Метод захисту файлових серверів на основі гешування

ст. гр. ЗІ-14м Миронюк В.В.

наук. керівн. к.т.н. доцент Баришев Ю.В.

Вінниця 2015

Актуальність, об’єкт, предмет дослідження

Необхідність розробки нових файлових серверів зумовлена відкритістю процесу автентифікації для зловмисника, який спостерігає за каналом обміну інформацією.

Запропоновано використовувати стійке до загальних атак гешування користувацьких паролів та використовувати геш-значення як ключів для шифрування.

Об’єктом МКР є процес передачі даних при використанні файлових серверів. Предметом МКР захист даних файлових серверів.

Мета та задачі

Метою МКР є збільшення стійкості захисту файлових серверів.

Основними задачами дослідження є:

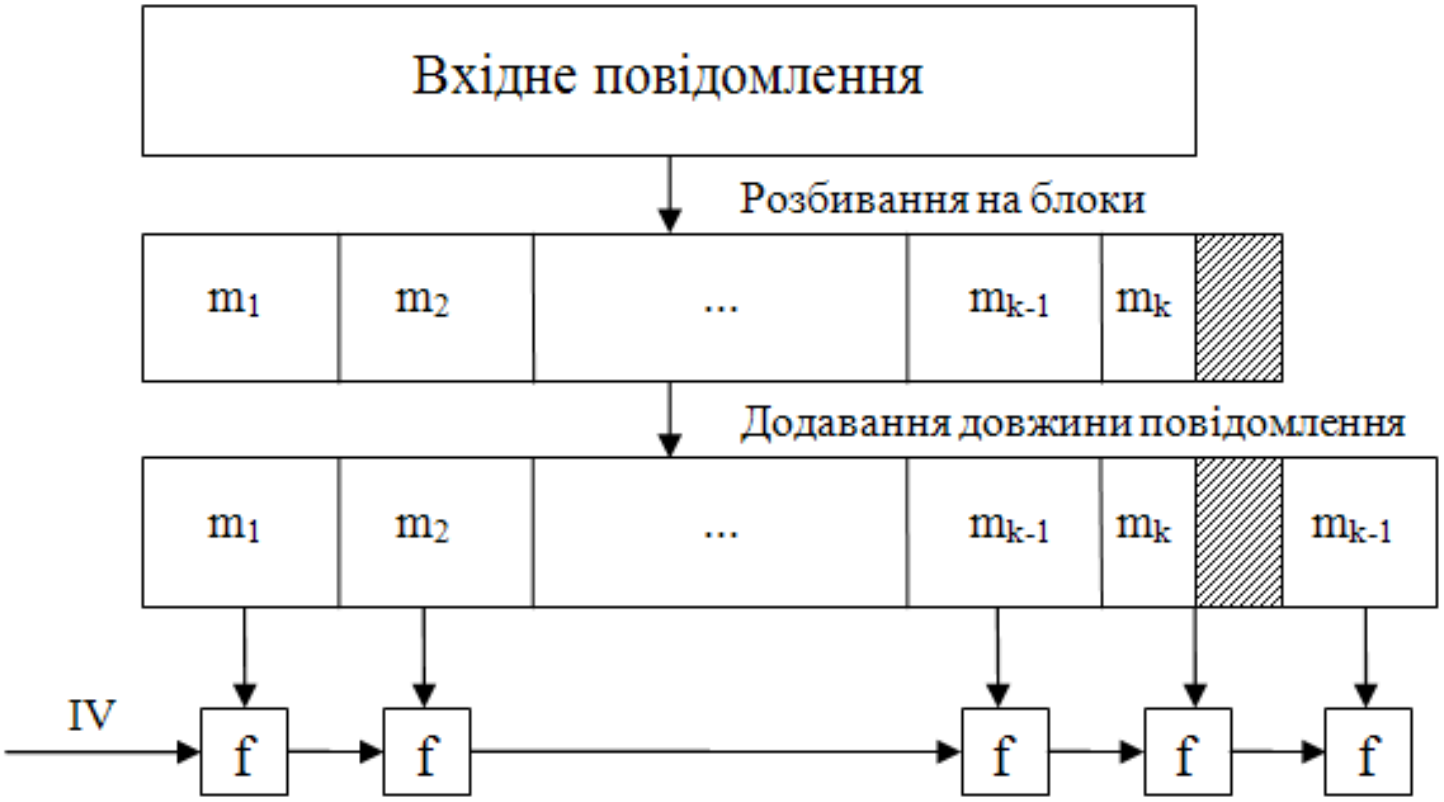
- проаналізувати існуючі методи і засоби для побудови файлових серверів з метою визначення нових підходів до підвищення їх захищеності;
- удосконалити методи гешування щодо їх стійкості до загальних атак;
- розробити методи захисту файлових серверів на основі цих методів гешування;
- розробити програмне забезпечення захищеного файлового серверу.

Порівняльна характеристика популярних геш-функцій

Назва	Розмір ключа (біт)	Обчислювальна складність	Вразливості
MD4	128	2^{64} - 2^{78}	Атака дня народження, прообраз I та II
MD5	128	2^{21} -2^{123}	Атака дня народження, прообраз I та II
RIPEMD	128/160/256/320	2^{18}-2^{51}	Атака дня народження
SHA-0	160	2^{34}	Атака дня народження
SHA-1	160	2^{51}	Атака дня народження
SHA-2	224/256/384/512	2^{28} - 2^{495}	Атака дня народження, прообраз I та II
SHA-3	256/384/512	-	-
ГОСТ 34.11-45	256	2^{105}-2^{192}	Атака дня народження, прообраз I та II
TIGER	128/160/192	2^{62}-2^{184}	Атака дня народження, прообраз I та II

Загальний підхід до побудови геш-функцій

$h_0 = IV;\ h_i = f(m_i, h_{i-1})\ H(m) = h_k$



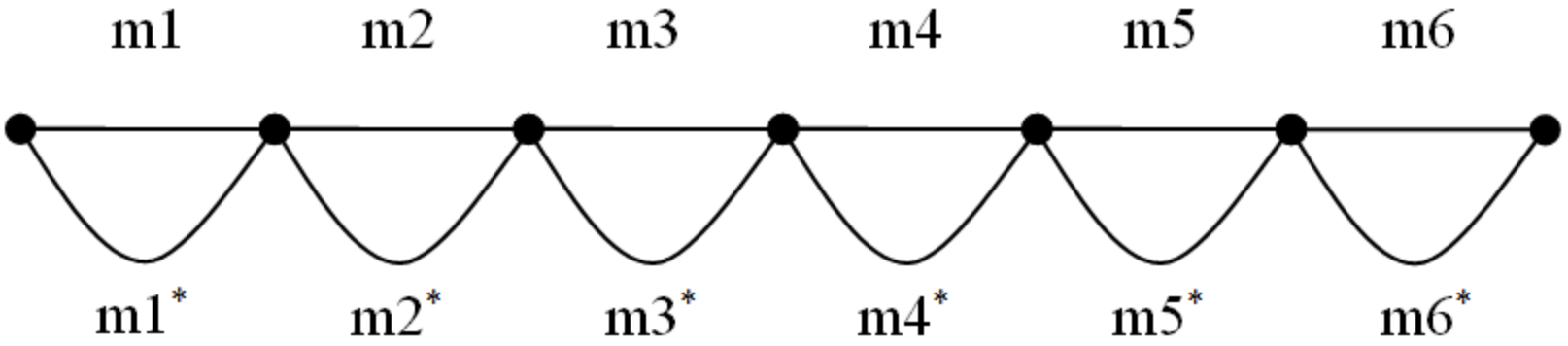
Функція гешування стійка до загальних атак

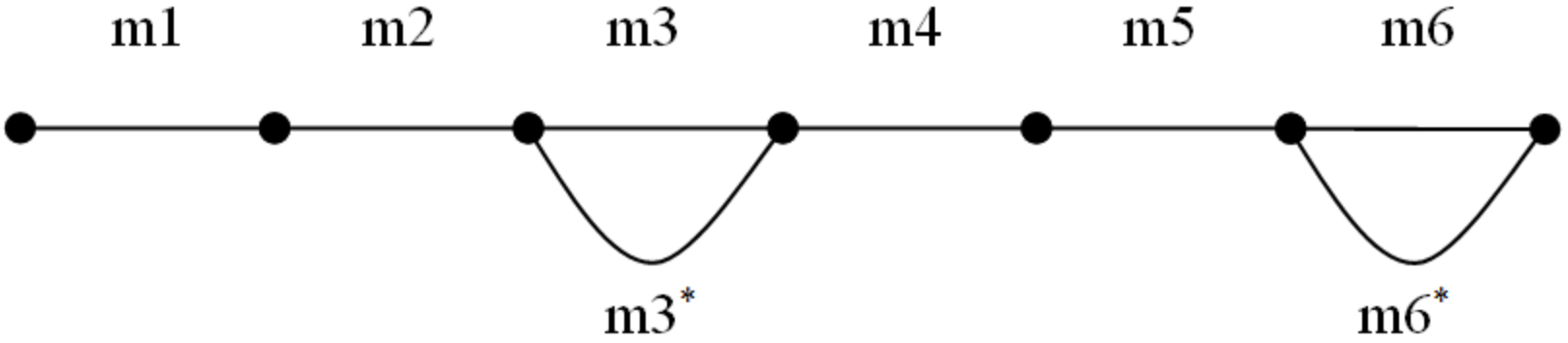
Для ускладнення проведення атак, пропонується використовувати перетворення, які породжують проблему дискретного логарифма.

У випадку правильного вибору примітивного елементу g за модулем простого числа p, результуюча послідовність блоків геш-значення рівномірно упорядкується. Результатом чого відновлення степеня, за умови зберігання в таємниці компонентів показника степеня, є експоненціально складн

$$\begin{cases} h_i = g^{h_{i-1}+m_{i-r_i}+m_i} \bmod p \\ r_i = \mathrm{rand}(m_i, h_{i-1}) \end{cases}$$

Атака Жу

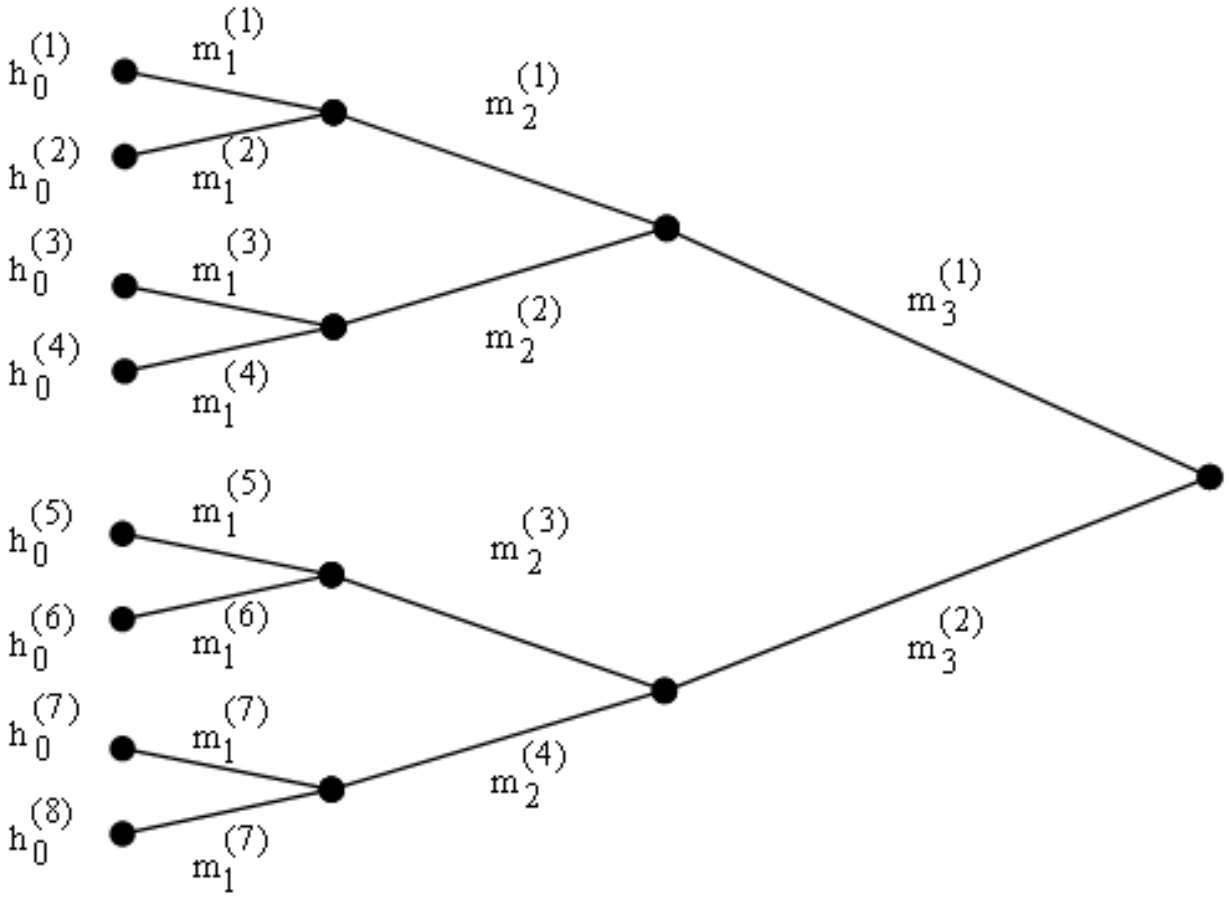




$$r_3 = \mathrm{rand}(m_3) = 1;$$

$$r_3^* = \mathrm{rand}(m_3^*) = 2.$$

Атака Келсі-Коно



Протокол передачі даних

Обміну файлами передбачає дві сторони – клієнт та сервер. Сервер має прослуховувати деякий порт. Після отримання ідентифікаційного номеру користувача з клієнтського додатку, сервер має надіслати список доступних файлів. Клієнт обирає потрібний файл та надсилає його ім’я серверу.

Визначений файл сервер шифрує та надсилає клієнту.

Метод захисту файлів

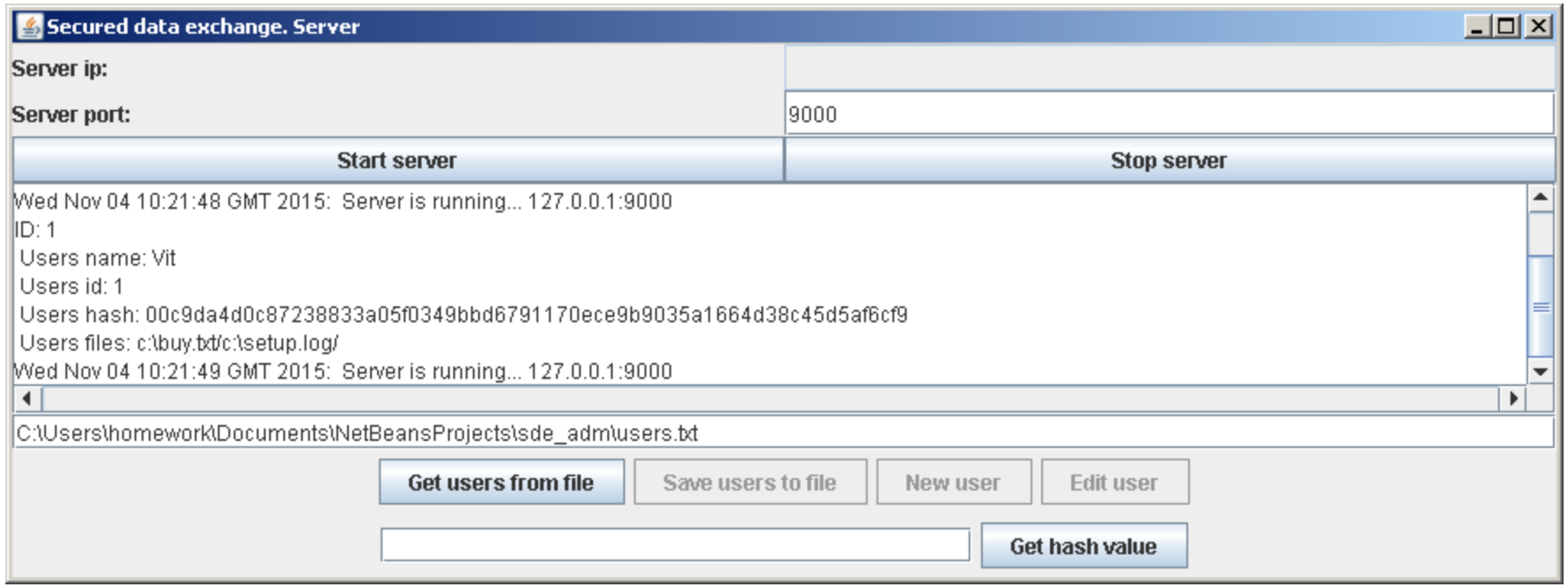
Для забезпечення захисту файлів необхідно:

1. Обчислити геш-значення на основі паролю та значення поточної дати.

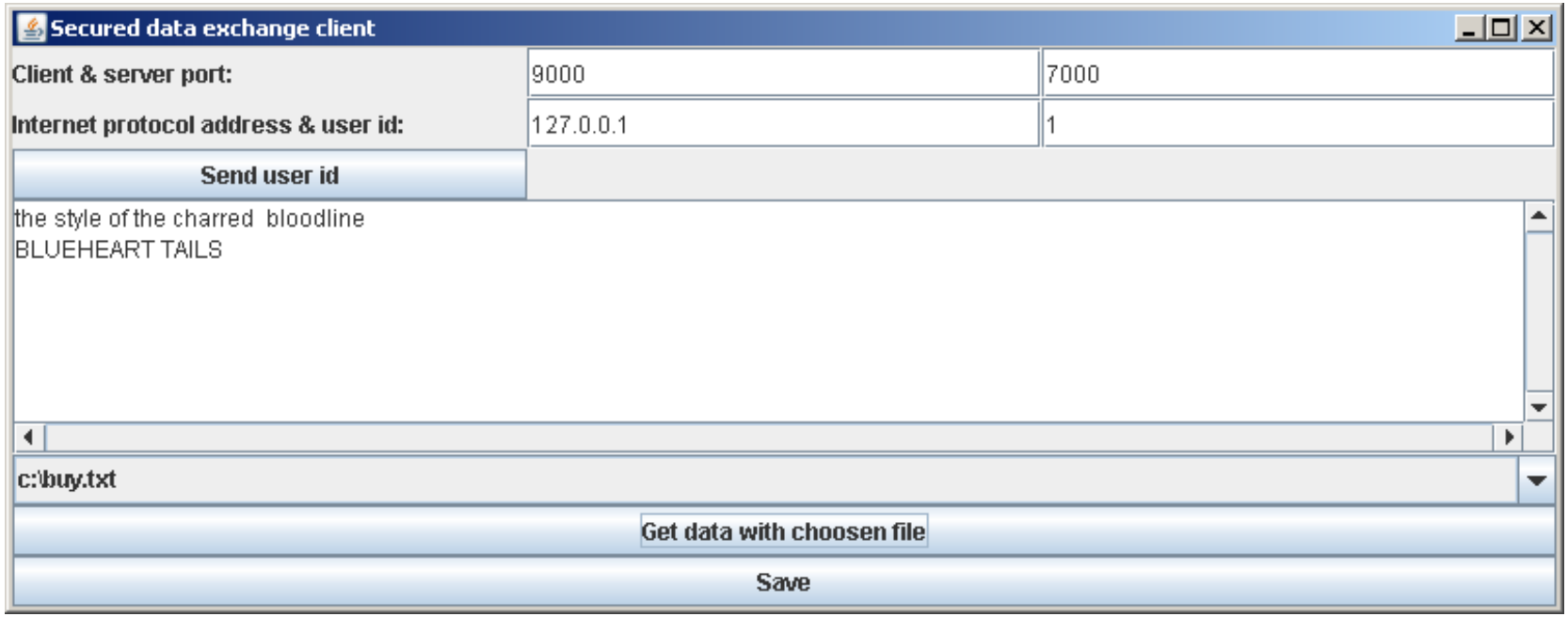
2. Встановити в якості ключа згенероване геш-значення додавши за модулем два геш-значення, обчислене на основі виконуваного файлу на стороні клієнта.

3. Зашифрувати файл.

Вигляд інтерфейсу програмного засобу. Сервер.



Вигляд інтерфейсу програмного засобу. Клієнт.



Економічна частина

Запропоноване технічне рішення є економічно доцільним, оскільки, крім підвищення ефективності технологічного процесу, це надасть змогу отримати чистий прибуток у розмірі 272555,71 грн.

Крім того, вкладені в розробку кошти окупляться за період 0,77 року.

Дякую за увагу!