Скрытый канал

Густавус Джеймс Си́ммонс (англ. *Gustavus James Simmons*, 27 октября 1930, Западная Виргиния, США) — американский криптограф, бывший руководитель факультета прикладной математики, старший научный сотрудник Национальной лаборатории «Сандия». Он занимался в основном теорией аутентификации, разрабатывал криптографические методы для решения проблем «взаимного недоверия».

Спустя 40 лет с начала своей работы по «теории аутентификации» Густавус стал известен как «отец теории аутентификации». Его работа нашла применение не только в сфере национальной безопасности, но и в сферах коммерческой и интернет безопасности.

В 1980-х он помог сформировать Международную ассоциацию по криптографическим исследованиям (IACR). Он также является создателем математической игры Sim, основанной на теории графов/теории Рамсея.

В Сандии Симмонс входил в штаб по контролю и управлению ядерным оружием, осуществлял криптографические испытания, проверяя факт соблюдения Договора о всеобъемлющем запрещении ядерных испытаний на предмет: «Действительно ли участники соглашения не используют технические устройства, для передачи и обмена запрещенной информацией, не скрывают ли факт продолжения испытаний ядерного оружия?»

Скрытый канал

Возможность организации скрытого канала в открытой сети на основе криптографических методов, а именно в криптосистеме с цифровой подписью, впервые была замечена и обоснована Густавом Симмонсом в 1984г. в работе «Проблема заключённых и подсознательный канал».

Задача имеет следующую интерпретацию. Алиса и Боб сидят в тюрьме в разных камерах, но у них есть право с помощью надзирателя Уолтера обмениваться сообщениями. Уолтер хочет знать о их возможных замыслах и поэтому имеет право читать их сообщения. Алиса и Боб могут подписывать свои сообщения с целью предотвратить подлог от третьих лиц. Уолтер имеет право проверять их подписи. Каким образом в заданных условиях Алиса и Боб могут организовать защищённый скрытый канал?

Ответ от Симмонса заключался в том, что они могут встраивать тайные сообщения в подпись так, что при этом роль подписи как инструмента аутентификации сохранялась в полном объёме.

Особенностью такого канала является, как правило, необходимость довольно высокого уровня доверия Алисы и Боба друг другу, поскольку они пользуются совместным секретным ключом. Схема это двухпроходного протокола имеет следующий вид:

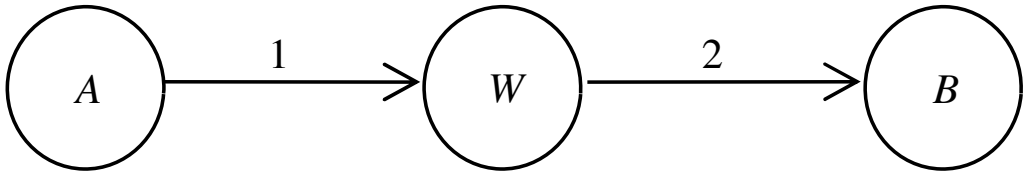
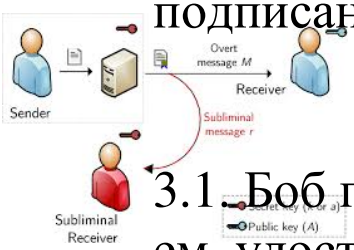


Рис. 1

Скрытый канал

1.1. Алиса генерирует открытое (невинное или безобидное) сообщение.
1.2. Алиса подписывает невинное сообщение, используя секретный ключ, общий с Бобом, и пряча в подписи скрытое сообщение. (Это — ядро протокола скрытого канала).
1.3. Алиса отправляет с Уолтером подписанное сообщение Бобу.

2.1. Уолтер читает невинное сообщение и проверяет подпись.
2.2. Не встретив ничего подозрительного, Уолтер передает Бобу подписанное сообщение.



3.1. Боб проверяет подлинность подписи под невинным сообщением, удостоверяясь, что сообщение поступило от Алисы и не было изменено.
3.2. Боб игнорирует невинное сообщение и, используя секретный ключ, общий с Алисой, извлекает скрытое сообщение.

Скрытый канал

Скрытый канал на основе схемы Онга-Шнорра-Шамира

Этот канал был открыт Густавов Симонсом. Основные параметры схемы следующие. Алиса подписывает открытое сообщение m, Боб проверяет подпись. Генерируются: p — большое (простое) число, с условием $m < p$, с условием $(m, p) = 1$; x — случайное число Алисы, $1 < x < p$, с условием $(x, p) = 1$; $y = -x^2 \bmod p$. Элементы $\{p, y\}$ объявляются открытым ключом, элемент $\{x\}$ — закрытым ключом Алисы. В случае скрытого канала $\{x\}$ должно быть известно и Бобу.

Генерация подписи.

1. A: $\{k\}$, где k — скрываемой сообщение Алисы, оно должно удовлетворять условиям $(k, p) = 1$, $1 < k < p$;
2. A: $\{a\}$, где $a = 2^{-1}(mk^{-1} + k) \bmod p$;
3. A: $\{b\}$, где $b = x2^{-1}(mk^{-1} - k) \bmod p$, подписью являются a и b.
4. $A \rightarrow W(B)$: $\{m, a, b\}$.

Проверка подписи.

5. W : проверяет, что $a^2 + yb^2 = m \bmod p$.
6. $W \rightarrow B$: $\{m, a, b\}$.
7. B : проверяет, что $a^2 + yb^2 = m \bmod p$.

Получение секретного сообщения.

8. B : извлекает секретное сообщение, $k = m(a + bx^{-1})^{-1} \bmod p$.

Эта схема работоспособна, но следует помнить, что сама схема Онга-Шнорра-Шамира была взломана.

Скрытый канал

Скрытый канал на основе схемы Эль-Гамаля

Напомним основные параметры схемы Эль-Гамаля. Алиса подписывает открытое сообщение m, Боб проверяет подпись. Генерируются: p — большое простое число, с условием $m < p$; g — примитивный корень по модулю p; x — случайное число Алисы, $1 < x < p$, с условием $(x, p-1) = 1$; $y = g^x \bmod p$. Элементы $\{p, g, y\}$ объявляется открытым ключом, элемент $\{x\}$ — закрытым ключом Алисы. В случае скрытого канала $\{x\}$ должно быть известно и Бобу.

Генерация подписи.

1. A: $\{k\}$, где k — скрываемой сообщение Алисы, оно должно удовлетворять условиям $(k, p-1) = 1$, $1 < k < p-1$;
2. A: $\{a\}$, где $a = g^k \bmod p$;
3. A: $\{b\}$, где $b = k^{-1}(m - xa) \bmod (p-1)$, подписью являются a и b, которые удовлетворяют уравнению $m = (xa + kb) \bmod (p-1)$. Для скрытого канала должно выполняться дополнительное условие: числа $(m - xa)$ и $(p-1)$ должны быть взаимно простыми. Это условие выполнить несложно, поскольку m (безобидное сообщение) при необходимости всегда можно немного подправить.
4. $A \rightarrow W\,(B)$: $\{m, a, b\}$.

Проверка подписи.

5. W : проверяет, что $y^a a^b \bmod p = g^m \bmod p$.
6. $W \rightarrow B$: $\{m, a, b\}$.
7. B : проверяет, что $y^a a^b \bmod p = g^m \bmod p$.

Получение секретного сообщения.

8. B : извлекает секретное сообщение, $k = b^{-1}(m - xa) \bmod (p-1)$.

Скрытый канал

Скрытый канал на основе ESIGN

Протокол ESIGN (Efficient digital SIGNature — эффективная цифровая подпись) — схема цифровой подписи с открытым ключом, основанная на проблеме факторизации чисел. Цифровая подпись была разработана в японской компании NTT в 1985 году. Отличительной чертой данной схемы является возможность быстрой генерации подписи.

Основные параметры схемы. Алиса подписывает открытое сообщение m, Боб проверяет подпись. Генерируются: p, q — большие простые числа одинаковой длины; вычисляется $n = p^2q$; выбирается $k \geq 4$ (параметр безопасности). Элементы $\{n, k\}$ объявляются открытым ключом, элементы $\{p, q\}$ — закрытым ключом Алисы.

Генерация подписи.

1. A: $\{h\}$, где $h = H(m)$ — хэш-функция со значением от 0 до $n - 1$, этот шаг можно опустить, если сообщение m удовлетворяет неравенству $0 \leq m \leq n - 1$;
2. A: $\{x\}$, где x случайное число из интервала $0 < x < pq$;
3. A: $\{a, b\}$, где $a = \left\lceil \frac{h - (x^k \bmod n)}{pq} \right\rceil$, $b = a(k \cdot x^{k-1})^{-1} \bmod p$, $\lceil z \rceil$: R $\to$ Z функция округления сверху, т.е. $\lceil z \rceil = \min\{n \in \mathrm{Z} \mid n \geq z\}$ (не путать с функцией $[z]$ целой части числа z, для целых z выполняется $\lceil z \rceil = [z]$, для нецелых z выполняется $\lceil z \rceil = [z] + 1$);
4. A: $\{s\}$, где $s = x + bpq$;
5. $A \to B$: $\{m, s\}$.

Проверка подписи.

6. B : $\{h\}$, где $h = H(m)$;
7. B : $\{c\}$, где $c = \left\lceil \frac{2}{3}\log_2 n \right\rceil$, ($\frac{2}{3}\log_2 n$ —это $\frac{2}{3}$ от числа бит в n)
8. B : проверяет неравенство, что $h \leq s^k \bmod n \leq h + 2^c$.

Скрытый канал

Скрытый канал на основе ESIGN

Основные параметры схемы в случае скрытого канала. Алиса подписывает безобидное сообщение m, Боб проверяет подпись. Вместе в этим передаётся секретное сообщение m^*. Генерируются: p, q, r — большие простые числа одинаковой длины; вычисляется $n = p^2qr$; выбирается $k \geq 4$ (параметр безопасности). Элементы $\{n, k\}$ объявляются открытым ключом, элементы $\{p, q, r\}$ — закрытым ключом Алисы. Часть этого ключа, а именно r, должна быть известна Бобу для извлечения секретного сообщения и необходимо выполнение неравенства $m^* < r$.

Генерация подписи.

1. A: $\{h\}$, где $h = H(m)$ — хэш-функция со значением от 0 до $n - 1$;
2. A: $\{x\}$, где $x = m^* + ur$ и u — случайное число из интервала $0 < u < pq - 1$;
3. A: $\{a, b\}$, где $a = \left\lceil \frac{h - (x^k \bmod n)}{pqr} \right\rceil$, $b = a(k \cdot x^{k-1})^{-1} \bmod p$;
4. A: $\{s\}$, где $s = x + bpqr$;
5. $A \rightarrow W(B)$: $\{m, s\}$.

Проверка подписи.

6. W : $\{h\}$, где $h = H(m)$;
7. W : $\{c\}$, где $c = \left\lceil \frac{2}{3}\log_2 n \right\rceil$, ($\frac{2}{3}\log_2 n$ —это $\frac{2}{3}$ от числа бит в n)
8. W : проверяет неравенство, что $h \leq s^k \bmod n \leq h + 2^c$.
9. $W \rightarrow B$: $\{m, s\}$.

Получение секретного сообщения.

10. B : Боб также проверяет подпись и извлекает секретное сообщение, $m^* = s \bmod r$.

Скрытый канал

Скрытый канал на основе DSA

Основные параметры схемы. Алиса подписывает открытое сообщение m, Боб проверяет подпись. Генерируются: q — большое простое число с условием $h = H(m) < q$; p — большое простое число , такого, что $(p - 1)$ делится на q, а именно имеет вид $p - 1 = 2^t q$. Выбирается число g такого, что его мультипликативный порядок по модулю p равен q. Для его вычисления можно воспользоваться формулой $g = h^{(p-1)/q} \bmod p$, где h — некоторое произвольное число, $h \in (1; p - 1)$ такое, что $g \neq 1$. В большинстве случаев значение $h = 2$ удовлетворяет этому требованию. Далее выбирается случайное число $x \in (0; q)$ и вычисляется $y = g^x \bmod p$. Элементы $\{p, q, g\}$ могут быть общими для группы пользователей, Элемент $\{y\}$объявляется открытым ключом, элементы $\{x\}$ — закрытым ключом Алисы.

Генерация подписи.

1. A: $\{k\}$, выбирается случайное число $k \in (0; q)$;
2. A: $\{r\}$, где $r = (g^k \bmod p) \bmod q$;
3. A: $\{s\}$, где $s = k^{-1}(H(m) + x \cdot r) \bmod q$;
4. A: если $r = 0$ или $s = 0$, то выбор нового k;
5. $A \rightarrow B$: $\{m, r, s\}$.

Проверка подписи.

6. B : $\{u\}$, где $u = s^{-1} \bmod q$;
7. B : $\{a\}$, где $a = H(m) \cdot u \bmod q$;
8. B : $\{b\}$, где $b = r \cdot u \bmod q$;
9. B : $\{v\}$, где $v = (g^a \cdot y^b \bmod p) \bmod q$;
10. B : Если $v = r$, то подпись верна.

Скрытый канал

Скрытый канал на основе DSA

Основные параметры схемы в случае скрытого канала те же, только с добавлением простого числа P (отличающегося от параметра p в схеме подписи). Это секретный ключ для скрытого канала, известный Алисе и Бобу. Следующая схема позволяет Алисе и Бобу обмениваться в каждой подписи одним битом скрытой информации.

1. Алиса подписывает безобидное сообщение m и на шагах 1 и 2 выбирает случайное число $k \in (0; q)$ так, чтобы параметр r подписи являлся квадратичным вычетом по модулю P, если она хочет передать скрытый бит 1, или являлся квадратичным невычетом по модулю P, если она хочет передать скрытый бит 0. Так как числа, являющиеся квадратичными вычетами и невычетами, равновероятны, то добиться результата не сложно.
2. Алиса посылает Бобу подписанное сообщение.
3. Боб проверяет подпись и убеждается в подлинности сообщения. Затем он проверяет, является ли r квадратичным вычетом по модулю P и восстанавливает скрытый бит.

Передача описанным выше способом нескольких битов $b_1, b_2, \ldots, b_n$ подразумевает подбор такого значения r, которое является квадратичным вычетом или невычетом по нескольким модулям $P_1, P_2, \ldots, P_n$.

Скрытый канал

Уничтожение скрытого канала в DSA

Скрытый канал использует то обстоятельство, что Алиса может выбирать k для передачи скрытой информации. Чтобы уничтожить скрытый канал связи, необходимо запретить Алисе возможность свободного выбора k. Однако свободный выбор k должен быть запрещен и для всех других лиц, иначе они получат возможность подделать подпись Алисы.

Единственным решением в таких обстоятельствах является проведение генерации k вместе с другой стороной, в нашем случае Уолтером, так, чтобы Алиса не могла управлять ни одним битом k, а Уолтер не мог определить ни один бит k. И у Уолтера должна быть возможность проверить, что Алиса использовала именно совместно созданное k.

1. $A \to W$: $\{u\}$, где $u = g^{k'} \bmod p$ и k' случайное число $k' \in (0; q)$;
2. $W \to A$: $\{k''\}$, где k'' случайное число $k'' \in (0; q)$;
3. A: $\{k\}$, где $k = k' \cdot k'' \bmod (p - 1)$, далее продолжается основной протокол подписи DSA с шага 2, когда наступает время проверки подписи Уолтером, этот протокол продолжается;
4. W: $\{r'\}$, где $r' = (u^{k''} \bmod p) \bmod q$; если $r = r'$, то Уолтер знает, что для подписи m использовалось k.

После этапа 4 Уолтер знает, что в r не было включено никакой скрытой информации, но не сможет доказать этот факт третьей стороне, воспроизведя запись протокола.

Более того, Уолтер, если захочет, может использовать этот протокол для создания собственного скрытого канала. Он может включить скрытую информацию в одну из подписей Алисы, выбрав k'' с определенными характеристиками. Когда Симмонс открыл такую возможность, он назвал её «Каналом кукушки». Предотвратить «Канал кукушки» можно с помощью трехпроходного протокола генерации k.

Скрытый канал

Задание 1. В чём преимущество скрытого канала на основе ESING над двумя предыдущими?
Задание 2. Проверить корректность схемы подписи ESING и оценить её комбинаторную сложность.
Задание 3. Определить границы параметра x в скрытом канале на основе схемы подписи ESING.
Задание 4. Проверить корректность восстановления секретного сообщения в секретном канале на основе ESING.
Задание 5. Скрытый канал можно встроить почти в любую из известных схем подписи. ЗАДАНИЕ: Встроить скрытый канал в схему подписи Фейге-Фиата-Шамира.
Задание 6. Проверить корректность схемы подписи DSA.
Задание 7. Можно ли уничтожить скрытый канал в других схема подписи (помимо DSA)?