TIMESTAMPING

ВРЕМЕННАЯ ШТАМПОВКА

Амосов Евгений, 012гр.

ВВЕДЕНИЕ

Во многих ситуациях возникает необходимость удостоверить время создания или последней модификации документа. Например, в вопросах интеллектуальной собственности иногда важно определить время, когда изобретатель впервые изложил на бумаге патентоспособную идею, чтобы удостоверить, что она предшествовала конкурирующим заявкам.

Существуют разные методы временной штамповки, все они основываются на двух допущениях. Во-первых, записи должны быть проверяемы на предмет признаков подделки. Во-вторых, должен участвовать некто, проверяющий документ, чья честность или беспристрастность удовлетворяет требования безопасности.

Эти допущения должны быть поставлены на серьёзное рассмотрение в случае, когда документы создаются и хранятся исключительно в электронном виде. Цифровая временная штамповка – это процесс, который связывает электронный документ с датой и временем. Эффект временной штамповки подобен и датированию и заверению бумажного документа у общественного нотариуса. Она также позволяет владельцу электронного документа доказать, что документ существовал в определённое время и что он не был изменен после того, как это был проштампован.

ТЕХНОЛОГИЯ ЦИФРОВОЙ ВРЕМЕННОЙ ШТАМПОВКИ

Есть много способов проектировать систему временной штамповки. Простая, но менее безопасная система может быть сформирована, используя только цифровые подписи. Более сложные системы используют совокупность методов, для осуществления защиты и универсальности. У всех подходов есть достоинства и недостатки, и выбор зависит от требований, наложенных на систему.

Схема простая временная штамповки

Первая система будет использовать некое третье лицо, которому доверяют, назовём его Штамповщик (Time-stamping Authority, TSA). Чтобы проштамповать документ, пользователь посылает его копию Штамповщику.

Штамповщик считывает время со своих системных часов и добавляет его в конец документа. Затем подписывает результат и возвращает это всё дело пользователю в виде свидетельства. Чтобы проверять временной штамп, пользователь открытым ключом Штамповщика расшифровывает информацию в свидетельстве. Если информация расшифровывается должным образом, то штамп достоверен. Подписание документа вместе со временем защищает его от модификации. В принципе, этот способ удовлетворяет основным требованиям для временной штамповки электронного документа. Однако такой подход вызывает несколько опасений:

Секретность. Метод подвергает риску секретность документа двояко: в момент его передачи документ может перехватить злоумышленник, и после передачи документ неопределённо доступен у самого Штамповщика.

Пропускная способность и хранение. Время, необходимое для отправки документа, а так же количество памяти, необходимое для хранения документа у Штамповщика зависят от размера документа. Поэтому, время и расходы на штамповку большого документа могу быть чрезмерно высоки.

Некомпетентность. Копия документа может быть повреждена в процессе передачи её Штамповщику, может быть неправильно проштампована, может быть повреждена или вообще утеряна в любой момент, пока хранится у Штамповщика.

Доверие. Главная проблема остаётся: ничто в этой схеме не препятствует Штамповщику и пользователю тайно сговориться и проставить штамп с временем, отличающимся от настоящего.

Относительное время и односторонние хеш-функции

Не всегда можно доверять любому времени, поставленному третьим лицом. Это время, называющееся абсолютным временем, считывается с некоторых часов. Трудно гарантировать, что любые часы показывают правильное время, или что третье лицо правильно считывает время.

Решение этой проблемы заключается в использовании относительного времени. Здесь мы связываем событие не с фактическим временем, а с парой других событий. Вместо того чтобы говорить, что документ был проштампован в x часов, мы говорим, что документ был проштампован после события A и перед событием B. Если выбранные события случайны и широко засвидетельствованы (например, солнечная активность, мировые события и т.д.), на них нельзя повлиять. Итак, мы хотим создать штамп относительного времени, мы хотим зажать штамп между двумя событиями. Чтобы доказать, что штамп был создан после некоторого времени, мы должны сделать штамп, зависящий от некоторого случайной, широко засвидетельствованный события. Чтобы доказать, что штамп создан до некоторого времени, штамп должен повлиять на некоторое широко известное событие.

Чтобы проверить временной штамп, пользователь должен иметь доступ к обоим событиям, предшествующим и последующим штампу. Поэтому, все события, связанные со всеми временными штампами должны быть как-то сохранены. Требования памяти для всех этих данных стали бы невообразимыми. Чтобы осуществлять такую систему, размеры данных должны быть некоторым способом сокращены. Сделать это нам позволяют односторонние хеш-функции.

Схема цепного связывания

Системы цепного связывания используют хеш и относительное время. Они связывают вместе временные штампы в длинные цепочки, которые трудно подделать. В большой системе временной штамповки, с большим числом пользователей, невозможно предсказать какие документы будут представлены для штамповки. Поэтому, сами документы достаточно случайны, чтобы использоваться как основание для относительной временной штамповки.

Все документы, полученные системой, связаны в супер-хеш. Некоторая произвольная строка выбрана как начальный супер-хеш H_0. Документ Doc1 добавляется в конец H_0 и хешируется, получаем супер-хеш

H_1. Затем каждый следующий полученный документ Doc_i добавляется в конец к супер-хешу H_{i-1} и хешируется ещё раз, формируя новый супер-хеш H_i. Через некоторый фиксированный промежуток времени (например, каждый день, или после каждой сотни документов), супер-хеш H_n публикуется. Публикация супер-хеша – широко засвидетельствованное событие, и привязывает хеш к ральному времени. Другие случайные события (например, оперативная служба рассылки новостей) тоже могут использоваться для временной штамповки, чтобы усилить защиту системы.

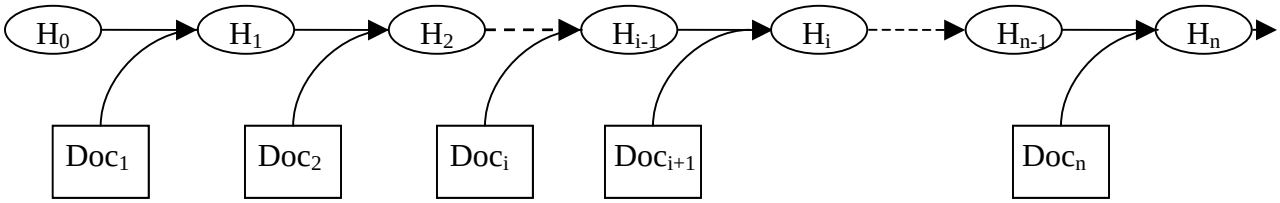

рис.1 Временная штамповка по схеме цепного связывания

Проверяется такой временной штамп просто «в лоб». Сначала документ (Doc_i) хешируется с предыдущим супер-хешем предыдущим (H_{i-1}), потом хешируется со всеми последующими документами ($Doc_{i+1},...,Doc_{n-1}$), до тех пор, пока не будет получен публикуемый хеш (H_n). Если полученный хеш соответствует опубликованному, то временной штамп документа достоверен.

Надёжность. Если предположить, что надёжна схема подписи, используемая службой, и её секретный ключ всё ещё является секретным, то атака на эту систему может быть удачной только в результате сотрудничества службы штамповки со злоумышленником.

Замечания. Недостатком схемы является то, что всем пользователям необходимо хранить свои временные штампы, чтобы сделать возможной проверку. Чтобы разрешить это, нужно связать документ не только с предыдущим и последующим, но и с некоторым k-ым.

Недостаток в том, что увеличивается размер временного штампа, но также и повышается его надёжность. Для проведения атаки нужно будет изменить не только ID_{n-1} и ID_{n+1} но и также ID_{n-k},…, ID_{n-1} ,ID_{n+1},…, ID_{n+k} .

Схема цепочного связывания для системы временной штамповки безопасна и проста. Она гарантирует надежное, хотя и относительное время. Так как хеши уникальны по отношению к данным, от которых они получены, любая модификация документа изменила бы хеш, делая временной штамп недействительным. Это защищает документ от подделки. Однако процесс проверки занимает много времени. Например, если хеш публикуется после каждой сотни документов, пользователю, возможно, придётся хешировать документ с девяноста девятью другими, чтобы проверить временной штамп. Штамповка хэша документа вместо самого документа может облегчить эту проблему. Это уменьшает размер данных, который должен быть сохранен и хеширован, но не уменьшает число шагов, которые должны быть выполнены для проверки. Кроме того, системы связывания не масштабируются. Для каждой системы, может существовать только одна цепочка временных штампов. Только один компьютер может использоваться для создания новых супер-хешей. Если объем запросов на штамповку будет высок, один компьютер не будет в состоянии обработать их вовремя.

Схема, использующая деревья

Схема временной штамповки, основанная на деревьях, создает зависимости между документами способом, как в схеме связывания. Однако, вместо того, чтобы связывать документы в прямую цепочку, эта схема связывает документы в *n*-арные деревья. Двоичные деревья - самый простой пример. Выбирается произвольная строка в качестве начального супер-хеша. Документы штампуются по раундам. В конце каждого раунда,

все документы Doc_1,…,Doc_8, обрабатываемые в течение этого раунда собираются в дерево. Начиная снизу, документы, формирующие листья дерева хешируются с документами своих уровней (Doc_1 хешируется с Doc_2, Doc_3 с Doc_4 и т. д.). Получившиеся в результате хеши H_1,…,H_4 формируют листья на следующем уровне дерева. Хеши хешируются с хешами того же уровня и так далее вверх по дереву, до тех пор пока не будет получен корневой хеш RH_i (рис. 2.1).

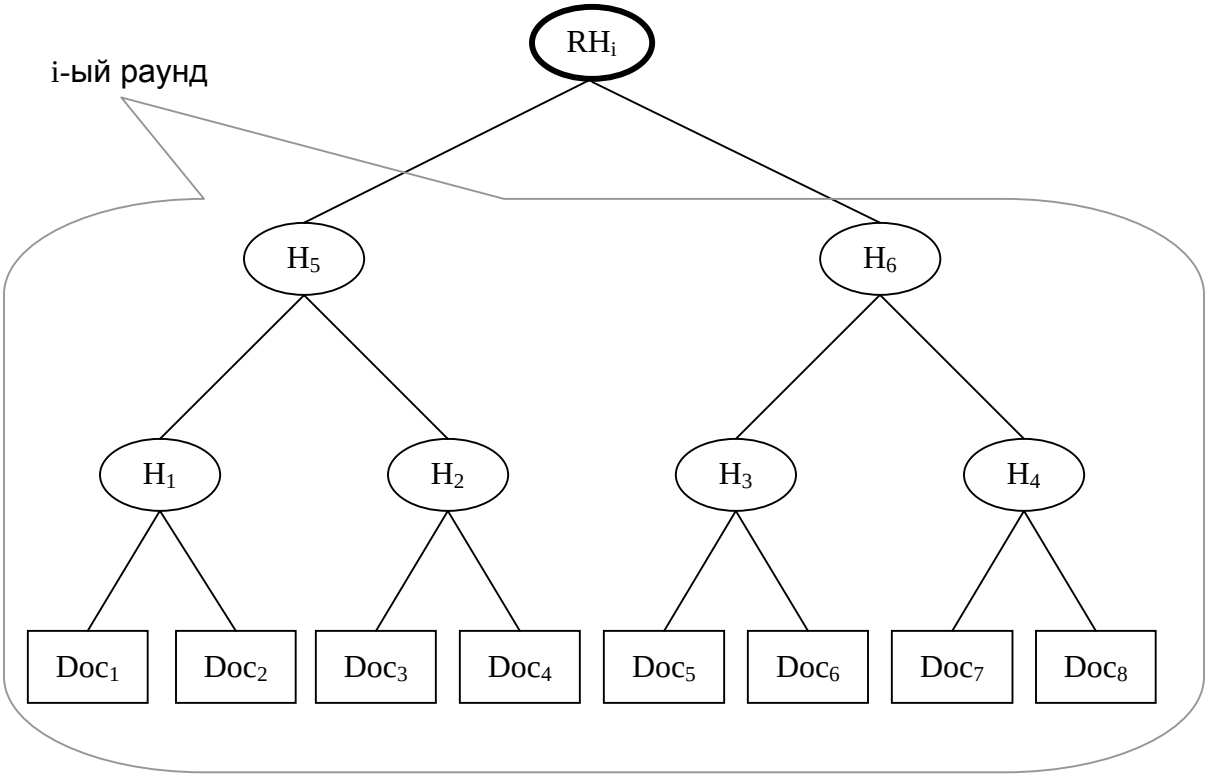

рис. 2.1

Далее, корневой хеш RH_i тогда хешируется с супер-хешем предыдущего раунда SH_{i-1} – получаем новый супер-хеш SH_i (рис. 2.2). Таким образом, корень дерева каждого раунда включен в следующее дерево. Как в схеме связывания, супер-хеш публикуется; другие случайные значения могут быть использованы как листья дерева, чтобы увеличить защиту.

Для проверки временного штампа документа (скажем, Doc_1) в раунд i, документ хешируется со всеми элементами того же уровня от основания дерева к его вершине (Doc_2, H_1 и H_5), пока не получен корень раунда i (H_6).

Этот корень хешируется с супер-хешеи предыдущего раунда (SH_{i-1}), чтобы получить супер-хеш раунда i (SH_i). Если вычисленный супер-хеш соответствует опубликованному, то временной штамп достоверен.

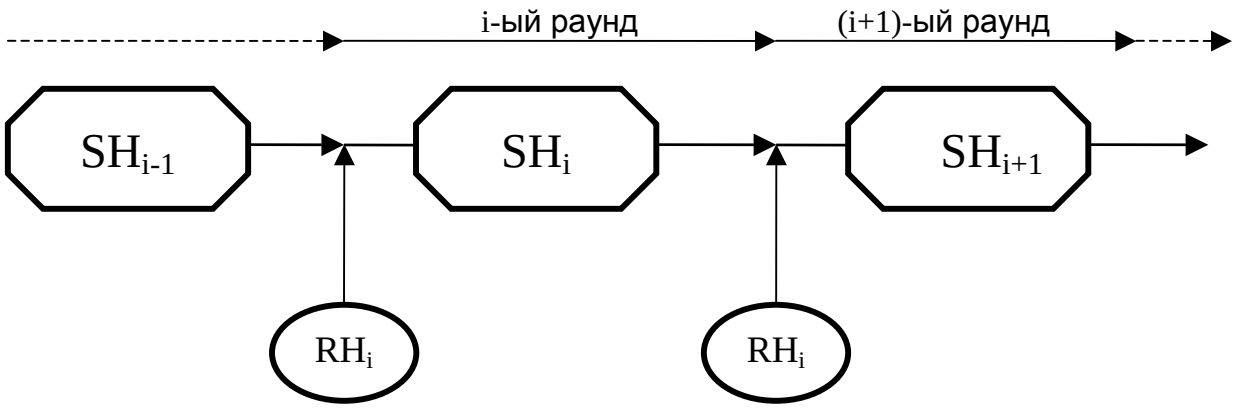

рис 2.2

Использование деревьев для связи документов уменьшает необходимое для проверки число шагов. Максимальное число шагов в схеме связывания равно числу документов, созданных в период между публикациями двух супер-хешей. Для деревьев, максимальное число шагов равно высоте дерева, или $\log_n N$ для *n*-арного дерева, где N - количество документов в раундах. Связывание листьев нижних уровней с листьями, находящимися на несколько уровней выше может ещё больше сократить путь проверки. Эта схем является масштабируемой, так как дерево составлено из меньших деревьев, и вычислять части дерева можно на разных компьютерах. Результаты вычислений всех этих компьютеров будут объединены в супер-хеш отдельным центральным компьютером.

Надёжность. Злоумышленник хочет совершить атаку. Допустим, он не может публиковать супер-хеши вместо службы штамповки. Он перехватывает все документы, которые должны быть проштампованы, и выдаёт себя за службу штамповки. Это не сложно сделать, если между пользователями и службой нет протокола аутентификации, а пользователи

обнаружат обман только когда супер-хеш будет опубликован. А это невозможно, т. к. служба подписывает временные штампы.

Замечания. Достоинство метода в том, что проверка не требует хранения большого числа временных штампов пользователями, как это было в схеме цепочного связывания. Недостаток – нужно накопить достаточное число запросов для каждого раунда.

Деревья решают многие проблемы схемы связывания. Система производит надёжное относительное время. Хеш защищает документы от вмешательства, и структура деревьев позволяет масштабированные вычисления.

ТЕКУЩЕЕ СОСТОЯНИЕ ТЕХНОЛОГИИ ВРЕМЕННОЙ ШТАМПОВКИ

Временная штамповка – всё ещё новая технология. Первый главный документ по теме был издан в 1990. Методы временного штампования до сих пор предлагаются, проверяются и осуществляются. С распространением PKI, интерес во временной штамповке усилился, и были основаны несколько организаций, изучающих эту технологию. В результате был предложен протокол и введены в пользование некоторые схемы.

Организации

Есть две главных организации, изучающие временную штамповку. Первая, Cybernetica, основана в Эстонии. Члены группы изучают новые методы связки документов безопасным способом. Они издали несколько важных документов по теме. Группа сыграла важную роль в формулировке Эстонского Закона Цифровых Подписей.

Вторая организация - европейская группа по Защите Телекоммуникаций и Информационных Систем, называемая INFOSEC. Эта группа в настоящее время работает над проектом Public Key Infrastructure with Time-Stamping Authority (PKITS). PKITS это всестороннее изучение, обсуждение различных схем осуществления временного штампования, различных услуг, которые могут быть с этим интегрированы, и различных типов документов, которые, потенциально, могут быть проштампованы.

Конечная цель проекта состоит в том, чтобы смоделировать технически, экономически и юридически осуществимую службу временной штамповки в ближайшем будущем.

В мае 1999The Internet Engineering Task Force (IETF) предложил Протоколы Временных Штампов. Протокол определяет роль TSA, он прелагает механизм для запроса и проставления временных штампов. Однако он использует простую модель временной штамповки. TSA ответственен за обеспечение временем от достоверного источника, защищают штамп цифровые подписи. Хотя, на данный момент, найти систему, использующую такой протокол сложно.

Текущие реализации

Существует несколько реализаций систем временного штампования. Большинство из них не являются коммерческими, или все ещё находится в испытательной стадии. Digital Notary и Stamper - две самые стабильные системы. Digital Notary – коммерческая служба временного штампования, предоставляемая компанией Surety Technologies (http://www.surety.com), действует где-то с 1994 года. Stamper – бесплатная служба, основанная на PGP, предоставляемая компанией I. T. Consultancy Limited в Великобритании, работает с 1995 года.

Digital Notary.

Surety использует комбинацию схем деревьев и связывания для формирования своих временных штампов. Группы, документов связаны в деревья, главный координирующий сервер Surety связывает корни деревьев в цепочки. Супер-хеш такой связанной цепочки публикуется. Для пользования службой, клиенты должны зарегистрироваться на Surety и установить на своих компьютерах клиентское программное обеспечение. Используя эту систему, Surety может отслеживать, кто что штампует, так что временные штампы Surety также включают слабую аутентификацию. Время периода равно 1 секунде.

1. Пользователь устанавливает клиентскую программу на свой компьютер и подключается к службе временной штамповки через Интернет.
2. Используя эту программу он хеширует документ в 128 битный хеш. Пользователь может либо работать с этим отдельным хешем, либо скомбинировать его с хешами других документов, прежде чем послать его службе штамповки.
3. Служба комбинирует этот(эти) документ(ы) вместе с документами, полученными от других пользователей, с помощью схемы, основанной на деревьях.
4. Каждую секунду служба вычисляет супер-хеш. Он публикуется в нескольких местах, доступных через сеть, а также на CD-ROM. Значение публикуется еженедельно в воскресном выпуске New-York Times.
5. Служба посылает пользователю всё необходимое для удостоверения временного штампа: хеши всех документов, цепочку вычислений всех хешев, время и дату корневого хеша.

PGP Digital Timestamping Services.

Stamper применяет модифицированную версию схемы простой временной штамповки. Есть отдельный Stamper сервер, пользователи системы представляют хеши своих документов этому серверу, который добавляет в конец хеша монотонно увеличивающийся серийный номер, а затем подписывает результат. Все документы и серийные номера хранятся на сервере. В конце каждого дня, Stamper собирает все документы, накопившиеся за день, в отдельный хеш. Этот хеш, наряду с последним серийным номером, полученным в этот день, публикуется в нескольких сетевых телеконференциях. Хеш и серийный номер используются, чтобы гарантировать верное проставление даты. Услуги доступны по электронной почте.

СПИСОК ЛИТЕРАТУРЫ

1. Haber, S. and Stornetta,S. *"How to timestamp a digital document"*. Journal of Cryptography,Vol.3, No. 2,1991, p. 99-111.
2. Massias, H., Qusiquater, J.-J. *"Time and Cryptography"*. TIMESEC Technical report WP1, 1997.
3. Ismail, S. *"Time-Stamping for Malaysia"*, 2000
4. Surety Technologies. *"Digital Notary Service Technical Overview"*, http://www.surety.com
5. Richardson, M. *"PGP Digital Timestamping Service"*, http://www.itconsult.co.uk/stamper/stampinf.htm