Тезисы доклада на конференции «Рус Крипто» 2008.
Веденьёв Л.Т., Леонтьев С.Е., Попов В.О.

Вопросы повышения безопасности ключей пользователей в среде вычислительной системы

Рассмотрены вопрсы уязвимости ключей СКЗИ в среде вычислительной системы и использования интеллектуальных карт для обеспечения их повышенной защищённости.

1. Потенциальные атаки на ключи в вычислительной системе

Использование криптографических ключей в ВС связано с потенциальной возможностью их компрометации на этапах генерации, хранения и выполнения криптографических преобразований.

Типичное использование криптографического ключа в вычислительной системе (ВС) характеризуется следующим:

- ключ хранится на ключевом носителе в формате ключевого контейнера, защищенным на пароле пользователя. Как правило, в алгоритме защиты ключа используется также рандомизатор с изменением его случайного значения при каждом обращении ВС к ключевому носителю;
- ключ с сохранением защиты считывается в память ВС в том же формате ключевого контейнера, включая рандомизатор. Защита с ключа снимается в ВС только на время выполнения криптографических операций. Однако, в ВС на все время актуализации ключевого контейнера для оперативного использования в приложении сохраняется и вся информация, необходимая для снятия защиты ключа при обращении к нему криптографических функций.

Потенциально на ключевую информацию могут осуществляться атаки:

- перехват ключевого контейнера при считывании с носителя в ВС и записи его из ВС на носитель;
- перехват пароля при вводе его в ВС;
- перехват ключевого контейнера и пароля (выработанного из пароля ключа) при их хранении в ВС;
- перехват ключа в открытом виде из памяти ВС;
- перехват из памяти ВС информации о ключе при выполнении использующих его криптографических функций.

Указанные атаки могут приводить к опасным последствиям. Так перехват ключевого контейнера дает возможность определения ключа опробованием пароля. Возможность перехвата ключа, информации о ключе, пароля из памяти ВС требует применения эффективных мер разграничения доступа к ключевым контейнерам и к инициируемым пользователями процессам.

Поэтому требуется применение других альтернативных решений по использованию в ВС криптографических ключей.

2. Функциональный ключевой носитель на смарткарте

Альтернативным направлением обращения с ключами в ВС, противодействующим атакам, приведенным в п.1, может быть использование функциональных ключевых носителей (ФКН) на смарткартах (SC).

С использованием ФКН на SC связаны следующие возможности:

- доступ к работе с SC только по предъявлении пароля (pin-кода);
- генерация, хранение, использование и уничтожение (вывод из действия) ключей в SC;
- опциональная возможность доступа к ключу в SC по предъявлении пароля на ключ;
- защита ключа от экспорта из SC штатными средствами SC;
- выполнение в SC криптографических функций (формирование ЭЦП, вычисление ключа Диффи-Хеллмана).
- экспорт из SC только результатов выполнения криптографических функций.

Для использования ФКН на SC требуется решение вопросов:

- аутентификация ВС с SC;
- защита от перехвата паролей доступа к SC и опционального доступа к ключам в SC;
- обеспечение качественной генерации ключа в SC с учетом слабого по доверию штатного ДСЧ SC;
- защита от несанкционированного использования ключа и криптографического функционала SC.

3. Проблема доверия к системе SC – ВС

На качественном уровне доверие к системе SC – ВС характеризуется следующей таблицей:

Функционал	**Уровень доверия к SC**	**Уровень доверия к ВС**
Генерация ключей	Нет доверия к ДСЧ	Полное доверие к ДСЧ
Хранение ключей	Полное доверие	Нет полного доверия
Криптографический функционал	Требует обоснования	Полное доверие

Из этой таблицы следует, что необходимо повышение уровня доверия к системе SC – BC в целом. Этого можно достичь разработкой и использованием протокола взаимодействия SC с BC, учитывающего слабые и сильные стороны обеих составляющих системы.

В частности, должны быть обеспечены:

- статистически качественная генерация ключа в SC, в частности, с поддержкой ДСЧ SC источником случайной последовательности BC;
- защита от неавторизованного доступа к использованию ключей в SC.

4. Распределенные вычисления

При использовании в системе SC – BC криптографических алгоритмов, допускающих распределенные вычисления, имеется возможность при выполнении криптографической функции часть операций выполнить в SC и остальную часть - в BC.

Например, закрытый ключ d ЭЦП стандарта ГОСТ Р 34.10-2001 может быть аддитивно разложен на две (в общем случае, на большее число) части:

$$d = (d_{SC}+d_{BC})(\mathrm{mod}\ q)$$

и использоваться следующим образом: хэш подписывается на составляющей d_{SC} ключа d в SC и доподписывается на составляющей d_{BC} в BC. Ключ d при этом непосредственно не фигурирует и реализуется только через составляющие d_{SC} и d_{BC}. Открытый ключ Q, соответствующий закрытому ключу d, вычисляется раздельно через свои составляющие Q_{SC} и Q_{BC}:

$$Q = (Q_{SC} + Q_{BC}),$$

где $Q_{SC} = (d_{SC})P$, $Q_{BC} = (d_{BC})P$, P – порождающий элемент используемой группы точек эллиптической кривой G, q - порядок группы, Q, Q_{SC}, Q_{BC} – точки эллиптической кривой.

Использование аддитивного представления ключа d предоставляет:

- возможность разделения вычисления ЭЦП между SC и BC с использованием составляющих d_{SC} и d_{BC} закрытого ключа d соответственно;
- возможность синхронного маскирования составляющих d_{SC} и d_{BC} случайной маской Δ:

$$(d_{SC} +\Delta)\ (\mathrm{mod}\ q),\ (d_{BC} - \Delta)(\mathrm{mod}\ q)$$

с без изменения закрытого ключа d и открытого ключа Q.

Распределенное вычисление ЭЦП производится по схеме:

SC	**Обмен**	**BC**
d_{SC}		d_{BC}
h	$\Leftarrow$ h	h (подписываемый хэш)
Генерация случайного числа k_1		Генерация случайного числа k_2
Вычисление точки k_1P	$k_1P \Rightarrow$ $\Leftarrow (kP)_x$	Вычисление точки $kP = k_1P + k_2P =$ $=((kP)_x,(kP)_y)$
$S_1 = d_{SC}(kP)_x + k_1h$	$S_1 \Rightarrow$	$S_2 = d_{BC}(kP)_x + k_2h$
		$S = (S_1 + S_2)(\mathrm{mod}\ q)$
		ЭЦП (h) = (S, $(kP)_x$)

Проверка подписи ЭЦП(h) осуществляется в BC на сертификате открытого ключа *Q*. При этом опосредованно проверяется равенство $d_{SC} = d - d_{BC}$, чем обеспечивается аутентичность SC с BC. Это является также фактором аутентичности ключа *d* на базе сертификата открытого ключа *Q*.

Аналогично может производиться вычисление ключа Диффи-Хеллмана.

5. Распределение ключей в системе SC – BC

Принципиально возможно построение двух схем распределения ключей в системе SC – BC:

1) Создание и хранение в BC ключевого контейнера составляющей d_{BC} со случайной ее стартовой генерацией.

2) Создание ключевого контейнера составляющей d_{BC} в BC в сеансе работы с SC; при этом d_{BC} вычисляется с использованием специального переменного параметра, снимаемого с SC, и параметра, разрешающего проведение сеанса работы с SC (пароль пользователя).

Первый вариант привязывает SC к BC, на которой хранится ключевой контейнер составляющей $d_{BC.}$ Второй вариант свободен от этого недостатка, но требует организации протокола выработки составляющей d_{BC}.

6. Аутентификация пользователя на ключ в системе SC - BC

Исходя из принципа парольной аутентификации ключей в системе SC– BC будем предполагать, что каждому ключу (составляющей ключа) в SC должен соответствовать собственный пароль. Процедура парольной аутентификации должна удовлетворять следующим требованиям:

- перехват пароля ключа в BC должен быть исключен организационно-техническими мерами;

- определение пароля по данным обмена между SC и BC должно быть гарантированно сложным;

- для затруднения определения пароля допустимое число ложных попыток обращения к ключу должно быть ограничено и мало.

Протокол парольной аутентификации на ключ в системе SC– BC может быть построен на базе протокола EKE, [1, п. 22.5]. В ряде работ данный протокол исследовался в случае парольной аутентификации, [2].

Приведем примеры возможных протоколов передачи параметра x из BC в SC и из SC в BC.

Протокол $EKEinSC(x)$ используется для передачи параметра x (точка эллиптической кривой, число, бинарный массив) из BC в SC. По принципу открытого распределения ключей в ФКН и в CSP образуется ключ K_{EKE} в формате точки эллиптической кривой: $K_{EKE}=(x_{K_{EKE}}, y_{K_{EKE}})$. Ключ K_{EKE} используется следующим образом:

- точка x передается точкой $x+K_{EKE}$.

- число (бинарный массив) x передается числом (бинарным массивом) $x \oplus x_{K_{EKE}}$, $\oplus$ - операция сложения по модулю 2. Ключ K_{EKE} вырабатывается при каждом обращении к протоколу $EKEinSC(x)$.

Протокол $EKEinSC(x)$ передачи параметра x из BC в SC

	SC	**BC**
	Начальное состояние: Q_{PW}, id_x	Начальное состояние: Q_{PW}, id_x, x
1		$rndm\ \alpha$, $Q_\alpha = e[id\_x]\alpha P$; $u_1 = Q_\alpha + Q_{PW}$;
2		$\Leftarrow u_1$
3	Проверка: $u_1 \in G$? $Q_\alpha = u_1 - Q_{PW}$; $rndm\ \beta$; $Q_\beta = e[id\_x]\beta P$; $u_2 = Q_\beta + Q_{PW}$	
4	$u_2 \Rightarrow$	
5		$Q_\beta = u_2 - Q_{PW}$; $K_{EKE} = \alpha Q_\beta$ $u_3 = x + \alpha(u_2 - Q_{PW})$, если x - точка, $u_3 = x \oplus x_{\alpha(u_2 - Q_{PW})}$, если x - число или бинарный массив
6		$\Leftarrow u_3$

7	$K_{EKE} = \beta Q_\alpha$; $data = u_3 - K_{EKE}$, если x - точка, ($data = u_3 \oplus x_{K_{EKE}}$, если x - число или бинарный массив); Контроль соответствия идентификатора параметру x и допустимого числа неуспешных операций: Если **ERROR,** возврат к 1, иначе $x = data$	
8	Двустороняя аутентификация на базе кюча K_{EKE}	Двустороняя аутентификация на базе кюча K_{EKE}

Здесь Q_{PW} - ключ аутентификации SC с ВС, вырабатываемый при инсталляции системы SC – ВС из пароля пользователя, должен доставляться в карту по защищённому каналу, вопросам обоснования выбора значения Q_{PW} и стойкости протокола EKE на паролях посвящено много работ, см., в частности, [2];

$e[id\_x]$ - значение идентификатора id_x параметра x.

Аналогично строится протокол $EKEoutSC(x)$ передачи параметра x из SC в ВС.

К особенностям данных протоколов относится использование механизмов, обеспечивающих невозможность опробования пароля при многократных ложных запросах, здесь этот механиз не представлен.

На базе протоколов $EKEinSC(x)$ и $EKEoutSC(x)$ реализуется доверенный канал SC – ВС, обеспечивающий защиту данных информационного обмена между SC и ВС, а также могут быть реализованы протоколы подтверждения идентичности критических параметров в SC и ВС, создания ключевого контейнера пользователя, открытия ключевого контейнера, смены пароля пользователя, формирования ЭЦП, формирования ключа согласования (ключа Диффи-Хеллмана), удаления ключевого контейнера в системе SC - ВС, депанирования ключей.

Анализ системы SC – ВС, построенной с использованием распределенных вычислений, протоколов типа EKE и порядка обращения с ключевыми контейнерами приводит к выводам о ее эффективной защищенности от атак потенциального нарушителя на ключи пользователей, на неавторизованное их использование и неавторизованное использование криптографических операций, определение паролей ключей по обмену протоколов.

Литература:

1. B. Schneier. Applied Cryptography.

2. Phillip MacKenzie. On the Security of the SPEKE Password-Authenticated Key Exchange Protocol.

3. Горелов Д. Интеллектуальные ключевые носители для российских систем PKI. Тезисы доклада на конференции «Рус Крипто» 2008.