УДК 004.732
Шинкар П. – гр. СН-51
Тернопільський національний технічний університет імені Івана Пулюя

АНОНІМНІ МЕРЕЖІ ТА TIMING-АТАКИ

Науковий керівник: к.т.н. Козак Р. О.

Уперше анонімні системи зв'язку були представлені у фундаментальній роботі Чаума (Chaum 1981). Анонімність досягається шляхом пересилання повідомлень через серію передаючих вузлів – mix-вузли. Кожний mix-вузол виконує два основні завдання:

- забезпечення побітової нерозрізненості (bitwise unlinkability) повідомлень;
- перемішування потоку повідомлень.

Щоб на виході з вузла зловмисник (атакуючий) не зміг ідентифікувати повідомлення за його змістом, всі вхідні повідомлення зводяться до одного розміру (короткі повідомлення доповнюються випадковими даними) і шифруються. Власне, це і є "забезпечення побітової нерозрізненості". Перемішування потоку повідомлень використовується для того, щоб атакуючий не зміг зіставити час входу повідомлення у вузол з часом його виходу, і в такий спосіб зрозуміти, яке саме вихідне повідомлення відповідає шуканому. Вузол якийсь час накопичує вхідні повідомлення, перемішує їх і відправляє далі у випадковому порядку.

Системи анонімного зв'язку через Інтернет можна розділити на дві категорії: системи з великими затримками (high-latency systems); системи з малими затримками (low-latency systems).

Повідомлення у системах обох категорій неможливо простежити завдяки реалізації ідей Чаума: ланцюжка вузлів між відправником і одержувачем, і шифрування, що приховує дані повідомлення. Кожний вузол у ланцюзі знає тільки свого попередника, від кого він одержав повідомлення, і свого спадкоємця, якому він передасть повідомлення. Системи з більшими затримками спеціалізуються на пересиланні одиночних повідомлень, а системи з малими затримками на підтримці з'єднання. Це означає, що в системах з більшими затримками для кожного повідомлення створюється свій новий шлях, нове повідомлення – новий шлях. А в системах з малими затримками один шлях використовується в плині деякого часу для пересилання цілого потоку пакетів. Такі системи більше уразливі до атак аналізу трафіку, зокрема, до timing-атак. Прості timing- атаки можуть зводитися до обчислення часу, який потрібний пакету, щоб пройти мережу. Більше складні timing-атаки можуть включати аналіз відмінних рис використовуваного жертвою з'єднання – виявлення патерна трафіку.

Timing-атаки використовують той факт, що всі вузли мережі вводять різні затримки. Знаючи час затримок, можна здогадатись про зв'язок вхідних у вузол і вихідних з нього потоків. Іншими словами, вгадати, який вихідний потік відповідає вхідному потоку, що відслідковується. Атакуючий може якийсь час спостерігати за зв'язками між вузлами, а потім, порівнюючи патерни трафіку всіх вузлів, виявити вузли зі схожими патернами – імовірно ці вузли утворять ланцюжок. Використовуючи статистичні методи, атакуючий може одержати інформацію про відправника й одержувача потоку, і навіть виявити весь шлях потоку. Для захисту від цієї атаки потрібно зробити так, щоб тимчасові характеристики всіх потоків були нерозрізнені. Для успішного проведення вищезгаданої атаки потрібний глобальний спостерігач, здатний спостерігати за всіма потоками, що проходять через мережу. Вважають, що анонімізуючі мережі з малими затримками, такі як Tor, можуть успішно протистояти більш слабкій моделі загроз, що не включає глобального спостерігача.