Тех. поддержка:
+7 (812) 458-01-12
info@welltell.com

Желаете сотрудничать с нами:
8-800-333-65-08
sale@welltell.com

welltell.com

VIP Secure

Модель угроз в системе GSM

Использование мобильных устройств в деловой жизни облегчает, ускоряет и оптимизирует бизнес-процессы. При этом необходимо понимать, что чем сложнее становится устройство, тем больше образуется угроз и рисков

Обращаем особое внимание на то, что данный список не является полным, но отражает основные пути утечки информации. Более полная модель угроз описана в документе «Mobile Security Reference Architecture», подготовленном Федеральным советом руководителей информационных служб (Federal CIO Council) США и Министерством внутренней безопасности США (май 2013 года).

Вся описанная информация является максимально упрощённой и предназначена только для ознакомления с процедурами. Более подробную информацию или технические спецификации можно найти в открытом доступе в сети интернет.

Основные источники угроз:

1. СОРМ - Система технических средств для обеспечения функций Оперативно-Розыскных Мероприятий.
2. Поставщик услуги (Оператор Сотовой Связи).
3. Производители мобильных устройств и систем управления (Операционная Система).
4. Перехват трафика в радиоканале (комплексы перехвата: активные, полуактивные, пассивные и другие средства перехвата).

Методы защиты:

1. Динамические идентификаторы (IMSI+Ki, IMEI).
2. Контроль алгоритма A5/1.2.3.0.
3. Политика безопасности на уровне SIM-карты VIP Secure.
4. Искажение голоса.
5. Подмена номера звонящего.
6. Отсутствие данных локации.
7. Отсутствие биллинговых данных.
8. Невозможность установления факта звонка между абонентами.
9. Блокирование атак на уровне HLR.
10. Перехват и блокирование SMS любого класса, в том числе, и так называемых Silent SMS или Stels SMS, на уровне SMSC.

Принципы противодействия:

Чтобы установить технический контроль за мобильным телефоном или SIM-картой, необходимо знать их идентификаторы. Все сети коммуникации во всём мире контролируются государственными регуляторами и технически подключены к СОРМ (вся информация по данной системе доступна в интернете).

Для мобильного устройства основным идентификатором является IMEI *(International Mobile Equipment Identity* — международный идентификатор мобильного оборудования). Данный параметр передаётся в сети.

Для абонента идентификатором является IMSI (*International Mobile Subscriber Identity* — международный идентификатор мобильного абонента (индивидуальный номер абонента)). Данный параметр передаётся в сети.

Публичный параметр MSISDN - (*Mobile Subscriber Integrated Services Digital Number*) — номер мобильного абонента цифровой сети с интеграцией служб для связи в стандартах GSM, UMTS и пр. Данный параметр не передаётся в сети, но сопоставим с IMSI.

Эти параметры достаточны для получения необходимой оперативной информации и использования этих данных для аналитических выводов. Имея эти идентификаторы с помощью СОРМ, комплексов перехвата и других мероприятий, можно получить следующую информацию по абоненту:

- ✓ по IMEI можно получить все IMSI SIM-карт, которые использовались в этом устройстве и, как следствие, все биллинговые данные по этим SIM-картам (локация, круг общения, SMS, MMS, голос, URL-адреса, логины и пароли и т.д.);
- ✓ по IMSI можно получить все IMEI аппаратов и IMSI SIM-карт, которые использовались в этих аппаратах и, как следствие, становятся доступными всё те же биллинговые данные, что и в предыдущем случае.

SIM-карта VIP Secure не имеет биллинга ни у одного из операторов, так как не является их собственностью. SIM-картf VIP Secure не имеет MSISDN в публичном доступе.

Алгоритм работы SIM-карты VIP Secure и обычной SIM-карты в сети GSM
Процедура регистрации телефона в сети и выбора соты

1. После включения телефона с обычной SIM-картой производится сканирование частот и выбор соты с наивысшим уровнем сигнала. SIM-карта VIP Secure работает только с сотой, уровень сигнала которой является вторым по своему значению. Данный алгоритм обеспечивает защиту от комплексов перехвата.

2. После процедуры синхронизации происходит идентификация оборудования и аутентификация абонента в сети. Обычная SIM-карта производит процедуру аутентификации в сети оператора согласно алгоритму А3. Данный протокол производит вычисление ключа SRES, который позволяет завершить процедуру аутентификации. Для вычисления ключа SRES в алгоритме А3 используются параметр IMSI и Ki. В обычной сим карте параметр IMSI вшит в SIM карту, и он не меняется. В SIM-карте VIP Secure несколько профилей со своими парами IMSI+Ki.

Шифрование в сети GSM

Уровень криптования определяется оператором, в сети которого находится абонент. Специальный апплет на SIM-карте VIP Secure оповестит абонента, если данная сеть снизила уровень шифрования.

Вызов

Абонент обычной SIM-карты после набора номер нажимает кнопку вызова. В этот момент телефон посредством высокоскоростного канала управления FACCH отправляет сигнал ALERT на BSS (подсистему базовых станций), а оттуда на MSC (центр коммутации). Далее коммутатор отправляет сообщение AddressComplete на вызывающего абонента. Абонент, сделавший вызов, слышит гудки, а второй абонент звонок вызова.

Зная мобильный номер абонента А или Б (MSIDIN), можно получить от биллинга оператора все детали звонка и саму сессию. Так же можно перехватить эту сессию по воздуху посредством комплекса перехвата.

Прямой вызов (call through) - Абонент VIP Secure после набора номера нажимает кнопку вызов. В этот момент специальный апплет SIM-карты перехватывает вызов и перенаправляет его на сервисный номер. Набранный номер от абонента передаётся на нашу АТС по сигнальному каналу в

зашифрованном виде. Таким образом, все исходящие звонки с SIM-карты VIP Secure производятся на сервисные номера нашей сети. Далее, наша АТС пробрасывает звонок до конечного абонента.

Обратный вызов (Call Back) - Абонент VIP Secure после набора номера нажимает кнопку вызов. В этот момент происходит сброс вызова. Одновременно по сигнальному каналу отправляется команда в зашифрованном виде на серверную АТС (автоматическую телефонную станцию) VIP Secure. АТС VIP Secure через ОКС№7 (SS7) запрашивает у VLR (визитный регистр) для данной SIM-карты и для данного звонка выделить временный номер MSRN (Mobile Station Roaming Number). Как только оператор выделил нашей SIM-карте MSRN, АТС VIP Secure начинает процедуру звонка на этот MSRN. В этот момент происходит вызов на SIM-карту. После того, как абонент VIP Secure поднял трубку, открывается первое плечо. Далее АТС VIP Secure начинает процедуру дозвона второму абоненту. После того, как второй абонент поднимает трубку, открывается второе плечо.

При данной логике совершения звонка невозможно получить информацию из биллинга оператора, так как неизвестно, у какого оператора зарегистрирована в данный момент SIM-карта VIP Secure, нет публичного идентификатора MSISDN, по которому можно было бы получить IMSI, Ki и IMEI. Даже если абонент Б находится на контроле, невозможно понять с кем был разговор, так как сессия состоит из двух плечей, а в разрыве стоит серверная АТС VIP Secure. Таким образом невозможно определить круг общения абонента.

Приём звонка

Звонок на обычную SIM-карту происходит согласно стандартным процедурам. После выполнения процедуры вызова и назначении TMSI (временного идентификатора мобильной станции) в зоне действия VLR, происходит приземление трафика, и сессия считается установленной. При этом биллинг оператора фиксирует, с какого устройства инициирован звонок, местоположение принимающего устройства в момент сессии (локация), длительность разговора и т.д.

Звонок на VIP Secure осуществляется следующим образом. SIM-карте VIP Secure присваивается виртуальный номер DID, который, принимая звонок из сети, преобразовывает его в SIP протокол и маршрутизирует на АТС VIP Secure. В свою очередь АТС VIP Secure определяет конкретного абонента, которому присвоен данный DID, и запускает процедуру вызова, описанную выше.

Таким образом невозможно определить местоположение абонента VIP Secure и взаимосвязи между обоими абонентами, так как в разрыве всегда находится АТС VIP Secure.

Фонетический контроль

Учитывая тот факт, что операторы активно внедряют в свои сети механизмы поиска абонента по фонетическим признакам (отпечатку голоса), VIP Secure даёт возможность искажать акустические характеристики для входящих и исходящих звонков. Данный механизм особенно полезен, если звонок с VIP Secure производится на обычную SIM-карту.

HLR запросы

Учитывая тот факт, что в сетях оператора существуют стандартизированные запросы для обеспечения роуминговых услуг гостевых абонентов, злоумышленники организуют атаки на сетях SS7. Данные атаки выглядят как обычные запросы в сторону HLR оператора эмитента посредством сигнальной системы SS7. Данные запросы нацелены на получение актуальной информации (IMSI, KI, IMEI и т.д.). Так как HLR является составной часть нашей инфраструктуры, мы однозначно перехватываем любые атаки и оповещаем нашего абонента об этом. Данная функция включена в механизм PING.

Stels SMS

Для управления функциями телефона или предустановленными приложениями злоумышленники используют SMS нулевого класса, которые никак не проявляют себя и не сохраняются в телефоне. Такие SMS ещё называют Silent SMS или Stels SMS. Все эти запросы направлены на HLR оператора эмитента. В нашем случае HLR находится в нашей инфраструктуре и, как следствие, мы гарантированно фиксируем все запросы, блокируем их и оповещаем наших абонентов о попытках атак. Данная функция включена в механизм PING.

ИТОГ

SIM-карта VIP Secure, не имея биллинга у операторов, делает невозможным получение необходимой информации для аналитической работы (круг общения (детализации), местоположения (локации), реальных идентификаторов, голоса).

Это стало возможным благодаря контролю всех процессов на трёх уровнях: абонентском устройстве (телефон с изменённой прошивкой), модуле идентификации (SIM-карта VIP Secure со специализированными апплетами) и сетевом уровне (полный контроль HLR, MSC и SMSC).

PS

Всегда надо помнить, что телефон – проприетарное устройство, чёрный ящик, какие в нём закладки, никто не знает кроме производителя, а часто и сам производитель может не знать о каких-то багах. Также необходимо понимать, что операторские инструменты постоянно совершенствуются. Постоянно модернизируются аналитические инструменты, выявляющие одноразовые телефоны по паттернам в биллинге: фиксируется дата первого и последнего звонка с телефона, общее количество звонков и пропорциональный состав уникальных абонентов, с которыми связывались с данной SIM-карты/аппарата. Имея доступ к биллинговым системам всех национальных операторов, можно определять, когда избавились от одного телефона и начали звонить со следующего, а, подключив сюда данные геолокации, можно выявить ареал обитания подозрительного абонента.