УДК 004.056.5

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3381-3350;
Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7755-3071

ПРОТОКОЛИ, МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ НА ТРАНСПОРТНОМУ РІВНІ

Вступ і постановка проблеми. В останнє десятиліття широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управлінні процесами призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах OSI (Open System Interconnection). Особливістю протоколів транспортного рівня таких систем, є відсутність перевірки джерел інформації, що сприяє таким загрозам, як перехоплення та підключення до відкритих портів протоколів транспортного рівня.

Захист від перехоплення потребує застосування додаткових протоколів, які підтримують шифрування даних та автентифікацію суб'єктів обміну даними. Для вирішення цієї задачі використовується протокол SSL/TLS (Secure Socket Layer / Transport Layer Security), який реалізує шифрування і автентифікацію між транспортними рівнями приймача і передавача.

Процедура роботи протоколу SSL/TLS включає в себе три основних фази:

– діалог між сторонами, метою якого є вибір алгоритму шифрування;

– обмін ключами на основі криптосистем з відкритим ключем або автентифікація на основі сертифікатів;

– передачу даних за допомогою симетричних алгоритмів шифрування [1].

Тобто протокол SSL/TLS виконує функції автентифікації, шифрування даних і забезпечення цілісності даних. Автентифікація здійснюється шляхом обміну цифровими сертифікатами при встановленні з'єднання [1]. Так як протокол SSL/TLS реалізується на транспортному рівні, захищене з'єднання встановлюється «з кінця в кінець» (захищений віртуальний тунель транспортного рівня).

Протокол прикладного рівня SSL/TLS зазвичай використовується для забезпечення шифрування HTTP трафіку (режим HTTPS).

Відкритий характер протоколів прикладного рівня зумовлює значну кількість загроз, пов'язаних з основною проблемою цих протоколів – передачею інформації у нешифрованому вигляді. Використання на прикладному рівні процедур ідентифікації та автентифікації користувачів із подальшою авторизацією утворює також загрозу перехоплення або підбору облікових записів та паролів. Значну загрозу також становлять віруси та шпигунське програмне забезпечення, які діють саме на прикладному рівні, DoS та DDoS-атаки на інформаційні системи.

Зазвичай, для засобів захисту комп'ютерних мереж на прикладному рівні, існує два підходи: використання proxy-серверів та використання механізмів контролю сесій (Statefull Inspection). Обидва ці підходи реалізують контроль за з'єднанням, але не вирішують задачу аналізу змісту пакетів та фільтрації пакетів з небажаним змістом, що не дозволяє запобігти розповсюдженню вірусів через електронну пошту, встановленню несанкціонованих програмних додатків через Інтернет на робочі станції, несанкціонованій зміні змісту веб-сайтів тощо. Для захисту від таких порушень може бути використана контентна фільтрація, яка базується на сигнатурному аналізі пакетів. Цей механізм передбачає аналіз інформації у пакеті, при чому як заголовка пакета, так поля даних. Це дозволяє встановити відповідність між інформацією з поля даних та конкретними додатками, контролювати передачу даних між конкретними додатками та проводити фільтрацію небажаної інформації. Враховуючи, що інформація аналізується окремими пакетами, цей механізм не дозволяє повністю аналізувати трафік мережних додатків [2].

Окремо слід відзначити забезпечення безпеки гетерогенних віртуальних обчислювальних середовищ, до яких відносять GRID-системи та «хмарні обчислення» (cloud computing). З кожним роком все більше різних підприємств і вищих навчальних закладів переводять обчислювальні та інформаційні ресурси у віртуальну інфраструктуру. У таких середовищах виникають нові загрози. Перш

за все, це атаки на засоби управління віртуальними машинами, хмарні контролери, сховища даних, неавторизований доступ до вузлів віртуалізації, використання віртуального середовища для несанкціонованої передачі даних.

Можливість проведення наведених атак із віртуальної мережі суттєво обмежує використання традиційних для комп'ютерних мереж методів захисту та потребує розробки спеціалізованих рішень. В основу таких рішень може бути покладено механізми контролю сесій (Statefull Inspection) та пакетної фільтрації. Так, у роботі [2] пропонується підхід до розмежування доступу на основі контролю віртуальних з'єднань та використання скритої фільтрації. Правила фільтрації можуть бути створені для різних рівнів опису потоків даних на підставі заголовків канальних, мережних, транспортних та прикладних протоколів.

Таким чином, враховуючи велику кількість та різноплановість протоколів та програмних додатків прикладного рівня, організувати ефективну протидію загрозам прикладного рівня можна тільки шляхом розробки та реалізації комплексних систем захисту інформації з використанням спеціалізованих механізмів розмежування та контролю доступу до ресурсів мережі, застосування технологій криптографічного захисту та електронних цифрових підписів, але розгляд останніх технологій виходить за рамки даних тез доповіді.

Одним з ефективних рішень комплексного захисту інформаційних систем корпоративних мереж є використання мережі доставки/поширення контенту (Content Delivery Network або Content Distribution Network, CDN). Системи на базі CDN ефективно вирішують питання захисту від DoS та DDoS-атак не тільки на прикладному, а і на мережевому і транспортному рівнях [3].

Провідні виробники мережевого обладнання пропонують спеціалізовані рішення для вирішення задач комплексного захисту корпоративних мереж. Наприклад компанія Cisco пропонує рішення за допомогою технології NAC (Network Admission Control) [4]. Дана технологія дозволяє не тільки перевіряти пристрої та користувачів ще на етапі підключення до корпоративної мережі, а і заблокувати доступ комп'ютерів, які не відповідають політиці безпеки (в тому числі заражених вірусами та шкідливими програмами, де не оновлено антивірусні бази, відсутні необхідні оновлення операційної системи тощо). Контроль відповідності політиці безпеки реалізується максимально близько до можливого джерела порушень – на порту комутатора, точки доступу Wi-Fi або маршрутизатора, які підтримують технологію NAC.

Висновок. Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. При виборі та реалізації технологій

захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи підприємства, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі моделі OSI.

Список бібліографічних посилань

1. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). *Мікросистеми, електроніка та акустика*. 2017. № 6. Том 22. С. 64-70. URL: http://elc.kpi.ua/article/view/113191 (дата звернення: 24.10.2018).

2. Заборовский В. С., Лукашин А. А., Купреенко С. В., Мулюха В.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений. *Вестник Уфимского государственного авиационного технического университета*. 2011. 5 (45). Том. 15. С. 170-174. URL: https://elibrary.ru/item.asp?id=18863047 (дата звернення: 24.10.2018).

3. Козлова М. 7 лучших сервисов защиты от DDoS-атак для повышения безопасности // HOSTING.cafe. 28 марта 2017 14:47. URL: https://habrahabr.ru/company/hosting-cafe/blog/324848/ (дата звернення: 24.10.2018).

4. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. URL: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html (дата звернення: 24.10.2018).

Одержано 24.10.2018