Использование атрибутной подписи в двухуровневой информационной системе с динамической структурой

С.В.Беззатеев, А.В.Афанасьева, К.А.Жиданов

Санкт-Петербургский Университет Аэрокосмического Приборостроения

22-25 марта 2022 г.
РУСКРИПТО 2022

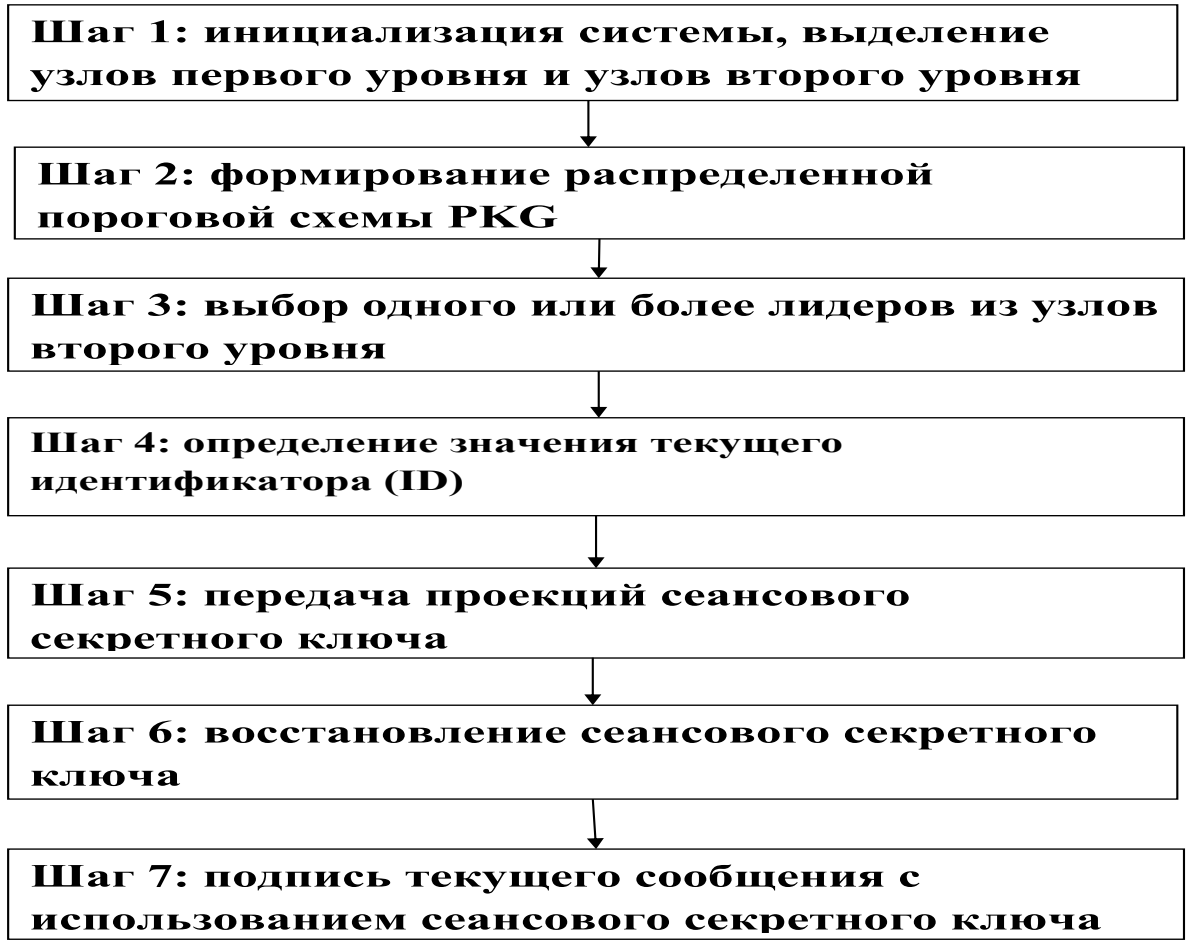
План

1. Введение
2. Основные этапы предлагаемого протокола подписи сообщений
3. Шаг 1 : Инициализация системы
4. Шаг 2 : Инициализация распределенного генератора секретного ключа (PKG)
5. Шаг3 : Выборы одного или нескольких лидеров из узлов второго уровня
6. Шаг 4 : Выбор текущего идентификатора (ID)
7. Шаг 5 : Создание теней сессионного ключа и их распределение
8. Шаг 6 : Восстановление сессионного ключа
9. Step 7 : Подпись сообщения
10. Заключение

Введение

К недостаткам известных решений относятся недостаточная защищенность электронной цифровой подписи и высокая сложность алгоритмов реализации формирования цифровой подписи.
Протокол, предлагаемый в данной работе, позволяет повысить надежность цифровой подписи и защищенность подписанных сообщений от несанкционированного вмешательства.

Основные этапы протокола подписи сообщений



Шаг 1: Инициализация

Узлы первого и второго уровня логически разделены.

1. Общеизвестными являются::
   - аддитивная группа $G1$ порядка q (группа точек на эллиптической кривой);
   - мультипликативная группа $G2$ (группа целых чисел в модульной арифметике).

Шаг 1: Инициализация

2. Выбираются, публикуются и становятся доступными для всех узлов системы, участвующих в протоколе, следующие функции
   - $H1 : \{0,1\}^* \longrightarrow G1$ (функция отображения произвольной двоичной строки в точку на кривой).
   - $e : G1 \times G1 \longrightarrow G2$ (билинейное преобразование используемое в "ID-based"криптографических примитивах).
3. Выбирается PKG секретный мастер SMK : $s \in Z_q$ (Z_q множество целых чисел по модулю q , где q - простое число).
4. Выбирается точка P: генераторная точка аддитивной группы $G1$ на эллиптической кривой.
5. Вычисляется открытый мастер ключ $PMK = s \cdot P$.

Шаг 2: Инициализация пороговой схемы PKG

Секретный мастер ключ *SMK* распределяется между узлами второго уровня.
Таким образом создается распределенная пороговая схема PKG в соответствии с (k, n) пороговой схемой следующим образом:

1. Выбирается случайный многочлен $f(x)$ с коэффициентами из Z_q

$$Z_q : deg\left(f\left(x\right)\right) = k - 1, SMK \equiv f(0)\, mod\, q$$

2. Каждый узел второго уровня, участвующий в распределенной пороговой схеме PKG, получает свою тень мастер ключа *SMK*

$$ss_i \equiv f(L_i)\, mod\, q,$$

Шаг 3: Выбор одного или более лидеров из узлов второго уровня

Выбирается один или более лидеров $\{L_1, L_2, ..., L_w\}$ из числа узлов второго уровня, используя для этого хэш-функцию (H_3), аргументами которой являются идентификаторы всех узлов второго уровня и дополнительные параметры.

$$H_3 : \{L_1, L_2, ..., L_w\} \times R \rightarrow \{L_1, L_2, ..., L_w\}$$

Шаг 4: Выбор текущего идентификатора (ID)

Сообщения m_i создаются узлами первого уровня. Таким образом, агрегированный набор сообщений $\{m_1, m_2, ..., m_n\}$ определяет значение текущего идентификатора (ID) и соответствует значению временного сессионного открытого ключа $PK_t^{(L_i)}$ для каждого из выбранных лидеров $\{L_{i_1}, L_{i_2}, ..., L_{i_w}\}$.

Шаг 5: Создание и распределение теней сессионного ключа

Каждый из k узлов второго уровня (участвующих в распределенной пороговой схеме PKG) вычисляют сессионный открытый ключ $PK_t^{(L_i)}$ следующим образом

$$PK_t^{(L_i)} = H1\left(L_i, m_1, m_2, ..., m_n\right) = Q,$$

где L_i - идентификатор (ID) выбранного лидера, и $Q \in G1$.
В случае, если схема работает в режиме выбора нескольких лидеров, то сессионный ключ вычисляется как

$$PK_t^{(L_{i_1}, L_{i_2}, ..., L_{i_w})} = H1\left(L_{i_1}, L_{i_2}, ..., L_{i_w}, m_1, m_2, ..., m_n\right) = Q,$$

Шаг 6: Восстановление сессионного ключа

Узлы второго уровня передают имеющиеся у них проекции(тени) сессионного секретного ключа

$$\left(SK_t^{(L_i)}\right)_j = ss_j * PK_t^{(L_i)},$$

выбранному на предыдущем шаге 3 лидеру L_i (либо нескольким лидерам $\{L_{i_1}, L_{i_2}, ..., L_{i_w}\}$ в режиме нескольких лидеров).
$SK_t^{(L_i)}$ - точка на эллиптической кривой, соответствующая идентификатору (L_j).

Шаг 6: Восстановление сессионного ключа

Каждый узел второго уровня L_i выбранный в качестве лидера собирает свой собственный секретный ключ $SK_t^{(L_i)}$ используя для этого проекции(тени) сессионного секретного ключа $\left(SK_t^{(L_i)}\right)_j$ которые он получит от узлов второго уровня, участвующих в схеме распределенного порогового PKG.

Шаг 6: Восстановление сессионного ключа

Получив множество из k пар $(\left(SK_t^{(L_i)}\right)_j, L_j)$ от k узлов второго уровня на шаге 6, один или более(в зависимости от режима работы схемы) лидеров второго уровня, выбранных в качестве лидерв, вычисляют свои собственные секретные ключи $SK_t^{(L_i)}$ используя формулу

$$SK_t^{(L_i)} = \sum_{j=1}^{k} \lambda_{(L_j,0)} \cdot \left(SK_t^{(L_i)}\right)_j = \sum_{j=1}^{k} \lambda_{(L_j,0)} \cdot ss_j \cdot PK_t^{(L_i)},$$

$\lambda_{(L_j,0)}$ – коэффициент Лагранжа для выбранной коалиции, вычисленный для узла второго уровня с идентификатором L_j и точки 0,
где коалиция- это группа из k узлов второго уровня выполняющих функции распределенного PKG

Шаг 7: Подпись сообщения

Для подписи сообщений генерируется случайное целое r_1 из Z_q ,
где Z_q множество целых чисел по модулю q, как было определено выше.
Далее вычисляется

$$R = r_1 \cdot P,$$

$$S = SK_t^{(L_i)} + r_1 \cdot H1\,(L_i, M) = s \cdot Q + r_1 \cdot H1\,(L_i, M),$$

где M - подписываемое сообщение ;
P генераторная точка аддитивной группы $G1$ на эллиптической кривой;
(R, S) - подпись для сообщения M ;
$SK_t^{(L_i)}$ сессионный секретный ключ лидера с идентификатором L_i, выбранного узлами второго уровня.

Заключение

Предлагаемый вариант протокола позволяет решить задачу повышения достоверности и безопасности цифровой подписи для сообщений в сети формируемой узлами разного уровня.

Спасибо за внимание

Беззатеев Сергей Валентинович
bsv@aanet.ru
Санкт-Петербургский Университет
Аэрокосмического Приборостроения

Проверка подписи сообщения

$$e(P,S) =? = e(PMK,Q) \cdot e(R, H1\ (L_i, M)),$$

$$e(P,S) = e(P,sQ) \cdot e(P, r_1 H1\ (L_i, M)) = e(P,Q)^s \cdot e((P, H1\ (L_i, M))^{r_1},$$

$$e(PMK,Q) = e(sP,Q) = e(P,Q)^s,$$

$$e(R, H1\ (L_i, M)) = e(r_1 P, H1\ (L_i, M)) = e(P, H1\ (L_i, M))^{r_1}.$$