

# ПРОТОКОЛ ВЗАЄМНОЇ АВТЕНТИФІКАЦІЇ В VoIP МЕРЕЖАХ

Д. А. Черкас<sup>1, а</sup>, О. М. Барановський<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

В роботі досліджена чинна проблема взаємної автентифікації (Peer-to-Peer Authentication) в мережі VoIP. Розглянуто найбільш небезпечні типи атак на VoIP мережу та розроблено механізм протидії цим атакам за допомогою взаємної автентифікації. Взаємна автентифікація реалізована на основі криптографічних протоколів: «Zero-knowledge proof» та «Secret sharing». В результаті створено тестовий застосунок, який на основі протоколу SIP імітує встановлення з'єднання та проведення взаємної автентифікації за запропонованими принципами.

**Ключові слова:** VoIP, взаємна автентифікація, Zero-knowledge proof, Secret sharing

## Вступ

За даними міжнародної компанії Nettitude[1], в першому кварталі 2015 року на VoIP (Voice over Internet Protocol) служби припало 67% усіх атак, що були зафіксовані на серверах, що розміщені в Великобританії. Разом з тим, все частіше звучать повідомлення[2], що зловмисники все більше відходять від автоматичної реалізації вразливостей і замість цього здійснюють свої атаки за допомогою соціальної інженерії.

Соціальна інженерія в 2015 році посіла перше місце в списку 10 найбільш популярних методів атак[3], замістивши вразливості пристроїв та ПЗ. Зловмисники можуть більше не вигадувати чи купувати дорогі технічні засоби. Все, що раніше могло залежати від шкідливого коду, може зробити людина: заразити систему, викрасти облікові дані, переказати грошові кошти.

Окремою сторінкою соціальної інженерії є Вішинг – злочинна практика, що використовує соціальну інженерію через телефонну систему для отримання доступу до приватної особистої та фінансової інформації.

## 1. IP-телефонія

IP-телефонія є одним із наймолодших видів зв'язку. Фактично, вона з'явилась в 1999 році коли був розроблений і затверджений Session Initiation Protocol.

IP-телефонія – телефонний зв'язок по протоколу IP. Набір комунікаційних протоколів, технологій та методів, що забезпечують традиційні для телефонії: набір номера, виклик абонента, двостороннє голосове спілкування по мережі Інтернет або будь-яким іншим IP-мережам. Для здійснення дзвінка абоненту, достатньо знання лише IP адреси.

## 2. Атаки на сеанс зв'язку

Навіть офіційні постачальники послуг[4] IP-телефонії надають можливості переадресації, переводу чи перехоплення дзвінків, що й вже казати про злочинні дії. Виділяється 4 типи атак з використанням переадресації чи перехопленням дзвінків, які становлять найбільшу небезпеку у поєднанні з вішингом.

Початкові умови: Аліса – користувач який хоче зв'язатись з Бобом, який є представником банку і вирішити питання зі зміною паролю до своєї банківської карти. Разом з тим Чак прагне отримати контроль над картковим рахунком Аліси. Аліса здійснює дзвінок з використанням IP-телефонії за номером, який зазначено на пластиковій картці банку. Чак має несанкціонований доступ до серверів постачальника VoIP послуг.

Шляхом незаконних дій зловмисник змінив таблицю маршрутизації таким чином, щоб всі IP пакети, які йдуть на IP адресу, яка відповідає вказаному номеру перенаправлялись на нього. Тепер ми бачимо (рис. 1), що подзвонивши в банк, Аліса насправді дзвонить до Чака, який представляється співробітником банку, Бобом. Аліса, вважаючи, що говорить з Бобом надає йому пароль від рахунку. Таким чином Чак отримав контроль над рахунком Аліси.

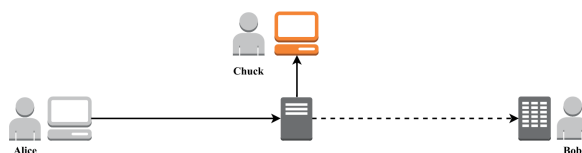


Рис. 1

Аналогічною (рис. 2) є ситуація коли Чак налаштував пренаправлення IP пакетів, які йдуть на IP адресу Аліси на свою адресу. Разом з тим, дізнавшись CVV2 код банківської карти він здійснив покупку на велику суму і коли банк зв'яжеться з Алісою за підтвердженням, то потрапить до Чака, який підтвердить списання коштів.

<sup>а</sup>dimacherkas@ukr.net

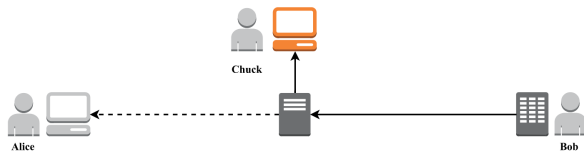


Рис. 2

Інша атака(рис. 3) полягає в тому, що Чак дізнався IP адресу банку, що обслуговує IP-телефонію і замаскував, змінив свою адресу на сервері на адресу банку. При встановленні зв'язку Чаком на телефоні Аліси відображатиметься номер телефону банку. Таким чином, довіряючи абоненту, Аліса може видати йому пароль від свого рахунку.

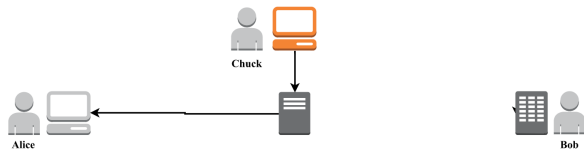


Рис. 3

Останнім варіантом здійснення атаки(рис. 4), є один із найпоширеніших зараз та і найбільш захищений, тобто найменш можливий, метод шахрайства, коли Чак видає себе за Алісу та зателефонує до банку з проханням про відновлення контролю над рахунком. Наразі банки ідентифікують користувачів за допомогою персональних даних (серія, номер паспорту) або слова-пароля. Та втрата цих даних ставить під загрозу банківські рахунки користувача.

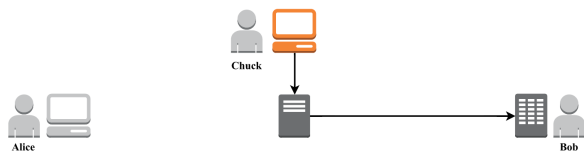


Рис. 4

### 3. Протокол взаємної автентифікації

Для недопущення реалізації вищезазначених загроз, було використано наступні концепти: «Zero-knowledge proof»[5] та «Secret sharing»[6].

- Zero-knowledge proof – інтерактивний криптографічний протокол, що дозволяє одній з інтерактивних сторін переконатись в істинності будь-якого твердження, не маючи при цьому жодної інформації про саме твердження.
- Secret sharing – метод розділення секрету між групою учасників, кожен з яких отримує лише частину секрету. Причому відновлення секрету можливе лише коаліцією учасників.

З використанням вищезазначених методів, встановлення зв'язку виглядає наступним чином(рис. 5). Нехай Аліса хоче зв'язатись з Бобом. Перед встановленням зв'язку обидвома сторонами було вибрано наступні параметри:  $s$  – секретний ключ обох абонентів (секрет),  $n$  – велике просте таке, що  $(s, n) = 1$ . Крім того,  $s$  – секрет, було розбито на 100 частин за допомогою схеми інтерполяційних поліномів Лагранжа. Ці 100 частин були рівномірно поділені між

обом абонентами. Отже, до встановлення зв'язку обидві сторони мають наступні параметри:  $s$  – секрет,  $n$  – велике просте,  $S$  – множина, що складається з 50 частин секрету.

Таким чином, під час встановлення зв'язку, Аліса, перш за все, «знаходить» Боба та надсилає йому запрошення для встановлення зв'язку. У відповідь автоматично «запускається» протокол підтвердження особи Боба методом підтвердження з нульовим розголошенням. Боб випадковим чином обирає деяке число  $r$ , обраховує  $x = r^2 \bmod n$  та надсилає отримане значення Алісі. Аліса ж у відповідь надсилає випадковий біт  $e = \{0, 1\}$ . Боб обраховує значення виразу  $y = r \times s^e$  та надсилає це значення Алісі. Аліса ж перевіряє чи виконується рівність  $y^2 = x^e$ . У випадку коли рівність виконується протягом  $t$  ітерацій, можна вважати, що Боб підтвердив свою особу. У випадку ж, коли хоча б 1 раз Боб не зміг підтвердити – автентифікація вважається проваленою.

Після того, як Боб підтвердив той факт, що він дійсно Боб, Аліса надсилає йому одну із своїх 50 частин ключа і Боб використовуючи свої фрагменти ключа та отриманий фрагмент відновлює секрет. У випадку, якщо відновлення секрету не можливо чи відновлений секрет не збігається з тим, що має Боб, автентифікація вважається проваленою. Крім того, секрет, який був направлений Бобу вважається скомпрометованим і більше в жодному випадку не може використовуватись в наступній автентифікації.

Аналогічно відбувається автентифікація і в зворотньому боці, коли Боб намагається зв'язатись з Алісою. Реалізація вищезазначених атак в такому випадку є неможливою оскільки серед іншого (в роботі проведена оцінка механізму автентифікації у відповідності до моделі загроз Долева-Яо):

- Під час автентифікації Боба жодна інформація, яка б могла допомогти відшукати секрет не передається.
- Аліса відправляє свою частину секрету лише у випадку підтвердження особи Боба

В свою чергу система має і недоліки:

- В залежності від того, наскільки важлива для нас наша система, і які вимоги до її безпеки встановлюється кількість ітерацій  $t$ . Чим більша кількість ітерацій – тим менші шанси підмінити особистість Боба, але тим більший час встановлення зв'язку.
- В залежності від кількості частин на які було розбито наш секрет, ми обмежені в кількості сеансів зв'язку які ми можемо встановити. (Разом з тим після встановлення зв'язку і створення захищеного каналу ми можемо хоч кожного сеансу змінювати наш секрет)

Даний протокол діє на етапі встановлення зв'язку перед початком передачі даних. Для безпечного функціонування нижчеописаної процедури необхідно в режимі *offline*, або в захищеному каналі зв'язку погодити деякі параметри системи. Натомість схема дозволяє здійснювати взаємну автентифікацію без третьої сторони (майже всі сучасні системи викори-

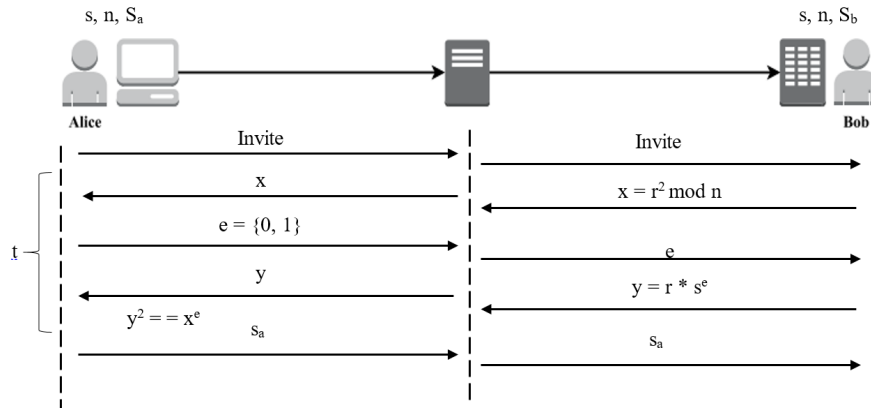


Рис. 5

стовують центр сертифікації ключів або довірений сервер).

#### 4. Результати роботи

Для моделювання роботи механізму автентифікації було вирішено модифікувати SIP (Session Initiation Protocol). Цей протокол було вибрано з причин:

- SIP – один з протоколів що лежить в основі VoIP
- Незалежність від транспортного рівня передачі даних
- SIP – ініціює початок з'єднання, а саме в цей час актуальна автентифікація
- Для протоколу характерна Розширюваність – можливість доповнення протоколу новими функціями (введення нових заголовків і повідомлень).

Нами було розроблено тестову програму для встановлення зв'язку та взаємної автентифікації на основі SIP та запропонованого вище механізму. Під час роботи програми були підтверджені теоретичні слабкості методу. А саме, залежність швидкості встановлення зв'язку від:  $t$  – кількості ітерацій,  $s$  – розміру секрету та  $N$  – кількості частин, з яких можливе відновлення секрету.

Для функціонування системи потрібне погодження вищезазначених параметрів параметрів. В тестовій програмі було обрано наступні параметри: розмір секрету – 40 *bit*, кількість ітерацій – 5, кількість частин з яких можливе відновлення секрету – 2. В реальних системах рекомендується використання параметрів: 56 або 128 *bit*, 15-20 ітерацій та кількість частин від 3-ох відповідно.

В результаті нам вдалося встановити сеанс зв'язку та автентифікувати обидві сторони за допомогою вищеприписаного механізму.

#### Висновки

На основі розробленого механізму автентифікації можна виконати взаємну автентифікацію без залуче-

ння третьої сторони. Також використання вищезазначеного механізму дозволить значно знизити можливість вішингових атак на VoIP мережі, оскільки вже на етапі встановлення зв'язку буде підтверджуватись чи не підтверджуватись особа співрозмовника, а зусилля необхідні на подолання захисту не співрозмірні отриманій інформації. Адже навіть компрометація системи не дає гарантію на отримати бажаних зловмисником даних.

#### Перелік використаних джерел

1. Co. Nettitude. VOIP Attacks On The Rise. — 2015. — P. 8 с. — URL: <https://www.nettitude.co.uk/wp-content/uploads/2015/06/VoIP-attacks-on-the-rise-Jules-Pagna-Disso.pdf>.
2. Ashford Warwick. Social engineering confirmed as top information security threat. — 2016. — URL: <http://www.computerweekly.com/news/4500273577/Social-engineerin-confirmed-as-top>.
3. Ashford Warwick. Social engineering is top hacking method, survey shows. — 2016. — URL: <http://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hacking-method>.
4. VoIPCloud. — 2016. — URL: <http://voipcloud.ru/capabilities/pereadresaciyanapravlenie-vxodyashhix-zvonk>.
5. Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — Триумф, 2002. — ISBN 5-89392-055-4.
6. Shamir Adi. How to Share a Secret // Massachusetts Institute of Technology. — 1979. — Vol. 22.