Звернемо увагу, що наше ключове значення не буде таким же, як зазначено вище. Кожен рядок списку включає ім'я та ключове значення. Коли ми викликаємо зробити mica2, перший ключ в ключ за замовчуванням файл буде встановлений. Це означає, що за замовчуванням, якщо ми встановимо програму на один сучок з нашого ноутбука, і встановимо програми на інший сучок на робочому столі, вони не зможуть взаємодіяти. Це відбувається тому, що вони будуть використовувати різні ключі. Таким чином, нам необхідно виконати одну з таких дій:

• використовувати той же ключ-файл на обох комп'ютерах

• скопіюйте ключовий файл з вашого ноутбука на робочому столі, перейменування файлів на "ноутбук-файл ключа". Тоді, при створенні на робочому столі, використання нових ключовий файл, якщо ви хочете створити порошинки, що "Інтер- працювати з порошинки запрограмований з ноутбуком:

зробити mica2 KEYFILE = ноутбук-Keyfile

• копія лінії від ключового файлу в якому йдеться "за замовчуванням 6D524 ..." з ноутбука на робочому столі ключового файлу (. ключовий файл). Крім того, перейменувати ярлик ключ від "за умовчанням" на "ноутбук". Потім, коли Будівля на робочому столі, використовуйте новий ключовий файл, якщо ви хочете створити порошинки, які взаємодіють з порошинками запрограмованими з ноутбуком:

зробити mica2 KeyName = ноутбук

Оновлення ключів. Інтерфейс TinySecControl експортує компоненти TinySecC, що дозволяє оновлювати ключі TinySec і запити і скидання вектором ініціалізації (IV). Інтерфейс TinySecControl має шість команд:

Команда result_t updateMACKey (uint8_t * Маккі);

Команда result_t getMACKey (uint8_t результат *);

Команда result_t updateEncryptionKey (uint8_t encryptionKey *);

Команда result_t getEncryptionKey (uint8_t результат *);

Команда result_t resetIV ();

Команда result_t getIV (uint8_t результат *)

Ці команди повернення будуть успішними, якщо ключ оновлено успішно.

Список використаних джерел

1. Романюк В.А. Мобильные радиосети-перспективы беспроводных технологий //Сети и телекоммуникации. –2003. – № 12. – С. 53 – 58.

2. J. Campbell, P.B. Gibbons, S. Nath, P. Pillai, S. Seshan,R. Sukthankar, IrisNet: an Internet-scale architecture for multimedia sensors, in: Proc. of the ACM Multimedia Conference, 2005.

3. P. Kulkarni, D. Ganesan, P. Shenoy, Q. Lu, Sens Eye: a multi-tier camera sensor network, in: Proc. of ACM Multimedia, Singapore, November 2005.

УДК 681.3.06

ПРОГРАМНЕ СЕРЕДОВИЩЕ ТА АПАРАТНІ ЗАСОБИ ОРГАНІЗАЦІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ СТІЙКОЇ ДО АТАК ТИПУ DOS/DDOS

Гончар Л.І., Сикотинська І.В.
Тернопільський національний економічний університет

Атаки відмови послуг становлять одну з найбільших загроз в мережі Інтернет. На сьогодні відсутній результативний та універсальний метод цілковитого запобігання цього типу атакам. Додатково, для здійснення атаки DoS/DdoS не треба володіти ґрунтовними знаннями в цій галузі. Це зумовлює виробників до створення щораз сучасніших технологій та засобів захисту комп'ютерних мереж (КМ) [3].

Найчастіше використовуються такі засоби захисту КМ:

- списки контролю доступу ACL (Access Control List);
- firewall;
- системи викриття зловмисників IDS (Intrusion Detection Systems) – NIDS, HIDS, NNIDS;
- система запобігання взломам IPS (Intrusion Prevention Systems) – In-Line IDS, інтегрований IDS із firewall).

Списки контролю доступу призначені для обмеження та контролю вхідного та вихідного трафіку в мережі або в її сегменті. Вони є частиною firewall зовнішніх і внутрішніх мережевих маршрутизаторів. В порівнянні з мережевими firewall, списки контролю доступу не надають функціональності, яка опирається на стані приєднання. Їх завданням на маршрутизаторах є часто здійснення вступного фільтрування пакетів перед мережевим firewall. Деяким імплементаціям ACL притаманні великі можливості контролю руху, зокрема спискам ACL, доступним на маршрутизаторах фірми CISCO.

Списки ACL дають змогу фільтрувати рух при атаках DoS і DDoS, в тому числі:

- атака SYN Flood;
- атака Land;
- атака Smurf;
- атаки, що опираються на протокол ICMP, зокрема ping Of Death.

Крім цього, списки контролю доступу дозволяють захиститися від деяких атак фальшування інформації (атаки Spoofing).

Мережевий firewall становить один засіб або набір засобів та має на меті запобігати рухові до захищеної мережі. Більшість мережевих пристроїв, зокрема маршрутизатори, містять нескладні фільтри пакетів, що пристосовані до вимог цього пристрою. Однак інколи маршрутизатор може становити лише частину цілої системи мережевого firewall. Firewall може бути також програма, яка дозволяє фільтрування на вищих рівнях моделі OSI.

На сьогодні мережеві firewall додаються до багатьох пристроїв, зокрема маршрутизаторів, безпровідних пунктів доступу, мостів IP. Також всі популярні операційні системи містять програмову імплементацію firewall. Однією з найпопулярніших є iptables, що призначена для системи Linux.

Firewall становить лише частину системи захисту. Для того, щоб ця система була найбільш ефективною, то її слід доповнити системою викриття зловмисників IDS. Метою цієї системи є моніторинг і повідомлення про підозрілі випадки. Викриття аномалії в мережі або на пристрої зумовить запис інформації в логах і повідомлення відповідних осіб. Дія системи IDS полягає в прослуховуванні мережевого руху та ідентифікації небезпечних дій в мережі .

Система IDS, окрім проведення аналізу пакетів, забезпечує аналіз потоку даних, що дозволяє викрити атаку в уявно правильних пакетах. Крім ідентифікації взлому чи атак, система IDS інформує також про спроби, які мають за мету підготовку до здійснення атаки, а саме – сканування портів, тощо.

Поява аномалій, пов’язаних з рухом в мережі, також підлягає контролю за допомогою цієї системи. Система IDS інформує про помилки в переданих пакетах.

Наприклад, помилка в полі зсуву пакету IP може свідчити про здійснення атаки типу Smurf або про пошкодження певного мережевого пристрою [1].

Також може трапитися, коли в мережі появиться велика кількість пакетів з малим полем TTL. Пакет не утворений помилково, лише значна кількість появи цього типу пакетів на даний момент може також свідчити про певну загрозу.

Тоді немає впевненості щодо причини, яка зумовлює цей випадок, оскільки такі пакети створюються діагностичною програмою traceroute.

Функціонування системи IDS полягає у розпізнаванні підозрілих дій шляхом прослуховування руху та пошук сигнатур атак, аномалій та ознак неправильних дій в мережі, що свідчать про атаку У системі IDS застосовано такі способи виявлення атак:

- виявлення атак, що базується на сигнатурах;
- дослідження частоти появи подій.

Кожний з цих методів є ефективним для виявлення атак DoS/DDoS та атак фальшування. До однієї з систем IDS належить програма Snort, яка є доступною в системі Unix. Містить вона комплект понад 2000 сигнатур, включаючи сигнатури атак DoS/DDoS. Згадані сигнатури базуються на характеристичних рисах кожного типу атаки.

В порівнянні з системою IDS більш функціональною є система IPS. Подібно як IDS виявляє спроби атаки, лише її дія не закінчується на інформуванні про них, але й на прийнятті відповідних дій, що забезпечують захист мережі. Система IPS базується на системі IDS, лише остання є розширена на механізм мережевого firewall [2].

Завдяки цьому можна уникнути атак DoS, що грунтуються на протоколах мережевого або транспортного рівня, зокрема атак UDP Flood, SYN Flood, ICMP Flood, IP Spoofing. Системами IPS є:

- In-Line IDS;

- комутатори 7-го рівня;
- інтегрований IDS з мережевим firewall;
- гібридні комутатори.

Крім застосування систем IDS чи мережевих firewall є можливість захисту від цього типу атак на більшості мережевих пристроїв, таких як маршрутизатори, безпровідні пункти доступу, міжмережеві інтерфейси VoIP, тощо шляхом активізації опції операційних систем пристроїв. Їх можливості не такими широкими в порівнянні з вищенаведеними системами, а лише становлять відповідне забезпечення для малих КМ. Нижче можемо побачити приклад міжмережевого інтерфейсу VoIP і маршрутизатора, що запобігають перед атаками DoS/DdoS (рис.1).

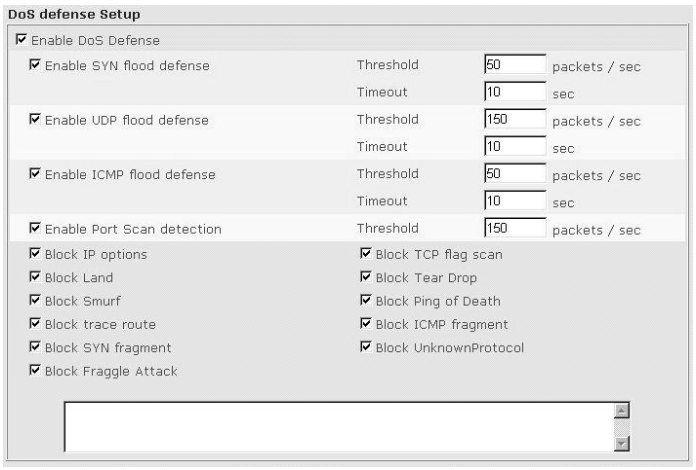

Рисунок 1. – Інтерфейс маршрутизатора при захисті від атак типу DoS/DDoS

Таким чином, в атаках типу DoS/DDoS загалом використовують прогалини існуючих інформаційних систем чи недосконалості специфікації мережевих протоколів. Слід використовувати операційні системи з високим рівнем захисту та безпечне програмне забезпечення, призначене для серверів мережевих послуг.

Список використаних джерел

1. http://www.netfilter.org.
2. http://www.snort.org/.
3. А.В. Уланов, И.В. Котенко Защита от Ddos-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. INSIDE, №1-3,2007.
4. Ганьжа Д. Мосты в локальних сетях // LAN Magazine,2006, №1.

УДК 004.056.5

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОТОКОЛУ IPSEC

Шевчук Р.П., Геник Г.Я.
Тернопільський національний економічний університет

І. Постановка проблеми

У сучасних телекомунікаційних системах широко використовуються протоколи захищеної передачі даних, де вирішення задач забезпечення конфіденційності, цілісності та автентичності інформації досягається шляхом криптографічного перетворення даних. Одним із основних криптографічних протоколів є IPSec (Internet Protocol Security) [1].

Зростання швидкості та об’ємів передавання даних, кількості одночасно працюючих захищених мереж приводять до зростання вимог щодо продуктивності оброблення даних згідно з протоколом IPSec. Реалізація оброблення даних згідно з протоколом IPSec базується на сумісному використанні як програмованих, так і спеціалізованих процесорів. Однак, існуючі структури операційних пристроїв процесорів IPSec створюються з недостатнім врахуванням особливостей комп’ютерних мереж, де ці процесори застосовуються. Зокрема, структури операційних пристроїв цих процесорів проектують так, щоб отримати мінімальні затрати обладнання. Часто ця вимога приводить до зменшення