субекспоненціальні методи. В результаті рівень стійкості, який досягається в RSA за допомогою 1024-бітових модулів, реалізується в системах на ЕК 160-бітним модулем.

В ході роботи розроблено систему обміну повідомленнями з використанням шифрування та архітектури системи, в основі якої лежить мережа, заснована на принципі рівноправності учасників, яка характеризується тим, що всі елементи мережі є автономними та можуть зв'язуватись між собою (вузли одночасно функціонують як клієнт та сервер) на відміну від клієнт-серверної архітектури, яка вимагає центрального сервера.

Програма для обміну повідомленнями написана на мові програмування Python [2], що дозволяє їй бути крос-платформенною та виконуватись на різних операційних системах (Windows, Linux, MacOS X). Також використання Python дає можливість редагування програми під конкретні потреби без її подальшої компіляції, так як Python використовує інтерпретацію замість компіляції.

Висновок

У даній роботі розроблено програмну реалізацію захищеного каналу обміну повідомленнями з використаням апарату ЕК.

Список використаних джерел

1. Болотов А.А. Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. - М.:КомКнига, 2006. – 280 с.
2. Прохоренок Н.А. Python 3 и PyQt. Разработка приложений / Н.А. Прохоренок. - Спб.:БХВ-Петербург, 2012. - 704 с.

УДК 004.056.5

МЕТОДИ ЗАХИСТУ КОРИСТУВАЧІВ ВІД ВІДСЛІДКОВУВАННЯ В НАПРАВЛЕНИХ АТАКАХ ІЗ ЗАСТОСУВАННЯМ ДОКУМЕНТІВ MICROSOFT OFFICE

Крахмалюк І.Г.

Національний технічний університет України "Київський політехнічний інститут", студент

І. Постановка проблеми

Програмне забезпечення Microsoft Office являється одним із найбільш розповсюджених офісних пакетів. Воно є стандартом де-факто обміну документами в корпоративних та державних інформаційних системах. В контексті інформаційної безпеки наслідком популярності стала активізація досліджень методів вторгнення із застосуванням документів Microsoft Office як засобу доставлення шкідливого програмного забезпечення у випадку цільових атак з боку кримінальних структур та доставлення систем легального перехоплення при проведенні слідчих дій уповноваженими державними органами.

Крім віддаленого виконання коду при відкритті документів в багатьох випадках важливою є ідентифікація факту відкриття документу, встановлення IP адреси користувача та конфігурації програмного забезпечення (версія MS Office та можливо іншого встановленого ПЗ). Наявність IP адреси користувача у випадку легального застосування може допомогти ідентифікувати фізичне місцезнаходження зловмисника, або у випадку цільової атаки перейти до аналізу вразливостей мережевого устаткування. Знання точної версії ПЗ дозволяє підвищити надійність експлоітів для віддаленого виконання коду в обох випадках.

В даній роботі пропонується метод захисту від атак деанонімізації користувачів із застосуванням документів Microsoft Office.

ІІ. Мета роботи

Метою даної роботи є запропонування методів захисту користувачів від відслідковування через документи Microsoft Office та дослідження їх ефективності на прикладі моделі системи деанонімізації, що використовує відслідковуючі посилання на зображення.

ІІІ. Використання малодокументованих частин функції Mail Merge для відслідковування розповсюдження документів формату Microsoft Office

Починаючи з ранніх версій офісний пакет Microsoft Office включає в собі функцію Mail Merge, яка дозволяє створювати поштові листи за попередньо визначеними шаблонами. Недокументованою функцією є підтримка контрольних слів (control words), пов'язаних з функцією Mail Merge у звичайних документах. Одним з таких слів є контрольне слово додавання зображення в документ.

Джерелом такого зображення може бути не лише локальний файл – а й гіпертекстове посилання. Програмне забезпечення Microsoft Office автоматично та без участі користувача спробує завантажити файл за даним посиланням при відкритті документу. У заголовках HTTP-запиту офісний пакет передає інформацію про версію операційної системи, встановлених версій .NET Framework та власну версію. При виконанні запиту автор документу також дізнається IP-адресу користувача, що відкрив документ.

IV. Модель атаки

В якості відслідковуючого посилання використовується посилання на картинку в форматі PNG розміром 1 на 1 піксель (завдяки цьому картинка невидима користувачу), додатково в строці запиту передається ідентифікатор документу (наприклад, довільне число).

Було створено програму на мові програмування Python, що дозволяє додати відслідковуюче посилання в довільний RTF документ. При відкритті модифікованого документу виконається завантаження контенту з контрольованого серверу.

Автор документу отримує IP-адресу користувача та додаткову інформацію у заголовках запиту (наприклад, «Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 14)» у заголовку User-Agent).

V. Захист від відслідковування

Пропонується гібридний метод на основі статичного аналізу аномальних елементів документів Microsoft Office та поведінкового аналізу при виконанні в контрольованому середовищі.

Розглянуті техніки відслідковування вимагають застосування контрольних слів та інших сутностей, нехарактерних для звичайних (легітимних) документів. Цей факт дає змогу системам захисту виявляти подібні аномалії в документах та захищати користувачів від розкриття інформації про них.

Швидким та досить ефективним методом захисту є виявлення відомих загроз та аномалій за допомогою парсерів та аналізаторів структури документу – цей метод може застосовуватись «на льоту» (наприклад, при надходженні пошти), проте він не гарантує абсолютного захисту та може пропускати нові невідомі види загроз (структура яких невідома).

Повільнішим (та надійнішим) є метод поведінкового аналізу – наприклад, запуск у «пісочниці» та моніторинг мережевої (та іншої підозрілої) активності. Цей метод дозволяє не лише виявити загрозу, а й вивчити її, проте, водночас, вимагає більшої кількості часу та ресурсів.

Висновок

У роботі запропоновано методи захисту користувачів від відслідковування через документи Microsoft Office. Запропоновані методи доведено до практичної реалізації та досліджено їх ефективність на прикладі моделі системи деанонімізації, що використовує спеціально сформовані посилання на зовнішні ресурси.

Список використаних джерел

1. Microsoft Corporation. Rich Text Format (RTF) Specification, version 1.9.1 - http://www.microsoft.com/en-us/download/details.aspx?id=10725
2. Mail merge - https://support.office.com/en-US/article/Mail-merge-507b5468-f771-485d-9ef0-27857168a266
3. How Call-Home Tracks PDF and Office Documents - http://stage.callhome.it/how-call-home-tracks-PDFs-and-Office-documents-that-already-exist-call-home.html
4. Document Tracking Service - http://www.readnotify.com/readnotify/pmdoctrack.asp
5. A peek inside ReadNotify - http://blog.jgc.org/2006/10/peek-inside-readnotify.html