УДК 004.7

М.В. Думанський,
здобувач ДНДІ МВС України,
К.В. Заїчко

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ДАНИХ У МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВЯЗКУ

Розглянуто основні джерела загрози витоку інформації каналами стільникового зв'язку. Проаналізовано уразливість процесу ідентифікації абонентів у мережі. Представлено технологічні принципи, алгоритми та наслідки дії сторонніх підключень несанкціонованих станцій GSM. Наведено аналіз функціонування пасток та ознаки перехоплення даних.

***Ключові слова**: джерело загроз, ідентифікація абонентів, витік інформації.*

Рассмотрены основные источники угроз утечки информации в каналах сотовой связи. Проанализировано уязвимость процесса идентификации абонентов в сети. Представлены технологические принципы, алгоритмы и следствие действия сторонних несанкционированных подключений ложных GSM станций. Представлено анализ функционирования ловушек и признаки перехвата данных.

***Ключевые слова:** источник угроз, идентификация абонентов, утечка информации.*

The main sources of threat information leakage channels of cellular communication are considered. Vulnerability of the process of identification of subscribers in the network is analyzed. Technological principles, algorithms and consequences of unauthorized connections in unauthorized stations GSM are presented. The analysis of the functioning of the trap and signs interception of data is carried out.

***Keywords:** source of threats, ID caller, information leakage.*

Вступ

Високий рівень упровадження стільникового зв'язку в більшість сфер діяльності особи, у тому числі банківських послуг, колосальні темпи розвитку мобільних пристроїв, висока маржинальність послуг операторів, зручність та надійність для абонентів зробили мобільний зв'язок невід'ємною частиною життя, в тому числі для вирішення завдань, які потребують певної конфіденційності.

Розвиток програмного-апаратного забезпечення та використання сучасних технологій дають змогу зловмисниками несанкціоновано отримувати різноманітні дані абонентів із загальних мереж стільникового зв'язку. На основі аналізу отриманих даних правопорушники завдають значних збитків, а в деяких випадках виток інформації може стати загрозою життю та здоров'ю користувачів.

Незважаючи на величезний обсяг обміну даними, переговорів, що відбуваються щодня мережами GSM, захист персональних даних абонентів залишається на низькому рівні.

Мета статті – проаналізувати уразливість мереж стільникового зв'язку та розглянути основні технологічні принципи передумови витоку інформації абонентів.

Основний розділ

Розглянемо основні джерела загроз у системі обробки даних стільникового зв'язку.

Джерело загроз № 1.

Постачальник послуг – оператор стільникового зв'язку.

Оператор стільникового зв'язку акумулює повну інформацію про абонентів. Причому надходить вона з двох джерел: з реєстраційної форми абонента (персональні дані) та передається в білінг при користуванні послугами. У мережі модулем ідентифікації абонента є SIM-карта, яка має кілька параметрів і в поєднанні зі спеціальними параметрами мобільного пристрою може розповісти про абонента все. Так, у базу даних білінгової системи завантажуються профілі дзвінків (напрямок, номер, тривалість), геопозиціонування (визначається за прив'язкою до базової станції та сотою), обсяг і профіль використання трафіку, SMS, MMS та ін. Зрозуміло, оператор вдається до безпрецедентних заходів захисту цієї інформації, проте трапляються витоки інформації.

Крім загрози компрометації білінгу, небезпека може виходити і від сервісів оператора зв'язку. Так, послуга батьківського контролю або будь-яка послуга трекінгу може використовуватися для відстеження переміщення абонента.

Джерело загроз № 2.

Виробники мобільних пристроїв і систем керування (операційна система).

Новітні пристрої мобільного зв'язку вкрай гнучкі в налаштуванні різних систем стеження, і пов'язано це саме з тим, що з'явилися повноцінні операційні системи, що призвело до можливості написання шпигунського програмного забезпечення і впровадження його в логіку операційної системи. Додаткову загрозу створює безперервне з'єднання з мережею Інтернет і передача міток геопозиціонування.

Джерело загроз № 3.

Перехоплення інформації в радіоканалі (комплекси перехоплення: активні, напівактивні, пасивні та ін. Засоби перехоплення).

У системах стільникового зв'язку першого покоління забезпечення конфіденційності розмови було складним завданням – оскільки на той час природа мовленнєвого сигналу була аналогова – перехоплення можна було здійснити досить простим приймальним пристроєм. У сучасних системах захистити розмову стало набагато простіше – завдяки цифровому кодуванню. При цифровому кодуванні аналогова мова перетворюється в потік двійкових даних, що підлягають шифруванню, скремблюванню та ін. Проте існує безліч способів перехоплення трафіку на "фізичному" рівні [1].

До способів перехоплення можна віднести впровадження хибної базової станції (пастка IMSI), яка знижує встановлений у мережі рівень шифрування та значно полегшує перехоплення даних. Вона працює з унікальним ідентифікатором, прописаним у SIM-карті – IMSI (International Mobile Subscriber Identity). Пастка IMSI – невеликий пристрій, що імітує вежі стільникового зв'язку. Стандарт зв'язку GSM передбачає обов'язкову автентифікацію апарату в мережі при

відсутності подібного зобов'язання від самої мережі. Пастка відключає шифрування, збирає дані і передає вже відкритий сигнал базової станції (з'єднувати абонента вона не вміє).

Незахищений доступ до мережі Wi-Fi або імітація точок також є способом перехоплення трафіку в радіоканалі. Використовуються спеціальні сніффери (аналізатори трафіку), які отримують інформацію від бездротового мережевого адаптера і декодують дані.

NFC (Near Field Communications) – технологія, яка дозволяє забезпечити ідентифікацію з використанням радіозв'язку на невеликих відстанях (від 1 міліметра до декількох десятків сантиметрів). NFC – "ближній зв'язок", працює на частоті 13,56 Мгц на відстані до 10 см зі швидкостю до 424 кбіт/с. Технологія заснована на використанні спеціальних чипів (у том числі в SIM-картах) в комунікаційних пристроях. Вона широко поширена в системах контролю доступу та платіжних системах, вбудована в деякі планшети і смартфони. Ця технологія може бути пов'язана зі зломом телефону в безпосередній близькості від нього.

Персональні дані абонента, що передаються як службова інформація

Абонент у мережі GSM – це поєднання специфічних ідентифікаторів SIM-карти і мобільного пристрою. SIM-карта – це пристрій забезпечення конфіденційності в мережах GSM. Саме вона містить на своєму мікроконтролері індивідуальну інформацію користувача, програми шифрування, ключі.

Для мобільного пристрою основним ідентифікатором є IMEI (International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання). Це заводський номер, який є унікальним для пристрою і зберігається в ньому. За допомогою IMEI можна розшукати вкрадений телефон, перевірити його оригінальне походження, заборонити підключення обладнання до базових станцій з метою безпеки. Крім цього, можливості IMEI допомагають відпрацьовувати випадки шахрайства і запобігати злочинному доступу. Цей параметр є одним із основних, що передається в мережі стільникового зв'язку.

Для абонента ідентифікатором є IMSI (International Mobile Subscriber Identity – міжнародний ідентифікатор мобільного абонента (індивідуальний номер абонента). Зазначений параметр також передається в мережі. Саме цей ідентифікатор, прописаний в SIM, перетворює телефон у мобільний термінал, який ідентифікує абонента, реєструє його в роумінгу і використовується для білінгу.

Публічний параметр MSISDN – (Mobile Subscriber Integrated Services Digital Number) – номер мобільного абонента цифрової мережі з інтеграцією служб для зв'язку в стандартах GSM, UMTS та ін. Саме його набирають під час виклику. Цей параметр не передається в мережі, але тісно пов'язаний з IMSI.

Зазначені вище параметри є достатніми для отримання необхідної оперативної інформації та використання цих даних для аналітичних висновків. Маючи ці ідентифікатори та доступ до баз даних, оператору можна отримати таку інформацію про абонента:

– за IMEI можна отримати всі IMSI SIM карт, які використовувалися в цьому пристрої, і, як наслідок, всі біллінгові дані за цими SIM картками (локація, коло спілкування, SMS, MMS, голос, URL-адреси, логіни і паролі і т.д.);

– за IMSI можна отримати всі IMEI апаратів і IMSI SIM карток, які використовувалися в цих апаратах, і, як наслідок, стають доступними все ті ж біллінгові дані, що і в попередньому випадку [2].

Розглянемо основні принципи аналізу даних для діагностики підключення сторонніх базових станцій.

1. Змінився LAC (Location Area Code – код географічної зони, яка обслуговується одним контролером базової станції (BSC). Коли відбувається вхідний дзвінок, то оповіщення одночасно отримують усі базові станції цієї зони) або Cell ID (ідентифікатор базової станції), при тому що частота залишилася незмінною. Дійсно, часто пастка займає наявну частоту, водночас надаючи сильніший сигнал, ніж оригінальна станція. Але ця метрика дуже ненадійна. По-перше, телефон може знаходитися в зоні дії двох станцій з різними LAC, і просто перескочити з однієї на іншу, залишаючись на однаковому каналі. По-друге, сам оператор може дати команду якійсь станції на перехід до іншого LAC.

2. Відбувається зміна LAC поточної станції, яка відрізняється від LAC оточуючих станцій. Завдання пастки – домогтися Location Update (коли телефон переходить з однієї Location Area (об'єднання баз в логічні групи, відповідно у кожної групи є свій LAC) на іншу, він посилає станціям це повідомлення. Також він його посилає і періодично від телефону, оскільки тільки в цьому випадку пастка може "стягти" з нього потрібну інформацію. Тому вона анонсує інший LAC, надаючи сильніший сигнал.

3. При незмінній парі Cell ID – LAC змінився номер каналу. Пастка часто маскується під невикористану частоту вже наявної базової станції.

4. LAC містить єдину станцію. Як уже зазначено в п. 2, зазвичай, пастки прагнуть ініціювати Location Update. Найпростіше цього досягти, піднявши псевдо-станцію з відмінним від усіх LAC і найсильнішим сигналом.

5. Станція не повідомляє інформацію про станції, що знаходяться поруч, хоча це повинно відбуватися в умовах щільного покриття. Пастка не анонсує інші станції, щоб у телефона "не було спокуси" на них переключитися. А іноді вона анонсує неіснуючі частоти наявних або неіснуючих сусідніх станцій.

6. Анонсування свідомо завищеної CRO (Channel Reselection Offset) – це один із параметрів, який впливає на алгоритм вибору телефоном найкращої базової станції.

7. Відключення шифрування (при тому, що воно раніше було на тій же парі LAC/Cell). Пастка може переключити телефон з A5/3 на A5/0, таким чином виключивши шифрування взагалі або перевівши на слабкий алгоритм A5/2.

8 Повідомлення CIPHER MODE COMPLETE не містить IMEISV. Розглянемо детальніше процес автентифікації і шифрування в GSM. Підключення до GSM-мережі складається з трьох етапів: автентифікація, вироблення ключа шифрування та вибір режиму шифрування.

8.1 Автентифікація:

На SIM-картці абонента зберігається 128-бітний ключ – Subscriber Key Authentication. Точно такий же зберігається в оператора. Оскільки SIM-картка формально належить оператору, а сам ключ зберігається захищеним чином, то це таке поєднання вважається надійним з точки зору організації GSM мереж [3].

Алгоритм взаємодії:

8.1.1 станція генерує випадкове 128-бітне число і посилає його абоненту;

8.1.2 обидві сторони подають на вхід алгоритму A3 128-бітне число і загальний ключ, отримують 32-бітне число SRES (від Signed Response);

8.1.3 абонент надсилає відповідь із цим числом, а станція порівнює зі своїм; якщо все зійшлося, то абонент аутентифікований.

До речі, підтвердження автентичності самої станції не передбачено.

8.2 Генерація ключа шифрування. Процедура ідентична, за винятком того, що випадкове число і ключ подаються на вхід алгоритму A8, а результатом є 64-бітний ключ симетричного шифрування A5.

8.3 Вибір режиму шифрування:

Станція посилає телефону команду CIPHER MODE SELECT, повідомляючи необхідний режим шифрування: A5/0, A5/1, A5/2 або A5/3. Проте в цьому повідомленні є ще регістр REQUEST_IMEISV, який означає, що телефон повинен передати у відповідному повідомленні CIPHER MODE COMPLETE свій унікальний ідентифікатор, причому це повідомлення вже закладено на раніше узгоджену ключі. За замовчуванням регістр завжди вимагає передачі унікального ідентифікатора. Однак пастка, можливо, не вимагає передачі унікального ідентифікатора, в результаті повідомлення CIPHER MODE COMPLETE міститиме передбачувану статичну інформацію. Після цього проводиться стандартна атака за відомим відкритим текстом (known plain text attack), і ключ розкривається. Отже, критерій № 8 реєструє відсутність зазначеного прапора. Ще є додаткова ознака – довге очікування підтвердження отримання станцією CIPHER MODE COMPLETE. Дійсно, розкриття ключа вимагає певного часу.

9. Після Location Update йде стандартний запит абоненту на ідентифікаційну інформацію (IMEI, IMSI), а далі станція відкидає телефон, змушуючи робити новий Update Location. Все це – ознака пастки, що працює в режимі збору інформації.

10. Якщо станція анонсує інший режим шифрування, відмінний від звичайного для зазначеної місцевості або оператора, то це пастка.

11. Занадто маленький інтервал регулярного Update Location. Телефон зобов'язаний періодично посилати Location Update – навіть якщо він не мігрує з однієї соти в іншу. А значення періоду приходить зі станції. Стандартне значення – 1–4 години. Але пастка може поширювати завідомо маленькі тайм-аути, щоб більш оперативно отримувати інформацію про розташування телефонів [4].

12. Прийшла команда Paging, за якою не було ні SMS, ні розмови. Це типова перевірка, чи "жертва" в зоні покриття в конкретний момент часу.

13. Встановлено канал даних (Traffic Channel або TCH), але при цьому не надходило ні SMS, ні встановлення розмови. Або він пішов, але через незвично довгий час. Згідно з протоколом, після встановлення цього каналу телефон безперервно шле порожні підтвердження, поки канал не закриється. Ці підтвердження можуть використовуватися пасткою для більш точного позиціонування телефону.

14. Підозрілий список сусідніх станцій (Neighboring Cells). Кожна станція передає підключеному до неї телефону список оточуючих станцій. Але якщо це пастка, то вона буде відсутня в цих списках – на відміну від інших, легітимних станцій.

15. Розбиття на велику кількість груп (Paging Group). Кожна станція об'єднує всі підключені телефони в групи. Це потрібно для оптимізації ресурсів. Коли відбувається вхідний дзвінок, усі телефони цієї групи отримують сповіщення на відповідному логічному каналі. Коли помилкова станція хоче повернути абонента

у свою стільникову мережу, вона посилає некоректні дані на каналі тієї групи, в яку входить абонент. У результаті всі члени групи почнуть процедуру Cell Reselection. Щоб вибірка була більш точна, помилкова станція робить групи з малою кількістю абонентів, а кількість груп буде великою, що і є ознакою роботи пастки.

В основі безпеки GSM лежить не стільки криптографічна стійкість, скільки висока можливість отримання потрібної інформації до початку роботи алгоритму криптографії. Тут панують виробники телекомунікаційного устаткування і оператори, а обговорення рівня уразливості рідко виходять за рамки експертів злому GSM мереж. З приходом нового стандарту UMTS захищеність була підвищена. Головні переваги нововведення:

– взаємна аутентифікація для захисту від помилкових базових станцій;

– захист цілісності керуючих команд;

– шифрування поширюється не тільки на ділянку "телефон — базова станція", але і на канали всередині серверної частини;

– більш сильне шифрування (128 біт проти 64 біт в GSM).

Висновки

З розвитком комп'ютерних технологій з'являються нові можливості щодо створення умов витоку інформації, у тому числі в галузі стільникового зв'язку. Дані, що обертаються в системі забезпечення та ідентифікації, можуть стати основою для проведення несанкціонованого їх оброблення та відповідно персоналізації особи.

Розгляд джерел загроз у системі обробки даних та ознак підключення сторонніх користувачів дає змогу підрозділам правоохоронних органів проводити детальний аналіз умов витоку даних, а використання засобів захисту дасть змогу збільшити вірогідність збереження персональної інформації абонентів. Впровадження нових стандартів стільникового зв'язку дозволить на певний час унеможливити витік даних з мереж комунікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Попов В.И.* Основы сотовой связи стандарта GSM / В.И. Попов. — М. : Эко-трендз, 2005. — 296 с. : илл. — Бібліогр.: с. 16–66.

2. Телекоммуникационные технологии. Введение в технологии GSM / С.Б. Макаров, Н.В. Певцов, Е.О. Попов и др. — 2-е изд., испр. — М. : Издательский центр "Академия", 2008. — 256 с. : илл. — Бібліогр.: с. 166–200.

3. GSM overview. – Режим доступу: http://personal.ee.surrey.ac.uk/Personal/L.Wood/constellations/tables/gsm.html. – Назва з екрану.

4. Avi Freedman. Handoff in GSM/GPRS Cellular Systems [Електронний ресурс] / Avi Freedman – Режим доступу: http://ieee802.org/21/archived_docs/Documents/OtherDocuments/Handoff_Freedman.pdf. – Назва з екрану.

Отримано 14.09.2016

Рецензент Марченко О.С., к.т.н.