Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 11 (138)/2004

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Хакер Джеймс Хедли Чейз

Алексей Галатенко

Проблемы информационной безопасности, разумеется, существуют не только в компьютерном, виртуальном, но и в реальном, «физическом» мире (хотя, конечно, там они не носят столь масштабный, всепроникающий характер). Любопытно и, на наш взгляд, весьма поучительно сопоставлять действия, приемы и методы компьютерных хакеров и «физических» мошенников, а также тех, кто оказывается объектом их атак.

Обильную пищу для подобных сопоставлений дают два детективных романа Джеймса Хедли Чейза (James Hadley Chase) — «Все дело в деньгах» («What's better than money?») и «Двойная сдача» («The Double Shuffle»), опубликованные в русском переводе московским издательством «Центрполиграф», соответственно, в 2001-м и 2000-м годах. (Дальнейшее цитирование производится по этим изданиям. Естественно, оно носит фрагментарный характер).

В романе «Все дело в деньгах» события происходят в конце 1950-х годов. (Заметим в скобках, что уже тогда компьютеризация производственных процессов достигла весьма высокого уровня. Несомненным лидером среди производителей ЭВМ была корпорация IBM, большие машины которой управляли, например, работой сборочных конвейеров крупнейших автозаводов, что уже в то время давало возможность осуществлять конвейерную сборку автомобилей по индивидуальным заказам, в индивидуальной комплектации). Главный герой романа — Джефф Холлидей. Его шантажирует женщина по имени Рима Маршалл.

Предоставим слово Дж. Х. Чейзу и его персонажам.

... Она улыбнулась мне, и от ее улыбки у меня все похолодело внутри.

— Я знаю, что ты задумал, Джефф. ... Ты ведь решил убить меня, не так ли, Джефф?... На этот случай у меня есть меры предосторожности. — Она швырнула мне на колени клочок бумаги. — Будешь переводить мне деньги на этот счет. Это счет в банке «Пасифик энд Юнион» в Лос-Анджелесе. Это не мой банк, но у них есть указание переводить деньги на другой счет, и ты никогда не узнаешь, куда именно.

Я не оставлю тебе никаких шансов. Ты никогда не сможешь узнать, куда мне переводят деньги и где я буду жить. Так что не надейся, что сможешь убить меня, Джефф, потому что после этой встречи ты никогда меня больше не увидишь.

Я с трудом поборол отчаянное желание схватить ее за горло и задушить прямо здесь.

— Я смотрю, ты обо всем позаботилась?

— Думаю, что да. ... Я ухожу.

Если она сейчас уходит, мне надо пойти за ней. Если потеряю ее из виду, не смогу больше найти. ...

Жирный итальянец снова появился на пороге своей каморки, на этот раз в сопровождении двух очень подозрительных личностей, и они встали возле выхода.

— Я попросила этих ребят задержать тебя здесь, пока я исчезну, — сказала Рима. — На твоем месте я бы не стала с ними связываться. Они ребята крепкие...

Рима вышла из отеля, быстро сошла по ступенькам и исчезла в темноте...

Процитированный фрагмент богат любопытными моментами. Главный герой хотел бы разделаться с шантажисткой, но та, даром что наркоманка и вообще женщина легкого поведения, применила анонимизатор, чтобы Холлидей не смог ее найти. Дополнительным защитным рубежом, предназначенным для того, чтобы на некоторое время задержать атакующего, послужили меры физической защиты.

Итак, перед героем встала задача найти Риму Маршалл (подчеркнем — с двумя «л» в конце фамилии) по косвенной ссылке — номеру промежуточного банковского счета. Для ее решения в усло-

виях отсутствия сетевой связности Холлидею пришлось физически добираться до банка.

... Самолет приземлился в аэропорту Лос-Анджелеса около часа дня. Я взял такси и поехал в банк «Пасифик энд Юнион».

В последние две недели каждую свободную минутку я напрягал свой мозг, пытаясь придумать, как разузнать адрес второго банка, куда Риме пересылали деньги. Ясно, что в «Пасифик энд Юнион» он есть, и я должен был разузнать, где могут содержаться эти данные.

Расплатившись с таксистом я вышел и с облегчением увидел, что банк довольно крупный; ведь я боялся, что он окажется небольшим отделением с маленьким штатом сотрудников, которые легко запомнят меня.

... В глубине офисного помещения сидели клерки, занятые работой с калькуляторами, копировальными аппаратами и тому подобным. Еще дальше находились специальные кабинки для служащих банка.

Я встал в конец небольшой очереди, предварительно взяв со стойки бланк на открытие счета. Вытащил из бумажника десять пятидолларовых купюр. Через несколько минут я был уже вторым и, облокотившись на стойку, в нужных местах написал на бланке большими печатными буквами «РИМА МАРШАЛ» и «Оплачено Джоном Гамильтоном»....

Операционист взглянул на квитанцию, поднял резиновую печать, но вдруг нахмурился.

...

— Боюсь, вы ошиблись, сэр, — сказал он, посмотрев на меня.

Я повернул к нему голову.

— Что значит «ошибся»?

Поколебавшись, он еще раз посмотрел на бланк:

— Сейчас, одну секунду...

Все сработало как нужно. Он взял с собой квитанцию и, отойдя от своего места, быстро прошел вдоль стойки к лестнице, которая вела наверх. Я отошел от стойки, чтобы мне было его видно. Он поднялся по лестнице на галерею, которая шла по всему периметру холла, и подошел к девушке, сидевшей возле большого аппарата, и что-то сказал ей. Она повернулась на крутящемся стуле к большой таблице, которая висела на стене. Она провела пальцем по таблице вниз, мне показалось, по какому-то списку имен, потом повернулась к своему аппарату, нажала кнопку, и через секунду оттуда выскочила карточка, которую она отдала операционисту.

Сердце мое учащенно забилось. Я знал, что это был за аппарат — автоматическая поисковая машина. У каждого клиента банка был свой код, в обмен на который машина выдавала все данные клиента.

Я видел, как операционист внимательно смотрит в карточку, потом на мою квитанцию. Он отдал карточку обратно девушке и заспешил ко мне.

— Вероятно, вкралась какая-то ошибка, сэр, — сообщил он. — У нас нет такого клиента. Вы уверены, что имя написано правильно?

Я подернул плечами:

— Ну, не знаю. Это карточный долг. ... Она дала мне название вашего банка. По-моему, у нее другой банк, и вы просто пересылаете ей туда деньги.

Он пристально посмотрел на меня.

— Все верно, сэр, мы оказываем эту услугу нашим клиентам, но среди них нет дамы с таким именем. Может быть, Рима Маршалл? С двумя «л»?

— Откуда я знаю, — сказал я. — Лучше еще раз уточню. — Потом небрежно, как бы между прочим, я спросил: — Кстати, может быть, вы просто дадите мне ее адрес, и я вышлю ей чек?

Он и глазом не моргнул:

— Если вы пошлете письмо на адрес банка, сэр, можете не сомневаться, что мы немедленно перешлем его ей.

Я знал, что он ответит именно так, но все равно почувствовал разочарование...

Как мы видим, герой задумал осуществить несанкционированный доступ к информационной системе банка с целью раскрытия конфиденциальной информации.

Первым этапом операции, как и положено, является разведка. Отслеживание обработки пробного (и заведомо некорректного) запроса позволило определить расположение основных компонентов ИС (этому способствовала физическая открытость инфраструктуры обработки данных) и точно определить цель атаки — автоматическую поисковую машину.

Отметим, что фактором, способствующим сокрытию следов и успеху злоумышленной деятельности, является большой объем регистрационной информации и связанные с этим сложности ее анализа и выявления подозрительной активности (в большом банке не запоминают посетителей и нюансы их поведения).

Обратим внимание на образцовые действия операциониста. Он не дал вовлечь себя в выполнение запроса, запрещенного политикой безопасности, и переадресовал атакующего к соответствующему штатному сервису, сохраняющему анонимность адресата.

После разведки наступает очередь следующей фазы — прямой атаки.

... Первый шаг сделан. Теперь я знал, где содержатся данные о клиентах. Оставалось их только достать. Я взял такси и приехал в тихий недорогой отель, снял там комнату и, как только зашел в свой номер, сразу же позвонил в банк «Пасифик энд Юнион». Я попросил, чтобы меня соединили с управляющим.

Когда управляющий взял трубку, я представился Эдвардом Мастерсом и спросил, не можем ли мы встретиться завтра в десять утра. Я сказал, что у меня к нему деловое предложение. Он назначил мне встречу на десять пятнадцать...

Герой применил маскарад — стандартный прием злоумышленников.

... В банке я был за минуту до назначенного времени. Меня сразу же провели в кабинет управляющего. ...

Я начал с того, что являюсь представителем крупной строительной фирмы. ... В ближайшее время мы намерены открыть филиал в Лос-Анджелесе. А посему решили открыть счет в «Пасифик энд Юнион». Я намекнул, что у нас весьма солидная фирма с большим оборотом. ... Похоже, я произвел на него впечатление. ...

Все, что в его силах, сказал он, он будет счастлив исполнить. Мне стоит только попросить, и все услуги банка в моем распоряжении.

— Думаю, больше мне пока ничего не понадобится, — сказал я. Помолчав, добавил: — Впрочем, вот еще что. Я заметил, у вас тут очень современное оборудование. Нечто подобное я хочу установить у себя в офисе. К кому мне обратиться? ... В некотором роде наш бизнес сродни вашему. . — Я осторожно приближался к цели визита. — У нас есть клиенты по всей стране. И мы постоянно должны поддерживать с ними связь. Причем приходится все время обновлять данные. Я заметил, у вас есть автоматическая поисковая машина. Похоже, она довольно удобная. Вы сами ею довольны?

Мне повезло. По-видимому, этот агрегат составлял предмет его гордости.

...

— Прошу вас, мистер Мастерс, если она вас заинтересовала, я буду счастлив показать, как она работает. Мы ею очень довольны. Хотите посмотреть машину в действии? ... Я сейчас попрошу мистера Флемминга показать ее вам.

...

Я поднялся. Ноги у меня слегка обмякли. Я уже был на полпути к цели, но впереди маячила вторая половина...

В отличие от операциониста, управляющий поддался на уловку героя, предъявившего поддельный, самоподписанный атрибутный сертификат. Вместо того, чтобы этот сертификат верифицировать, он соблазнился привлекательными для банка значениями атрибутов и делегировал права доступа к поисковой машине.

... Девушка, сидевшая за машиной, повернулась на своем стуле и вопросительно посмотрела на нас. Флемминг представил меня, затем, подавшись чуть вперед, начал свой рассказ.

— У нашего банка три тысячи пятьсот клиентов, — говорил он. — Каждому присвоен номер. Список номеров размещен на этом табло.

Он указал на уже известную мне таблицу. Я подошел поближе и принялся ее разглядывать, лихорадочно пробегая по столбцам имен. Наконец нашел имя Римы. Ее номер был 2997.

Мой мозг впитал эти цифры, как никогда еще ничего не впитывал, быстро и жадно.

— После того как мы нашли номер, — продолжал Флемминг, — все, что нам остается, — это набрать его на клавиатуре, и регистрационная карточка немедленно выскакивает вот на этот поднос.

— Объясняете вы понятно, — сказал я. Но как это работает?

Девушка снисходительно улыбнулась мне:

— Поверьте, эта машина работает безотказно.

— Тогда продемонстрируйте нам, — попросил я, улыбнувшись ей в ответ.

— Возьмем первый номер в нашей таблице, — сказал Флемминг. — Р. Айткен. Номер 0001. Мисс Лейкер, дайте нам карточку мистера Айткена.

Девушка повернулась к машине, и пальцы пробежали по клавишам. Машина ожила, загудела и точно выплюнула на поднос карточку.

— Вот так она работает, — сказал Флемминг, улыбаясь счастливой улыбкой.

Я протянул руку:

— Позвольте мне. Я скептик. Может быть, это карточка не мистера Айткена.

По-прежнему улыбаясь во весь рот, он протянул мне карточку. Наверху жирным шрифтом было напечатано имя Айткена.

— Пожалуй, впечатляет. Наверное, действительно имеет смысл платить за нее такие деньги. А можно, я сам попробую набрать номер?

— Конечно, господин Мастерс. Прошу вас.

Я склонился над клавиатурой. Я нажал клавиши, которые сложились в номер 2997. Сердце мое так бешено стучало, что я испугался, как бы Флемминг и девушка не услышали его.

Машина снова загудела. Карточка показалась в металлической щели. Я почувствовал, как у меня на лице выступает пот. Я смотрел на машину не отрываясь и ждал. Наконец карточка оказалась на подносе.

Флемминг и девушка улыбнулись.

— Номер, который вы набрали, принадлежит мисс Риме Маршалл, — провозгласил Флемминг. — Посмотрите сами и убедитесь, что это ее карточка.

Я протянул руку. Вот что я увидел: «Рима Маршалл. Счет. Санта-Барбара. Кредит $10 000».

— Просто чудо. — Я, как мог, старался скрыть дрожь в голосе. — Что ж, большое спасибо. Это как раз то, что мне нужно.

Полчаса спустя я уже мчался в Санта-Барбару на взятой напрокат машине...

Получив физический доступ к поисковой машине, герой выполнил нужный запрос и раскрыл необходимую ему конфиденциальную информацию. Дальше требовалось сделать следующий шаг — пройти по ссылке и найти саму Риму. Холлидей едет в известную всем Санта-Барбару.

... Прямо напротив банка располагался небольшой отель. ... Я попросил комнату с видом на улицу. ... Я подошел к окну. Банк был как на ладони. ... Я знал, что не посмею повторить тот же трюк, что использовал в Лос-Анджелесе, дабы взглянуть на ее регистрационную карточку. ... Если я буду сидеть у окна и наблюдать, возможно, мне удастся увидеть, когда она придет в банк, а потом выследить ее.

Но для этого нужно много времени. А я должен быть на работе не позже послезавтрашнего утра. Но может быть, мне повезет, и завтра я увижу ее. Я решил ждать, хотя шансов, что она появится здесь именно завтра, ой как мало.

На следующее утро ... я придвинул стул и сел к окну. ... Я надеялся до последнего. Но когда двери банка закрылись, я впал в такое отчаяние, что готов был перерезать себе горло. ... Похоже, шансов найти Риму до того, как придет срок второго платежа, больше не было.

Весь вечер я лихорадочно пытался придумать какой-нибудь другой способ ее поиска, кроме безнадежного наблюдения за банком, но не смог.

Совершенно бесполезно было ходить по улицам в надежде случайно ее встретить. К тому же это было опасно. Вдруг она заметит меня первой и исчезнет из моего поля зрения навсегда.

Внезапно мне в голову пришла идея. А может быть, обратиться в детективное агентство? Но потом понял, что не посмею этого сделать.

Потому что, когда ее найдут, я должен буду ее убить.

А в агентстве меня наверняка запомнят. Они скажут полиции, что это я их нанял, и полиция начнет розыск.

Я должен сделать все сам...

Для достижения цели герой не придумал ничего лучшего, кроме как прослушивать (просматривать?) сетевой трафик вблизи сервера в надежде на то, что разыскиваемый клиент обратится в это время к этому серверу. Поскольку эту деятельность не представлялось возможным автоматизировать или перепоручить агенту-посреднику (прокси-агенту), пришлось осуществлять ее самому. Как и следовало ожидать, результат оказался отрицательным.

Отметим, что атакующий опасается действовать там, где хорошо налажен сбор и анализ регистрационной информации (в небольшом отделении банка, в детективном агентстве), считая опасность прослеживания источника атаки реальной.

Прошло несколько дней. Герой перевел на счет шантажистки очередную сумму, ударным трудом заработал еще несколько отгулов и решил повторить попытку, вернувшись в Санта-Барбару. Наблюдение за банком вновь ничего не дало. В отчаянии Холлидей решает расширить зону прослушивания сети, осуществляя его в случайных точках. Он отправился бродить по улицам; как и следовало ожидать, в полном соответствии с законами жанра ему повезло...

... Я собрался уже было идти дальше, как вдруг из ресторана выбежал крупный мужчина и, нагнув голову, ринулся по деревянному пирсу в мою сторону. Когда он пробегал под фонарем, свет упал на его плечи, и я вдруг узнал кремовое пальто и брюки бутылочного цвета. Это был приятель Римы!

Если бы не дождь, ему не пришлось бы бежать, нагнув голову, и он бы заметил меня и наверняка узнал. ...

Теперь он искал что-то в бардачке «понтиака»-кабриолета. ... Потом он, видимо, нашел, что искал, развернулся и рванул назад в ресторан.

Некоторое время я смотрел ему вслед. Затем неторопливо подошел к «понтиаку» и осмотрел его. Это был выпуск 1957 года, в довольно плохом состоянии. ... Я быстро нащупал регистрационный ярлычок на руле и поднес к нему зажигалку. На нем было аккуратно выведено: «ЭД ВАЗАРИ. Бунгало. Восточный берег, Санта-Барбара».

...

Была ли Рима с ним в ресторане? Живут ли они вместе по этому адресу?

...

И тут я их увидел. Они бегом выскочили из ресторана, ... нырнули в «понтиак» и умчались. Если бы я внимательно не следил за машиной, наверняка пропустил бы их, так молниеносно все это произошло...

В информационных системах у объектов может быть несколько представлений. Если права доступа к этим представлениям различаются, есть вероятность раскрытия конфиденциальной информации. В данном случае общедоступная информация о владельце автомобиля оказалась альтернативным представлением тщательно скрываемого адреса Римы Маршалл.

Обратим внимание на важность постоянной готовности и высокого уровня детализации при сборе регистрационной информации. Смотреть надо всегда и все — вдруг пропустишь что-нибудь интересное?

Итак, герой получил нужную ему информацию. Что было дальше — спросите у Чейза...

Центральная проблема романа «Двойная сдача» — идентификация и аутентификация. Это и неудивительно, поскольку там действуют сестры-близнецы, похожие как две капли воды, только одна из них — брюнетка, а вторая — блондинка. Начальник отдела претензий страховой компании (его фамилия Мэддакс) поручает следователю Стиву Хармасу разобраться с подозрительным полисом. Стиву помогает его жена Элен.

Сначала, как положено, Мэддакс вводит Хармаса в курс дела. Он упоминает страхового агента Алана Гудьера, продавшего полис.

... — Пока меня не было — пояснил Мэддакс, — эта компания приняла полис, к которому я бы не рискнул притронуться даже двадцатифутовой палкой. ... Все наши агенты думают только о комиссионных и ни о чем другом.

...

— Что за проблемы с этим полисом?

...

— Это нестандартный полис. Это первое. Компания с такой репутацией, как наша, не имеет права выдавать нестандартные полисы. ... Мы тратим тысячи долларов каждый год, чтобы платить юристам, которые составляют нам надежные типовые договоры, и вдруг ни с того ни с сего принимаемся писать договор сами!

...

— ... После того как Гудьер продлил страховку, он пошел в бар, видимо, чтобы это дело отпраздновать. Вот тебе пример того, как наши агенты тратят рабочее время. ... По его словам, он разговорился с парнем, который назвался Брэдом Деннн, мелким театральным агентом. Разговор у них зашел о страховании от несчастных случаев, и Деннн сообщил Гудьеру, что как раз такая страховка интересует актрису, которую он представляет. Одно только это должно было бы насторожить Гудьера: полисы на страхование от несчастных случаев клиентам приходится всучивать насильно, на них спроса нет, и когда кто-то заводит разговор о такой страховке для другого, то сигнал тревоги звенит вовсю! Но этот болван Гудьер подумал только о новом куске комиссионных, который ему пригодится, чтобы заплатить за свою распрекрасную машину. В тот же вечер он назначил встречу с этой девицей в отеле «Корт». ... Даже мне известно, что отель Корт — это такое место, где можно снять номер на час, и никаких вопросов! ... Агент, знающий свое дело, не будет иметь дело со страхователем, который живет в отеле «Корт»!...

В процитированном фрагменте представлен целый букет признаков подозрительной активности (в данном случае — нетипичного поведения), на которую у начальника отдела претензий особый нюх. То, что страховой агент эти признаки проигнорировал, Мэддакс объяснил желанием получить комиссионные. Гипотеза правдоподобная, но не единственно возможная...

Очень важный и поучительным момент — опасность использования нестандартных решений (нестандартной политики безопасности, архитектуры, реализации и т.п.). С вероятностью единица можно утверждать, что в сложных нестандартных решениях есть уязвимости, поддающиеся эксплуатации злоумышленниками. Апробированность и простота — краеугольные камни информационной безопасности.

Продолжим цитирование...

... — Он встретился с этой девицей, — продолжал Мэддакс. — Ее зовут Сьюзен Джеллерт. Ее интересовало личное страхование от несчастного случая на сумму сто тысяч долларов. По-видимому, она занята в шоу-бизнесе и готовит новый номер. Частью этой подготовки является использование страховки в рекламных целях. Не понимаю, чего ради прессу должен потрясти тот факт, что какая-то актриса застраховалась от несчастного случая на сто тысяч долларов, а Гудьер и не подумал полюбопытствовать.

...

— Эта девица и Денни внесли некое предложение. Они сказали, что пока не заинтересованы в страховании жизни этой девицы, полис им нужен был для того, чтобы ее имя попало в газеты. Они предложили сделать так, чтобы мы не несли ответственности за любые известные риски, и эти риски должны быть перечислены в страховке. Поэтому, по их словам, взносы можно было бы сделать чисто символическими. ... Вот он, этот полис. ... Втроем они соорудили список известных рисков смерти, и эти риски здесь перечислены. ... Улавливаешь смысл? Если эта девица погибнет по одной из указанных здесь причин, мы не платим, но если она умрет по какой-нибудь другой причине, которая здесь отсутствует, то мы платим. Ты понял? ... Я сейчас тебе его зачитаю. Слушай внимательно, он довольно длинный. — Он начал читать. — «Гражданин, застрахованный по этому полису, не имеет претензий к компании, если его смерть наступит вследствие выстрела, удара ножом, действия яда, пожара или утопления в воде, любого несчастного случая, связанного с общественным транспортом, воздушным транспортом или автомобилями, велосипедами, мотоциклами или любыми другими средствами передвижения, вследствие самоубийства или болезни, падения с большой высоты или ранения упавшими сверху предметами, вследствие удушения, асфиксии, ожогов или черепно-мозговых травм, в связи с нападением домашних или диких животных, насекомых или рептилий, в связи с неисправностью электропроводки или оборудования любого типа». ... Перечислив эти риски, она получает страховку на сто тысяч при взносах пятнадцать долларов в год!

— Это просто грабеж, — улыбнулся я. — Гудьер предусмотрел все риски.

— Ты уверен? — Мэддакс подался вперед. — Ладно, мы к этому еще вернемся. ...— Он схватил полис и потряс им передо мной. — Здесь черным по белому написано, что мы заплатим сто тысяч долларов, если девица умрет по любой причине, кроме тех, что указаны в полисе! По любой другой причине! Разве не чудная ситуация для какого-нибудь хитрого негодяя, который хочет нас надуть?

— Неужели? — с некоторым раздражением осведомился я. — По-моему, Гудьер предусмотрел все риски...

Как известно, есть два разных подхода, закладываемых в основу политики безопасности. Первый звучит как «разрешено все, что не запрещено», второй — «запрещено все, что не разрешено». Страховой полис Сьюзен Джеллерт построен в соответствии с первым подходом. Его родовой дефект в том, что на практике предусмотреть все опасные случаи и запретить их невозможно. Описываемые в романе Чейза события наглядно демонстрируют это. Вне всяких сомнений, следует применять только второй подход.

... — Понимаю. Вчера я думал точно так же. Но теперь я так не думаю. ... Я сегодня обедал с Эндрюсом из «Дженерал лайабилити» и упомянул эту девицу Джеллерт. Он мне сказал, что его компания приняла полис на точно таких же условиях и для той же самой девицы! ... Я пошел и поговорил еще кое с кем. ... Мисс Джеллерт заключила такие же договоры на ту же сумму еще с девятью страховыми компаниями, что в итоге дает миллион долларов при ежегодных взносах в сто пятьдесят долларов. Ну и что ты теперь скажешь?

— Миллион! — присвистнул я. — Большая сумма, но это не доказывает, что сделка мошенническая.

— Еще какая мошенническая, — мрачно произнес Мэддакс. — Более того, это план убийства!

— Но постойте...

— Да, именно так! — заявил Мэддакс, треснув кулаком по столу. — За двадцать лет я в таких вещах ни разу еще не ошибся. Я чую убийство!...

Если в системах активного аудита применяется пороговый подход, а злоумышленникам требуется получить определенное количество ресурсов, они могут осуществить распределенную атаку, запрашивая необходимые ресурсы у нескольких систем и при этом не превышая индивидуальных пороговых значений контролируемых параметров. Один полис на миллион долларов — это слишком, а десять на сто тысяч каждый — приемлемо. У сетевых систем по сравнению с изолированными свои риски, поскольку у злоумышленников в распределенной среде имеется масса дополнительных возможностей для проведения успешных атак.

Далее Мэддакс и Хармас делают слабую, несистематичную попытку протестировать нестандартную политику безопасности и найти в ней изъян, но это им не удается, что, конечно, не доказывает, что подобного изъяна не существует. Мэддакс абсолютно прав, что не заостряется на конкретном способе убийства, а желает решить проблему кардинально — аннулировать полис.

... — Но скажите мне, каким образом он [Денни] собирается ее убить и предъявить нам претензию?

...

— Да, понимаю, все это кажется вполне надежным, не так ли? Но я поставлю свой последний доллар на то, что этот парень знает, как обойти список.

— Хорошо, допустим, но это ничего не говорит о том, каким образом он мог бы ее убить. Если бы вы придумали хотя бы один способ, я бы больше поверил в то, что это мошенничество.

Немного поразмыслив, Мэддакс неуверенно предположил:

— Ну, она может умереть от страха. В полисе этого нет.

— Вы шутите? Да, люди умирают от страха, но судебный следователь называет это инфарктом, а инфаркт — это болезнь, и в полисе она предусмотрена. Нет, нужно что-нибудь более оригинальное.

Мэддакс пожал плечами:

— Кто бы ни стоял за всем этим, он придумал заковыристую идею, которую мы за пять минут не разгадаем. Меня это не волнует. Я хочу аннулировать этот полис, пока на нас не свалился какой-нибудь сюрприз. ... Кроме перечисленных причин смерти, которые вызвали бы подозрения у любого мало-мальски опытного человека, есть еще вот эта штучка внизу страницы. Взгляни-ка.

Он бросил мне полис. Под незамысловатой, словно нацарапанной детской рукой подписью, я увидел чернильное пятно и четкий отпечаток большого пальца.

— Узнай у Гудьера, — сказал Мэддакс, — ее ли это отпечаток. Выясни, как он оказался на полисе. Мне кажется, его оставили намеренно, и причина может быть в их желании гарантировать, что мы не попытаемся увильнуть от оплаты, усомнившись в подлинности документа...

Вот, наконец, мы добрались до проблем аутентификации, причем биометрической и, кроме того, удаленной (Мэддакс и Хармас не видели, кто и как оставил отпечаток большого пальца). Далее она будет всплывать многократно, и каждый раз будет отсутствовать важнейший элемент надежной аутентификации — целостность сеанса, в рамках которого аутентификация проводится. В наличии оказываются либо идентификационные, либо аутентификационные данные, но не то и другое вместе.

Стив Хармас и его жена Элен встречаются со Сьюзен Джеллерт в ее артистической уборной. После встречи между супругами произошел следующий диалог.

... — Пока она тебя охмуряла, — холодно сказала Элен, — я стянула ее зеркальце. На нем есть два великолепных отпечатка большого пальца. Не хочешь сравнить с тем, что на полисе?

— Конечно хочу! Какая же ты умница! А я и не подумал о том, чтобы добыть ее отпечаток.

...

— Ты не дашь мне свою пудру? — попросил я Элен и сдул на зеркальце немного тонкого порошка. — Вот прекрасный отпечаток, совершенно четкий. Посмотрим, нет ли характерных особенностей. Вот, взгляни, здесь вилочка вверх и влево и четкий завиток в центре. — Я поднес полис к свету и исследовал смазанный отпечаток под подписью Сьюзен. — Да, то же самое: вот вилочка, а вот завиток. Ну что, теперь ты довольна?...

Еще один экземпляр аутентификационных данных был добыт при посещении острова, на котором проживали темноволосая сестра-близнец Сьюзен по имени Коррин и ее муж по фамилии Конн.

... Пока Элен пожимала ей руку на прощание, я достал портсигар и предложил Коррин закурить.

— О, спасибо! — воскликнула она и протянула руку за сигаретой.

Тут я нарочно отпустил портсигар, и она была вынуждена его поймать. ... Что ж, по крайней мере мы не зря потратили время. Теперь у меня были ее отпечатки пальцев.

...

Минута возни с пудрой — и внимательный осмотр отпечатков, оставленных Коррин на блестящей поверхности портсигара, убедил меня, что она не имела отношения к тому отпечатку на полисах...

Если отпечаток на полисе поставила одна из сестер, то на острове Стив и Элен явно встречались с другой. Но кто из них на самом деле Сьюзен, а кто — Коррин? Пока с уверенностью определить это не удалось.

А через несколько дней произошло предсказанное Мэддаксом убийство.

... Я листал страницы, проглядывая заголовки, и где-то через полчаса мне на глаза попалась маленькая заметка внизу страницы. Пробежав глазами заглавие, я начал было читать следующую заметку, но вдруг насторожился и вернулся к предыдущему заголовку. На этот раз он поразил меня как удар в лицо: «Трагическая гибель танцовщицы. ... Истекла кровью на пустынном острове».

...

— Ты это читал? — отрывисто спросил Мэддакс и хлопнул по лежащей перед ним газете.

— Да, — ответил я, подвинув себе ногой стул и садясь. — Там мало что сказано, но, видимо, наши полисы стали дороговато нам обходиться.

— Значит, ты считаешь, что они заявят претензию?

— Не знаю, но смерть от потери крови в списке не значится. Пока подробности неизвестны, я пытаюсь учитывать все возможности.

— Я знаю подробности, — сказал Мэддакс. — ... Девица умерла вчера днем. Очевидно, она жила на острове у Конна в ожидании переезда в Нью-Йорк. Конн говорит, что покинул остров сразу после десяти утра. Сьюзен ему сказала, что собирается убрать в доме, пока его не будет. Она хотела вымыть окна и попросила у Конна стремянку. Он сказал, где ее взять, но предупредил, что она плохая: одна из ножек могла вот-вот сломаться. Все окна там не выше семи футов, и она ответила, что падать будет невысоко. ... Мытьем окон она занялась только во второй половине дня. Когда она мыла одно из них, ножка стремянки подломилась, и Сьюзен рухнула вперед прямо на окно. Инстинктивно она пыталась защититься, упершись руками в стекло, оно разбилось и глубоко порезало ей запястья, повредив артерии.

Тут мелкая неприятность превратилась в угрозу для жизни. Когда ты один, порезанные артерии на обеих руках нелегко перевязать. Крови при этом море, и Сьюзен впала в панику. Кровь обнаружена во всех комнатах: видимо, она бесцельно бегала по дому, то ли искала бинты, то ли просто металась в страхе. Там валялось два пропитанных кровью полотенца. Она порвала на бинты какую-то тряпку и завязала себе запястья, так ее и нашли. Повязки не были достаточно тугими, чтобы остановить артериальное кровотечение, и это неудивительно. Сделать тугую повязку на собственном запястье, когда руки скользят от крови, практически невозможно.

Должно быть, она уже больше не надеялась сама остановить кровотечение и пошла к лодке, стремясь добраться до берега и людей. Но было уже поздно. Судя по следам, по дороге к причалу она несколько раз падала. Вернувшись на остров, Конн нашел ее рядом с лодкой. К тому времени она была мертва около двух часов.

— Какой кошмар, — сказал я.

Мэддакс пожал плечами:

— Коронерское расследование назначено на завтра. Очевидно, вердикт будет таким: смерть от несчастного случая. Нет никаких доказательств, что это было подстроено. Когда она истекала кровью, Конн был в отеле «Спрингвилл», забирал свою почту. Его видели несколько человек. Его жена была в это время на пути в Буэнос-Айрес; Денни — в Нью-Йорке, а все передвижения Райса отслеживаются копами, что сидят у него на хвосте. У них у всех железное алиби. И вообще, нет никаких оснований склонить шерифа к мысли о нечестной игре.

— Кроме того, что она застрахована на миллион, — напомнил я...

Мы не будем заниматься крючкотворством и дискутировать о том, является ли стремянка оборудованием, и можно ли считать, что причиной смерти стала предусмотренная полисом поломка оборудования (гнилой ножки стремянки), а не потеря крови.

Не сомневаясь в том, что страховая претензия будет заявлена, Стив Хармас пытается доказать факт убийства. Сделать это можно, только установив личность жертвы. Хармас несанкционированно проникает в морг, находящийся в том же здании, что и офис шерифа.

... Там лежала Сьюзен Джеллерт; мертвое печальное лицо было восковым и белым, как первый снег. Это действительно была Сьюзен: те же черты лица, те же светлые волнистые волосы. Я еще немного откинул покрывало и над правой грудью заметил маленькую темно-красную родинку в форме полумесяца. Секунду я смотрел на нее, пытаясь вспомнить, видел ли ее раньше. При первой встрече я достаточно близко видел Коррин, чтобы заметить эту родинку; майка, которая тогда была на ней надета, не смогла бы ее скрыть. Но когда Сьюзен танцевала на сцене, я сидел слишком далеко, и такое маленькое пятнышко могло быть просто запудрено, чтобы издалека быть заметным. Лишь по этой родинке можно было судить, что лежащая передо мной мертвая девушка — Сьюзен.

С собой у меня был прибор для снятия отпечатков пальцев. Торопясь, я снял отпечатки с холодной, мертвой руки. Быстрое изучение результатов сообщило мне, что отпечаток большого пальца тот же, что и на полисах.

Кладя в карман прибор, я почувствовал разочарование. Я надеялся доказать, что мертвая девушка — не Сьюзен, но теперь не оставалось никаких сомнений в обратном...

Появился еще один биометрический атрибут — родинка. Но кому из сестер она принадлежит? Пока можно утверждать только одно — убита девушка, оставившая свои отпечатки пальцев на страховых полисах.

Тем временем шериф застает Хармаса в морге и требует объяснений.

... — Да, история странная, — произнес он [шериф], когда я закончил. Но вы на ложном пути. Эта девушка погибла случайно... Я тщательно все проверил... Она была одна на острове, когда погибла... Есть тут у нас один тип, Джейк Оукли... Он

рыбачил там до половины пятого вечера. Никто на остров не приезжал... Там не было никого, кроме девушки. Я частым гребнем прочесал всю хижину и весь остров и могу поклясться, что там никого не было. Это несчастный случай. Можешь выбросить из головы мысль об убийстве.

— Извините, — возразил я, — но я не верю. Это было убийство, но я понять не могу, как его провернули... У вас есть ее фотография?

— К завтрашнему дню будет. Я тебе ее вышлю.

— Мне нужно, чтобы была видна родинка. Можете так сделать?

— Конечно.

Я оставил ему свой адрес...

Упомянутый шерифом Джейк Оукли по сути выполнил роль межсетевого экрана, контролируя пути сообщения между сушей и островом. Можно было бы сказать «контролируя потоки данных», но потоков, по-видимому, не было — «никто на остров не приезжал».

Наконец-то «хорошие парни» стали использовать сетевые технологии — Хармас не стал дожидаться изготовления фотографии, а оставил свой адрес (harmas@national_fidelity.com?), на который шериф обещал прислать графический файл.

Хармас с женой после упорных поисков находят женщину, у которой сестры в свое время снимали комнату. К сожалению, она не вполне вменяема, но нужной информацией владеет. Беседа с ней дает ответ на главный вопрос, завершая, наконец, процедуру идентификации и аутентификации.

... — Считается, что мисс Джеллерт погибла в результате несчастного случая. Как говорят, она мыла окно, стремянка упала, и она порезала себе артерии на запястьях. Я — следователь страховой компании. Она была у нас застрахована, и мы совершенно уверены в том, что ее убили. Мы ищем информацию, любую, которая может пригодиться.

— Мыла окна! Эта девица мыла окна! Да в жизни этому не поверю. Она и пальцем не шевельнула бы, чтобы что-то вымыть.

...

— Они были близнецами, только одна — блондинка, а вторая — брюнетка. Когда-то, по-моему, Сьюзен надевала темный парик, и никто не мог сказать, кто из них кто. Когда она была в парике, вы могли как-то их отличить друг от друга?

— В любой момент — ответила миссис Пейси и ухмыльнулась, обнажив пустые десны. — У них обеих не было стыда, расхаживали, в чем мать родила. ... У Коррин была родинка, по ней я всегда отличала ее от сестрицы. Маленькое пятнышко в форме полумесяца, вот тут. — Она ткнула костлявым пальцем себе в грудь.

— Вы хотите сказать, родинка была у Сьюзен?

— У Коррин... Маленькое пятнышко в форме полумесяца...

...

Если покойница была Коррин Конн, претензия не имела силы и мы могли возбудить иск о мошенничестве...

Упомянем попутно еще один признак нетипичного поведения — «девица мыла окна» — и продолжим цитирование.

... — Нам еще нужно решить проблему с отпечатком большого пальца на полисе, — напомнила Элен. — У нас есть отпечаток пальца Коррин, и он не подходит.

— Давай порассуждаем немножко, — предложил я. — Нам все время казалось, что с этими отпечатками что-то неладно. Ты предположила, что Коррин выдает себя за Сьюзен и заставила ее поставить свой отпечаток на полисы. ... А что, если предположить, что все оказалось как раз наоборот? Что это Сьюзен выдавала себя за Коррин? ... Разве не просто было ей поехать на Мертвое озеро ночью, пока мы спали в Виллингтоне, надеть темный парик, вымазаться темным кремом «под загар» и встретить нас в качестве Коррин Конн, когда мы на следующее утро так доверчиво прибыли на остров? Ты ведь тогда сказала, что она вела себя так, будто сама стремилась дать нам свои отпечатки.

— Но ведь у нас есть и отпечатки Сьюзен, — возразила Элен. — Я взяла с ее столика зеркальце, и отпечатки совпали с теми, что на полисе.

— Однако ты же не видела, чтобы она брала его в руки, правда? Может, это было подстроено. А вдруг это было зеркальце Коррин, и Сьюзен выложила его на столик специально для нас?...

Итак, Сьюзен, осуществляя маскарад, посредством зеркальца воспроизвела аутентификационные данные сестры.

Тут Хармас спохватывается, что в морге он сделал не все, что следовало бы.

... Мне вдруг пришло в голову, и я не знаю, почему не подумал об этом раньше, что раз Коррин темноволосая, а Сьюзен — блондинка, то, если покойница — Коррин, значит, ее волосы должны быть крашеными.

Я разозлился на себя за то, что не додумался до этого раньше, когда осматривал ее в Спрингвилле. Выпрыгнув из машины, я вернулся в аптеку и позвонил шерифу Питерсу.

— Шериф, — сказал я, — у меня есть причины считать, что эта мертвая девушка — Коррин Конн. Это легко доказать. Вы не могли бы посмотреть на ее волосы и проверить, не темные ли у них корни?

— Уж не думаешь ли ты, сынок, что тело еще здесь? — удивленно ответил он. — Его затребовал Джек Конн. Кремация состоялась через два дня после коронерского расследования.

— Ее кремировали? — заорал я. — Вы в этом уверены?...

Как и положено опытному хакеру, Джек Конн позаботился об оперативном уничтожении регистрационной информации. Стиву Хармасу приходится искать другие пути.

... Я открыл дверь телефонной будки и постоял, вдыхая аптечный воздух и раздумывая, что делать дальше. Если я не могу доказать, что Сьюзен — это Коррин, значит, нужно доказать, что Коррин — это Сьюзен.

...

Я набрал номер Алана Гудьера. Он почти сразу снял трубку.

— Это Стив. Я в трех минутах от тебя. Хочешь, подъеду: ты ведь хотел поговорить?

...

Гудьер ждал меня у дверей своей квартиры.

...

— Алан, с тех пор, как погиб Хофман, я стал тебя подозревать. ... Ты организатор. ... Кроме того, я знаю, как убили ту девушку на острове. Видишь ли, Алан, если бы ты затеял только одно мошенничество, тебе это могло бы сойти с рук, но два — это уже перебор. ... Ты убил ее, Алан.

— Оукли все время наблюдал за островом, — сказал он. — Он бы увидел, как я приехал или уехал. Хотелось бы мне знать, как ты докажешь, что ее убил я.

— Я понятия об этом не имел, пока не просмотрел сегодня утром твое досье. Но как только я узнал, что во время войны ты служил в спецслужбах, на подводной лодке, я сразу понял, как ты это проделал. Бьюсь об заклад, что где-нибудь у озера я отыщу костюм аквалангиста. Ты запросто мог проплыть под водой до острова, убить девчонку и незаметно уплыть обратно. Прелестная идея, Алан, но ты забыл про свое досье...

Джейк Оукли оказался плохим межсетевым экраном, не контролируя перемещения под водой и не обеспечивая непрерывность защиты.

Хармасу же разобраться в механизме убийства помог корреляционный анализ регистрационной информации (и то, что в страховой компании такая информация — данные о сотрудниках — вообще была, хотя, казалось бы, какая разница, чем занимался во время войны нынешний страховой агент?).

Распутав дело, Хармас рассказывает Сьюзен (естественно, как обвиняемой) и Мэддаксу о его деталях.

... Идея состояла в следующем. Вы [Сьюзен] должны были купить десять полисов на страхование от несчастных случаев при максимально низких взносах и общей сумме страховки на миллион. Гудьер должен был продать Коррин страховку на полмиллиона долларов от похищения. После этого Конну предстояло похитить Коррин и доставить ее на остров. Ее волосы нужно было осветлить, а потом ее следовало убить таким способом, чтобы можно было заявить претензию страховым компаниям. Потом вы перекрасили бы свои волосы в темный цвет, появились в качестве Коррин и забрали деньги.

Сначала за дело взялся Гудьер, продал Коррин полис, страхующий ее от похищения. Он был первоклассным агентом и без труда уговорил Коррин купить страховку. Потом, дождавшись, пока наш друг Мэддакс уедет, он убедил главу моей компании принять вашу страховку от несчастного случая.

Поскольку вместо вас должна была погибнуть Коррин, необходимо было позаботиться о том, чтобы ни одна из компаний не усомнилась в личности покойной. Для гарантии нужно было поставить на все полисы отпечаток пальца Коррин. Это взял на себя Райс. Он подождал, пока Коррин напьется, и поставил отпечаток ее пальца на полисы.

...

Тем временем Гудьер следил за мной. Он узнал, что я собираюсь к вам, и предупредил вас, чтобы вы подготовились. Вы взяли у Райса зеркальце с отпечатками пальцев Коррин и положили его на видное место, чтобы я его взял. Вы знали, что я захочу встретиться с вашей сестрой, и были к этому готовы...

И последний и, может быть, самый важный урок. В нарушениях информационной безопасности корпоративных систем нередко оказываются замешанными штатные сотрудники, владеющие информацией для служебного пользования и способные, не вызывая подозрений, оперативно добывать новые сведения. Внутренние злоумышленники были и остаются опаснее внешних. Хакер Джеймс Хедли Чейз знал свое дело...

Рекомендации семейства X.500 как инфраструктурный элемент информационной безопасности

Алексей Галатенко

1. Введение

Судьба разных стандартов и спецификаций складывается существенно по-разному. Есть очень много стандартов, о которых не помнит никто, кроме разработчиков (которые хотели бы, но не могут забыть о них). Умеренное число стандартов периодически появляется в поле зрения, на них время от времени ссылаются. И уж совсем мало стандартов, которые постоянно у всех на виду и на слуху, а без ссылок на них не обходится ни одна сколько-нибудь солидная работа. К числу последних принадлежат рекомендации семейства X.500 (см. [1-4], вероятно, имеющие наивысший индекс цитирования).

В наше время стандарт в области информационных технологий можно считать полезным, жизнеспособным, если он находит применение в деятельности Интернет-сообщества. Спецификации IETF бесчисленное число раз ссылаются на «сертификаты в формате X.509v3» (см., например, [5-11]. Думается, одного этого достаточно, чтобы признать стандарты семейства X.500 исключительно важными и удачными и отнести их к классике жанра).

Данные рекомендации очень важны в концептуальном плане. Служба директорий, формат сертификатов открытых ключей и атрибутов — это базовые элементы инфраструктуры программно-технического уровня информационной безопасности, если можно так выразиться, «инфраструктура инфраструктуры».

Классические работы нередко включают в список литературы, не читая их. Так обычно происходит с описанием мандатной модели разграничения доступа Белла — Ла Падула [12], так поступают и со стандартом X.509 [3]. Однако, в отличие от модели Белла — Ла Падула, рекомендации семейства X.500, как и другие стандарты ISO, не остаются неизменными. Они продолжают развиваться, эволюционируя с периодом не более пяти лет. В редакцию от 2001-го года, которую мы будем рассматривать, вошло много новых, важных идей, что, на наш взгляд, оправдывает появление данной статьи.

2. Основные понятия и идеи рекомендаций семейства X.500

Рекомендации семейства X.500 описывают службу директорий. Среди возможностей, предоставляемых этой службой, обычно выделяют дружественное именование (обращение к объектам по именам, удобным с точки зрения человека) и отображение имен в адреса (динамическое связывание объекта и его расположения — необходимое условие поддержки «самоконфигурируемости» сетевых систем).

Основные понятия службы директорий зафиксированы в рекомендациях X.501 «Служба директорий: модели» [2] и X.511 «Служба директорий: абстрактное определение сервиса» [4].

Множество систем, обеспечивающих функционирование службы директорий, вместе с содержащейся в них информацией можно мыслить как единое целое — Директорию с большой буквы.

Информация, доступ к которой предоставляется Директорией, называется Информационной Базой Директории. Она обычно используется для облегчения взаимодействия между (или с) такими сущностями, как объекты прикладного уровня, люди, списки рассылки и т.д., а также для получения сведений о них.

Предполагается, что Информационная База имеет древовидную структуру, называемую Информационным Деревом Директории. Вершины этого дерева, отличные от корня, составляют элементы Директории, в которых хранится информация об объектах.

У каждого элемента есть однозначно идентифицирующее его различительное имя. В пределах поддеревьев Информационного Дерева могут использоваться относительные различительные имена.

Объекты, информация о которых хранится в Директории, могут иметь произвольную природу. Единственное требование к ним состоит в идентифицируемости (возможности именования).

Объекты объединяются в классы. Каждый объект должен принадлежать по крайней мере одному классу.

Элементы Директории могут быть составными, то есть являться объединением подэлементов, содержащих информацию об отдельных аспектах объектов.

Каждый элемент состоит из атрибутов, имеющих тип и одно или несколько значений. Набор атрибутов зависит от класса объекта.

Некоторые из концевых узлов (листьев) Информационного Дерева могут представлять собой синонимы, содержащие альтернативное имя и указатель на элемент с информацией об объекте.

Служба директорий предоставляет две группы операций:

- опрос;
- модификация.

В число операций опроса входят:

- чтение значений атрибутов элемента Директории;
- сравнение значения атрибута элемента Директории с заданной величиной (полезно, например, для проверки пароля без предоставления доступа к хранимому паролю);
- выдача списка (перечисление) непосредственных преемников заданного узла Информационного Дерева;
- поиск и чтение элементов, удовлетворяющих заданным фильтрам (условиям), в заданных частях Информационного Дерева;
- отказ от незавершенной операции опроса (например, если она выполняется слишком долго).

В группу операций модификации входят:

- добавление нового (концевого) узла Информационного Дерева;
- удаление концевого узла Информационного Дерева;
- модификация элемента Директории с возможным добавлением и/или удалением атрибутов и их значений;
- модификация относительного различительного имени элемента или перемещение узла Информационного Дерева к другому предшественнику.

Рекомендации X.501 описывают три возможные схемы управления доступом к Директории: базовую, упрощенную и основанную на правилах. Последняя может реализовывать принудительное (мандатное) управление доступом с использованием меток безопасности. Решения о предоставлении доступа принимаются с учетом принятой политики безопасности.

Разумеется, предусмотрена аутентификация системных агентов и пользователей, а также источников данных Директории.

Таковы необходимые для последующего изложения основные понятия и идеи службы директорий, зафиксированные в семействе рекомендаций X.500.

3. Каркас сертификатов открытых ключей

Мы приступаем к изучению четвертой редакции рекомендаций X.509 [3], которая регламентирует следующие аспекты:

- сертификаты открытых ключей;
- сертификаты атрибутов;
- сервисы аутентификации.

Идейной основой рекомендаций X.509 являются сертификаты открытых ключей, обслуживающие такие грани информационной безопасности, как конфиденциальность и целостность, и такие сервисы, как аутентификация и неотказуемость.

Сертификат открытого ключа — это структура данных, обеспечивающая ассоциирование открытого ключа и его владельца. Надежность ассоциации, подлинность сертификата подтверждаются подписью удостоверяющего центра (УЦ).

Сертификаты имеют конечный срок годности. Поддерживать актуальность информации об их статусе помогают списки отзыва, подписываемые удостоверяющими центрами и содержащими перечни сертификатов, переставших быть годными. Последнее может случиться как в результате естественного окончания срока, так и досрочно, например, из-за компрометации секретного ключа владельца.

Формат сертификата в простейшем случае выглядит так:

$$CA\ \langle\langle A \rangle\rangle = CA\ \{V, SN, AI, CA, A, Ap, TA\}$$

Здесь:

- A — имя владельца сертификата;
- CA — имя удостоверяющего центра;

- CA <<A>> — сертификат, выданный A центром CA;
- CA {I} — данные I, снабженные подписью CA;
- V — версия сертификата (в настоящее время используется версия 3);
- SN — порядковый номер сертификата;
- AI — идентификатор алгоритма, использованного при подписании сертификата;
- Ap — информация об открытом ключе A;
- TA — даты начала и конца срока годности сертификата.

Отметим, что в общем случае формат может быть существенно сложнее. За счет использования механизма расширений его можно приспособить для нужд различных приложений и сообществ пользователей. В X.509 предусмотрены полезные расширения, носящие универсальный характер.

Каждое расширение включает имя, флаг критичности и значение. Если при обработке (проверке) сертификата встречается неизвестное расширение с флагом критичности FALSE, оно может быть проигнорировано; если же у подобного расширения флаг равен TRUE, сертификат приходится считать некорректным.

Сертификаты открытых ключей подразделяются на два основных вида:

- сертификаты оконечных сущностей;
- сертификаты удостоверяющих центров.

Оконечные сущности не имеют права выпускать сертификаты. Удостоверяющие центры ведают выпуском и аннулированием сертификатов; их собственные сертификаты относятся к одному из двух классов:

- «Самовыпущенные» сертификаты (изготовленные для себя самим удостоверяющим центром). Они полезны, например, при смене ключей УЦ, чтобы обеспечить доверие новым ключам на основании доверия старым. Важным подклассом данного класса являются «самоподписанные» сертификаты, в которых секретный ключ, использованный для генерации электронной цифровой подписи (ЭЦП), соответствует заверяемому открытому ключу. Таким способом УЦ может афишировать свой открытый ключ или иную информацию о собственном функционировании.
- Кросс-сертификаты (выданные одним УЦ другому). Они могут использоваться как в иерархической структуре для авторизации нижестоящего УЦ вышестоящим, так и в произвольной структуре «распределенного доверия» как факт признания одним УЦ существования другого.

Рассмотрим процесс получения и проверки пользователем A открытого ключа пользователя B. Элемент Директории, представляющий A, содержит один или несколько сертификатов открытых ключей A, заверенных удостоверяющим центром, который мы обозначим CA (A) (а сертификат A — как CA (A) <<A>>) и которому, разумеется, соответствует свой узел в Информационном Дереве. Предполагается, что пользователь доверяет своему УЦ, поэтому, если существует сертификат CA (A) <<B>>, процесс выяснения открытого ключа B можно считать завершенным. В противном случае приходится строить так называемый сертификационный маршрут от A к B (обозначается A -> B), начинающийся сертификатом CA (A) <<X1>>, который CA (A) выдал некоторому другому УЦ, X1, ставшему вследствие этого доверенным для A. Маршрут продолжается сертификатом вида X1 <<X2>>, содержит промежуточные звенья вида Xi <<Xi+1>> и завершается сертификатом Xn <<B>>.

Элемент Директории, соответствующий удостоверяющему центру, содержит сертификаты двух типов: прямые (сгенерированные данным УЦ для других) и обратные (выданные данному УЦ другими). Если, кроме того, удостоверяющие центры образуют иерархию, соответствующую Информационному Дереву, то сертификационный маршрут можно построить без привлечения дополнительной информации, только на основе различительных имен A и B. Действительно, с помощью обратных сертификатов выполняется подъем от CA (A) до корня поддерева, общего для A и B, а затем, с помощью прямых сертификатов, осуществляется спуск до CA (B).

В рассмотренном выше процессе A является пользователем сертификата, B — его владельцем (субъектом), CA (B) — удостоверяющим центром. Эти три стороны несут друг перед другом определенные обязательства и, в свою очередь, пользуются предоставляемыми гарантиями. Обязательства и гарантии могут быть зафиксированы в политике сертификата, ссылка на которую хранится в одном из полей расширений. Обычно политика — это текст на естественном языке, но в ней могут присутствовать и формальные условия, допускающие автоматическую проверку.

При построении и использовании сертификационного маршрута может проверяться согласованность политик, присутствующих в кросс-сертификатах. Еще один пример использования данного поля расширения — наложение и про-

верка ограничений на длину сертификационного маршрута (вообще говоря, чем длиннее маршрут, тем меньше доверия он вызывает).

Еще одна группа дополнительных полей сертификатов обслуживает способы и сроки использования ключей. Для шифрования и цифровой подписи применяют разные ключи; следовательно, у одного субъекта может быть несколько пар ключей и, соответственно, несколько сертификатов. Чтобы выбрать среди них нужный, пользователь должен иметь возможность выяснить назначение представленного в сертификате открытого ключа. Аналогично, может потребоваться знание срока годности секретного ключа, посредством которого формируют ЭЦП, поскольку этот срок обычно меньше, чем у открытого ключа, служащего для проверки подписи.

Значительная часть рекомендаций X.509 посвящена спискам отзыва сертификатов, мы, однако, не будем останавливаться на этом техническом вопросе.

4. Каркас сертификатов атрибутов

Возможно, развитие механизма расширений натолкнуло авторов рекомендаций X.509 на мысль о том, что в заверенных сертификатах можно хранить не только открытые ключи, но и произвольные атрибуты субъектов — держателей (владельцев) сертификатов.

Сертификат атрибутов — это структура данных, снабженная цифровой подписью соответствующего удостоверяющего центра и связывающая значения некоторых атрибутов с идентификационной информацией держателя сертификата.

Вообще говоря, сертификаты атрибутов имеют универсальных характер, но в рекомендациях X.509 внимание акцентируется на их применении в качестве основы инфраструктуры управления привилегиями (авторизации).

У каркасов сертификатов открытых ключей и сертификатов атрибутов много общего.

Это и система удостоверяющих центров, и списки отзыва, и многое другое. Мы не будем повторять общие места, а сосредоточимся на специфике управления привилегиями.

Отметим в первую очередь, что жизненные циклы открытых ключей и привилегий устроены по-разному, имеют разную длительность. Привилегии могут делегироваться вспомогательным сущностям на короткие промежутки времени (порядка минуты). Для управления привилегиями могут использоваться свои понятия и механизмы, такие, например, как роли. Следовательно, хотя с синтаксической точки зрения для цели управления привилегиями могут использоваться сертификаты открытых ключей, снабженные соответствующими расширениями, с идейной и практической точек зрения каркасы открытых ключей и управления привилегиями нуждаются в разделении, что и было сделано в рекомендациях X.509.

В контексте управления привилегиями удостоверяющий центр называется центром авторизации. Выделяется главный центр авторизации, который может делегировать другим центрам права наделения привилегиями и их дальнейшего делегирования.

На протяжении маршрута делегирования должно действовать правило доминирования: промежуточный центр авторизации не может делегировать больше привилегий, чем сам имеет (для каждой привилегии должно быть определено, что значит «не больше»).

Вообще говоря, могут существовать две схемы выделения и проверки привилегий:

- Удостоверяющий центр по собственной инициативе наделяет некоторую сущность привилегиями путем создания сертификата атрибутов и помещения его в Директорию с предоставлением свободного доступа. В дальнейшем верификатор привилегий может использовать этот сертификат при принятии решения о предоставлении определенного вида доступа. Перечисленные действия могут происходить без ведома и участия субъекта — держателя сертификата.
- Субъект запрашивает центр авторизации на предмет получения определенной привилегии. При положительном решении созданный сертификат атрибутов возвращается держателю и явным образом предъявляется последним при доступе к защищенным ресурсам.

Независимо от принятой схемы можно выделить три основных понятия инфраструктуры управления привилегиями:

- объект (точнее, метод объекта), к которому осуществляется доступ и который может быть снабжен такими атрибутами, как метка безопасности;
- предъявитель привилегий;
- верификатор привилегий, принимающий решения (с учетом действующей политики безопасности и существующего окружения) о достаточности предъявленных привилегий для предоставления доступа.

Верификатор привилегий можно представлять себе как экранирующую сущность, логически располагающуюся между вызывающим и вызываемым методами объектов. Рекомендации X.509 не налагают ограничений на правила экранирования.

Ролевое управление доступом может быть реализовано за счет введения дополнительного уровня косвенности, трактовки допустимых ролей как атрибутов субъектов и ассоциирования привилегий с ролями путем выпуска соответствующих сертификатов.

Отметим, что каркас сертификатов атрибутов может быть использован не только для управления доступом, но и в контексте обеспечения неотказуемости. При этом предъявитель привилегий выступает в качестве субъекта свидетельства, верификатор привилегий оказывается пользователем свидетельства, а метод объекта трактуется как целевая сущность.

Можно видеть, что каркас сертификатов атрибутов обладает достаточной гибкостью и выразительной силой, чтобы служить основой инфраструктуры управления привилегиями, поддерживать контроль доступа и неотказуемость.

5. Простая и сильная аутентификация

Каркасы сертификатов открытых ключей и атрибутов — основа целого ряда сервисов безопасности, в число которых входят аутентификация, контроль целостности, управление доступом. Эти сервисы могут использоваться как самой Директорией, так и произвольными приложениями. В данном разделе мы рассмотрим предусмотренные в рекомендациях X.509 простую и сильную аутентификацию.

Простая аутентификация предназначена только для локального использования. Данные для нее могут вырабатываться и передаваться тремя способами:

- имя и пароль пользователя передаются в открытом виде;
- имя, пароль, случайное число и, возможно, временной штамп (метка) подвергаются воздействию односторонней функции, результат которой передается получателю для проверки;
- к описанному выше результату добавляется случайное число и/или временной штамп и еще раз применяется односторонняя функция (возможно, та же самая).

Рассмотрим более подробно реализацию разновидности 2 простой аутентификации.

Пользователь A сначала генерирует токен безопасности PT1:

PT1 = h1 (t1A, r1A, A, passwdA)

Токен PT1 используется для создания аутентификационного токена AT1:

AT1 = t1A, r1A, A, PT1

(то есть токен AT1 состоит из четырех компонентов). Пользователь A пересылает B токен AT1. Цель B — своими средствами создать аналог токена безопасности PT1 (реконструировать PT1) и сравнить его с оригиналом. Пользователь B запрашивает у службы директорий или извлекает локальную копию пароля passwdA (обозначим ее passwdA-B) и реконструирует PT1:

PT1-B = h1 (t1A, r1A, A, passwdA-B)

Если PT1 и PT1-B совпадут, подлинность пользователя A считается установленной.

Сильная аутентификация основана на применении асимметричных методов шифрования, пригодных для генерации электронной подписи. Подлинность пользователя A считается установленной, если он продемонстрирует владение секретным ключом, ассоциированным с хранящимся в сертификате на имя A открытым ключом.

Рекомендации X.509 описывают три возможные процедуры сильной аутентификации:

- Односторонний обмен. От пользователя A пользователю B передается один токен.
  При этом подтверждается подлинность A и B, а также то, что токен сгенерирован A, предназначен B, не был изменен и является «оригинальным» (то есть не посылается повторно).
- Двусторонний обмен. Дополнительно от B к A направляется ответ, допускающий проверку того, что он был сгенерирован B, предназначен A, не был изменен и является «оригинальным».
- Трехсторонний обмен. От A к B передается еще один токен. Обеспечивает те же свойства, что и двусторонний, без использования временных штампов.

Предполагается, что независимо от выбранной процедуры и до выполнения обменов пользователь A выясняет открытый ключ B и обратный сертификационный маршрут B -> A.

Рассмотрим более подробно процедуру одностороннего обмена.

В качестве первого шага пользователь A генерирует «уникальное» число rA, предназначенное для защиты от воспроизведения и подделки аутентификационного токена.

После этого A направляет B сообщение следующей структуры:

B -> A, A {tA, rA, B}

где tA — временной штамп, в общем случае представляющий собой пару (время генерации токена, срок годности токена). Напомним, что конструкция вида A {I} обозначает информацию I, подписанную открытым ключом A.

Получив это сообщение, B предпринимает следующие действия:

- по обратному сертификационному пути B -> A выясняет открытый ключ A (Ap), попутно проверяя статус сертификата A;
- проверяет подпись и, тем самым, целостность присланной информации;
- проверяет, что в качестве получателя указан B;
- проверяет, что временной штамп является «свежим», а число rA ранее не использовалось.

Двусторонний и трехсторонний обмены являются довольно очевидным развитием одностороннего.

На этом мы завершаем рассмотрение рекомендаций семейства X.500.

6. Заключение

Служба директорий, сертификаты открытых ключей, сертификаты атрибутов нужны всем и везде. Они — основа инфраструктуры с открытыми ключами, корпоративной, национальной и международной инфраструктуры цифровых подписей и электронной аутентификации. Без реализации рекомендаций семейства X.500 невозможно масштабное внедрение криптографических сервисов, не заработает на практике Федеральный Закон РФ «Об электронной цифровой подписи».

Важно подчеркнуть, что рекомендации семейства X.500 не замыкаются на криптографии. Сертификаты атрибутов могут служить основой еще одной широкомасштабной инфраструктуры — инфраструктуры авторизации, нужда в которой чрезвычайно велика, но которая только начинает формироваться.

Не приходится сомневаться, что у рекомендаций семейства X.500 впереди долгая «трудовая» жизнь, новые этапы эволюции и внедрения.

7. Литература

1. Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models and services. — ISO/IEC International Standard 9594-1:2001, ITU-T Recommendation X.500 (2001 E).
2. Information technology — Open Systems Interconnection — The Directory: Models. — ISO/IEC International Standard 9594-2:2001, ITU-T Recommendation X.501 (2001 E).
3. Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks. — ISO/IEC International Standard 9594-8:2000, ITU-T Recommendation X.509 (2000 E).
4. Information technology — Open Systems Interconnection — The Directory: Abstract service definition. — ISO/IEC International Standard 9594-3:2001, ITU-T Recommendation X.511 (2001 E).
5. Adams C., Farrell S. Internet X.509 Public Key Infrastructure Certificate Management Protocols. — Request for Comments: 2510, 1999.
6. Farrell S., Housley R. An Internet Attribute Certificate Profile for Authorization. — Request for Comments: 3281, 2002.
7. Dierks T., Allen C. The TLS Protocol. Version 1.0. — Request for Comments: 2246, 1999.
8. Kent S., Atkinson R. Security Architecture for the Internet Protocol. — Request for Comments: 2401, 1998.
9. Maughan D., Schertler M., Schneider M., Turner J. Internet Security Association and Key Management Protocol (ISAKMP). — Request for Comments: 2408, 1998.
10. Linn J. Generic Security Service Application Program Interface. Version 2, Update 1. — Request for Comments: 2743, 2000.
11. Wray J. Generic Security Service API Version 2 : C-bindings. — Request for Comments: 2744, 2000.
12. Bell D.E., La Padula L.J. Secure Computer Systems: Mathematical Foundations and Model. Technical Report M74-244. — The MITRE Corporation, 1973.

Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей» – база криптографической инфраструктуры

Алексей Галатенко

1. Введение

Компьютерной криптографии, как никакой другой области информационных технологий, присущ дух таинственности. Она традиционно считается уделом узкого круга избранных, владеющих искусством тайнописи. Ни в коей мере не пытаясь поколебать это мнение, отметим, однако, что у компьютерной криптографии при практическом использовании в информационных системах есть довольно много некриптографических аспектов. Среди них можно выделить интерфейсный, протокольный аспект (как обращаться к криптографическим сервисам пользователям и программистам?), а также аспект обеспечения собственной безопасности аппаратно-программных платформ криптографических систем (криптографических модулей). Эти аспекты (точнее, если можно так выразиться, некоторые аспекты этих аспектов) и являются предметом нашего рассмотрения.

Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей» [1] играет организующую роль, описывая внешний интерфейс криптографического модуля и общие требования к подобным модулям. Наличие подобного стандарта упрощает разработку сервисов безопасности и профилей защиты для них. Наверное, в любом американском нормативном документе, где фигурируют криптографические компоненты и требования безопасности к ним, имеются ссылки на данный стандарт. Создание аналогичного российского стандарта, несомненно, было бы весьма полезно отечественным разработчикам и системным интеграторам. К сожалению, в краткосрочной перспективе рассчитывать на это не приходится. Пока же, на наш взгляд, об этом стандарте явно недостаточно информации на русском языке. Мы попытаемся по мере сил хотя бы отчасти заполнить этот пробел.

2. Основные понятия и идеи стандарта FIPS 140-2

В федеральном стандарте США FIPS 140-2 «Требования безопасности для криптографических модулей» под криптографическим модулем понимается набор аппаратных и/или программных (в том числе встроенных) компонентов, реализующих утвержденные функции безопасности (включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию) и заключенных в пределах явно определенного, непрерывного периметра.

В стандарте FIPS 140-2 рассматриваются криптографические модули, предназначенные для защиты информации ограниченного доступа, не являющейся секретной. То есть речь идет о промышленных изделиях, представляющих интерес для основной массы организаций. Наличие подобного модуля — необходимое условие обеспечения защищенности сколько-нибудь развитой информационной системы; однако, чтобы выполнять предназначенную ему роль, сам модуль также нуждается в защите, как

собственными средствами, так и средствами окружения (например, операционной системы).

Согласно стандарту, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

- применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа;
- обеспечение защиты модуля от несанкционированного использования и нештатных методов эксплуатации;
- предотвращение несанкционированного раскрытия содержимого модуля (криптографических ключей и других данных, критичных для безопасности);
- предотвращение несанкционированной и необнаруживаемой модификации модуля и криптографических алгоритмов, в том числе несанкционированной модификации, подмены, вставки и удаления криптографических ключей и других данных, критичных для безопасности;
- обеспечение отображения (индикации) режима работы (состояния) модуля;
- обеспечение доверия тому, что модуль функционирует должным образом при работе в утвержденном режиме;
- обнаружение ошибок в функционировании модуля и предотвращение компрометации информации ограниченного доступа и данных модуля, критичных для безопасности, вследствие подобных ошибок.

Из перечисленных целей вытекают требования безопасности, относящиеся к этапам проектирования и реализации модуля и разбитые в стандарте на одиннадцать групп:

- спецификация криптографического модуля;
- требования к портам и интерфейсам модуля;
- роли, сервисы и аутентификация;
- конечноавтоматная модель;
- физическая безопасность;
- эксплуатационное окружение;
- управление криптографическими ключами;
- электромагнитная совместимость;
- самотестирование;
- доверие проектированию;
- сдерживание прочих атак.

Спецификация модуля включает определение криптографического периметра, реализуемых функций и режимов, описание модуля, его аппаратных и программных компонентов, а также документированную политику безопасности.

Среди портов и интерфейсов модуля должны быть выделены обязательные и дополнительные. Следует специфицировать все интерфейсы, а также все маршруты входных и выходных данных. Кроме того, порты для незащищенных параметров, критичных для безопасности, должны быть логически отделены от других портов.

Среди ролей и сервисов необходимо провести логическое разделение на обязательные и дополнительные, обеспечить персональную или ролевую аутентификацию.

Модель в виде конечного автомата должна описывать деление на обязательные и дополнительные состояния.

Меры физической самозащиты модуля включают замки, защитные кожухи и пломбы, сохраняющие свидетельства вторжений, средства оперативного выявления и реагирования на попытки вторжений, меры по противодействию атакам, основанным на использовании нештатных внешних условий.

Ядром допустимого эксплуатационного окружения должна служить операционная система (ОС), удовлетворяющая требованиям утвержденного профиля защиты, обеспечивающая произвольное управление доступом, протоколирование и аудит, доверенные маршруты. Кроме того, следует применять утвержденные методы контроля целостности и построить модель политики безопасности.

В число поддерживаемых механизмов управления ключами должны входить генерация случайных чисел, генерация, распределение, ввод/вывод, хранение и обнуление ключей.

На требованиях электромагнитной совместимости мы останавливаться не будем.

При включении питания и при истинности определенных условий должны выполняться тесты криптографических алгоритмов, контроль целостности программного обеспечения, проверка критичных функций.

Меры доверия проектированию должны включать конфигурационное управление, процедуры безопасной установки, генерации и распространения. Следует подготовить функциональную спецификацию, при реализации использовать язык высокого уровня, продемонстрировать соответствие проекта и политики, снабдить пользователей соответствующими руководствами.

Наконец, предусматриваются меры по сдерживанию атак, для которых пока нет стандартизованных требований.

Стандартом FIPS 140-2 предусмотрено четыре уровня защищенности криптографических модулей, что позволяет экономически целесообразным образом защищать данные разной степени

критичности (например, регистрационные журналы, счета на миллионы долларов или данные, от которых зависит жизнь людей) в разных условиях (строго охраняемая территория, офис, неконтролируемый объект).

К первому (самому слабому) уровню применяется минимальный набор требований безопасности, которым удовлетворяет, например, шифрующая плата для персонального компьютера. Программные компоненты соответствующих модулей могут выполняться на универсальных вычислительных системах с несертифицированной ОС.

На втором уровне требуются:

- ролевая аутентификация;
- наличие замков на съемных оболочках и дверцах, использование защитных покрытий и пломб, сохраняющих свидетельства вторжений;
- использование ОС, сертифицированных на соответствие определенным профилям защиты на основе «Общих критериев» с оценочным уровнем доверия не ниже второго.

К третьему уровню предъявляются следующие дополнительные требования:

- отделение портов и интерфейсов, используемых для нешифрованного ввода/вывода криптографических ключей и других данных, критичных для безопасности;
- персональная аутентификация с проверкой допустимости принятия определенных ролей;
- наличие средств оперативного выявления и реагирования на попытки вторжений (таких, как микросхемы, обеспечивающие обнуление критичных данных модуля при попытке вскрыть корпус);
- использование ОС, сертифицированных на соответствие определенным профилям защиты с оценочным уровнем доверия не ниже третьего и поддержкой доверенного маршрута.

Четвертый уровень является самым сильным. Его требования предусматривают полный спектр мер физической защиты, включая меры по противодействию атакам, основанным на использовании нештатных внешних условий (электрических или температурных).

Применяемая операционная система должна соответствовать оценочному уровню доверия не ниже четвертого.

Далее будут детально рассмотрены наиболее содержательные группы требований. Здесь же мы обратим внимание на параллель с профилем защиты для смарт-карт (см. [2]), общность целого ряда целей, предположений и требований безопасности для криптографических модулей и смарт-карт (что, разумеется, вполне естественно). На наш взгляд, сравнительный анализ этого профиля и стандарта FIPS 140-2 позволяет в полной мере оценить достоинства «Общих критериев» и ассоциированных спецификаций, высокую степень их полноты и систематичности. Конечно, «Общие критерии» можно критиковать, их нужно развивать и совершенствовать, но перевод стандарта FIPS 140-2 на рельсы «Общих критериев», несомненно, повысил бы его качество.

3. Требования безопасности для криптографических модулей

Мы приступаем к детальному рассмотрению перечисленных выше групп требований безопасности для криптографических модулей.

3.1 Спецификация криптографического модуля

В спецификации криптографического модуля должны фигурировать аппаратные и/или программные компоненты, влияющие на его безопасность и заключенные в пределах определенных физических границ — криптографического периметра. Если модуль является программным, в пределах периметра окажутся процессор, а также другие аппаратные компоненты, хранящие и защищающие программы.

В спецификации должны быть определены физические порты и логические интерфейсы, все входные и выходные маршруты данных.

Следует описать ручные и логические средства управления криптографическим модулем, физические или логические индикаторы состояния, применимые физические (в частности, электрические) и логические характеристики.

В представленной проектной документации должны присутствовать схемы взаимосвязей таких компонентов, как микропроцессоры, буферы ввода/вывода, буферы открытых и шифрованных данных, управляющие буферы, ключевая, рабочая и программная память.

Проект должен выполняться с использованием языка спецификаций высокого уровня.

Следует специфицировать все данные, критичные для безопасности, в том числе криптографические ключи, аутентификационные данные, параметры криптографических алгоритмов, регистрационные данные и т.д.

Обязательным элементом документации является политика безопасности криптографического модуля.

3.2 Порты и интерфейсы

Все информационные потоки, весь физический доступ к модулю должны производиться через определенный набор физических портов и логических интерфейсов. Интерфейсы должны логически различаться, хотя они могут разделять один порт (например, для ввода и вывода данных) или охватывать несколько портов (например, вывод данных может производиться через последовательный и параллельный порты). Прикладной программный интерфейс программного компонента модуля может трактоваться как один или несколько логических интерфейсов.

Следующие четыре логических интерфейса являются обязательными:

- Интерфейс ввода данных. Все данные, поступающие в модуль для обработки и/или использования (кроме управляющих данных, см. далее) должны вводиться через этот интерфейс.
- Интерфейс вывода данных. Все выходные данные (кроме информации о состоянии, см. далее) должны покидать модуль через этот интерфейс. При возникновении ошибочных ситуаций и во время выполнения тестов вывод должен быть запрещен.
- Входной управляющий интерфейс. Через этот интерфейс должны подаваться все команды, сигналы и управляющие данные (в том числе вызовы функций и ручные управляющие воздействия, такие как нажатие на переключатель или клавишу), применяемые для управления функционированием криптографического модуля.
- Выходной интерфейс состояния. Через этот интерфейс должны выдаваться все выходные сигналы, индикаторы и информация о состоянии (в том числе коды завершения и физические индикаторы, такие как показания светодиодов), отображающие состояние криптографического модуля.

Все внешнее электрическое питание должно поступать через порт питания. Его может и не быть, если применяются внутренние батарейки.

Каждому обязательному логическому интерфейсу соответствует свой маршрут данных. Маршрут вывода данных должен быть логически отсоединен от средств обработки в момент генерации, ручного ввода или обнуления ключей. Чтобы предотвратить непреднамеренный вывод данных, критичных для безопасности, следует предусмотреть два независимых внутренних действия, необходимых для использования интерфейсов, применяемых при выводе криптографических ключей, информации ограниченного доступа и т.п.

На уровнях безопасности 3 и 4 порты (интерфейсы), используемые для ввода или вывода данных, критичных для безопасности, должны быть физически (логически) отделены от других портов (интерфейсов), а критичные данные должны поступать непосредственно в модуль (например, по непосредственно подсоединенному кабелю или доверенному маршруту).

3.3 Роли, сервисы и аутентификация

В рамках криптографического модуля для операторов должны поддерживаться роли и ассоциированные с ними сервисы и права доступа. Один оператор может быть приписан нескольким ролям. Если модуль поддерживает параллельную работу нескольких операторов, он должен управлять разделением ролей.

Должны поддерживаться по крайней мере следующие роли:

- Роль пользователя. В рамках этой роли выполняются обычные сервисы безопасности, включая криптографические операции и другие утвержденные функции.
- Роль крипто-офицера. Эта роль предназначена для выполнения криптографической инициализации и иных функций управления, таких как инициализация модуля, ввод/вывод криптографических ключей, аудит и т.п.

Если операторам разрешается производить обслуживание модуля (например, диагностирование аппаратуры и/или программ), должна поддерживаться роль инженера, при активизации и завершении которой следует обнулять все незащищенные критичные данные.

Криптографический модуль должен предоставлять следующие сервисы:

- отображение состояния;
- выполнение тестов;
- выполнение утвержденных функций безопасности.

Если модуль поддерживает режим обхода (то есть режим без выполнения криптографической обработки данных), то для его активизации необходимы два независимых внутренних действия, а текущее состояние должно соответствующим образом отображаться.

Если не производится чтение, модификация или замена критичных данных (а, например, выполняется лишь изучение состояния или тестирование модуля), оператор не обязан активизировать какую-либо роль.

Начиная с уровня безопасности 2, активизации роли должна предшествовать аутентификация оператора: ролевая или, на уровнях безопасности 3 и 4, персональная.

В стандарте не оговорены требуемые механизмы аутентификации, специфицирована лишь их стойкость. Вероятность случайного успеха одной попытки должна составлять менее 1/1000000, вероятность случайного успеха какой-либо из нескольких попыток, производимых в течение минуты — менее 1/100000. Это весьма (на наш взгляд — чрезмерно) мягкие требования, если учитывать, что в году 525600 минут. Очевидно, необходимы меры противодействия многократным неудачным попыткам аутентификации.

3.4 Модель в виде конечного автомата

В конечноавтоматной модели криптографического модуля должны быть предусмотрены следующие состояния, соответствующие нормальному и ошибочному функционированию:

- включение/выключение питания (первичного, вторичного, резервного);
- обслуживание крипто-офицером (например, управление ключами);
- ввод ключей и других критичных данных;
- пользовательские состояния (выполнение криптографических операций, предоставление сервисов безопасности);
- самотестирование;
- ошибочные состояния (например, неудача самотестирования или попытка шифрования при отсутствии необходимого ключа), которые могут подразделяться на фатальные, требующие сервисного обслуживания (например, поломка оборудования) и нефатальные, из которых возможен возврат к нормальному функционированию (например, путем инициализации или перезагрузки модуля).

Могут быть предусмотрены и другие, дополнительные состояния, такие как:

- работа в режиме обхода (передача через модуль открытых данных);
- работа в инженерном режиме (например, физическое и логическое тестирование).

3.5 Физическая безопасность

Вопросы обеспечения физической безопасности криптографических модулей исключительно важны и сложны. В стандарте FIPS 140-2 им уделено очень много внимания. Мы, однако, остановимся лишь на основных моментах.

Стандартом предусмотрены четыре разновидности криптографических модулей:

- чисто программные (вопросы физической безопасности для них не рассматриваются);
- состоящие из одной микросхемы;
- состоящие из нескольких микросхем и встроенные в физически незащищенное окружение (например, плата расширения);
- состоящие из нескольких микросхем и обладающие автономной защитой (например, шифрующие маршрутизаторы).

Меры физической защиты структурированы в стандарте двумя способами.

Во-первых, вводится деление на меры выявления свидетельств случившихся ранее нарушений (обнаружение нарушений) и меры выявления нарушений в реальном времени с выполнением соответствующих ответных действий (реагирование на нарушения).

Во-вторых, защитные меры подразделяются на общие и специфические для той или иной разновидности модулей.

И, наконец, в соответствии с принятым в стандарте подходом, меры группируются по четырем уровням безопасности.

Мы ограничимся рассмотрением общих требований физической безопасности, применимых ко всем аппаратным конфигурациям.

Если разрешено производить обслуживание модуля и поддерживается роль инженера, должен быть определен интерфейс обслуживания, включающий все маршруты физического доступа к содержимому модуля, в том числе все съемные оболочки и дверцы (которые необходимо снабдить подходящими средствами физической защиты).

При доступе по интерфейсу обслуживания все хранящиеся в открытом виде секретные ключи и другие критичные данные должны быть обнулены.

На втором уровне безопасности предусмотрено обнаружение нарушений, а начиная с третьего — реагирование на нарушения.

Для четвертого уровня безопасности предусмотрена защита от создания нештатных внешних условий (электрических или температурных), которая может быть реализована двояко:

- путем постоянного отслеживания электрических и температурных параметров с выключением модуля или обнулением данных, критичных для безопасности, при выходе параметров за допустимые границы;
- путем обеспечения устойчивости модуля к нештатным внешним условиям (например, модуль должен нормально работать при температурах от -100 до +200 градусов).

3.6 Эксплуатационное окружение

Эксплуатационное окружение — это совокупность необходимых для функционирования модуля средств управления аппаратными и программными компонентами. В стандарте FIPS 140-2 рассматривается несколько видов окружения:

- универсальное, с коммерческой операционной системой, управляющей как компонентами модуля, так и другими процессами и приложениями;
- ограниченное, являющееся статическим, немодифицируемым (например, виртуальная Java-машина на непрограммируемой плате для персонального компьютера);
- модифицируемое, которое может быть реконфигурировано и может включать средства универсальных ОС.

Ядром универсального и модифицируемого окружения является операционная система.

На первом уровне безопасности к ней предъявляются следующие требования:

- должен использоваться только однопользовательский режим, параллельная работа нескольких операторов явным образом запрещается;
- доступ процессов, внешних по отношению к модулю, к данным, критичным для безопасности, должен быть запрещен, некриптографические процессы не должны прерывать работу криптографического модуля;
- программное обеспечение модуля должно быть защищено от несанкционированного раскрытия и модификации;
- целостность ПО модуля должна контролироваться утвержденными средствами.

Для второго уровня безопасности требуется использование ОС, сертифицированных на соответствие определенным профилям защиты на основе «Общих критериев» с оценочным уровнем доверия не ниже второго. Для защиты критичных данных должно применяться произвольное управление доступом с определением соответствующих ролей. Необходимо протоколирование действий крипто-офицера.

Характерная черта третьего уровня безопасности — использование доверенного маршрута.

На четвертом уровне безопасности криптографического модуля требуется ОС с оценочным уровнем доверия не ниже четвертого.

3.7 Управление криптографическими ключами

Требования безопасного управления криптографическими ключами охватывают весь жизненный цикл критичных данных модуля. Рассматриваются следующие управляющие функции:

- генерация случайных чисел;
- генерация ключей;
- распределение ключей;
- ввод/вывод ключей;
- хранение ключей;
- обнуление ключей.

Секретные ключи необходимо защищать от несанкционированного раскрытия, модификации и подмены, открытие — от модификации и подмены.

Компрометация методов генерации или распределения ключей (например, угадывание затравочного значения, инициализирующего детерминированный генератор случайных чисел) должна быть не проще определения значений ключей.

Для распределения ключей может применяться как ручная транспортировка, так и автоматические процедуры согласования ключей.

Допускается ручной (например, с клавиатуры) и автоматический (например, при помощи смарт-карты) ввод ключей. На двух нижних уровнях безопасности при автоматическом вводе секретные ключи должны быть зашифрованы; ручной ввод может осуществляться в открытом виде. На третьем и четвертом уровнях при ручном вводе ключей в открытом виде должны применяться процедуры разделения знаний.

Модуль должен ассоциировать введенный ключ (секретный или открытый) с владельцем (лицом, процессом и т.п.).

3.8 Самотестирование

Криптографический модуль должен выполнять самотестирование при включении питания, при выполнении некоторых условий (когда вызывается функция безопасности, для которой предусмотрено тестирование), а также по требованию оператора.

Тесты должны покрывать все функции модуля (зашифрование, расшифрование, аутентификацию и т.д.). Для определения правильности прохождения тестов может применяться как сравнение с заранее известными, эталонными результатами, так и анализ согласованности результатов двух независимых реализаций одной и той же функции.

Специфицированы следующие виды проверок:

- тесты криптографических алгоритмов;
- контроль целостности программного обеспечения;
- тесты функций, критичных для безопасности модуля.

В число проверок, выполняемых по условию, входят:

- проверка взаимной согласованности парных ключей;

- контроль загружаемых программ;
- контроль ключей, вводимых вручную;
- тест генератора случайных чисел;
- тест режима обхода.

3.9 Доверие проектированию

Меры доверия проектированию, регламентируемые стандартом, распространяются на конфигурационное управление, процедуры безопасной установки, генерации и распространения, процесс разработки и документацию.

Документация, представляемая разработчиком на первом уровне безопасности, должна специфицировать соответствие между проектом криптографического модуля и его политикой безопасности, а комментарии в исходном тексте — между проектом и программными компонентами.

На втором уровне предусмотрена функциональная спецификация с неформальным описанием модуля, внешних портов и интерфейсов, их назначения.

На третьем уровне программные компоненты должны быть реализованы на языке высокого уровня, за исключением, быть может, небольшого числа ассемблерных вставок. Высокоуровневая спецификация требуется и для аппаратуры.

На четвертом уровне требуется формальная модель политики безопасности с обоснованием ее полноты и непротиворечивости и неформальной демонстрацией соответствия функциональным спецификациям. В исходных текстах программных компонентов должны быть представлены необходимые предусловия и ожидаемые постусловия.

В комплект документации должны входить руководства крипто-офицера (аналог руководства администратора) и пользователя.

3.10 Сдерживание прочих атак

Криптографические модули могут стать объектом самых разных атак, основанных, например, на анализе потребляемого электропитания или времени выполнения операций, на переводе модуля в сбойный режим, на анализе побочных электромагнитных излучений и наводок и т.д.

Для противодействия анализу потребляемого электропитания в модуль могут встраиваться конденсаторы, использоваться внутренние источники питания, вставляться специальные инструкции для выравнивания потребления электропитания в процессе выполнения криптографических функций.

Средство сдерживания атак, основанных на анализе времени выполнения операций — вставка дополнительных инструкций, сглаживающих различия во времени работы.

Для противодействия атакам, основанным на переводе модуля в сбойный режим, стандарт рекомендует описанные выше меры физической защиты.

3.11 Прочие рекомендации

В качестве приложений стандарт FIPS 140-2 содержит рекомендации, дополняющие одиннадцать групп требований безопасности. Это:

- сводка требований к документации;
- рекомендуемые правила разработки программного обеспечения;
- рекомендуемое содержание политики безопасности криптографического модуля.

4. Заключение

В заключение хотелось бы еще раз подчеркнуть роль стандарта FIPS 140-2 как базового элемента других спецификаций в области информационной безопасности, таких как профили защиты сервисов безопасности, их комбинаций и приложений. Очевидно, весьма желательна разработка российского аналога данного документа.

5. Литература

1. FIPS PUB 140-2: Security Requirements for Cryptographic Modules. — U.S. Department of Commerce, NIST, May, 25, 2001.
2. Бетелин В.Б., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Трифаленков И.А. Профили защиты на основе «Общих критериев». Аналитический обзор. — Jet Info, 2003, 3.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555