моделювання в обмеженій області параметрів достатньо потужностей персонального комп'ютера. Моделювання дозволило визначити ефективність стратегій генерації стійких еліптичних кривих, а також отримати уявлення про їх кількісний розподіл за рівнями стійкості.

1. *Жданов О.Н.* Применение эллиптических кривых в криптографии / О.Н. Жданов, Т.А. Чалкин. – Красноярск: СибГАУ, 2011. – 65 с.
2. *Баричев С.Г.* Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2002. – С.123.
3. *Lencier R.* Finding good random elliptic curves for cryptosystems defined F2n / R. Lencier // Lecture Notes in Computer Science. – 1997. – Vol.1233. – P.379-392.
4. *Oorschot P.C.* Parallel collision search with cryptanalytic application / P.C. van Oorschot, M.J. Wiener // J. Cryptology. – 1999. – Vol.12. – P.1-28.
5. *Пылин В.В.* Параметры асимметричной криптосистемы на эллиптических кривых / В.В. Пылин // Информационные технологии в профессиональной деятельности и научной работе: сборник материалов региональной научно-практической конференции. – Йошкар-Ола: Марийский государственный технический университет, 2006. – С.90-92.
6. ANSI. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, ANSI X9.62, 1998.
7. *Пылин В.В.* Алгоритмы и методы генерации эллиптической кривой для асимметричной криптосистемы: дис. канд. техн. наук. Марийский. гос. техн. университет, Йошкар-Ола, 2008.
8. Atkin A.O. Elliptic curves and primality proving / A.O. Atkin, F. Morain // Mathematics of Computation. – 1993. – Vol. 61. – P.29-68

Поступила 27.08.2018р.

УДК 004.7

В.Ю. Зубок, Київ

РОЗПІЗНАВАННЯ АНОМАЛІЙ В ГЛОБАЛЬНІЙ ІНТЕРНЕТ-МАРШРУТИЗАЦІЇ ПРИ НЕЧІТКОМУ ОПИСІ ПОДІЙ

Abstract. As part of any network computing system, there are monitoring subsystems – the software which monitors the changes in the numerous network parameters, as well as the state and performance of the servers. It uses flexible alerting mechanisms, allowing the administrator to set up alerts via e-mail, sms, online messengers for virtually any event. Knowledge of the principles and mechanisms of implementing cyber attacks on global routing makes it possible to formulate criteria for changing the status of routing tables under the influence of cyber attacks. Multifactor analysis of the data obtained as a result of observing the changes in the routing tables makes it possible to detect harmful external influences in the absence of clear characteristics of such impact and without a prior description of the inherent

effects of such events. The paper gives an overview of some of the methods of analysis that are acceptable for a given task, and a certain functional approach to detecting anomalies in routing with the help of popular performance monitoring systems.

Актуальність. В останні роки все частіше спостерігаються інциденти з глобальною маршрутизацією в Інтернеті, які перетворюються на нову масштабну кіберзагрозу. Поки що жодного разу офіційно не заявлено, що ці інциденти були атаками. Втім, масштаб цих інцидентів на кілька порядків перевершує широко відомі атаки класу DDoS і Ransomware. Таким же може бути і масштаб збитку, оскільки атака на глобальну маршрутизацію здатна забезпечити шкідливий вплив на мільйони мережевих пристроїв (а також і користувачів) значно меншими зусиллями, ніж згадані вище популярні атаки.

У складі будь-якої ІТС присутні системи моніторингу (контролю працездатності). Програмне забезпечення моніторингу численних параметрів мережі а також стану і працездатності серверів використовує гнучкий механізм повідомлень, що дозволяє користувачам налаштовувати оповіщення по e-mail, sms, онлайн-месенджерам практично для будь-якої події. Накопичення та аналіз даних від таких підсистем дозволяє вести спостереження за груповими відхиленнями від звичайного стану в компонентів ІТС. Такі відхилення, в свою чергу, можуть бути наслідками прихованого шкідливого зовнішнього впливу чи використання ІТС для реалізації кібератак. Знання принципів і механізмів реалізації кібератак на глобальну маршрутизацію дає можливість сформулювати критерії зміни виявлення змін в маршрутизації, що виникли під впливом кібератаки. Багатовекторний аналіз даних, отриманих від систем моніторингу працездатності, дає можливість виявлення штучних втручань в маршрутизацію при відсутності чітких характеристик таких втручань та без попереднього опису притаманних такому впливові подій. Тому необхідно зробити огляд деяких методів аналізу, прийнятних для поставленої задачі, та певний функціональний підхід до розпізнавання аномалій в глобальній маршрутизації за допомогою популярних систем моніторингу працездатності.

Постановка задачі. Системи моніторингу ІТС відстежують критичні характеристики мережі в режимі реального часу або з певною періодичністю, та сигналізують про перехід числових характеристик через певні встановлені рівні. В глобальній маршрутизації задіяні понад 70 тисяч вузлів, що обмінюються понад 700 тисячами маршрутів. Багатовекторний аналіз накопичених даних змін в глобальній маршрутизації може слугувати альтернативним джерелом інформації для виявлення шкідливого зовнішнього впливу при відсутності чітких характеристик такого впливу та без попереднього опису притаманних такому впливові подій. Для цієї мети необхідно:

– розробити моделі збору та накопичення даних про зміни в глобальній маршрутизації за допомогою існуючих та широко вживаних систем моніторингу;
– обрати методи та моделі дослідження даних, зібраних та накопичених системами моніторингу для автоматичного виявлення аномалій, спричинених шкідливим зовнішнім впливом на маршрутизацію.

Аналіз методів та моделей виявлення аномальних станів. Як відомо з принципів організації глобальної маршрутизації та протоколу BGP-4, основним транзитивним параметром, що характеризує привабливість маршруту, є довжина шляху (AS_PATH) [1]. Довжина шляху – це фактор, який дозволяє маршрутам до однакових префіксів конкурувати. Інтернет на цьому рівні являє собою незважений граф, вершинами якого є автономні системи. В загальному випадку граф є циклічним та обов'язково зв'язним. Математично цей граф можна представити або квадратною матрицею суміжності, або квадратною матрицею відстаней розмірності N, де N – кількість вузлів [2].

Якщо існує підмножина вузлів, об’єднана якоюсь сутністю, топологія цієї підмножини може розглядатись окремо. Назвемо цю підмножину цільовою групою вузлів. Такою групою можуть бути вузли – учасники будь-якої мережі обміну трафіком чи вузли-клієнти одного провайдера доступу до Інтернет. Якщо зловмисник вдало провів перехоплення маршруту чи захоплення префіксу, це означає, що для певної цільової групи вузлів маршрут до префікса жертви через вузол зловмисника став коротшим, ніж інші, природні маршрути, а отже – буде перехоплено трафік до цього префіксу від згаданої групи вузлів.

Загалом, аномалії глобальної маршрутизації можуть досліджуватись:
– по змінах в глобальній таблиці маршрутизації у певного Інтернет-вузла;
– по змінах інформації в офіційних реєстрах маршрутів, що мають вільно доступні бази даних;
– за допомогою зовнішніх мережевих сервісів, прикладом яких є BGPmon (www.bgpmon.net).

В залежності від місця дослідження мають бути обрані засоби збору та накопичення даних, а також та методи їхнього дослідження.

Для визначення атаки за характером змін в маршрутизації, система повинна навчатись визнавати нормальний стан вузла та відхилення. Для цього потрібні дві фази: тренування, де будується профіль звичайної поведінки, та тестування, де поточний трафік чи картина подій порівнюється з профілем, створеним на етапі навчання. Аномалії виявляються кількома способами, найчастіше з використанням методів штучного інтелекту. Вже понад 10 років досліджується можливість повністю автоматичного поведінкового аналізу трафіку з метою виявлення атак.

В роботі [3] використовується навчання детектора «типовому» профілю трафіку та виявлення аномалій на основі відстані Магаланобіса. Детектор аномалії фіксує вхідні "корисні навантаження" (payload) та перевіряє корисне навантаження на його узгодженість (або відстань) від моделі центроїда. Це досягається шляхом порівняння двох статистичних розподілів.

Використовувана метрика відстані являє собою метрику відстані Магаланобіса, яка застосовується до кінцевої дискретної гістограми частоти символів, що обчислюються на етапі навчання. Будь-яке нове тестове корисне навантаження, яке виявилося занадто далеким від нормального очікуваного корисного навантаження, вважається аномальним та генерує попередження.

Попередження може бути співвіднесено з іншими даними датчиків, і процес прийняття рішення може відповісти кількома можливими діями. Залежно від політики безпеки захищеного сайту, можна фільтрувати, переадресовувати або навпаки, перехоплювати мережеве з'єднання та доправляти "отруйний" трафік на дослідження.

В роботі [4] пропонуються методи виявлення вторгнень шляхом складання профілю легітимних користувачів. Запропоновано трактування аномалії як події, які впливають на "спектр" трафіку, де обсяг трафіку є одним з показників. Такий трафік-аналіз має дві основні переваги.

По-перше, це дозволяє виявити аномалії, які важко ізолювати дослідженням обсягу трафіку. Деякі аномалії такі як сканування (probing) або специфічні атаки DOS прикладного рівня можуть мати незначний вплив на обсяг трафіку магістральної лінії, і, мабуть, краще можуть бути виявлені шляхом систематичного аналізу змін в розподілі замість зміни обсягу.

По-друге, незвичайні розподіли виявляють цінні відомості про структуру інформаційних аномалій, які відсутні при вимірюванні обсягів трафіку. Досліджується структура впливу аномалії на характер трафіку і за допомогою цього проводиться автоматична класифікація аномалій по значимих категоріях. Автори вважають це прогресом порівняно з евристичним дослідженням аномалій, заснованим на правилах, бо саме такий метод може виявити нові, невідомі аномалії.

Важливим напрямком захисту є виявлення аномалій в поведінці користувачів шляхом аналізу протоколів рівня застосувань. В роботі [5] запропоновано розширену напівмарківську модель для опису поведінки веб-користувачів. Щоб зменшити обсяг обчислень, пов’язану з просторовою складністю моделі, запропоновано модифікований алгоритм.

У якості критерію вимірювання нормальності користувача використовується ентропія його HTTP-запитів. Поведінка користувача описується як періодична зміна станів між «кліком» на гіперпосилання та читанням отриманого матеріалу і описується за допомогою прихованої напівмарківської моделі (HsMM). Веб-сайт, який є потенційно атакованим, описується за допомогою марківського простору станів. Кожен основний напівмарковський стан використовується для представлення унікальної веб-сторінки, натиснутою веб-користувачем. Таким чином, матриця ймовірності

стану переходу представляє відношення гіперпосилання між різними веб-сторінками. Тривалість стану представляє кількість HTTP-запитів, отриманих веб-сервером, коли користувач переходить за «кліком» на відповідну сторінку. Вихідна символьна послідовність кожного стану представляє ті запити на натиснутій сторінці, які проходять через всі проксі або кеш браузера і, нарешті, надходять на веб-сервер.

Метод містить декілька послідовностей спостереження за поведінкою декількох користувачів, отримується алгоритм переоцінки HsMM для декількох послідовностей спостережень за частотою в цій статті. Автори розробили алгоритм переоцінки, встановлюється новий HsMM для опису звичайної поведінки веб-користувачів, просуваючи модель із набору послідовностей запитів, зроблених багатьма звичайними користувачами. Визначається відхилення від середньої ентропії даних тренувань і це й є аномалія спостережуваної послідовності запиту, яку виконує користувач. Чим менше відхилення, тим вище нормальність спостережуваної послідовності.

Огляд систем моніторингу та аналіз придатності для виявлення аномалій в маршрутизації. Існує багато вдалих та широко вживаних рішень з автоматизації такого моніторингу, зокрема, для серверів на базі UNIX-подібних операційних систем. Збір, накопичення та збереження даних для такого аналізу можуть виконувати системи моніторингу працездатності. Найбільш широко вживаними системами, за власними спостереженнями автора, є Nagios, Cacti та Zabbix.

Nagios (офіційний сайт – www.nagios.org) складається з двох складових. Перша – це серверна частина (Nagios Core), основне завдання якої – обробка даних (отриманих від агентів і зовнішніх програм) і оповіщення при досягненні критичних станів. Сервер Nagios встановлюється тільки на Unix-подібні ОС. Для включення в моніторинг будь-якого сервісу чи системи необхідно в конфігураційних файлах прописати їх параметри, а також підключити графіки і плагіни. Статистика може виводитися по хостах, по процесах і службах, по помилках, як окремо, так і у вигляді груп. В результаті виходить сформований звіт зі зведеними таблицями і діаграмами в процентному і числовому співвідношенні за потрібний період, який є помічником при аналізі інцидентів. Можливість розширення штатного функціоналу Nagios досягається за рахунок підключення великої кількості плагінів (ручна установка), які дозволяють створювати свої способи перевірки служб і обробників подій.

Cacti (офіційний сайт – www.cacti.net) є веб-застосунком, збирає статистичні дані за певні часові інтервали і дозволяє відобразити їх у графічному вигляді. Переважно використовуються стандартні шаблони для відображення статистики по завантаженню процесора, виділенню оперативної пам'яті, кількістю запущених процесів, використання вхідного та вихідного трафіку. Для візуалізації використовується стандартний інструмент реєстрації даних RRDtool. Так Cacti дозволяє користувачеві опитати послуги

за заданими інтервалами та графік отриманих даних. Він зазвичай використовується для графіка даних про часові ряди таких показників, як завантаження процесора та використання пропускної здатності мережі. Також звичайно використовується для моніторингу мережевого трафіку шляхом опитування мережевого комутатора або інтерфейсу маршрутизатора через простий протокол керування мережею (SNMP).

Основними особливостями Cacti є:

– гнучкість конфігурування джерел даних за допомогою шаблонів;
– гнучкість механізму та періодичності отримання даних;
– необмежена кількість графічних елементів;
– автоматична побудова мережі у вигляді графа;

Окремої згадки потребує *RRDTool* (офіційний сайт – oss.oetiker.ch/rrdtool/). «Round Robin Database Tool» – це програмний засіб для зберігання, впорядкування та аналізу великої кількості даних від моніторингу. Частина аналізу даних RRDtool базується на здатності швидко генерувати графічні уявлення значень даних, зібраних протягом певного періоду часу. RRDtool приймає дані про часові змінні в інтервалах певної довжини. Цей інтервал, який зазвичай називається «крок», вказується при створенні файлу RRD і не може бути змінений пізніше. Оскільки дані не завжди доступні в потрібний час, RRDtool буде автоматично інтерполювати будь-які надані дані, щоб відповідати його внутрішнім крокам часу.

Значення для певного кроку, який був інтерпольований, називається первинною точкою даних (PDP). Кілька PDP можуть бути об'єднані відповідно до функції консолідації (CF) для формування консолідованої точки даних (CDP). Типова функція консолідації – середня, мінімальна, максимальна.

Після того, як дані були об'єднані, результуючий CDP зберігається в циклічному архіві (RRA). Циклічний архів зберігає фіксовану кількість CDP і вказує, скільки PDP потрібно об'єднати в один CDP і який CF використовувати. Коли архів добіг останнього «кроку», він буде «обертатися»: наступна вставка перезапише найстаріший запис. Завдяки цій властивості бази даних RRDTool завжди мають однаковий фіксований об’єм. Аналіз та візуалізація даних моніторингу є типовими сферами застосування RRDTool.

Zabbix (офіційний сайт – www.zabbix.com) також є системою моніторингу, яка складається з декількох компонентів. Zabbix-сервер – ядро системи, яке може віддалено перевіряти мережеві сервіси і є сховищем, в якому зберігаються всі конфігураційні, статистичні та оперативні дані. До функцій сервера також належить оповіщення. Zabbix-проксі збирає дані про продуктивність і доступність від імені Zabbix-сервера.

Всі зібрані дані заносяться в буфер на локальному рівні та передаються Zabbix-сервера, до якого належить проксі-сервер. Він може бути також використаний для розподілу навантаження одного Zabbix-сервера. В цьому

випадку, проксі тільки збирає дані, тим самим на сервер лягає менше навантаження на процесор і системи введення-виведення. Zabbix-агент – програма контролю локальних ресурсів і додатків (таких як накопичувачі, оперативна пам'ять, статистика процесора і так далі) на мережевих системах, ці системи повинні працювати з запущеним Zabbix-агентом.

Отже, обидві системи надають широкі можливості для моніторингу, звітування, візуалізації зібраних даних. Інструменти моніторингу обох систем допрацьовуються до потреб певної ІТС завдяки широким можливостям конфігураційних параметрів та наявності власних мов скриптового програмування для побудови власних процедур. Також, ці системи чудово піддаються горизонтальному і вертикальному масштабуванню.

Шляхи практичного використання обох систем з метою виявлення аномальних змін в глобальній маршрутизації. Завдяки засобам зберігання та накопичення результатів моніторингу та наявності засобів розширення функціоналу, перелічені системи можуть використовуватись для сигналізування про зміну поведінки елементів системи в разі розробки і підключення модуля для аналізу, який можна назвати аналізом поведінки.

Наступний набір функцій для системи виявлення аномалій дозволить їй функціонувати та розвиватись:

1) збір даних;
2) навчання: визначення характеристик нормального стану;
3) моніторинг;
4) виявлення відхилень;
5) отримання негативного зворотного зв’язку;
6) коригування порогових значень для характеристик нормального стану.

Негативний зворотний зв’язок необхідний для навчання системи. Із плином часу топологія зв’язків між вузлами в Інтернеті змінюється, отже необхідно передбачити можливість автокорекції – переходу аномалії в стан норми.

Розглянемо приклади деяких даних, збір та накопичення яких необхідно забезпечити системами моніторингу для подальшого профілювання системи та виявлення аномалій в глобальній маршрутизації, викликаних кібератаками:

– зміна атрибуту origin у мережевого префіксу;
– поява маршруту до префіксу з іншим origin;
– поява маршруту до «деагрегованого» префіксу, тобто підмережі з довшой маскою;
– зміна довжини кращого маршруту до префіксу;
– поява нового маршруту до префіксу.

Кожна окрема ознака не є чіткою ознакою кібератаки, втім, різні комбінації таких аномалій мають бути досліджені.

Висновок. Знання принципів і механізмів реалізаіцї кібератак на глобальну маршрутизацію дає можливість сформулювати критерії виявлення

аномалій в маршрутизації під впливом кібератаки. Для виявлення таких змін можуть бути використані звичайні системи контролю працездатності (моніторингу) що широко застосовуються в сучасних ІТС. Таке програмне забезпечення пропонує широкі можливості звітності і візуалізації, чудово піддаються горизонтальному і вертикальному масштабуванню.

Багатовекторний аналіз даних, зібраних цими системами, може бути застосований для виявлення аномальних змін під впливом кібератаки, в тому числі дозволить виявляти аномалії маршрутизації від подій, чіткого опису яких ще не існує. Це відкриває перспективу підвищення ефективності виявлення прихованих атак на глобальну маршрутизацію в Інтернеті.

1. *Y.Rekhter, T.Li and S.Hares.* [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc4271. Дата доступу: Чер.29, 2018.
2. *В. Зубок.* Практические аспекты моделирования изменений в топологии глобальных компьютерных сетей // Реєстрація, зберігання і оброб. даних. – 2012. – Т. 14, № 2.
3. *Ke Wang.* Anomalous Payload-Based Network Intrusion Detection / Ke Wang, Salvatore J. Stolfo // RAID 2004: Recent Advances in Intrusion Detection. – P.203-222.
4. *A.S.Syed Navaz.* Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud / A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi // International Journal of Computer Applications (0975 – 8887). – Vol.62. – No.15. – Jan.2013.
5. *Yi Xie.* A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors / Yi Xie, Shun-Zheng Yu // IEEE/ACM Transactions On Networking. – Vol. 17. – №1. – Feb. 2009.

Поступила 10.09.2018р.

УДК 504.054:05 510.24

Т.М. Яцишин, Івано-Франківськ

ВИЗНАЧЕННЯ МЕТОДУ ДОСЛІДЖЕННЯ БАГАТОФАКТОРНИХ СИСТЕМ НА ПРИКЛАДІ РОЗЛИВІВ ФЛЮЇДІВ ПРИ НАФТОГАЗОВИДОБУТКУ

Abstract. The components of the system "Pollutant – Pollution Environment – External Environment" have been considered, where the pollutant is the fluids formed during the life cycle of oil and gas wells, and the environment of pollution – the soil cover. The external and internal factors contributing to the intensity of penetration into the soil of the fluid have been analyzed. The use of the nomogram method for the convenience of representing the results of multifactorial analysis in establishing the negative effects of emergency spills and in the course of regulated technological processes have been proposed.

