УДК 004.738.5

Я.Ю. Дорогий, асист.
С.О. Халавчук, магістрант
Національний технічний університет України «КПІ»

АРХІТЕКТУРА ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ В ІНТЕРНЕТІ

(Представлено д.т.н., проф. Теленик С.Ф.)

Розглянуто питання забезпечення безпеки міжмережевої взаємодії, а саме контролю достовірності інформації про досяжність ресурсів мережі, що передається протоколами маршрутизації, для попередження можливих атак та запропонована архітектура та алгоритми розв'язання даної проблеми.

Постановка проблеми та її актуальність. Взаємодія мереж в Інтернеті будується на протоколах маршрутизації типу "вектор-шлях", тобто без обміну повною інформацією про структуру мереж, тому помилки або зумисні дії можуть призвести до недосяжності певних мереж або таких змін шляху передачі повідомлень, що повідомлення можуть бути перехоплені та змінені зловмисником. Таким чином можливих атак на протоколи маршрутизації та способів їх попередження є актуальною задачею.

Метою даної роботи є розробка рішення, що дозволить доповнити існуючий протокол маршрутизації мережі Інтернет можливостями протидії можливим атакам.

Аналіз існуючих рішень. Історично протоколи маршрутизації вважаються "внутрішніми", тобто вся інформація, яку вони передають, є достовірною і довіреною. Існуючі механізми безпеки, що є частиною сучасних протоколів маршрутизації, – механізми виявлення модифікацій повідомлень за допомогою криптографії та контрольних сум; механізми виявлення повідомлень з невідомих джерел за допомогою секретних паролів; механізми контролю маршрутної інформації на основі статичних фільтрів (списків мереж, часткової інформації про шлях); використання реєстру маршрутної інформації (так званого IRR) для формування правил перевірки повідомлень [1], [2]. Проте ці засоби або не дають рішення проблеми недостовірності інформації, або мають недоліки, що не дозволяють їх використовувати у великих мережах (низька масштабованість, великий час реагування на зміни топології мережі тощо). Існують проекти принципово нових протоколів маршрутизації, що дозволяють поділити топологічну інформацію та інформацію про досяжність мереж. Це дозволяє значно спростити перевірку правдивості інформації, проте через складність переходу від існуючих протоколів вони не впроваджуються [3].

Метою проведення дослідження є доповнення існуючих методів контролю маршрутної інформації такими, що дозволять гарантувати достовірність отримуваної маршрутної інформації та забезпечити максимальну ефективність роботи таких методів навіть у великих мережах.

Суть досліджень. Нагадаємо механізми роботи протоколу BGPv4, описаного в документі RFC4251 [4]. Взаємодія між маршрутизаторами відбувається за допомогою з'єднання TCP, яке забезпечує надійну передачу повідомлень, причому з'єднання налаштовується вручну на обох маршрутизаторах. Існує три основні типи повідомлення: OPEN – узгодження параметрів з'єднання, KEEPALIVE – підтримка з'єднання та визначення досяжності сусіда, UPDATE – передача інформації про досяжність або недосяжність мереж. Автентичність та цілісність повідомлення забезпечується за допомогою механізмів хешування із закритим паролем. Маршрутизатори належать "автономним системам" – групам мереж та маршрутизаторів, що належать одній організації; автономні системи об'єднуються в рамках Інтернету та вважаються найменшою одиницею його маршрутизації.

Нас, у першу чергу, цікавить повідомлення UPDATE. Воно складається з двох частин: списку префіксів мереж, що є недосяжними та вилучаються з таблиці маршрутів, та списку досяжних префіксів мереж та відповідного маршруту до них. Маршрут (англ. path) можна описати як множину необов'язкових та обов'язкових атрибутів (AS_PATH, ORIGIN, NEXTHOP). Маршрутизатор може отримати інформацію про досяжність мережі від кількох сусідніх маршрутизаторів і повинен вибрати найкращий з них (як правило, маршрут з найкоротшим AS_PATH). Найкращий маршрут про досяжність передається сусіднім маршрутизаторам. Проблемою є те, що кожний маршрут при передачі між автономними системами може та буде змінюватись: додається номер автономної системи-відправника маршруту, змінюється атрибут NEXTHOP, можуть додаватись або видалятись атрибути. При цьому протокол не передбачає механізмів захисту від небажаних змін або від повідомлень, що несуть хибну інформацію. А це може призвести до того, що недіючий, хибний або створений зловмисником маршрут буде вибраний як найкращий. Якщо зловмисник може впливати на вибір кращого маршруту, то він може

перехоплювати дані, що будуть передаватись по даному маршруту, або призвести до того, що певна мережа стане недосяжною. Пошуку механізмів протидії таким атакам присвячена дана стаття.

Критеріями оцінки того, що запропоновані механізми є коректним рішенням, є:

1. Можливість гарантувати, що отримане повідомлення UPDATE було відправлене саме сусіднім маршрутизатором, не було змінене при передачі та є актуальним (тобто не старішим, ніж останнє отримане) і що повідомлення адресоване саме нам.
2. Можливість перевірити, що сусідній маршрутизатор, який відправив повідомлення, має право діяти від імені автономної системи, що вказана в повідомленнях.
3. Можливість гарантувати, що перша автономна система в отриманому маршруті має право повідомляти про доступність (або недоступність) даної мережі, тобто що дані префікси мереж належать саме їй.
4. Можливість гарантувати, що сусідній маршрутизатор (а також маршрутизатори попередніх автономних систем маршруту) коректно обробляє повідомлення, не вносить у нього зміни, на які не має права (наприклад, не змінює попередні автономні системи атрибуту AS_PATH).

Крім того, необхідно ввести кількісні оцінки, що дозволять порівнювати варіанти реалізації з метою оцінки ефективності їх роботи. Такими кількісними оцінками обрано:

– обсяг додаткової службової інформації, що необхідно передати для перевірки одного префіксу мережі;

– складність обчислень, які необхідно виконати для прийому та передачі одного повідомлення про досяжність префіксу мережі.

Запропоноване рішення базується на криптографічних механізмах цифрових підписів маршрутної інформації. Головною умовою є використання лише стандартних та взаємозамінних компонентів рішення для забезпечення максимальної гнучкості та сумісності. Для реалізації даних механізмів необхідно розробити та впровадити такі компоненти рішення:

1. Сертифікати, що будуть використовуватись для перевірки підписів.

За основу обрано існуючий стандарт x509 [5]. Даний стандарт дозволяє в сертифікаті вказувати практично всю необхідну інформацію. Необхідно додати лише кілька нових полів: номер автономної системи, що належить організації, список префіксів мереж і термінів їх делегування та зареєстровані автономні системи висхідних провайдерів (upstream providers) [6].

2. Інфраструктура сертифікатів та відкритих ключів, механізми отримання сертифікатів та способи перевірки їх достовірності. Для забезпечення максимальної гнучкості необхідно передбачити незалежність рішення від конкретного механізму розповсюдження сертифікатів. З цією метою необхідно ввести поняття сховища сертифікатів, у якому будуть зберігатися всі відомі маршрутизатору сертифікати. Сховище може поповнюватись:

– вручну, наприклад, запит і отримання сертифіката поштою, імпортування сертифікатів з файлів, ручне налаштування ступеня довіреності сертифіката;

– автоматично, наприклад, по запиту адміністратора сертифікат запитується з централізованого сховища і передається через захищене з'єднання (наприклад, за допомогою протоколів обміну сертифікатами (SCEP [7] тощо);

– за допомогою розширень протоколу BGPv4 в повідомленнях про досяжність префіксів мереж.

Друга проблема готової інфраструктури ключів – дерево довіри. Доцільно прив'язати мережу довіри та центрів видачі сертифікатів до існуючої системи реєстрів видачі об'єктів Інтернету (кореневий реєстр – IANA, реєстри другого рівня – RIPE, ARIN, APNIC, AfriNIC, LACNIC) [8], [9].

Третя проблема – відклик скомпрометованих сертифікатів. Для забезпечення відклику сертифікатів необхідно для кожного виданого сертифіката вказувати інформацію про досяжність списку відкликаних сертифікатів (crl-списку) [10]. Цей список має регулярно оновлюватись та бути доступним засобам протоколу обміну сертифікатами.

3. Механізм підпису маршруту та шляху маршруту, що забезпечить автентичність маршрутних даних, неможливість атак типу "відтворення" (англ. replay), проте дозволить законні зміни атрибутів.

Необхідно ввести новий об'єкт, що містить:

– всі необхідні для зв'язку з криптографічною системою атрибути: інформацію про власника та сертифікат;

– інформацію про алгоритми хешів та асиметричної криптографії;

– цифровий підпис центру видачі сертифіката.

Такий об'єкт зручно створити на базі існуючого стандарту криптографічних повідомлень [11] з додаванням до нього чіткого формату змісту, а саме інформації про об'єкт, що підписується (список мереж, список автономних систем AS_PATH, список атрибутів, зміни яких небажані).

4. Повідомлення та атрибути протоколу BGPv4, що реалізують обмін сертифікатами та підписами. Для реалізації такого розширення протоколу необхідно передбачити такі елементи:

– додаткові коди "можливостей" (англ. capabilities) для виявлення підтримки сусідом даного розширення протоколу та забезпечення сумісності [4];

– додаткові атрибути, що дозволять ідентифікувати маршрути, для яких доступні цифрові підписи, роль такого атрибута виконує розширений атрибут community, що повинен кодувати ідентифікатор домену, в якому використовується єдина інфраструктура сертифікатів та номер версії маршруту;

– додаткові повідомлення: запит об'єкта-підпису, відповідь з об'єктом-підписом, які дозволять запросити окремим повідомленням об'єкт-підпис для заданого шляху або для заданого префіксу мережі, адже через значний розмір об'єкта-підпису його неможливо представити атрибутом.

5. Алгоритм роботи з підписами, створення об'єктів-підписів, обробки повідомлень. Виділено два типи об'єктів-підписів: перший для контролю змін шляху, другий для перевірки прав оголошувати доступність мережі. Розглянемо дії, які повинні виконуватись з кожним з об'єктів при отриманні та відправленні повідомлень.

Автономна система, якій належить мережа, повинна створити об'єкт-підпис, що підтверджує право повідомляти про досяжність мережі та дозволяє перевірити і автономну систему, і її граничний маршрутизатор. Це повідомлення повинне мати певний номер послідовності (можливо, прив'язаний до часу) для попередження атак повтором; інформацію про граничний маршрутизатор та автономну систему, у яку дане повідомлення адресоване. Даний об'єкт зберігається локально в таблиці BGP і при запиті може відправлятись сусіднім маршрутизаторам. При прийомі повідомлення UPDATE, якщо маршрутизатори підтримують дане розширення, вони повинні запитати об'єкт-підпис мережі та перевірити цей підпис. Якщо підпис невірний, повідомлення ігнорується.

Для попередження незаконних модифікацій маршруту AS_PATH автономна система, якій належить мережа, повинна створити об'єкт-підпис шляху автономних систем. Для попередження змін попередніх елементів шляху необхідно реалізувати даний об'єкт як ланцюжок підписів усіх автономних систем, при цьому підпис включає номер наступної автономної системи (якій адресоване повідомлення). Таким чином, перша автономна система повинна включити в нього підпис першої та другої автономної системи AS_PATH, а кожна наступна автономна система повинна додавати підпис наступної автономної системи. Таким чином, є можливість по ланцюжку об'єкт-підпис перевірити кожну автономну систему AS_PATH та виявити незаконні його зміни. При отриманні повідомлення про досяжність мережі маршрутизатор повинен запитати об'єкт-підпис шляху, і при перевірці ланцюжка підписів можна дозволити виконувати перевірку з кінця ланцюжка до першої автономної системи, що є безумовно довіреною. Це дозволить реалізовувати ізольовані групи автономних систем з власною системою довіри, групи довірених автономних систем тощо. Об'єкт-підпис шляху не може існувати у випадку, коли не існує об'єкт-підпис префіксу мережі.

Оскільки дана архітектура передбачає механізми сумісності, необхідно забезпечити налаштування для вибору маршрутів таким чином:

– маршрут, що має об'єкти-підписи, але які не є коректними, має визнаватись недійсним;

– при н аявності двох маршрутів, з яких один має дійсні підписи, а другий не має, пріоритет повинен, безумовно, віддаватися першому;

– при наявності двох маршрутів з дійсними підписами вибір відбувається за стандартним алгоритмом вибору кращого маршруту.

Дана стаття містить загальний опис архітектури забезпечення захищеної маршрутизації та основні обрані рішення та механізми. Повну специфікацію протоколів та алгоритмів навести в одній статті неможливо. Також варто зазначити, що необхідно розробити рекомендації з реалізації та впровадження, стандартизувати зміни в роботі реєстрів Інтернету або способи реалізації окремих груп автономних систем, що бажають використовувати захищену маршрутизацію незалежно від Інтернету.

Висновки. Запропонований метод дозволяє перевірити достовірність маршрутної інформації та попередити можливі атаки на маршрутизацію Інтернету, що можуть призвести до перехоплення даних та відмови в обслуговуванні. Дане рішення складається з інфраструктури ключів і реєстрів маршрутної інформації та розширень існуючого протоколу маршрутизації і дозволяє виконувати поступовий перехід та взаємодію з існуючими рішеннями. Подальшої оптимізації потребує ефективність системи: кількість обчислень та розмір повідомлень нелінійно зростають з ростом складності топології мережі та кількості вузлів.

Область використання. Протоколи маршрутизації між автономними системами, мережа Інтернет.

ЛІТЕРАТУРА:

1. *Martin O. Nicholes* A Survey of Security Techniques for the Border Gateway Protocol (BGP)" / *Martin O. Nicholes*, *Biswanath Mukherjee* // IEEE Communications Surveys and Tutorials. – 2009. – 11 (1).
2. *Rick Kuhn* Border Gateway Protocol Security / *Rick Kuhn*, *Kotikalapudi Sriram*, *Doug Montgomery* // Recommendations of the National Institute of Standards and Technology. – 2007.
3. *Farinacci D.* Locator/ID Separation Protocol (LISP) / *D.Farinacci*, *V.Fuller*, *D.Meyer*, *D.Lewis* // IETF Draft. – 2010.
4. *Rekhter Y.* A Border Gateway Protocol 4 (BGP-4) / *Y.Rekhter*, *T.Li*, *S.Hares* // RFC 4271. – 2006
5. ITU-T. Recommendation X.509: The Directory – Authentication Framework. – 2000.
6. *Lynn C.* X.509 Extensions for IP Addresses and AS Identifiers / *C.Lynn*, *S.Kent*, *K.Seo* // RFC 3779. – 2004.
7. *Pritikin M.* Cisco Systems' Simple Certificate Enrollment Protocol / *M.Pritikin*, *A.Nourse*, *J.Vilhuber* // IETF Draft. – 2009.
8. *Hawkinson J.* Guidelines for creation, selection, and registration of an Autonomous System (AS) / *J.Hawkinson*, *T.Bates* // BCP 6, RFC 1930. – 1996.
9. *Hubbard K.* Internet Registry IP Allocation Guidelines / *K.Hubbard*, *M.Kosters*, *D.Conrad*, *D.Karrenberg, J.Postel* // BCP 12, RFC 2050. – 1996.
10. *Cooper D.* Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile / *D.Cooper*, *S.Santesson*, *S.Farrell*, *S.Boeyen*, *R.Housley*, *W.Polk* // RFC5280. – 2008.
11. *Housley R.* Cryptographic Message Syntax / *R.Housley* // RFC 3852. – 2004.

ДОРОГИЙ Ярослав Юрійович – асистент кафедри автоматики та управління в технічних системах Національного технічного університету України «КПІ».

Наукові інтереси:
– розпізнавання даних;
– штучний інтелект;
– нейронні мережі;
– телекомунікаційні та обчислювальні мережі.

Тел.: +38(097)006–00–25.

E-mail: argusyk@gmail.com

ХАЛАВЧУК Сергій Олегович – студент магістратури кафедри автоматики та управління в технічних системах Національного технічного університету України «КПІ».

Наукові інтереси:
– телекомунікаційні та обчислювальні мережі;
– моделювання телекомунікаційних систем і мереж;
– технології конвергентних мереж.

Тел.: +38(097)905–28–37.

E-mail: sergey.khalavchuk@gmail.com

Подано 15.01.2010

Дорогий Я.Ю., Халавчук С.О. Архітектура забезпечення захищеної міжмережевої взаємодії в Інтернеті.
Дорогой Я.Ю., Халавчук С.О. Архитектура обеспечения защищенного межсетевого взаимодействия в Интернет.
Dorogyy Y.Y., Khalavchuk S.O. Architecture of secure inter-network interaction in Internet.

УДК 004.738.5

Архитектура обеспечения защищенного межсетевого взаимодействия в Интернет / Я.Ю. Дорогой, С.О Халавчук

Рассмотрены вопросы обеспечения безопасности межсетевого взаимодействия, а именно контроля достоверности информации о доступности сетевых ресурсов, которая передается с помощью протоколов маршрутизации с целью предотвращения возможных атак, и предложена архитектура и алгоритмы по решению данной проблемы.

УДК 004.738.5

Architecture of secure inter-network interaction in Internet / Y.Y. Dorogyy, S.O. Khalavchuk

The questions of security interworking, namely the control of reliability of information on the availability of network resources which is transmitted by routing protocols to prevent possible attacks are considered, and proposed architecture and algorithms for solving the problem.