Рис. 2. Класифікація методів захисту від DoS-атак

Основними механізмами захисту проти подібних DoS-атак є:

- захист від DoS-атак на основі рефлексії/ампліфікації. Такі методи захисту спрямовані на виявлення шкідливого трафіку, який був створений при використанні таких протоколів як DNS та SIP та за допомогою різних прикладних методів, таких як, наприклад, технології машинного навчання;
- DDoS-щит - характеристики отриманих HTTP-запитів обчислюються за допомогою статистичних методів та детектор аномалій;
- захист від DDoS-атак типу Tilt призначений для моніторингу мережевого трафіку, і для різних користувачів забезпечує різні можливості.

Гібридні або розподілені механізми забезпечують захист мережі за допомогою взаємодії механізмів захисту як на стороні клієнта, так і на стороні сервера. Прикладами гібридних механізмів захисту є:

- метод Speak-Up. Принцип дії даного методу полягає у диференціації справжніх користувачів від зловмисників. Даний метод використовується для захисту від сесійних флуд-атак;
- метод DOW (Defense and Offense Wall). Даний механізм захисту використовує метод кластеризації K-Means, який призначений для виявлення та фільтрації сесійних атак, флуд-атак на основі запитів та асиметричних атак;
- диференціація DDoS-флуд-ботів від реальних користувачів. Цей механізм призначений для розрізнення звичайних користувачів та мережевих ботів;
- контроль доступу до сервера. Даний метод використовується для обмеження кількості одночасно підключених до сервера клієнтів. Контроль доступу до сервера здійснюється за допомогою приховування портів;
- метод TMH (Trust Management Helmet). В даному методі захисту використовується так зване “управління довірою”, яке призначене для розрізнення звичайних користувачів від зловмисників. Метою методу є забезпечення попереднього захисту зв’язку користувачів під час кібератаки;
- гібридне виявлення. Даний механізм захисту призначений для фільтрування підозрілих потоків та визначення параметрів поведінки користувача у мережі (швидкість HTTP-запиту, час перегляду сторінки).

Науковий керівник – науковий ступінь, д.т.н, доцент, Лисенко С.М.

Безпечна ідентифікація клієнта в протоколах передачі інформації без збереження стану

УДК 004.056.53 (043.2)

Василь Буковецький[1], Василь Різак[2]

Ужгородський Національний Університет, [1]bukovetsky@outlook.com, [2]vrizak@uzhnu.edu.ua

Стрімкий розвиток мережі Інтернет та технологій відкрив шлях до створення динамічних веб-ресурсів та клієнт-серверних додатків, які можуть надавати користувачеві персоналізовані сервіси. Такий функціонал досягається постійним обміном даними клієнтського додатку із сервером. Найпоширенішим

протоколом передачі даних в мережі Інтернет є HTTP, який є протоколом без збереження стану. Використання протоколу без збереження стану потребує постійної передачі ідентифікуючих користувача даних в кожному запиті. Одним з найрозповсюдженіших методів ідентифікації при такій комунікації є прикріплення певного маркера (токена) доступу до кожного нового запиту. Прикладами таких маркерів є ідентифікатор сесії та JSON Web Token.

Передача таких даних через мережу відкриває чимало можливостей для атак, головною ціллю яких буде саме маркер доступу. Отримання цієї інформації дозволить зловмиснику представлятися користувачем, навіть не знаючи його основних даних для входу у веб-сервіс (зазвичай це ім'я користувача та пароль). Такими веб-сервісами можуть бути онлайн-банкінг, керування системою розумного будинку, тощо.

Найрозповсюдженішим методом захисту є використання шифрування протоколів SSL/TLS. SSL/TLS — криптографічні протоколи, які забезпечують встановлення безпечного з'єднання між клієнтом та сервером.

Саме на ці криптографічні протоколи покладається функція захисту конфіденційності даних в більшості сучасних веб-додатків, відповідно саме ці протоколи захищають такі важливі дані як маркери доступу.

Нажаль, протоколи HTTPS та SSL/TLS мають свої недоліки та по тим чи іншим причинам можуть не вберегти конфіденційні маркери доступу від рук зловмисника

Метою даної роботи є покращення захисту маркерів доступу за допомогою методу ідентифікації клієнта, в якому ідентифікатор сесії не буде передаватись в доступному для використання зловмисником виді.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної

відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

При використанні запропонованого методу, даних які відправляються з кожним запитом не буде достатньо для формування зловмисником нового запиту від імені справжнього користувача. Звичайно, такий метод передачі не захистить дані які відправляються від розкриття, але значно зменшить шанси зловмисника на отримання повного контролю над обліковим записом користувача.

Слід зауважити, що маркери доступу можуть бути перехоплені при початковому обміну секретом, тому на цьому етапі рекомендується використовувати протокол Діффі-Гелмана (або аналогічний асиметричний протокол) для обміну ключами та подальшій зашифрованій передачі секрету.

ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЄЮ СУЧАСНОЇ КОМПАНІЇ

УДК: 330.47

Людмила Кургузенкова

Приватний вищий навчальний заклад «Європейський університет»

kurguzenkova@ukr.net

У умовах сьогодення, коли четверта промислова революція (4IR) має яскраві прояви майже у всіх сферах життєдіяльності, цінність інформації як фактора конкурентоспроможності сучасних компаній набуває дедалі вагомішого значення. Сучасним компаніям доводиться вести діяльність в умовах стрімких змін, жорсткої конкурентної боротьби, необхідності забезпечення індивідуального підходу до кожного клієнта і підвищених вимог урядів і регуляторів до термінів підготовки звітності і достовірності наданої інформації. Коли доступ до традиційних ресурсів стає відкритим, коли майже зникають границі між економічними регіонами та системами внаслідок активного застосування інформаційно-комунікаційних технологій, коли класичні підходи до забезпечення конкурентоспроможності не спрацьовують, об'єктивно виникають передумови для пошуку нових джерел конкурентних переваг, перш за все — «всередині» організації, що знаходить своє відображення в концепції інформаційного менеджменту.

Управління інформацією (Enterprise Information Management, EIM) є окремою галуззю знань, метою якого є координація діяльності по роботі з інформацією, включаючи інформаційні технології, інформаційну безпеку, маркетинг, рекламу; спеціалізується на рішеннях щодо раціонального використання інформації в межах організацій, наприклад, для підтримки управлінських рішень або операційної діяльності, що вимагає наявності знань.