальший аналіз не потрібно. Потім ці дані можуть бути допущені до передбачуваного місця призначення для обробки, виконання або іншої операції.

Фахівцю в даній області буде зрозуміло, що, оскільки загальна кількість відомих безпечних додатків для пристроїв мобільного зв'язку мало, використання компонента безпеки 107, з'єднаного з базою даних відомих безпечних ідентифікаторів додатків, може значно зменшити число помилкових позитивних виявлень шкідливих програм. Також буде зрозуміло, що використання компонента відомої безпеки 107 може бути особливо ефективно для даних, які містять виконуваний код програмного забезпечення. Виконуваний код програмного забезпечення в межах цієї програми рідко змінюється між різними пристроями мобільного зв'язку, створюючи таким чином базу даних відомих безпечних хеш-ідентифікаторів або логічних схем для оцінки відомих безпечних хеш ідентифікаторів, що може бути ефективним методом для розпізнавання безпечних і надійних даних. Ця база даних може варіюватися в залежності від розміру наявних ресурсів на пристрої мобільного зв'язку. В якості альтернативи, аспекти цього винаходу, такі як компонент відомої безпеки, може мати доступ до віддаленого сервера з великим сховищем хеш-ідентифікаторів для відомих безпечних даних або додатків. Крім того, як обговорюється далі в наступному розділі, компонент відомої безпеки 107 може бути в змозі оцінити безпеку даних в залежності від того чи мають дані достатніми характеристиками, спільними з іншими відомими безпечними даними.

Другий компонент системи здійснення даного винаходу може включати в себе компонент, здатний розпізнавати, чи є дані шкідливими, або "відома не безпечними" (106 на рис. 1). Компонент відомою не безпеки 106 може мати доступ до бази даних, логічних схем або іншого сховища даних, що містить інформацію про відомих сигнатури атак або визначень, які можуть бути збережені на пристрої мобільного зв'язку, не займаючи значний обсяг пам'яті. Наприклад, вірус або інші шкідливі сигнатури можуть бути зведені в хеш ідентифікатор і збережені в базі даних. Іншими словами, можливе існування хеш ідентифікатора відомою не безпечної бази даних, який буде доповнювати хеш-ідентифікатор відомої безпечної бази даних збереженого на пристрої мобільного зв'язку. Крім того, чи в якості альтернативи, компонент відомою не безпеки 106 може бути здатний ідентифікувати шкідливі програми за допомогою характеристик, спільних для інших видів шкідливого програмного коду. При застосуванні до мережевих файлів даних або файлів даних, компонент відомою не безпеки 106 може мати доступ до бази даних, що містить зразки або інші характеристики даних протоколу або формату файлу, які становлять загрозу для безпеки. Подібно компоненту відомої безпеки 107 і бази даних, будь-які дані, ідентифіковані як містять шкідливі програми можуть бути видалені, поміщені в карантин, або відхилені від подальшої обробки за допомогою пристрою мобільного зв'язку. При виявленні об'єкта містити не безпечні дані, даний винахід може також відображати повідомлення або інше повідомлення, подібне описаному в спільно поданій патентній заявці США № 12 / 255,635, під назвою "Стан Безпеки І Система відображення інформації" яка включена в повному обсязі в цьому документі.

Третій компонент системи здійснення даного винаходу, може бути вирішальним компонентом 105. Цей компонент може бути використаний для оцінки даних, які не можуть бути охарактеризовані як відомі безпечні або небезпечно. Так як більшість даних, отриманих пристроєм мобільного зв'язку можуть також підпадати під цю категорію, цей компонент може використовувати більшу частину ресурсів, що виділяються для здійснення системи винаходу. Цей компонент може застосовувати нечітку логіку, евристичні алгоритми або інші методи аналізу, для визначення, чи будуть отримані дані передані за цільовим призначенням, або вони будуть відхилені, з метою запобігання нанесення шкоди пристрою. Приклади цього аналізу обговорюються нижче. Здійснення системи може існувати незалежно від пристрою мобільного зв'язку, або може бути включено в існуючу систему безпеки на пристрої мобільного зв'язку, такий як описано в знаходиться на розгляді патентній заявці США № 12/255614. Також для реалізації винаходу на різних мобільних комунікаційних платформах пристрої, може виникнути необхідність програмування аспектів даного винаходу з використанням цільової платформи, такої як та, що описана в спільно поданій заявці на патент США № 13/313937, під назвою "СИСТЕМА І СПОСІБ використання цільової платформи ", патент США № 8271608, який включений в якості посилання в повному обсязі в цій заявці. Крім того, аспекти цього винаходу можуть бути використані для визначення стану безпеки на пристрої мобільного зв'язку, як описано в спільно поданій патентній заявці США № 12/255632, під назвою "Платформа безпеки мобільних систем", тепер патент США № 8087067 якого включено в якості посилання в повному обсязі в цій заявки.

Також буде зрозуміло, що хоча даний винахід описується як встановлене на пристрої мобільного зв'язку, частини цього винаходу можуть комунікувати або працювати спільно з віддаленим сервером або декількома серверами. Наприклад, система здійснення даного винаходу може бути виконана з можливістю поновлення своїх вірусні визначень або порівняння отриманих даних з більш широкою базою даних сигнатур вірусів на віддаленому сервері. В якості альтернативи, пристрій мобільного зв'язку може бути налаштований таким чином, щоб мати можливість відправляти хеш-ідентифікатор для прийнятих даних на один або кілька серверів для аналізу і / або оцінки. Один сервер може містити компонент відомої безпеки 107, компонент відомою не безпеки 106 і вирішальний компонент 105 відповідно до даного винаходу, або компоненти можуть бути розподілені за двома або більше серверів. Один або кілька серверів можуть, таким чином, виконувати аналіз з використанням хеш ідентифікатора, і в разі якщо аналіз показує, що хеш-ідентифікатор ідентифікує безпечні дані, то один або кілька серверів, можуть повідомити мобільний пристрій зв'язку або проінструктувати пристрій, про можливість прийому і обробки даних. Якщо аналіз показує, що хеш-ідентифікатор ідентифікує шкідливі дані, то один або кілька серверів можуть повідомити пристрій мобільного зв'язку або проінструктувати пристрій, про відхиленні даних. Якщо аналіз не дає бажаних результатів, то один або кілька серверів можуть зажадати, щоб пристрій мобільного зв'язку відправило дані, ідентифіковані хеш ідентифікатором на сервер для подальшого аналізу. Подальший аналіз може бути виконаний відповідно до вирішальним компонентом 105 або вручну. Також можливі інші варіанти, які не виходитимуть за рамки цього винаходу.

**B. Шкідливі програми і виявлення атак за допомогою характеристик даних**

Архітектура системи, яка обговорювалася раніше, має переваги в порівнянні з попередньому рівнем систем безпеки пристроїв мобільного зв'язку, які, як правило, включають тільки метод відомого безпечного або небезпечно виявлення. Оскільки даний винахід включає в себе вирішальний компонент 105, а також, можливість зводити до мінімуму помилково-позитивні або помилково-негативні помилки виявлення, загальні для систем попереднього рівня техніки. Інші переваги і поліпшення обговорюються в даному розділі, який описує деякі з аналізів, виконуваних системою здійснення даного винаходу.

1.Характеристика відомої безпеки

В одному з варіантів здійснення, даний винахід може бути виконано з можливістю розпізнавання характеристик безпеки, якими відомі безпечні дані повинні володіти. Аналіз даних на виявлення характеристик безпеки може включати в себе еквівалент застосування бази даних або інших даних сховища до відомим характеристикам безпеки або логічним схемам, і порівняння їх з базою даних. В якості альтернативи або додатково, аналіз даних на виявлення характеристик безпеки може включати в себе еквівалент застосування логіки затвердження характеристик відомої безпеки. База даних або логічний блок не може включати в себе всі характеристики, які можуть визначати безпеку даних; Проте, якщо у об'єкта даних відсутні ключові характеристики відомої безпеки, то система може зробити висновок про те, що дані можуть бути шкідливими і повинні бути додатково проаналізовані, або в якості альтернативи, повинні бути відхилені. База даних характеристик відомої безпеки або логічні схеми характеристик відомої безпеки можуть замінити компонент безпеки 107 описаний вище, або в деяких випадках можуть замінити його в якості спрощеної альтернативи. Іншими словами, список всіх відомих безпечних файлів даних і мережевих даних може бути нескінченно великою, але список характеристик, спільних для відомо безпечних файлів даних і відомих безпечних мережевих даних може бути значно менше. Таким чином, база даних характеристик відомої безпеки може бути менше за розміром, ніж база даних відомої безпеки, і, отже, може бути більш практичною, в мобільних пристроях зв'язку витрачаючи менше пам'яті і ресурсів на обробку.

Існує цілий ряд характеристик, спільних для відомих безпечних даних, але ці характеристики можуть відрізнятися в залежності від того, являються дані мережевими даними, файловими даними, або виконувані файлові дані. Винахід може оцінити всі типи даних, що отримуються за допомогою пристрою мобільного зв'язку. Наприклад, мережеві дані та файлові дані можуть бути перевірені на предмет структури та стану. До цього може відноситься перевірка даних щодо пов'язаних з ними метаданих для підтвердження того, що розмір, тип і опис відповідають описаним даними. За допомогою цього аналізу, компонент відомої безпеки 107 може бути налаштований таким чином, щоб давати допуск або відхиляти дані, які мають кваліфіковану характеристику і структуру, і надавати дані, які не проходять ці тести, проведені компонентом відомою не безпеки 106 для подальшого аналізу або просто відхиляти їх безпосередньо. Однак ясно, що показник кваліфікованої характеристики і структури не є достатнім для висновку про повну безпеку мережевих даних або файлових даних, і саме для цього може знадобитися подальший аналіз проводиться компонентом відомої небезпеки 106 і / або вирішальним компонентом 105. Іншими словами, навіть якщо дані проаналізували за допомогою компонента відомої безпеки 107 покажуть позитивний збіг, що означає що дані мають безпечні характеристики, або якщо дані співпадуть з безпечними даними хеш ідентифікатора, дані все одно можуть бути проаналізовані за допомогою компонента відомої небезпеки 106 і / або вирішального компонента 105.

Що стосується виконуваних даних, список відомих безпечних виконуваних додатків для пристроїв мобільного зв'язку невеликий. Таким чином, компонент відомої безпеки 107 може просто порівняти хеш-ідентифікатори з зібраними виконуваними даними із збереженою базою даних відомих безпечних виконуваних файлов.Также можуть бути застосовані інші методи, такі як перевірка структури формату файлу виконуваного файлу або перевірка будь-яких криптографічних підписів виконуваних файлів .

2. Характеристики відомої небезпеки

В одному з варіантів здійснення, дані можуть бути співставлені з допомогою логічної схеми або бази даних або інших сховищ даних з характеристиками відомої небезпеки. Таким чином, якщо дані мають характеристики відомої небезпеки, вони можуть розглядатися в якості шкідливих і можуть бути відхилені, видалені або поміщені в карантин. Таким чином, ясно, що цілком весь об'єкт даних може мати характеристики відомої небезпеки або частина об'єкта даних може мати характеристики відомої небезпеки, або один з шаблонів в об'єкті може бути визнаний шкідливим, або об'єкт даних може показати позитивний результат після аналізу проведеного логічним компонентом, який виконує певний тест на наявність характеристик відомої небезпеки. У таких ситуаціях може виникнути привід для проведення подальшого аналізу або підтвердження з метою уникнення неточного результату. Подальший аналіз здатний уникнути ситуацій, в яких даний винахід може не розпізнати специфічно шкідливі об'єкти даних, які можуть бути не розпізнані як такі до Того. Звичайно ж, в ситуаціях, які можуть поставити під загрозу безпеку, краще, уникати помилкових характеристик об'єктів, які можуть назвати їх швидше безпечними, ніж небезпечними. Дані, які визнаються безпечними або тими, що мають досить характеристик відомо безпеки, можуть бути передані за їх призначенням. Дані, в яких не виявляються характеристики відомої безпеки або додатки, визначаються як швидше небезпечні ніж безпечні, або просто непрізнаються, можуть бути передані вирішального компоненту 105 для подальшого аналізу.

Як було зазначено раніше, дані можуть бути проаналізовані по-різному в залежності від того, чи є це мережеві дані, файлові дані або виконував дані. Мережеві дані і файлові дані можуть бути суміщені в різних протоколах або рівневих форматах. Ці протоколи або формати можуть бути проаналізовані за допомогою системи і способів, описаних в спільно поданій патентній заявці США. № 12/255614. Якщо будь-які з даних мають відхилення по передбачуваному протоколу або формату, мають невідповідне утримання або переходи стану, або є невідповідними для процесора або підсистеми, для якої вони призначені, компонент відомої небезпеки 106 може відхилити ці дані як потенційно шкідливі.

Відомі небезпечні виконувані файли можуть оцінюються з використанням хеш-підпису, порівняння рядка в будь-якому місці або за відносним або абсолютним зміщення в файлі, або шаблоном в будь-якому місці або за певним зміщення в файлі відповідно до відомими частинами або групами шкідливих програм. Якщо зустрічаються, будь-які з цих характеристик, то компонент відомої небезпеки 106 може ідентифікувати дані як шкідливі і відхилити їх. Також можуть бути використані інші методи виявлення відомих небезпечних даних, в тому числі, блокуванням виконуваних файлів, які використовують частину або певну комбінацію привілейованих функціональних можливостей, або блокування виконуваних файлів, які, як вважатиме сервер, мають частоту доступу характеристик у багатьох мобільних пристроях, що вказує на наявність вірусів і шкідливих програм, і не тільки ними.

3. Подальший аналіз

У деяких випадках дані можуть не відразу бути визнані, як відомо безпечні або небезпечні, і в цих випадках використовується вирішальний компонент 105.Ключевим аспектом цього винаходу є його здатність аналізувати дані, які не відразу зізнаються безпечними або шкідливими. Як уже згадувалося раніше, це може викликати необхідність в аналізі, для визначення чи є дані досить безпечними, ніж небезпечними і навпаки. Таким чином, даний винахід забезпечує ковзаючу шкалу, для оцінки ступеня безпеки або небезпеки прийнятих даних. Це дозволяє більш точно виміряти не тільки те, чи здатні дані пошкодити пристрій мобільного зв'язку, але і то наскільки може зміниться загальний стан безпеки пристрою.

Вирішальний компонент 105 може використовувати один або кілька типів внутрішніх систем прийняття рішень, для характеризації безпеки або небезпеки даних. Вирішальний компонент 105 призначений для виявлення загроз безпеки без конкретних підписів загроз від яких він захищає. Іншими словами, вирішальний компонент 105 може функціонувати в якості додаткового компонента безпеки, для компенсації будь-яких слабких сторін, які має компонент відомої безпеки 107 або компонент відомої небезпеки 106.

Існує цілий ряд вирішальних систем, які можуть бути використані вирішальним компонентом 105, в тому числі, евристичні алгоритми, продукційні і непродукціонние експертні системи, системи нечіткої логіки, нейронні мережі, або інші системи які можуть бути використані для характеризації об'єкта. В одному з варіантів здійснення даного винаходу, вирішальний компонент 105 може аналізувати мережеві дані або файли на предмет можливих загроз безпеки. Наприклад, нечітка система може бути налаштована для можливості проведення аналізу часу пов'язаного з аутентифікацією дії над даними протоколом, таким як Bluetooth. Віддалений пристрій, підключений до локального пристрою через Bluetooth може повторно спробувати запросити доступ до привілейованого ресурсу на пристрої. Кожен раз, коли віддалений пристрій відправляє запит на аутентифікацію, на цільовому пристрої може з'явитися вікно, яке буде запитувати дії користувача перед тим як відновитися нормальну взаємодію пристрою.

Тому що часто в системі аутентифікації Bluetooth в мобільних телефонах не вбудовано лімітування швидкості передачі, і віддалений пристрій може продовжувати заважати локальному користувачеві запитуючи доступ до привілейованого ресурсу до тих пір поки локальний користувач не почне дратуватися і просто підтверджує запит.

Нечітка система може аналізувати дані, такі як тимчасові рамки між запитами аутентифікації, результатами попередніх запитів аутентифікації і часу, необхідного користувачеві, для відповіді на попередні запити перевірки автентичності. Така система може виявити, коли віддалений пристрій намагається повторно запросити дозвіл і користувач швидко його відхиляє, для запобігання ситуацію, коли користувач дратується і дає доступ да його пристрій віддаленому зловмисникові. Така система також може бути використана для виявлення відхилення атак сервісу, сканування портів або інших атак, які мають істотну тимчасову складову.

В іншому прикладі, евристичний алгоритм може бути використаний для виявлення наявності шеллкодов в пакетних даних, потокових даних або файлових даних, в яких не передбачається їх наявність. Такий шеллкод може свідчити про те, що дані містять експлойти призначені для виконання корупційної атаки пам'яті, при якій метою зловмисника є обробка процесором цільового пристрою міститься шеллкода.

В іншому прикладі вирішальний компонент 105 може містити систему для виявлення аномалій в поведінці протоколу або вмісту файлу, для попередження загроз безпеки, які можуть впливати на непередбачені, або раніше не зворушені механізми.

В іншому прикладі вирішальний компонент 105 може містити систему для аналізу автентичності або інші рядки в мережевих даних або файлах, які можуть бути використані для "соціальної інженерії" користувача. Атаки "Соціальної інженерії" часто маніпулюють користувачем у виконанні дій, які не в його інтересах, використовуючи неправдиву інформацію або будь-яким іншим способом представляючи інформацію користувачеві, яку він або вона може інтерпретувати як законну, але, яка по суті, такою не є. Така система може аналізувати вміст рядків, для визначення, чи мають дані законне походження або це атака "Соціальної інженерії". Приклади атак які цей тип системи може запобігти наступним: "фішинг", "SMS-фішинг," маніпуляції з ім'ям Bluetooth пристрої та інші.

В одному варіанті здійснення даного винаходу, вирішальний компонент 105 може аналізувати програми, бібліотеки або інші виконувані файли на пристрої мобільного зв'язку. Як приклад, вирішальний компонент 105 може містити нейронну мережу, яка аналізує характеристики виконуваного файлу і визначає оцінку безпеки на основі характеристик встановленого з'єднання. Такі характеристики можуть бути визначені на основі інформації, що міститься у виконуваному форматі файлу або в результаті обробки зміст виконуваного файлу.

Як приклад, вирішальний компонент 105 може містити віртуальну механізовану систему рішень, за допомогою якої виконуваний файл може бути класифікований по набору правил, які можуть оновлюватися незалежно від самого вирішального компонента. Така система здатна додати нову логічну схему, для виявлення деяких нових класів вірусів на льоту без необхідності оновлення всього вирішального компонента. Система може попередньо обробити виконуваний файл, так що віртуальна механізована логічна схема може символічно посилатися на виконуваний файл, замість того, щоб обробляти сам виконуваний файл.

Як приклад, вирішальний компонент 105 може містити експертну-систему, яка аналізує поведінку виконуваного файлу за допомогою функціональних викликів, системних викликів або дій, які виконуваний файл може застосувати до операційної системи. Якщо доступ виконуваного файлу до чутливих системних викликів, яким чином нагадує поведінку шкідливих програм, система може подати сигнал про те, що виконуваний файл є потенційно шкідливим і певні дії можуть бути прийняті.

Наведені вище приклади ілюструють, як вирішальний компонент 105 може використовувати ряд аналітичних методів для того, щоб повною мірою оцінити рівень загрози даних, отриманих або переданих на пристрій мобільного зв'язку. Інші приклади можуть бути розглянуті в рамках цього винаходу.

З Аналіз даних.

На рис. 2 і 3 наведені приклади того, як система, описана вище, може використовувати свій алгоритм для оцінки даних для виявлення шкідливих програм і запобігти нападу. Рис. 2 ілюструє оцінку мережевих даних або файлових данних.Ріс. 3 ілюструє даний винахід, яке проводить оцінку виконуваного коду. Кожен з них розглядається далі.

1. Аналіз мережевих даних або файлових даних

Як показано на рис. 2, етап 201 може включати в себе збір даних, відправлених або отриманих на пристрій мобільного зв'язку. Дані можуть бути проаналізовані, для визначення його протоколу та відстеження стану (етап 203) .Понятно, що ці етапи можуть бути виконані повністю або частково за допомогою системи, описаної в одночасно знаходиться на розгляді патентній заявці США. № 12/255635. На етапі 205, компонент відомої безпеки 107 може оцінювати зібрані дані на наявність характеристик відомої безпеки. Характеристики відомої безпеки можуть включати в себе характеристики, які раніше обговорювалися. Якщо дані містять достатню кількість характеристик, відомої безпеки, вони можуть отримати доступ до місця призначення (етап 211) для обробки або іншої операції. В якості альтернативи, вони можуть бути додатково проаналізовані за допомогою компонента відомою не безпеки 106 для підтвердження того, що дані дійсно безпечні (крок 207). Якщо компонент відомою не безпеки 106 визначає, що дані дійсно безпечні, то дані можуть отримати доступ до місця призначення (етап 211). Вирішальний компонент 105 також може провести остаточну перевірку (етап 209), перш ніж дати доступ даними (етап 211).

У будь-який момент під час аналізу, якщо або компонент відомої безпеки 107 або компонент відомою не безпеки 106 або вирішальний компонент 105 визначає, що дані недостатньо безпечні, або абсолютно точно містять загрозу для безпеки, невідповідність даних і т.д., то на етапі 213 дані будуть заблоковані, відхилені, видалені або поміщені в карантин. Як вже обговорювалося раніше, інформація про сигнал тривоги або сигналі загрози безпеки я може бути оновлена ​​в записах про зіткнення з забрудненими даними.

Ясно, що етапи, показані на рис. 2 є лише ілюстративними і жодним чином не обмежують методи винаходу.

2. Аналіз виконуваних даних

На рис. 2, рис. 3 зображені зразкові способи оцінки виконуваних даних, включаючи, додатки, програми і / або бази на пристрої мобільного зв'язку. На етапі 301, виконуваний файл повинен бути класифікований як безпечний або небезпечний в зв'язку із запитом доступу або коли виконуваний файл завантажується або іншим чином передається на мобільний пристрій. Виконуваний файл може або не може бути попередньо оброблений для визначення хеш-ідентифікатора або інших характеристик перш, ніж він буде оцінений компонентом відомої безпеки 107. Ця оцінка може включати в себе порівняння хеш-ідентифікатора виконуваного файлу з базою даних характеристик відомої безпеки, з метою визначення того, чи має виконуваний файл досить характеристик відомої безпеки, або будь-якого з критеріїв, описаних вище. Якщо виконуваний файл розпізнається як безпечний, то на етапі 311, він може отримати дозвіл на виконання свого коду або дозвіл на перехід до прямим призначенням для обробки або іншої операції. Якщо компонент відомої безпеки 107 не может дати дозвіл виконуваним даним, компонент відомої не безпеки 106 може виконати свій аналіз (етап 305). Якщо компонент відомої не безпеки 106 підтверджує, що виконуваний файл є шкідливим, то виконуваний файл може бути поміщений в карантин, відхилений, або видалений, і ця подія може бути зареєстрована (етап 309). Якщо компонент відомої не безпеки 106 не може охарактеризувати виконуваний файл, то вирішальний компонент 105 може виконати свій аналіз, як описано вище (етап 307). Якщо вирішальний компонент 105, в кінцевому рахунку визначає, що виконуваний файл є безпечним, то виконуваний файл отримує дозвіл на доступ (етап 311). Якщо вирішальний компонент 105, в кінцевому рахунку визначає, що виконуваний файл не є безпечним, або залишаються сумніви в цьому, то виконуваний може бути поміщений в карантин (етап 309). І так як виконувані файли можуть містити код, який може завдати значної шкоди пристрою мобільного зв'язку, він може зажадати більш ретельного аналізу, перш ніж виконуваний файл отримає дозвіл на доступ. Будь-який з етапів, показаний на рис. 3, може бути змінений в рамках цього винаходу без відхилення від нього.

Наведені вище приклади припускають, що даний винахід працює в повному обсязі на пристрої мобільного зв'язку. Проте, як обговорювалося раніше, частини цього винаходу можуть знаходиться на одному або декількох віддалених серверах. На прикладі антивірусної системи, хеш-ідентифікатори файлу можуть бути передані на віддалений сервер, який потім ідентифікує файл, як відомо безпечний або не завжди безпечний, або якщо файл містить інформацію про характеристики відомої безпеки або небезпечно. Якщо сервер не розпізнає хеш-ідентифікатор файлу, він може запросити передачу самого файлу на сервер для аналізу. Цей аналіз може проводитися автоматично, або може бути виконаний людиною. Сервер може додатково аналізувати моделі доступу даного файлу між декількома пристроями, для визначення, чи має виконуваний файл поширені характеристики вірусу або шкідливого ПЗ.

В одному варіанті здійснення даного винаходу, аналіз на сервері проводиться одночасно або разом з аналізом, виконуваних на пристрої мобільного зв'язку. Якщо антивірусної системи пристрою мобільного зв'язку не вдається класифікувати файл, вона може запросити результати у сервера. В якості альтернативи або на додаток, даний винахід на пристрої мобільного зв'язку може виконувати евристичний аналіз за допомогою вирішального компонента, описаного вище. Результати локального вирішального компонента на пристрої мобільного зв'язку можуть бути зареєстровані на місцевому рівні і / або передані на сервер.

Як було описано вище, даний винахід забезпечує надійну і гнучку систему безпеки для запобігання атак на пристрій мобільного зв'язку. При здійсненні винаходу, атаки з боку кібер-терористів та інших злочинних угруповань можуть бути зірвані. В результаті, пристрої мобільного зв'язку можуть бути використані для вирішення багатьох завдань з зниженим ризиком загроз безпеки, таких як експлойтів, вірусів, шкідливих програм, соціотехніки, мережевих атак, тощо.

Зрозуміло, що в наведеному вище описі численні докладні деталі викладені з метою забезпечення повного розуміння цього винаходу. Проте, фахівцям зі звичайною кваліфікацією в даній області, буде зрозуміло, що даний винахід може бути реалізовано на практиці без цих конкретних деталей. В інших випадках добре відомі структури і пристрої показані у вигляді блок-схеми для полегшення пояснення. Опис бажаних варіантів здійснення даного винаходу не призначені для обмеження обсягу формули винаходу, що додається до цього документу.

Таким чином, заявлено, що:

Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, їм присвоюється хеш-ідентифікатор, який порівнюється з базою безпечних даних, яка зберігається в пристрої мобільного зв'язку та отримується від сервера. Коли ідентифікатор не отримує позитивну мітку на прийомній стороні сервера, це означає отримання ідентифікатора, який є сигналом від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

на сервері шкідливих даних отриманий хеш- ідентифікатор даних порівнюється з базою даних, що зберігається в пам'яті сервера, який зберігає ідентифікатори шкідливих даних, та:

коли хеш-ідентифікатор даних співпадає з ідентифікатором шкідливих даних, то сервер надсилає пристрою мобільного зв'язку команду відхилити обробку прийнятих пристроем даних.

2. Метод заявки 1 також передбачає, що:

коли хеш-ідентифікатор даних не співпадає з ідентифікатором шкідливих даних, то сервер, використовуючи вирішуючий пристрій, виконує аналіз хеш-ідентифікатора даних для того, щоб визначити, чи є дані, які приймаються, шкідливими чи безпечними.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, показує, що дані є шкідливими, надсилається команда пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

3. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, їм присвоюється хеш-ідентифікатор, який порівнюється з базою безпечних даних, яка зберігається в пристрої мобільного зв'язку та отримується від сервера. Коли ідентифікатор не отримує позитивну мітку на прийомній стороні сервера, це означає отримання ідентифікатора, який є сигналом від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

Якщо пристрій мобільного зв'язку отримує дані, їм присвоюється хеш-ідентифікатор, який порівнюється з базою безпечних даних, яка зберігається в пристрої мобільного зв'язку та отримується від сервера. Коли ідентифікатор не отримує позитивну мітку на прийомній стороні сервера, це означає отримання ідентифікатора, який є сигналом від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

тоді на сервері шкідливих даних отриманий хеш-ідентифікатор даних порівнюється з базою даних, що зберігається в пам'яті сервера, який зберігає ідентифікатори шкідливих даних, та:

коли хеш-ідентифікатор даних не співпадає з ідентифікатором шкідливих даних, тоді на сервері безпечних даних отриманий хеш- ідентифікатор даних порівнюється з базою даних, що зберігається в пам'яті сервера, який зберігає ідентифікатори безпечних даних.

якщо хеш-ідентифікатор даних співпадає з ідентифікатором безпечних даних, то сервер надсилає пристрою мобільного зв'язку команду дозволити обробку прийнятих пристроем даних.

коли хеш-ідентифікатор даних не співпадає з ідентифікатором безпечних даних, то сервер, використовуючи вирішуючий пристрій, виконує аналіз хеш-ідентифікатора даних для того, щоб визначити, чи є дані, які приймаються, шкідливими чи безпечними.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними , надсилається команда пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими , надсилається команда пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

4. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, їм присвоюється хеш-ідентифікатор (використовуючи для порівняння компонент завідомо небезпечних даних) , який порівнюється з базою небезпечних даних, яка зберігається в пристрої мобільного зв'язку та отримується від сервера. Коли ідентифікатор не отримує позитивну мітку на прийомній стороні сервера, це означає отримання ідентифікатора, який є сигналом від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

тоді на мобільному пристрої отриманий хеш- ідентифікатор даних порівнюється з компонентом завідомо небезпечних даних. Якщо результат порівняння не є позитивним, отриманий хеш-ідентифікатор даних порівнюється з базою даних, що зберігається в пам'яті сервера, який зберігає ідентифікатори безпечних даних.

коли хеш-ідентифікатор даних співпадає з ідентифікатором безпечних даних, то сервер надсилає пристрою мобільного зв'язку команду дозволити обробку прийнятих пристроем даних.

коли порівняння з ідентифікатором безпечних даних не дає позитивного результату, то сервер, використовуючи вирішуючий пристрій, виконує аналіз хеш- ідентифікатора даних для того, щоб визначити, чи є дані, які приймаються, шкідливими чи безпечними.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними , сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими , сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

5. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, щодо них використовується завідомо безпечна компонентна логікадля порівняння даних з базою завідомо безпечних даних, яка отримується з сервера, для того, щоб визначити, чи є дані безпечними. Якщо позитивного результату не досягнуто, це означає отримання сервером даних з мобільного пристрою , які є сигналами від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

на сервері, використовуючи логіку завідомо небезпечного компонента щодо прийнятих даних, відбувається порівняння характеристик даних з базою небезпечних даних, щоб визначити, чи є дані однозначно безпечними чи шкідливими.

якщо завідомо небезпечна компонентна логікавизначає, що дані є шкідливими, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

6. Метод заявки 5 також передбачає:

якщо завідомо небезпечна компонентна логікане визначає, що дані є однозначно шкідливими, тоді на сервері за допомогою вирішуючого пристрою виконується аналіз отриманих даних, щоб визначити, чи є дані однозначно безпечними чи шкідливими.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

7. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, це означає отримання сервером даних з мобільного присторою, які є сигналами від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

на сервері для визначення, чи є дані однозначно безпечними, використовується завідомо безпечна компонентна логіка.

якщо завідомо безпечна компонентна логіка визначає, що дані є безпечними, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних.

якщо не досягається позитивний результат, тоді на сервері за допомогою вирішуючого пристрою виконується аналіз отриманих даних, щоб визначити, чи є дані однозначно безпечними чи шкідливими.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

8. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, це означає отримання сервером даних з мобільного пристрою, які є сигналами від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

на сервері для визначення, чи є дані безпечними, використовується логіка завідомо безпечного компонента.

Якщо використання завідомо безпечної компонентної логіки не дає позитивного результату, то для визначення, чи є дані шкідливими, використовується завідомо небезпечна компонентна логіка, а також

якщо завідомо небезпечна компонентна логіка визначає, що дані є небезпечними, сервер надсилає команду пристрою

мобільного зв'язку відхилити обробку прийнятих пристроем даних.

9. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

коли пристрій мобільного зв'язку отримує дані, це означає отримання сервером даних з мобільного пристрою, які є сигналами від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

на сервері для визначення, чи є дані небезпечними, використовується завідомо небезпечна компонентна логіка.

якщо завідомо небезпечна компонентна логіка визначає, що дані є небезпечними, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

якщо на сервері порівняння з завідомо безпечним компонентом дає позитивний результат, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних.

якщо порівняння з завідомо безпечним компонетом не дає позитивний результат, тоді на сервері за допомогою вирішуючого пристрою виконується аналіз отриманих даних, щоб визначити, чи є дані однозначно безпечними чи шкідливими.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.

10. Сервер, який має мережевий інтерфейс для отримання та передачі даних мобільному пристрою, який має програмні компоненти для обробки та аналізу даних, використовує метод, що передбачає наступне:

якщо пристрій мобільного зв'язку отримує дані, використовується завідомо небезпечна компонентна логіка, відбувається отримання сервером даних з мобільного пристрою, які є сигналами від мобільного пристрою, що аналіз даних компонентом безпеки мобільного пристрою не розпізнав дані як однозначно безпечні чи шкідливі.

якщо використання завідомо небезпечної компонентної логіки не дає позитивного результату, то для визначення чи є дані безпечними, сервером використовується завідомо безпечна компонентна логіка.

якщо на сервері порівняння з завідомо безпечним компонентом дає позитивний результат, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних.

якщо порівняння з завідомо безпечним компонетом не дає позитивний результат, тоді на сервері за допомогою вирішуючого пристрою виконується аналіз отриманих даних, щоб визначити, чи є дані однозначно безпечними чи шкідливими.

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є безпечними, сервер надсилає команду пристрою мобільного зв'язку дозволити обробку прийнятих пристроем даних, а також:

якщо аналіз, виконаний вирішуючим пристроєм на сервері, визначає, що дані є шкідливими, сервер надсилає команду пристрою мобільного зв'язку відхилити обробку прийнятих пристроем даних.