УДК 004.49

Білий В.С.
Кіровоградський національний технічний університет

Огляд методів захисту електронної пошти

В умовах широкого поширення глобальної мережі Інтернет в сучасному світі, зокрема на підприємствах та установах найвищого рівня, значення електронної пошти, як засобу швидкого пересилання повідомлень, документів, графічних, аудіо- та відеоматеріалів складно переоцінити. Надійність захисту даних в системі електронної пошти має безпосередній захист на загальний рівень інформаційної безпеки організації і, як наслідок, на ефективність її діяльності, що обумовлює важливість створення надійного захисту цього виду комунікацій.

Спам, лавинне розсилання, витік конфіденційної інформації - основні проблеми, з якими зустрічаються користувачі електронної пошти - пов’язані з недостатнім рівнем захисту сучасних поштових систем.

Розробники систем, спрямованих на захист електронної пошти, на власному досвіді знають, що миттєве вирішення проблеми захисту таких систем неможливе, оскільки хакери, творці та розповсюджувачі вірусів винахідливі, що спонукає постійно розвивати та вдосконалювати методи захисту. Слід також враховувати, що для забезпечення найвищого рівня захисту, необхідно застосовувати комплексний та систематичний підхід, з урахуванням всіх загроз та ризиків щодо безпеки пересилання електронних листів.

PGP (від англ. Pretty Good Privacy - «Досить хороша приватність») комп'ютерна програма, а також бібліотека функцій, що дозволяє виконувати операції шифрування та цифрового підпису повідомлень, файлів та іншої інформації, що представлена в електронному вигляді, в тому числі прозоре шифрування даних на запам’ятовуючих пристроях, наприклад, на жорсткому диску.

Перевагою такого методу є наявність сервера ключів keyserver.pgp.com., який дозволяє користувачам обмінюватись ключами та усуває необхідність публікації ключів, або передавати їх кожному адресату в особистому порядку. До особливостей програми слід також віднести її спосіб захисту електронної пошти, точніше перехоплення трафіку поштового клієнта на рівні драйвера. Система опрацьовує трафік, шифрує повідомлення, що надсилаються і автоматично розшифровує вхідні повідомлення.

Цей метод має і свої недоліки, а саме: вже розшифровані повідомлення залишаються незахищеними в клієнті. Проблемою також є те, що якщо поштовий клієнт вже отримав повідомлення, а PGP Desktop не було запущено, то дешифрування листа стає непосильною задачею. Було розроблено спеціальні плагіни на такий випадок, але наразі їхня робота не є досить стабільною та задовільною.

S/MIME (від англ. Secure/Multipurpose Internet Mail Extensions – «Безпечне/багатоцільове розширення для електронної пошти») — це стандарт для шифрування і підпису в електронній пошті за допомогою відкритого ключа. Під час роботи реалізується класична схема асиметричного шифрування з усіма її недоліками та перевагами, а саме: користувач генерує відкритий та закритий ключ, налаштовує свій поштовий клієнт і надсилає відкритий ключ всім бажаючим, які шифрують свої листи

отриманим ключем і дешифруються лише закритим ключем.

Переваги S/MIME:

- листи в поштовому клієнті лишаються зашифрованими до тих пір, доки користувач сам їх не розшифрує. Для здійснення операції дешифрування необхідне введення паролю, що вказується під час створення ключової пари (відкритого/закритого ключа);

- на відміну від PGP Desktop, дешифрування відбувається поштовим клієнтом, а не окремою програмою, тому розшифрувати лист можна за будь-якої нагоди;

- підтримка більшості поштових клієнтів (в тому числі мобільних).

Недоліками є перш за все те, що постає питання про програму, яка згенерувала б сертифікат. Також необхідно обдумати питання реалізації обміну ключами між учасниками. Потрібно також згадати про складнощі при зміні ключа, особливо, якщо користувачі не повністю розуміють суть своїх дій.

Однак, для нівелювання недоліків S/MIME було створено спеціальний плагін CyberSafe Mail, що дозволяє публікувати свій ключ на сервері ключів. Також є можливість пошуку ключів, опублікованих іншими користувачами. Втім, даний плагін доступний поки що лише для Microsoft Outlook.

HushMail – сервіс електронної пошти з шифруванням. Користується великим популярністю у недосвідчених користувачів, як захищений сервіс, що не потребує попередніх налаштувань і одразу готовий до роботи. Перевагами такої і подібних їй систем є простота у використанні та відсутність необхідності налаштувань. Недоліком же є здійснення криптографічних операцій на сервері.

Також для здійснення захисту електронної пошти застосовуються різні плагіни для браузерів:

1) плагін браузера PGP Mail. Даний плагін використовує асиметричне шифрування на стороні клієнта та підтримує браузери Firefox, Chrome, Opera, Safari. Недоліками є рекомендації щодо використання TOR (система забезпечення анонімності в мережі Інтернет), що не є зручним для недосвідчених користувачів та маленька кількість підтримуваних браузерів.

2) плагін браузера SecureGmail ввикористовує симетричне шифрування, що є зручним лише при спілкування з невеликою кількістю адресатів. Також цей плагін працює лише з браузером Chrome.

3) плагін браузера Encrypted Communication за своїми можливостями схожий на SecureGmail, але працює лише в браузері Firefox.

Найпростіший спосіб захисту електронної пошти – використання симетричного шифрування. Для його реалізації можна використовувати плагіни браузера SecureGmail і Encrypted Communication. Для забезпечення більш надійного захисту конфіденційності даних в ідеалі рекомендується використовувати S/MIME, надійність якого полягає в тому, що повідомлення зберігаються в поштовому клієнті в зашифрованому вигляді і розшифровуються лише при зверненні до них.

Список використаних джерел

1. *Защита электронной почты: [Електронний ресурс]. – Режим доступу: http://www.ibm.com/support/knowledgecenter/ru/ssw_ibm_i_71/rzaj4/rzaj45zoemail.htm.*
2. *Защита почты: [Електронний ресурс]. – Режим доступу: http://cybersafesoft.com/rus/blogs/cybersafe-mail/.*
3. *Защита электронной почты: [Електронний ресурс]. – Режим доступу: http://infocity.kiev.ua/hack/content/hack213.phtml.*
4. *Обзор средств защиты электронной почты: [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/cybersafe/blog/269513/.*