УДК 681.3.067

А. И. Колыбельников

Московский физико-технический институт (государственный университет)
ООО «Код Безопасности»

Обзор методов формирования списков отозванных сертификатов

Инфраструктура открытых ключей (PKI) получила широкое распространение как в обычных компьютерных сетях, так и в интернете вещей (IoT). PKI применяется для аутентификации узлов сети и контроля целостности, эти процедуры построены на проверке электронной подписи данных. Наиболее сложной операцией при проверке электронной подписи является проверка статуса сертификата. Данная проверка может быть реализована двумя методами — с использованием CRL (certificate revocation list) или с OCSP – (Online Certificate Status Protocol). В данной статье рассматриваются преимущества и недостатки каждого из этих методов, приведена оценка безопасности и рассмотрена применимость наиболее эффективного из методов для IoT.

Ключевые слова: инфраструктура открытых ключей, список отозванных сертификатов, интернет вещей, сетевое кодирование.

A. I. Kolybelnikov

Moscow institute of physics and technology (State University)
Security Code LTD

Methods of optimization of storage and delivery of CRL

Public Key Infrastructure (PKI) became widespread in common computer networks and the Internet of Things (IoT). PKI is used forthe authentication of network nodes and integrity control; these procedures are based on verifying the electronic signature of data. When verifying the electronic signature, the most complicated operation is checking the certificate status. This check may be carried out using two methods: either using CRL (certificate revocation list) or using OCSP (Online Certificate Status Protocol). This article discusses advantages and disadvantages of each method, provides a safety assessment and discusses the applicability of the most e ective method for IoT.

Key words: PKI, CRL, IoT, VANET, network coding.

1. Введение

Операция проверки электронной подписи состоит из нескольких проверок: проверки корректности вычисления хэша и подписи с точки зрения математики, проверки доверия к сертификату подписанта и проверка статуса сертификата подписанта. Проверка статуса сертификата требует получения данных о сертификате от УЦ, который его выпустил, эти данные предоставляются одним из методов. Использование CRL – наиболее распространенный метод информирования пользователей о том, что сертификат их контрагента был отозван. Недостаток метода состоит в том, что существует «окно опасности», разница во времени между временем отзыва сертификата пользователя и временем, когда публикуется новый CRL. Использование протокола OCSP – это наиболее точный способ информирования пользователей о том, что сертификат их контрагента был отозван. Недостатком

© Колыбельников А. И., 2018
© Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)», 2018

данного протокола является то, что он требует сетевой доступности УЦ выпустившего сертификат подписанта на момент проверки его подписи, кроме того не все реализации УЦ поддерживают данный протокол. Для данного метода «окно опасности» так же существует, но оно меньше чем для CRL. Далее в статье приводится обзор наиболее эффективных методов информирования о статусе сертификата пользователя и их применимость в IoT. Описание методов дается от самых старых к самым современным и эффективным.

2. Система отзыва сертификатов Микали

В первой версии системы использовалась офлайн/онлайн схема подписи для ежедневного обновления подписи. Схема включает в себя однонаправленную функцию f. Выбирается случайное значение y_0 и вычисляется $f^k(y_0)$ и сохраняется в сертификате. Вычисления $f^k(y_0)$ производятся рекурсивно: $f^k(y_0) = f(f^{k-1}(y_0))$, обновление может быть выпущено k раз, актуальный сертификат содержит самое актуальное на данный момент число, что служит подтверждением действительности сертификата.

Для проверки подлинности сертификата пользователь должен запросить в УЦ текущее значение f^j. В этом случае время проверки пропорционально количеству обновлений сертификата и ограничивают его срок жизни.

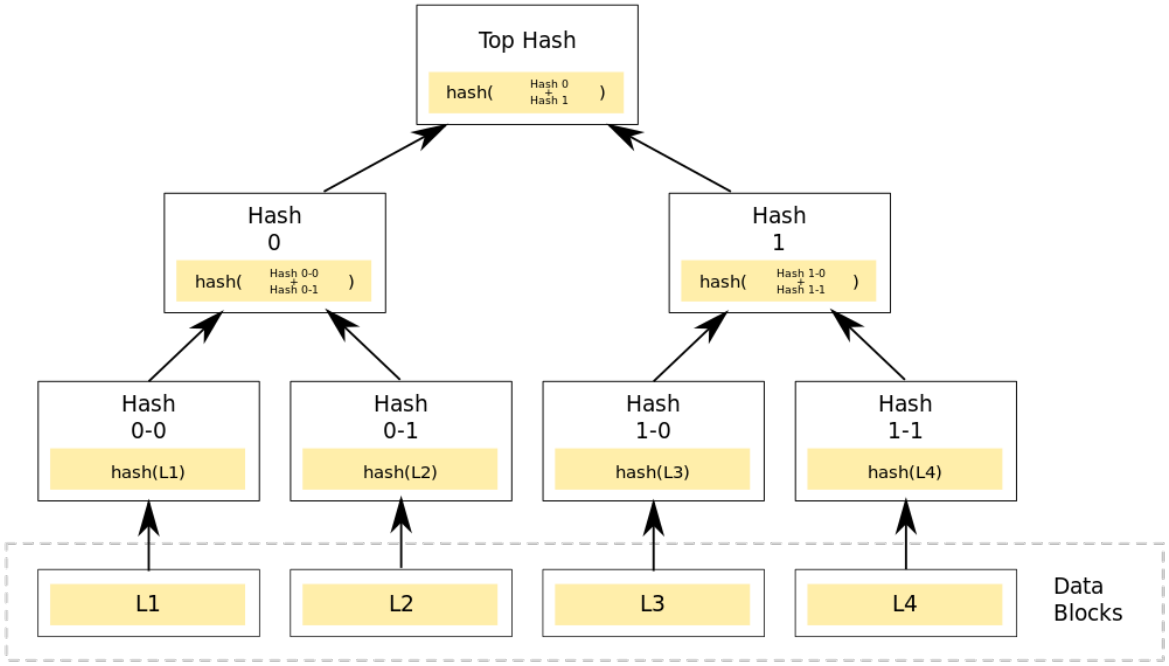

Рис. 1. Дерево хэшей Меркла

Вторая версия системы Микали использует деревья Меркла. Хеш-деревом, деревом Меркла, называют полное двоичное дерево, в листовые вершины которого помещены хеши от блоков данных, а внутренние вершины содержат хеши от сложения значений в дочерних вершинах. Корневой узел дерева содержит хеш от всего набора данных, то есть хеш-дерево является однонаправленной хеш-функцией. В этом случае каждый серийный номер сертификата содержит два бита, указывающие на то, был ли сертификат выпущен или остановлен в своем действии. Эти биты хранятся в листьях дерева (64 сертификата или 128 бит на лист), и каждый родительский узел в дереве сохраняет хэш ценностей детей. Наконец, корень подписывается УЦ. Недостатком системы является то, что кроме статуса конкретного сертификата система сообщает пользователю много дополнительной инфор-

мации о других выпущенных сертификатах, что может быть использовано для атак и не соответствует нормативам в части безопасности персональных данных.

3. Дерево отзыва Кохера

Данная схема, предложенная Кохером, так же, как и вторая версия системы Микали, базируется на деревьях Меркла. Только в качестве листа дерева выступает один сертификат. В результате получится дерево существенно меньше, чем в системе Микали, но отзыв одного сертификата будет приводить к пересчету всего дерева.

4. Словари аутентификации(2–3 Trees)

В данной схеме единое дерево Меркла из схемы Микали заменено на 2–3 дерево. Сделано это для того, что бы отзыв одного сертификата не требовал изменения всего дерева. При этом размер самого дерева увеличен на значение логарифма относительно схемы Микали. Также следует отметить, что два последних метода предназначены только для доставки информации об отзыве сертификата пользователя и никак не решают задачу построения цепочки доверенных сертификатов.

5. Новый метод формирования CRL

Новый метод формирования CRL, предложенный в работе 2017 года, выглядит следующим образом:

$$(M_n \| T_n \| Hash_{n-1} \| (M_n \| T_n \| Hash_{n-1})_{Hash_n} \| (Hash_n)_{\mathrm{Sign}_n}. \quad (1)$$

От выше описанных систем перелагаемая система отличается следующим. Предлагаемый алгоритм позволяет формировать один CRL на протяжении всего срока жизни УЦ, не исключая из него информацию об сертификатах, закончивших свое действие. Это позволяет увеличить срок актуальности подписи, если ее надо хранить в архиве. Дополнение CRL производится по факту обновления одной записи, этот подход позволяет кардинально сократить объем информации, передаваемый от УЦ к пользователю для проверки статуса сертификата. Для случая, когда частота проверки подписи совпадает с частотой обновления CRL, объем передаваемых данных равен OCSP-запросу. В случае если частота проверки подписи выше, чем частота обновления CRL, то предлагаемая схема будет передавать наименьший объем данных среди всех существующих схем. В случае если частота проверки подписи ниже, чем частота обновления CRL, то для проверки будет передаваться не весь CRL, а разница между ранее скачанным и самой последней записью. По сравнению с ранее рассмотренными схемами изменение одной записи в CRL не приводит к пересчету всего дерева хэшей, достаточно посчитать хэш и ЭП для новой записи. Основная масса методов оптимизации работы с CRL направлена на оптимизацию структуры CRL для ускорения поиска информации в нем. В новом методе формирования CRL предлагается оптимизация направленная на:

1) продление срока действия сертификатов пользователей;

2) ускорение доставки информации о статусе сертификата пользователям;

3) оптимизацию объема передаваемых данных;

4) уменьшение количества подписей в CRL, подписан только последний хеш, остальные с ним связаны.

5.1. Оценка вероятности компрометации CRL

Считается, что самым большим недостатком CRL является наличие временной дельты между фактом компрометации ключей в момент t и фактом сообщения данной информации пользователю в момент $t+dt$, проверяющему электронную подпись. Временная дельта $dt = t_1 + t_2$ состоит из двух частей: $t_1 = t_0 - t$, где t_0 – момент сообщения о компрометации удостоверяющему центру, t_2 – время на добавление информации об отзыве в CRL и доставку CRL проверяющему.

В случае, если УЦ имеет много клиентов и клиенты проверяют подпись в произвольный момент времени, обращения к УЦ за обновлениями CRL будут подчиняться распределению Пуассона, где v – скорость проверки сертификатов за единицу времени. Вероятность того, что n сертификатов будет проверено за период $[0, t]$:

$$\left[\frac{(vt)^n}{n!}\right] e^{-vt}, n = 1, 2, 3, \ldots \tag{2}$$

Вероятность того, что n сертификатов не будет проверено за период $[0, t]$ равна

$$e^{-vt}. \tag{3}$$

Вероятность проверки одного сертификата $n = 1$ в интервале времени $[t, t + dt]$ – это $vdte^{-vdt}$. Вероятность неудачи в получении CRL в интервале $[0, t]$ равна e^{-vth}, где h – длина цепочки сертификации. Исходя из этого получаем вероятность успешной проверки по CRL в диапазоне времени $[t, t + dt]$:

$$e^{-vt}vdte^{-vdt}e^{-vth} = vdte^{-vt(h+1)}e^{-vdt} = ve^{-vt(h+1)}, \tag{4}$$

учитывая, что $dt \longrightarrow 0$. Оценка со стороны УЦ будет

$$R(t) = Nve^{-vt(h+1)}, \tag{5}$$

где N – количество пользователей конкретного УЦ, h является константой в конкретной системе, а N и v фиксированы на коротком промежутке времени.

6. Методы смены алгоритмов хеширования и подписи

Смена алгоритмов хеширования происходит по причине вывода алгоритмов хеширования из употребления в качестве стандартов. Как правило, это происходит, когда для определенных алгоритмов находят более не менее эффективную атаку или по причине создания мощных вычислительных систем, способных подобрать коллизии для хешей определенной длины. В случае формирования CRL классическим способом, когда хеш и подпись расчитываются от всего CRL, этот файл требует периодического перерасчета хеша и переподписания действительной ЭП, такую процедуру также называют заверением. Частота заверения зависит о срока действия сертификата ЭП под CRL. Чаще всего, это от года до трех.

Для методов формирования CRL с использованием связанных записей путем построения хеш-функций срок действия CRL практически не зависит от стойкости хеш-функции, так как вероятность взлома такого CRL будет $\prod_{i=0}^{t} p_i$, где p_i – вероятность взлома хешей цепочки записей CRL в момент времени t. То есть с течением времени стойкость всей цепочки записей растет. Но ограничение все же существует – для избежания коллизий один CRL – не более $2^{n/2}$ записей в цепочке, где n – длина блока хеша. Если злоумышленник нашел коллизию для одного из хешей, он сможет подменить записи только одной записи, все остальные должны остаться неизменными, в противном случае не сойдется последний хеш и подпись под всем CRL.

Ключ формирования подписи в новом методе формирования CRL меняется аналогично использованию классического CRL. Ключ проверки электронной подписи должен иметь максимальный срок действия. В противном случае необходимо заверение CRL новым ключом.

7. Атака и меры защиты новой схемы CRL

Если коллизия была получена УЦ в ходе легального формирования CRL то у криптоаналитика появляется возможность «выкинуть» записи между коллизиями. Противостоять этому можно двумя способами – добавив поле номер записи, что бы обеспечить непрерывность записей или добавить поле содержащее случайное число, которое можно будет менять в случае обнаружения коллизии в процессе расчета CRL.

8. Использование CRL в сетях с сетевым кодированием

Использование сетевого кодирования CRL рассматривалось в [6] для ускорения передачи CRL в автомобильной сети VANET.

8.1. Кодирование

1) Пересылаемый CRL делится следующим образом: $x_{crl} = \{x_1, x_2, \dots x_N\}$.

2) Создается кодирующий вектор $c = (c_1, c_2, \dots c_N)$, где $c \in_R GF(2^m)$.

3) Из разделенного CRL x_{CRL} и кодирующего вектора c создается кодированный вектор $y = c_{i,1}x_1 + c_{i,2}x_2 + \dots c_{i,N}x_N$.

4) Посылается кодированный пакет $\{c, y\}$.

Для передачи всего CRL требуется N отправлений.

8.2. Декодирование

1) Создается декодирующий вектор: $\widetilde{c} = (\widetilde{c_1}, \widetilde{c_2}, \dots \widetilde{c_M})$ где $c \in_R GF(2^m)$.

2) Повторно кодируются закодированные данные $\widetilde{y}$ с $\widetilde{c}$ и присланными закодированными данными y:

$$\widetilde{y} = \widetilde{c}y. \tag{6}$$

3) Вектор кодирования $\widehat{c}$ восстанавливается следующим образом:

$$\widehat{c} = \widetilde{c}C. \tag{7}$$

4) Отправляет пакет $\{\widehat{c}, \widetilde{y}\}$.

Результаты моделирования показывают, что предложенная схема работает в плотном потоке транспортных средств и может полностью распределить CRL, размер которого меньше чем или равняется 200 Кбайтам на перекрестке, подразумевая, что на перекрестке есть от 1 до 6 точек передачи данных. Инфраструктура открытых ключей(PKI) в Интернете вещей (IoT) применяется для решения нескольких задач:

- контроль целостности узла сети, например, автомобиля;
- аутентификация узлов сети при взаимодействии, например при получении обновлений ПО.

Методы, применяемые в VANET:

- распространение CRL методом эпидемии;
- УЦ создает цепочку хеш-значений сертификатов, каждое из значений уникальное, для отзыва достаточно добавить это значение в CRL;
- для хранения CRL используется фильтр Блома;
- подписывается каждая запись в CRL.

Если для данной модели предположить использование нового метода формирования CRL [2], то необходимый объем передаваемой информации можно существенно уменьшить. В среднем одна запись в CRL с учетом доработок, предложенных в [2], имеет размер не более 512 байт. Если предположить, что сертификаты всех машин выпущены одним УЦ, на каждом перекрестке автомобиль проверяет целостность всех окружающих машин, то частота проверки должна в 400 раз превосходить скорость внесения записей в CRL, например по причине выхода из строя автомобилей. Если сравнить эту цифру с количеством ДТП в России за сутки — 501 (за 2015 год), то можно утверждать, что за два проезда перекрестка в сутки машина получит полное обновление CRL в рамках страны.

9. Заключение

Новый алгоритм формирования списков отозванных сертификатов, предложенный в работе [2], эффективнее ранее созданных алгоритмов [1, 3–5, 7] по объему передаваемых данных от УЦ к пользователю. Эффективность зависит от объема данных, представленных в CRL, чем больше данных, тем эффективнее новый метод. Он также позволяет продлить срок проверки ЭП, в случае, если УЦ не убирает из CRL информацию о старых сертификатах.

Литература

1. *Gassko I., Gemmell P.S., MacKenzie P.* Efficient and Fresh Certification. H. Imai, Y. Zheng (Eds.) // PKC 2000. LNCS. V. 1751. P. 342–353.
2. *Колыбельников А.И.* Новый алгоритм формирования списков отозванных сертификатов // Труды МФТИ. 2017. Т. 9, № 2. С. 111–116.
3. *Jason J. Haas, Yih-Chun Hu, Kenneth P.* Laberteaux Efficient Certificate Revocation List Organization and Distribution // IEEE Journal on selected areas in communications. 2011. V. 29, N 3.
4. *Naor M., Nissim K.* Certificate Revocation and Certificate Update // IEEE Journal on selected areas in communications. 2000. V. 18, N 4.
5. *Zhao Qiu* A Study on CRL Issue by P2P Network // Third International Symposium on Intelligent Information Technology and Security Informatics
6. *Akkaya K., Rabieh Kh., Mahmoud M., Tonyali S.* Customized Certificate Revocation Lists for IEEE 802.11s-Based Smart Grid AMI Networks // IEEE Transactions on smart grid. 2015. V. 6, N 5.
7. *Yamamoto T., Fukuta Y., Mohri M., Hirotomo M., Shiraishi Y.* A Distribution Scheme of Certificate Revocation List by Inter-vehicle Communication Using a Random Network Coding ISITA2012. Honolulu. Hawaii. USA. October 28–31, 2012.

References

1. *Gassko I., Gemmell P.S., MacKenzie P.* Efficient and Fresh Certification. H. Imai, Y. Zheng (Eds.). PKC 2000. LNCS. V. 1751. P. 342–353.
2. *Kolybelnikov A.I.* New algorithm for formation of certificate revocation lists. Proceedings of MIPT. 2017. V. 9, N 2. P. 111–116.
3. *Jason J. Haas, Yih-Chun Hu, Kenneth P.* Laberteaux Efficient Certificate Revocation List Organization and Distribution. IEEE Journal on selected areas in communications. 2011. V. 29, N 3.
4. *Naor M., Nissim K.* Certificate Revocation and Certificate Update. IEEE Journal on selected areas in communications. 2000. V. 18, N 4.
5. *Zhao Qiu* A Study on CRL Issue by P2P Network. Third International Symposium on Intelligent Information Technology and Security Informatics.
6. *Akkaya K., Rabieh Kh., Mahmoud M., Tonyali S.* Customized Certificate Revocation Lists for IEEE 802.11s-Based Smart Grid AMI Networks. IEEE Transactions on smart grid. 2015. V. 6, N 5.
7. *Yamamoto T., Fukuta Y., Mohri M., Hirotomo M., Shiraishi Y.* A Distribution Scheme of Certificate Revocation List by Inter-vehicle Communication Using a Random Network Coding ISITA2012. Honolulu. Hawaii. USA. October 28–31, 2012.

Поступила в редакцию 27.11.2018