УДК 004.031.4
М.І. Колендюк, В.М. Козел
Херсонський національний технічний університет
E-mail: max_kolendyuk@mail.ru
k_vic@ukr.net

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАСІБ АТАКИ НА КОМП'ЮТЕРНУ МЕРЕЖУ

На сьогоднішній день дуже популярною атакую на комп'ютерну мережу є атака «людина посередині» (англ. Man in the middle (MITM)). За цією атакою атакуючий повинен стати між точками що передає інформацію та точкою куди інформація передається і прослуховувати канал зв'язку, але для цього йому необхідно під'єднатись до мережі, одже атакуючий повинен знати пароль. Зазвичай для того щоб отримати пароль атакуючий виконував ряд дій в результаті отримував handshake паролю і йому залишалось розшифрувати його. Але для розшифровки використовувався метод brute-force і handshake міг розшифровуватись дуже довго або взагалі не бути розшифрован якщо пароль був складним. Тому на поміч приходить технологія соціальної інженерії, за якою атакуючий вимушує користувача надати йому пароль у незашифрованому вигляді.

Ключові слова: соціальна інженерія, man in the middle, атака посередині, комп'ютерна мережа, атака, канал зв'язку, handshake.

М.И. Колендюк, В.Н. Козел
Херсонский национальный технический университет
E-mail: max_kolendyuk@mail.ru
k_vic@ukr.net

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СРЕДСТВО АТАКИ НА КОМПЬЮТЕРНУЮ СЕТЬ

На сегодняшний день очень популярной атакую на компьютерную сеть является атака «человек посередине» (англ. Man in the middle (MITM)). По этой атакой атакующий должен стать между точками передает информацию и точкой куда информация передается и прослушивать канал связи, но для этого ему необходимо подключиться к сети, одже атакующий должен знать пароль. Обычно для того, чтобы получить пароль, атакующий выполнял ряд действий в результате получал handshake пароля и ему оставалось расшифровать его. Но для расшифровки использовался метод brute-force и handshake мог расшифровываться очень долго или вообще не быть расшифрованы если пароль был сложным. Поэтому на помощь приходит технология социальной инженерии, по которой атакующий вынуждает пользователя предоставить ему пароль в незашифрованном виде.

Ключевые слова: социальная инженерия, man in the middle, атака посередине, компьютерная сеть, атака, канал связи, handshake.

M.I. Kolendyuk V.M. Kozel
Kherson National Technical University
E-mail: max_kolendyuk@mail.ru
k_vic@ukr.net

SOCIAL ENGINEERING AS A MEANS OF ATTACK ON A COMPUTER NETWORK

Man-in-the-middle (MITM) is a very popular attack on the computer network today. For this attack, the attacker must be between the transmitting point and the point where the information is transmitted and listening to the communication channel, but in order to do so, the attacker must know the password. Usually in order to get the password, the attacker performed a series of actions as a result of receiving a handshake of the password and he had to decrypt it. But the decryption method used the brute-force method, and handshake could decrypt for a very long time or not be decrypted at all if the password

was complex. Therefore, social engineering technology comes to the fore, where the attacker forces the user to give him or her an unencrypted password.
Keywords: social engineering, man in the middle, middle attack, computer network, attack, communication channel, handshake.

Постановка проблеми. У даній роботі ми розглянемо випадок коли потрібно під'єднатись до мережі для подальшої ретрансляції трафіку, але перехоплений handshake не піддається розшифровки. На цей випадок існує техніки напрямку – соціальної інженерії.

Аналіз останніх досліджень та публікацій. Соціальна інженерія (СІ) – сукупність прийомів, методів та технологій створення простору, умов і обставин, які максимально ефективно приводять до необхідного результату, за допомогою напрямів психології та соціології.

СІ найчастіше розглядають у контексті незаконного методу отримання приватної інформації, однак якщо розглядати її початкову природу, а на даний час як професійну СІ, то область її застосування цілком стримується у рамках закону. Наприклад, вона допомагає реалізувати досягнення мети, яка початково недосяжна, або «програмувати» людину або групу людей для звершення будь яких корисних дій.

Сьогодні СІ найчастіше використовують в інтернеті для отримання закритої (конфіденційної) інформації. Сучасні соц-інженери використовують дану технологію і свої навички у ній для підвищення результатів у житті та бізнесі.

Техніки СІ.

Перед тим як описувати техніки, приведемо небагато теорії про самі техніки, визначення та базиси на яких базується СІ.

Усі техніки СІ основані на когнітивних викривленнях. Когнітивне викривлення – це поняття когнітивної науки або когнітивістики (лат. cognitio – пізнання) – наукового напрямку, що об'єднує теорію пізнання, когнітивну психологію, нейрофізіологію, когнітивну лінгвістику, невербальну комунікацію та теорію штучного інтелекту, рисунок 1, що значить систематичне відхилення у поведінці, сприйнятті та мислені, що зумовлені суб'єктивними переконаннями, упередженнями та стереотипами, соціальними, моральними й емоційними причинами, збоями в обробці і аналізі інформації, а також фізичними обмеженнями та особливостями будови людського мозку.

Когнітивні спотворення виникають на основі дисфункціональних переконань, впроваджених в когнітивні схеми, і легко виявляються при аналізі автоматичних думок. Люди схильні створювати свою власну «суб'єктивну соціальну реальність», залежну від їх сприйняття, і ця суб'єктивна реальність може приймати рішення щодо поводження в соціумі. Таким чином, когнітивні спотворення можуть призводити до неточності суджень, нелогічним інтерпретацій або до ірраціональності в поведінці в широкому сенсі слова.

Деякі когнітивні спотворення можуть сприяти більш ефективним діям особистості в конкретних умовах. Крім того, деякі когнітивні спотворення дозволяють швидше приймати рішення в ситуаціях, коли швидкість прийняття рішення важливіше його точності. Інші когнітивні спотворення є прямим наслідком обмежених можливостей обробки людиною інформації або відсутності відповідних психічних механізмів (обмежена раціональність).

Дослідження когнітивних спотворень мають велике значення для когнітивної науки, соціальної психології і поведінкової економіки, оскільки дозволяють «виділити» психологічні процеси, що лежать в основі процесів сприйняття і прийняття рішень.

Когнітивні спотворення можуть виникати через різні причини, зокрема:

- «збоїв» у обробці інформації (евристика).
- «ментального шуму».
- обмежені можливості мозку з обробки інформації.
- емоційних і моральних причин.
- соціального впливу.

У когнітивної науці використовуються два стандартних обчислювальних підходу до моделювання когнітивних систем: сімволіціізм (класичний підхід) і коннекціонізм (більш пізній підхід). Сімволіціізм ґрунтується на припущенні про те, що людське мислення подібно мисленню комп'ютера з центральним процесором, послідовно обробного одиниці символьної інформації. Коннекціонізм ґрунтується на припущенні, що людське мислення не може бути уподібнено центральному цифровому процесору через несумісність з даними нейробіології, а може імітувати

за допомогою штучних нейронних мереж, які складаються з «формальних» нейронів, що виконують паралельну обробку даних.

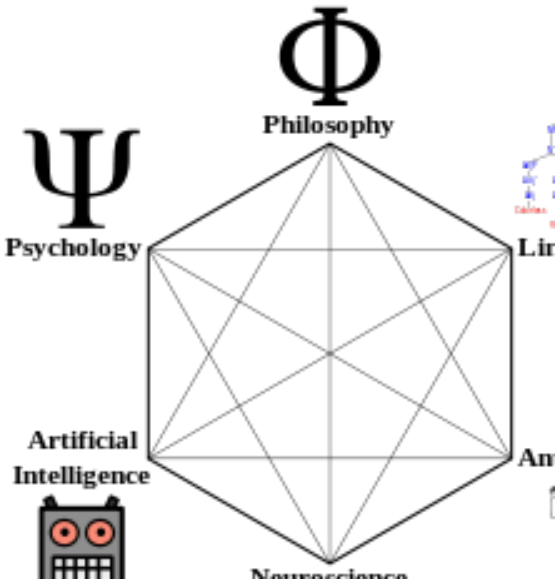

Рисунок 1 – наукові напрямки, що покладені в основу зародження когнітивної науки.

Як вже було сказано, усі техніки СІ основані на когнітивних викривленнях. Ці помилки у поведінці використовуються соц-інженерами для створення атак, направлених на отримання конфіденційної інформації, частіше із згоди жертви.

Так прямим прикладом доступу до даних методом СІ є наступна ситуація: атакуючий під видом простої людини входить до будівлі компанії і вішає на інформаційному бюро об’яву, що виглядає як офіційне, з інформацією про зміну телефону довідкової служби інтернет-провайдера. Від тепер працівники компанії будуть дзвонити за цим номером, а атакуючий може запрошувати будь які особисті дані, логіни, паролі та ідентифікатори для отримання доступу до конфіденційної інформації.

Рисунок 2 – Основні техніки СІ.

Розглянемо основні техніки СІ в окремості.

Кви про кво – (лат. qui pro quo – «хто замість кого») – фразеологізм латинського походження, що означає плутанину, пов'язану з тим, що хтось або щось приймається за кого-то або щось інше. За цією технікою атакуючий звертається до фірми/компанії за корпоративним телефоном під видом працівника технічної підтримки, що повідомляє про технічні неполадки або проблеми на робочому місці працівника та пропонує допомогу в її виправленні. У процесі вирішення проблеми атакуючий просить виконувати дії за допомогою яких він може запускати команди або встановлювати програмне забезпечення для своїх цілей.

«Дорожнє яблуко» – техніка, що являє собою адаптацію «троянського коня», суть якої у використанні фізичних носіїв (карт пам'яті і т.п.). Атакуючий підкидує «інфіковані» шкідливим кодом цифрові носії у багатолюдні місця, де ці носії можуть бути знайдені. Подібні носії оформлюються як офіційні для компанії або супроводжуються провокуючою на інтерес підписом, хоча найчастіше досить просто підкинути носій, тому розділимо цю технологію атаки на спрямовану та вільну.

Обернена СІ – про цю техніку згадують коли жертва сама пропонує атакуючому цікаву йому інформацію. Люди що мають певний авторитет у соціальній сфері, або технічній, часто отримують ідентифікатори та паролі або подібну інформацію користувачів тільки тому, що користувачі не сумніваються у їх непорядності. Наприклад, працівники служби підтримки ніколи не запитують у користувачів ідентифікатори та пароль, тому що вони не потребують цю інформацію, але користувачі для скорішого вирішення питання по своїй волі повідомляють цю інформацію. Тому атакуючому навіть не приходиться запрошувати ці дані.

Претекстінг – техніка, за якою атакуючий представляється іншою людиною під завчасно підготовленим сценарієм, та дізнається конфіденційну інформацію. Ця техніка має на увазі завчасну підготовку, створення історії людини: день народження, інн, номер паспорту та подібне, для того щоб не викликати підозри у жертви. Зазвичай реалізується через телефон або електрону адресу.

Фішинг – від англ. fishing – ловля риби, видобування – техніка інтернет- шахрайства, метою якої є отримання доступу до конфіденційних даних користувачів (логіну та паролю). Це найпоширеніша техніка СІ на сьогодні. Жодний крупний витік даних не обходиться без фішингових розсилок. Найліпшим прикладом фішингової атаки є повідомлення до жертви за електронною адресою, зроблені у стилі офіційного письма банку, або платіжної системи, потребуючої перевірки певної інформації для проведення певних дій. Зазвичай такі повідомлення мають посилання на фальшиві веб-сторінки, які у точності схожі на офіційні і містять форму, що вимагає ввести конфіденційну інформацію.

Телефонний фрікінг – (англ. phreaking) – термін, що описує експерименти та злом телефонних систем за допомогою звукових маніпуляцій с тоновим набором. Ця техніка з'явилась у кінці 50-х у Америці, телефона корпорація Bell, що на той момент покривала практичну усю територію США, використовувала тоновий набір для передачі різноманітних службових сигналів. Ентузіасти, які спробували повторити деякі з цих сигналів, отримували можливість безкоштовно дзвонити, організовувати телефонні конференції та адмініструвати телефонну мережу.

Збір інформації з відкритих джерел.

Застосування технік соціальної інженерії вимагає не тільки знання психології, а й уміння збирати про людину необхідну інформацію. Наприклад, такі сайти як «Livejournal», «Facebook», «ВКонтакте», «Instagram», та інші, містять величезну кількість даних, які люди й не намагаються приховати. Як правило, користувачі не приділяють належної уваги питанням безпеки, залишаючи у вільному доступі дані і відомості, які можуть бути використані зловмисником.

Навіть обмеживши доступ до інформації на своїй сторінці в соціальній мережі, користувач не може бути точно впевнений, що вона ніколи не потрапить до рук шахраїв. Наприклад, бразильський фахівець-дослідник з питань комп'ютерної безпеки довів, що існує можливість стати одним будь-якого користувача Facebook протягом 24 годин, використовуючи методи соціальної інженерії. В ході експерименту дослідник Нельсон Новаєс Нето, вибрав жертву і створив фальшивий аккаунт людини з її оточення - її начальника. Спочатку Нето відправляв запити на дружбу друзям друзів начальника жертви, а потім і безпосередньо його друзям. Через 7,5 години дослідник домігся додавання в друзі від жертви. Тим самим дослідник отримав доступ до особистої інформації користувача, якій той ділився тільки зі своїми друзями.

Плечовий серфінг – (англ. Shoulder surfing) – включає в себе спостереження особистої інформації про жертву, в буквальному сенсі, через її плече. Цей тип атаки поширений в громадських місцях. Опитування ІТ-фахівців в білій книзі (офіційне повідомлення в письмовому вигляді, зазвичай цей термін застосовується в США, Великобританії, Ірландії та інших англомовних країнах. Це може бути: державне повідомлення, що пояснює політику; довідковий

документ для корпоративних клієнтів; офіційна документація, яка містить опис рішення; документація, що описує новий технологічний процес або алгоритм. Такі документи можуть бути використані для прийняття рішень.) Про безпеку показав, що:

• 85% опитаних зізналися, що бачили конфіденційну інформацію, яку їм не належало знати;

• 82% зізналися, що інформацію, що відображається на їх екрані, могли б бачити сторонні особи;

• 82% слабо впевнені в тому, що в їх організації будь-хто буде захищати свій екран від сторонніх осіб.

Формулювання цілі дослідження. Ціллю даної статті є заміна процесу дешифрування паролю, тому що він може бути не розшифрован.

Виклад основного матеріалу дослідження. За загальним алгоритмом, для реалізації атаки «людина посередині» для того щоб атакуючий зміг «стати» між двома точками зв'язку, нехай то клієнт і сервер, або канал зв'язку за яким йде обмін інформацією, потрібно, знайти необхідну мережу, та під'єднатись до неї. За другим пунктом, атакуючий перехоплював handshake, далі залишалось розшифрували цей handshake, та якщо пройшло вдале розшифрування (handshake може бути і не розшифровано), атакуючий від'єднувався до мережі і далі міг проводити атакуючи дії – прослуховування трафіку тощо. Процес розшифровування handshake'у може зайняти дуже великий проміжок часу і як було сказано вище може бути невдалим, це зумовлюється складністю паролю користувача, та часто користувачі не дотримуються рекомендацій до складних паролів, тому алгоритми шифрування паролів у wifi построєні таким чином, щоб максимально ускладнити пароль до етапу шифрування (нагадаємо, що на сьогодні самим поширеним алгоритмом захисту на сьогодні є WPA2).

Процес розшифровки handshake'у був замінений CI, вчасності методом фальшивої точки доступу, називаємого «злий двійник». «Злий двійник» – різновид фішингу, схема якого представлена на рисунку 3, що застосовується в бездротових комп'ютерних мережах. Атакуючий створює копію бездротової точки доступу, що знаходиться в радіусі прийому користувача, тим самим підміняє оригінальну точку доступу двійником (рисунок 4), на рисунку можна побачити помилку аутентифікації користувача в оригінальній точці доступу. Різниця у тому, що до оригінальної точки доступу, після того як атакуючий від'єднав жертву від маршрутизатора, жертва під'єднатись не може, але бачить у переліку точок доступу, двійник.

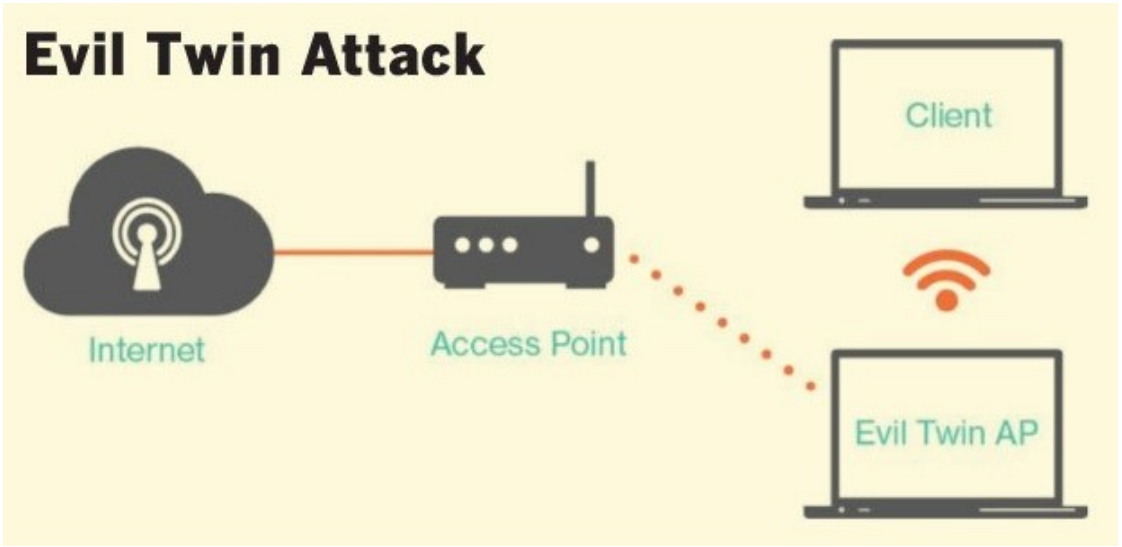

Рисунок 3 – Схема атаки «злий двійник»

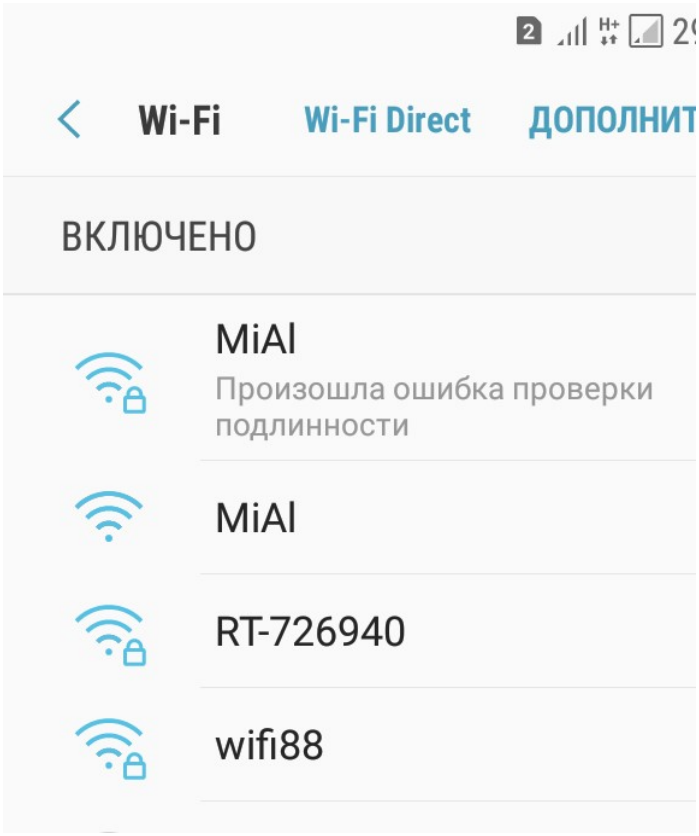

Рисунок 4 – Фальшива точка доступу (двійник) MiAI.

Першим етапом зловмисник повинен провести радіорозвідку місця, де він передбачає встановити бездротову точку-двійника. В результаті даної розвідки атакуючий отримає інформацію про всіх доступних Wi-Fi-мережах, їх SSID і типі шифрування. Також він отримає інформацію про активні клієнтів бездротових мереж у вигляді MAC-адрес як клієнтів, так і точок доступу (BSSID).

Далі атакуючий може використовувати отримані на етапі аналізу SSID і BSSID обраної для атаки точки доступу для створення свого двійника цієї точки. Фальшива точка доступу може розташовуватися як фізично ближче до жертви, так і перебувати на достатній відстані, в разі чого зловмисник може використовувати спрямовані антени для посилення сигналу в зоні прийому жертви.

Коли фальшива точка встановлена, і потужність прийому/передачі двійника в зоні прийому клієнта перевищує потужність компонованої точки доступу, велика ймовірність, що жертва підключиться саме до двійника, а не до оригінальної точки доступу.

Після підключення клієнта до точки доступу зловмисника стає можливим не тільки зберегти весь мережевий трафік з метою подальшого аналізу, але і підміняти сторінки авторизації популярних сайтів, таких, як google.com і vk.com та інші, непомітно для користувача. При цьому жертва вводить свої персональні дані у форму у результаті чого їх отримує атакуючий.

Після цього атаку можна вважати завершеною, і атакуючий може просто вимкнути свою точку, тим самим приховавши факт своєї присутності.

Отож для того що під’єднатись до мережі потрібно дістати пароль. Сьогодні це можливо зробити двома шляхами: 1) перехопленням handshake’у та подальшим його розшифруванням, та 2) створенням фальшивої точки доступу. Перший метод 100% перехопить handshake але чим складніший пароль тим довше буде за часом процес його розшифровки, також є шанс, що handshake’у не буде розшифрован взагалі. За соціальною інженерією, атакуючий 100% отримує пароль від користувача але за умови якщо користувач поведеться на фальшиву точку доступу або інші «трюки» СІ основані на психології людини, найчастіше такі методи дають результат із звичайними працівниками та людьми, що не дуже добре знаються на цьому. Люди на кшталт системних адміністраторів, або студентів технічних вузів, що мають робото з мережею скоріше за все не поведуться на таке, знаючи про існування таких методів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Tanmay Patange. How to defend yourself against MITM or Man-in-the-middle attack (10 ноября 2013).
2. Рудниченко А. К., Колесникова Д. С. Актуальность MiTM-атак в современных Wi-Fi-сетях // Молодой ученый. — 2017. — №3. — С. 48-49.
3. Kirk, Jeremy. ′Evil Twin′ Hotspots Proliferate // IDG News Service. — 2007.
4. Smith, Andrew D. Strange Wi-Fi spots may harbor hackers: ID thieves may lurk behind a hot spot with a friendly name. The Dallas Morning News, Knight Ridder Tribune Business News. — 2007.
5. Social Engineering Fundamentals — Securityfocus.com.
6. Social Engineering, the USB Way — DarkReading.com.
7. Social-Engineer.org — social-engineer.org.
8. Социальная инженерия: основы. Часть I: тактики хакеров https://ru.scribd.com/document/19676093/Social-Engineering-Fundamentals