Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Технология безопасности SIM-карт

Коротков Павел, гр.111
9.04.2005

В настоящее время беспроводные локальные сети являются одним из основных направлений развития сетевой индустрии. Конечно, вопрос безопасности передаваемых данных, защиты от несанкционированного взлома является очень важным. Ведь SIM-карты в частности, и смарт-карты вообще, являются распространенными объектами для атак различного рода. Это обусловлено рядом причин:

- Успешные атаки дают довольно большие возможности. Иногда профессиональные атаки могут дать существенную выгоду.
- Смарт-карты достаточно дешевые и очень распространенные, и, следовательно, не составляет труда достать их. Соответственно, атакующей стороне предоставляется широкое поле объектов для взлома или сбора статистики.
- При этом смарт-карты являются достаточно маленькими объектами, что существенно облегчает их использование.

При этом обеспечение безопасности в беспроводных сетях – задача, которая намного сложнее, чем аналогичные проблемы в обычных сетях передачи информации, так как в данном случае добавляется сложность охраны данных, связанная с мобильностью клиента, использующего этот сервис.

Стандарт GSM (Global System for Mobile Communications) наиболее распространен в данный момент во всем мире (приблизительно 80% абонентов). Операторы сетей данного стандарта используют для аутентификации клиента специальный модуль SIM (Subscriber Identity Module). Соответственно, SIM-карты играют одну из важнейших ролей в модели операторов GSM и должны надежно хранить информацию, зашитую в них. Но почему-то провайдеры слабо обеспокоены данным вопросом, и новые усовершенствования данного стандарта не намного лучше предыдущих (и, вообще говоря, все алгоритмы в GSM взломаны). Для обеспечения безопасности служат несколько особенностей SIM-карт. Это, прежде всего, дороговизна изготовления новой такой же карты. В настоящее время всего несколько компаний в мире занимаются изготовлением SIM-карт, которые они впоследствии продают всем провайдерам сотовой связи.

Также сейчас SIM-карты содержат больше информации и обладают большей функциональностью нежели раньше, что затрудняет криптоаналитикам их взлом и сбор хранимой информации. Например, некоторые разновидности SIM-карт могут хранить различные аплеты: кроме аплета, стандартного для GSM сетей, также, к примеру, аплета, служащего для биллинга клиента. В настоящее время существует технология, называемая Java-card, которая является подмножеством Java. При этом данная технология является открытой, что, с одной стороны, дает некую возможность для взлома, с другой стороны, обеспечивает легкость расширяемости и масштабируемости рынка. В принципе, этому стандарту (Java-card) удовлетворяет любая карта, на которой реализована JVM (Java Virtual Machine). Для Java-card используются чипы с малой памятью, такие, как в SIM-картах или банковских смарт-картах. Для этой цели (реализации на мобильных телефонах) специально разработан «язык» Java2ME.

Вообще говоря, SIM-карты являются одним из видов смарт-карт. И, соответственно, имеют все преимущества и способы защиты от несанкционированного доступа к ресурсам сети, что и вышеупомянутые смарт-карты.

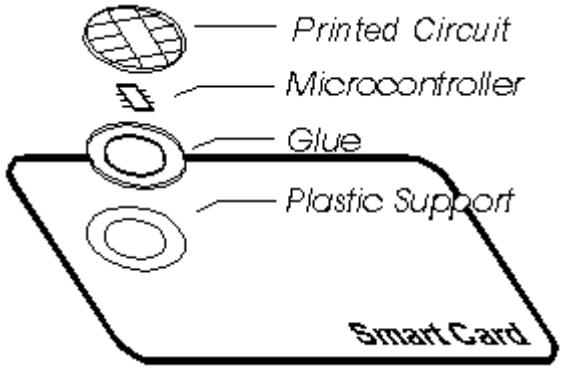
Так как смарт-карты довольно сильно распространены в настоящее время, производители позаботились о том, чтобы информация на них была надежно защищена. Прежде всего, они попытались обеспечить безопасность от физических атак, то есть от попыток взлома сокрытой информации физическим способом. Смарт-карта помещена в эпоксидную резину, которая не дает легкого доступа к чипу, расположенному в смарт-карте, и, тем более, не позволяет считать информацию на нем простым способом. Таким образом, для физической атаки требуется специальное дорогое оборудование.

Вообще говоря, безопасность смарт-карты обеспечивают четыре составляющие.

- Корпус карты
- Полупроводниковая аппаратная структура
- Операционная система
- Прикладное ПО

Три последних средства в данном списке обеспечивают безопасность информации, хранимую на смарт-карте, и программы, исполняемые ее чипом.

Каждая смарт-карта, а, следовательно, и SIM-карта хранит информацию, содержащую ее уникальный идентификационный номер, даваемый ей производителем, тип карты, серийный номер и так далее. При потере карты ее уже бывший владелец может сообщить в организацию, где зарегистрирована эта карта, и данная фирма может записать эту карту в «черный список», то есть они не будут принимать эту карту в своих отделениях. Это особенно актуально при использовании банковских карт.



Также для защиты хранимой информации, а также для защиты передаваемых данных используются криптографические алгоритмы, а именно – RSA, DSA.

Рассмотрим внимательнее SIM-карту и ее взаимодействие с сетью GSM. Механизмы обеспечения безопасности в сети GSM, вообще говоря, обеспечиваются тремя различными элементами. Это, прежде всего, SIM-карта, мобильная станция и сама GSM сеть. В SIM-карту зашита следующая информация: так называемый IMSI (International Mobile Subscriber Identity), уникальный идентификатор данной карты, по которому однозначно определяется абонент, ключ для аутентификации, индивидуальный для каждого абонента, персональный идентификационный номер (PIN – Personal Identification Number). Также в SIM-карте реализованы алгоритм формирования ключа для шифрования A8, алгоритм аутентификации A3. Для шифрования данных в стандарте GSM используется алгоритм A5. Соответственно в базе данных в центре аутентификации содержится база данных с информацией для идентификации и аутентификации, а именно содержит базу данных IMSI, TMSI (Temporary Mobile Subscriber Identity), идентификатор местоположения (LAI – the Location Area Identity), и индивидуальный ключ для аутентификации для каждого абонента данной сети. Чтобы аутентификация прошла успешно, а также, чтобы механизмы обеспечения безопасности правильно функционировали, необходимо

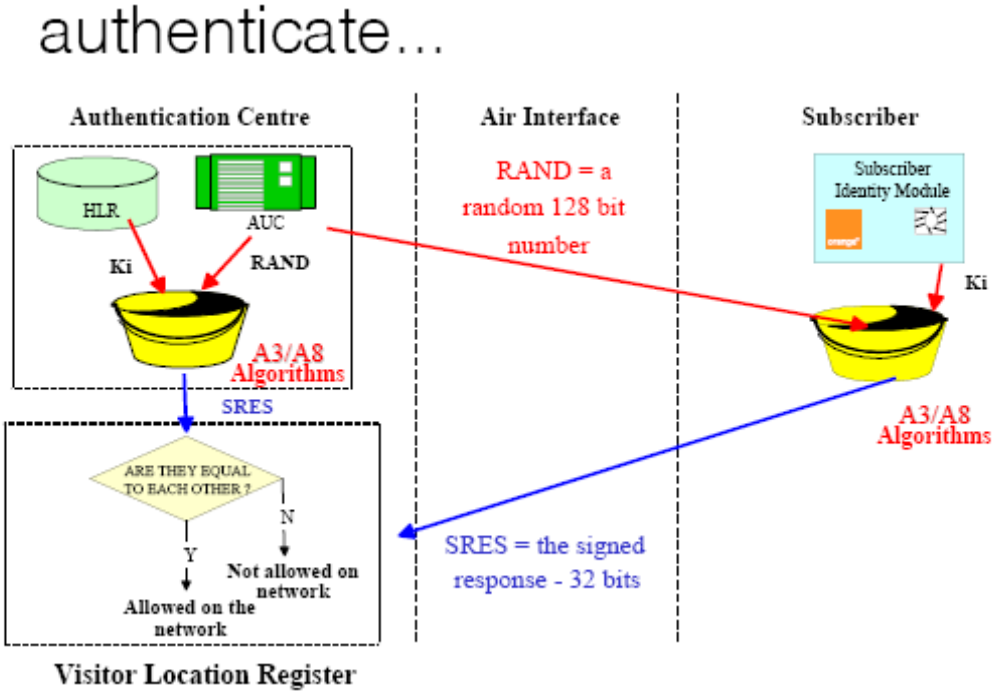
наличие и правильное взаимодействие всех трех элементов. Такое разделение дает дополнительную меру безопасности.

Рассмотрим механизм аутентификации в GSM сети.

Аутентификация происходит в режиме «запрос-ответ». Рассмотрим ее по шагам.

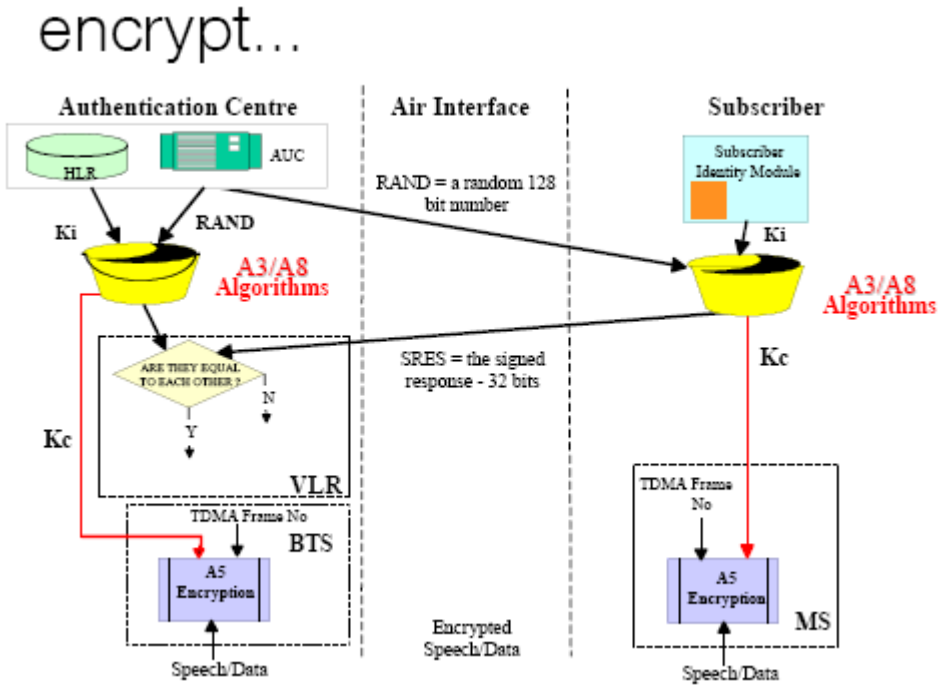
1. Мобильная станция инициирует вызов. Базовая станция устанавливает канал между собой и мобильной станцией, и, далее, мобильная станция посылает свой код IMSI.
2. Базовая станция сопоставляет полученный код с имеющимися у нее в базе данных и генерирует случайное число размером 128 бит.
3. Мобильная станция в свою очередь вычисляет ответное число по вышеупомянутому алгоритму аутентификации A3 на основании этого самого полученного случайного числа и индивидуального ключа аутентификации.
4. После получения этого ответа центр в GSM сети проделывает те же вычисления, что и мобильная станция, для того чтобы проверить аутентификацию пользователя. Естественно, что если данная проверка завершилась удачно, то есть полученное значение и вычисленное совпали, то базовая станция аутентифицирует клиента. В противном случае она разрывает канал.

Из рассмотрения данного протокола видно, что индивидуальный ключ для аутентификации не передается по радиоканалам, все вычисления происходят внутри SIM-карты или центра мобильной связи, и данный ключ не покидает SIM-карту во время процесса аутентификации, что, несомненно, улучшает безопасность данного стандарта...



Для шифрования передаваемых данных мобильной и базовыми станциями используется алгоритм A5. Данный алгоритм использует сессионный ключ выработанный независимо мобильной и базовой станциями по алгоритму A8, по которому генерируется 64-битный ключ. Для этой цели алгоритм A8 использует индивидуальный секретный ключ аутентификации, хранящийся в SIM-карте (и в базе данных GSM сети), и случайное число, сгенерированного базовой станцией и полученного мобильной станцией в процессе аутентификации. Как и в случае

аутентификации, ключ для шифрования не передается по радиоканалам, а вычисляется независимо внутри SIM-карты и в мобильном центре.



Разбор и описание данных алгоритмов (A3, A5, A8), используемых в стандарте GSM, я производить не буду, скажу лишь, что для взлома алгоритмов A3 и A8, служащих для выполнения аутентификации и генерирования ключей шифрования соответственно, надо достаточное количество раз произвести аутентификацию, чтобы на основе собранной статистики найти зашитый в SIM-карте секретный ключ. Алгоритм A5 был разработан в восьмидесятых годах прошлого столетия и официально нигде не публиковался и вроде как является тайной. Но на данный момент он полностью взломан. Данный шифр используется для сокрытия информации, передаваемой во время связи между мобильной станцией и базовой станцией. Можно построить криптоаналитическую атаку с известным открытым текстом. Так как сеансовый ключ генерируется на основе секретного ключа SIM-карты и случайного числа, передаваемого в открытой форме, то с помощью успешных атак для вскрытия сеансового ключа можно вскрыть секретный ключ. Таким образом, в сетях GSM используются старые алгоритмы, которые в настоящее время могут быть довольно быстро взломаны при наличии мощного компьютера.

Чтобы взломать систему аутентификации криптоаналитику надо перехватить какое-то количество триплетов, состоящих из случайного числа, генерируемого сервером, ответом мобильной станции и ключа, необходимое для составления статистики. Для подобной атаки «третьей» стороне необходимо располагать SIM-картой, с помощью которой она будет выполнять многократную аутентификацию. В настоящее время количество возможных соединений для совершения аутентификации ограничено, то есть после определенного числа таких попыток SIM-карта приходит в негодность, и дальнейшие попытки взлома бесполезны. Компании, производящие SIM-карты, утверждают, что количество таких попыток достаточно для обычного использования и его хватает на весь срок жизни карты, но существенно мало того количества, которое нужно для взлома кодов, используемых в данных алгоритмах.

Помимо попытки завладеть секретным ключом SIM-карты, описанной выше, криптоаналитик может попытаться завладеть данными, хранимыми на карте, либо изменить их. Стандарт SIM предусматривает, что для доступа к большому количеству данных необходимо ввести PIN код. В большинстве случаев есть сильное ограничение

на количество попыток ввести правильный пин-код. После достижение этого предела, карта блокируется и пользователь должен ввести другой секретный код, называемый PIN2. На ввод этого кода тоже есть ограничение попыток. Если же вдруг пользователь и на этот раз не набрал нужный код с выделенного количества попыток, то карта приходит в негодность и больше не может быть использована.

В настоящее время выпускаются также карты с разделенным модульным дизайном и разделением приложений. Распространенная операционная система для таких карт называется Java-карты. Такие операционные системы являются очень гибким и мощным средством разработки. Приложения могут быть написаны и внедрены после того, как карта спроектирована и даже выпущена. Соответственно, как подразделение смарт-карт, выпускаются SIM-карты, в которых реализовано использование аплетов, которые нужны для поднятия функциональности. Соответственно GSM аплеты и GSM структура являются расширением структуры Java-карт. Механизмы защиты в среде GSM позволяют оператору удаленно управлять его базой данных SIM-карт. Аплеты, написанные на языке Java, обладают широким набором средств по обеспечению безопасности хранимых данных. Криптографические алгоритмы могут быть имплементированы в аппаратные средства, но всегда должна быть программа, контролирующая их запуск, которая хранится в долговременной памяти. Поэтому применение языка Java является хорошим решением для защиты хранимых данных.

Использование возможностей Java сильно увеличивает защищенность смарт-карт. В Java-карты интегрированы три дополнительных средства безопасности. Это так называемая атомарность транзакций (Transaction atomicity), дополнительные криптографические классы, защитная система аплетов (applet firewall). Первое упомянутое средство, то есть атомарность транзакций, решает проблему прерывания запросов и изменений в памяти карты. То есть, если транзакция прошла успешно, то изменения будут занесены и сохранены, если же что-то помешало закончится транзакции правильно, изменения не будут учитываться и система вернет память в исходное состояние, в котором она находилась до начала выполнения этой транзакции.

Идея «фаерволла» (firewall) заключается в обеспечении полной изоляции памяти, используемой аплетом от других кусков памяти, в частности, от памяти, которую используют другие аплеты в этой карте. Таким образом, исключается возможность воздействия одних Java-приложений на другие и операционную систему в целом.

Криптографические классы, упомянутые выше, дают возможность шифрования и расшифрования алгоритмами симметричных и асимметричных криптосистем, создание подписи и проверка и так далее. Также, они дают возможность управлять PIN-кодами.

Литература:

1. Ameen Ahmad, Roger Chandler, Abhay A. Dharmadhikari, Uttam Sengupta, *"SIM-based WLAN authentication for open platforms",* Technology@Intel, August 2003. *www.linuxdevices.com/articles/AT7681519444.html*
2. Jane Dashevsky, Edward C. Epp, Jose Puthenkulam, and Mrudula Yalemanchi, *"SIM Trust Parameters",* Intek Developer Update Magazine, January 2003. *www.intel.com/technology/ magazine/communications/wi01032.pdf*
3. Florian Eisl*, "Smart Card Security Services for an Open Application Environment used in Mobile Phones"*, Sony Ericsson Mobile Communications AB, Lund, June 2004. *www.iicm.edu/thesis/feisl_magisterarbeit.pdf*
4. Marc Witteman, *"Advances in Smartcard Security"*, Information Security Bulletin, July 2002. *www.riscure.com/articles/ISB0707MW.pdf*
5. CHAN, Siu-cheung Charles, *"An Overview of Smart Card Security" http://home.hkstar.com/~alanchan/papers/smartCardSecurity/*
6. "GSM Security" *www.orange.co.uk/business/corporate/office/channelpartner/**gsm_security**.pdf*