Процесс обслуживания имеет распределение с "тяжелым хвостом". В этом случае рассматривается распределение Парето с параметрами, которые оцениваются по экспериментальным данным. Полученная марковская цепь является стационарной, если $p = \lambda\mu_B < 1$.

Таким образом, в докладе предложена модель трафика гибридной компьютерной сети передачи информации системы криминогенного мониторинга Украины, которая учитывает гетерогенный характер сети, особенности слияния трафика от нескольких независимых источников и интегральный трафик обладает распределением с «тяжелым» хвостом, таким как, распределение Паретто.

Список використаних джерел:

1. Можаєв О. О. Передача інформації у гетерогенних комп'ютерних мережах: монографія. Х. : НТУ «ХПІ», 2012. 220 с.

Одержано 17.10.2017

УДК 004.056.53

Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Катерина Костянтинівна ПЕТРОВА,
студентка групи факультету комп'ютерних наук Харківського національного університету радіоелектроніки

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, ЯК ЗАСІБ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Двофакторна автентифікація – це метод ідентифікації користувача в якому-небудь сервісі за допомогою запиту автентифікаційних даних двох різних типів, що забезпечує двошаровий, тобто більш ефективний захист акаунта від несанкціонованого доступу.

Двофакторна автентифікація вже сьогодні застосовується у сфері фінансів при створенні сервісів Internet-банкінгу, мобільного банкінгу і тому подібних рішень для кінцевих користувачів. Вона заснована на спільному використанні декількох чинників автентифікації, що значно підвищує безпеку використання інформації, щонайменше, з боку користувачів, що

підключаються до інформаційних систем по захищених і незахищених каналах комунікацій.

Розглянемо сильні й слабкі сторони двофакторної автентифікації. До переваг можна віднести її здатність захистити інформацію від зовнішніх і внутрішніх загроз, наявних при використанні парольної або однофакторної автентифікації. Додавання другого чинника значно мінімізує вірогідність злому: шанси виникнення ситуації, при якій зловмисник окрім логіна і пароля також оволодів іншим чинником, досить малі, і такий спосіб авторизації є досить надійним. При цьому для забезпечення такого захисту необхідно використовувати додаткові програмно-апаратні комплекси, облаштування зчитування даних, їх зберігання, що вимагає певних витрат на їх придбання, впровадження і обслуговування. Безумовно, для того, щоб автентифікація була насправді надійною, важлива не кількість типів ознак, а й якість реалізації механізму на обох сторонах взаємодії як в частині, що знаходиться у користувача, так і в частині, що знаходиться у перевіряючої сторони. Тому, особливу увагу треба приділити способу зберігання ідентифікаційних даних.

Сьогодні використовуються декілька способів реалізації двофакторної автентифікації. Кожен з них передбачає наявність чинника знання, тобто паролів, які користувачі зберігають у своїй пам'яті, і одного з наступних чинників:

– речовий чинник. В першу чергу, під цим розуміються апаратно-програмні системи ідентифікації і автентифікації. До них належать: токени (електронний (USB) ключ, автономний генератор OTP – One Time Password Token Generator); смарт-карти; телефони/смартфони (відправка SMS з OTP, генератори OTP);

– біометричний чинник (включає біометричні дані, для зняття яких, як правило, потрібні спеціальні програмно-апаратні засоби – так звані, біометричні сканери, які розрізняються за характером даних, що зчитуються. До них належать: відбитки пальців; геометрія рук; райдужна оболонка ока; розпізнавання голосу тощо).

Перш ніж приступити до порівняння систем двофакторної автентифікації, необхідно сформувати вимоги безпеки, яким вони повинні відповідати: безпечно зберігати ідентифікаційну інформацію; забезпечити гарантований захист від крадіжки ідентифікаційних даних через Internet; використовувати одноразові паролі при роботі в не довіреному середовищі; вико-

ристовувати криптографічну стійку автентифікацію при доступі до робочих станцій, веб-порталів, електронної пошти.

Перш ніж зробити вибір методу автентифікації, необхідно зрозуміти принципові відмінності технологій і їх реалізацій в плані адекватності вирішуваної задачі. Так, автономні генератори OTP, генератори OTP в смартфонах найчастіше використовуються для віддаленого доступу до сервісів, додатків, VPN і Web-порталів. Смарт-карти і USB-токени добре себе зарекомендували в шифруванні та підписі пошти, документообігу, корпоративних single-sing-on (технологія єдиного входу) або VPN-доступі. Передача OTP по мобільному зв'язку частіше використовується для віддаленого доступу на платіжні портали і банківські акаунти.

Для того, щоб остаточно визначитися з вибором, необхідно ввести якісні критерії оцінки, що відбивають вимоги безпеки, вимоги до вартості і простоти використання. Загальна вартість складається з вартості придбання і впровадження, а також подальшої підтримки інфраструктури. Вимоги безпеки складаються з вимог до суворості автентифікації, можливості інтеграції з існуючими застосуваннями, надійності засобу в перспективі найближчих років. Безпосередні користувачі системи зацікавлені в простоті використовуваного засобу.

Мають перевагу два методи: USB-ключі і OTP-генератори на смартфоні. Тепер необхідно зробити вибір між ними. Важливо відмітити основні переваги двофакторної автентифікації з використанням OTP. До них належать: застосування одноразових паролів замість статичних; відсутність необхідності встановлювати яке-небудь додаткове програмне забезпечення на клієнтській частині комп'ютерної системи, оскільки користувач вводить пароль вручну, використовуючи ті ж програмні інтерфейси, що і при застосуванні статичних паролів; низька вартість; застосування генераторів OTP можливе в тих випадках, коли користувач не має можливості використовувати USB-порт або він просто відсутній.

Зважаючи на те, що кількість користувачів об'єкту захисту сягає тисяч, недоцільно використовувати USB-ключ з точки зору витрат і умов використання. Таким чином, виходячи з характеристик об'єкту захисту, основних критеріїв вибору, переваг кожного з методів, доцільно зробити вибір на користь OTP-генератора як додатка для смартфону.

Одержано 17.10.2017