Network Working Group
Request for Comments: 4686
Category: Informational

J. Fenton
Cisco Systems, Inc.

September 2006

Анализ угроз, связанных с протоколом DKIM

Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задаёт каких-либо стандартов Internet и может распространяться свободно.

Аннотация

В этом документе приводится анализ некоторых угроз для почтовой системы Internet, связанных с аутентификацией на основе подписей (signature-based mail authentication), в частности DKIM[1]. Обсуждается природа и местоположение отрицательных персонажей, их возможности и цели проведения атак.

Оглавление

[1]DomainKeys Identified Mail.

1. Введение

Протокол DomainKeys Identified Mail (DKIM) был разработан группой IETF DKIM. Этот протокол определяет механизм, с помощью которого сообщения электронной почты подписываются с использованием криптографии. Наличие подписи домена в сообщении указывает на то, что домен принимает на себя ответственность за использование данного почтового адреса. Получатели могут проверить цифровую подпись, запрашивая подписавший сообщение домен напрямую для получения соответствующего открытого ключа, подтверждающего, что сообщение проверено владельцем закрытого ключа, подписавшего это сообщение домена. В этом документе рассматриваются угрозы, связанные с двумя ещё незавершёнными работами группы DKIM - спецификацией подписей DKIM [DKIM-BASE] и практическими рекомендациями по подписанию сообщений отправителем [DKIM-SSP].

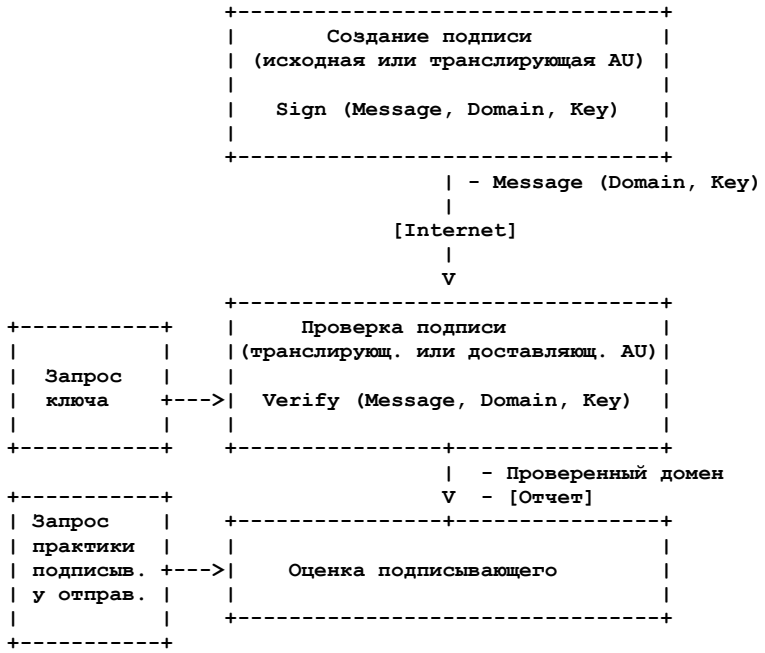
После того, как подтверждение получено, принимающая сторона может оценить сообщение с использованием дополнительных методов таких, как локально поддерживаемые «белые списки», проверенные службы общего пользования и/или гарантии третьей стороны. Описание таких механизмов не входит в число задач рабочей группы IETF DKIM. Ставя подпись, легитимные отправители дают проверяющему возможность связать с этим сообщением позитивную репутацию в надежде, что она будет подобающим образом трактоваться получателем.

Этот метод не защищает от угроз конфиденциальности электронной почты и не обеспечивает долгосрочных сигнатур для архивирования.

1.1. Терминология и модель

Административная единица (AU[1]) представляет собой часть пути, проходимого электронной почтой, находящуюся под единым административным контролем. Отправитель и получатель обычно создают доверительные отношения с административными единицами, через которые передаётся и принимается (соответственно) электронная почта, для подписывания и проверки сообщений.

Адрес отправителя (origin address) представляет собой адрес в почтовом сообщении, который обычно имеет формат RFC 2822 From:, - адрес, связываемый с заявленным автором сообщения и выводимый пользовательским почтовым агентом (MUA[2]), как адрес источника сообщения.



На рисунке показан типовой пример для DKIM.

DKIM полностью работает в контексте сообщения (тело и некоторые поля заголовка), как определено в RFC 2822 [RFC2822]. Передача сообщения по протоколу SMTP определена в RFC 2821 [RFC2821] и такие элементы, как адреса envelope-from и envelope-to, а также домен HELO не имеют отношения к верификации DKIM. По специальному решению для верификации сообщений могут использоваться протоколы, отличные от SMTP, - такие, как POP [RFC1939] и IMAP [RFC3501], которые может использовать агент MUA, являющийся проверяющей стороной.

Запрос практики подписывания у отправителя[3], показанный в нижней части схемы, является способом, посредством которого проверяющий может запросить в домене указанного автора используемую этим доменом практику подписывания сообщений, которая, в свою очередь, может влиять на принятие решения о судьбе данного сообщения. Например, если сообщение приходит без какой-либо корректной подписи и домен указанного автора говорит, что он подписывает все сообщения, проверяющий может обрабатывать такое сообщение иначе, нежели в том случае, когда подписи могло не быть.

1.2. Структура документа

В оставшейся части документа рассматривается проблема, с которой может столкнуться DKIM и расширение протокола, которое поможет решить проблему. Описание приводится с учётом потенциальных отрицательных

[1]Administrative unit.
[2]Mail User Agent.
[3]Sender Signing Practices Query.

персонажей, их возможностей, местоположения в сети и негативных действий, которые эти персонажи могут совершить.

Далее следует описание предполагаемых атак на подписанные с помощью DKIM сообщения и использование практики подписывания на стороне отправителя SSP[1] для трактовки не подписанных сообщений. Представлен также список производных требований, которые предназначены в качестве руководства при разработке DKIM.

Параграфы, посвящённые атакам на DKIM начинаются с таблиц, содержащих список потенциальных атак в каждой категории вместе с ожидаемым воздействием и вероятностью атаки. Ниже приведены критерии, используемые при оценке атак.

Влияние

Сильное: воздействие на верификацию сообщений из целого домена или множества доменов.

Среднее: воздействие на верификацию сообщений от отдельных пользователей, агентов MTA[2] и/или в течение ограниченного интервала времени.

Слабое: воздействие лишь на верификацию отдельных сообщений.

Вероятность

Высокая: пользователям электронной почты следует ожидать частых атак этого типа.

Средняя: пользователям электронной почты следует время от времени ожидать таких атак; атаки могут быть достаточно частыми для отдельных пользователей.

Низкая: атаки предполагаются редкими.

2. Отрицательные персонажи

2.1. Характеристики

Набор проблем, с которыми может столкнуться DKIM, характеризуется широким диапазоном атакующих в терминах мотивации, изощрённости и возможностей.

На нижнем краю диапазона находятся отрицательные персонажи, которые могут просто передавать электронную почту (в некоторых случаях с использованием коммерчески доступных инструментов), которую получатель не желает принимать. Упомянутые инструменты обычно позволяют фальсифицировать адрес отправителя а в будущем могут оказаться способными к генерации подписей.

Следующий уровень можно рассматривать как «профессиональных» отправителей нежелательной почты. Эти могут развёртывать специальную инфраструктуру, включающую агенты MTA, зарегистрированные домены и сети взломанных компьютеров (зомби), для передачи сообщений, а в некоторых случаях и для сбора адресов получателей. Такие отправители часто действуют как коммерческие структуры и передают сообщения «от имени» третьих лиц.

Наиболее изощрённые и финансово заинтересованные отправители нежелательной почты - это те, кто получает от таких рассылок солидный куш (например, участники мошеннических операций, основанный на почтовых сообщениях). Предполагается, что эти игроки будут использовать все перечисленные выше механизмы и могут также атаковать всю инфраструктуру Internet, включая атаки на отравление кэшей DNS и атаки на маршрутизацию IP.

2.2. Возможности

В общем случае следует ожидать, что перечисленные выше отрицательные персонажи имеют доступ:

1. большому массиву сообщений из доменов, которыми они могут пожелать воспользоваться (имперсонифицировать);
2. информации о задачах бизнеса и моделях работы для доменов, которыми они могут пожелать воспользоваться;
3. к открытым ключам и связанным с ними записям для домена.

Предполагается также возможность выполнять по крайней мере часть перечисленных действий:

1. подавать сообщения агентам MTA и MSA[3] во множестве точек Internet;
2. создавать произвольные поля заголовков, включая те, которые используются списками рассылки, средствами пересылки (resender) и другими почтовыми агентами;
3. подписывать сообщения от имени доменов, находящихся под их контролем;
4. генерировать значительное число не подписанных или явно подписанных сообщений, которые могут использоваться для организации DoS-атак;
5. заново отправлять (resend) сообщения, которые ранее были подписаны доменом;
6. передавать сообщения с использованием в конверте (envelope) любой желаемой информации;
7. действовать в качестве уполномоченного агента подачи сообщений (authorized submitter) на захваченных компьютерах;

Как было отмечено выше, некоторые классы отрицательных персонажей имеют сильную финансовую мотивацию своих действий и, следовательно, от них можно ожидать наличия больших возможностей, включая:

1. манипуляцию маршрутами IP; это может использоваться для подачи сообщений с определённого адреса IP, использование адресов, трассировка которых затруднительна, или направление сообщений в заданный домен;

[1]Sender Signing Practices
[2]Mail Transfer Agent - агент передачи почты.
[3]Message Submission Agent - агент подачи сообщений.

2. ограниченное влияние на часть системы DNS с использованием таких механизмов, как “отравление” кэша (cache poisoning); это может служить для воздействия на маршрутизацию сообщений и фальсификации анонсов основанных на DNS ключей или практики подписывания сообщений;

3. доступ к значительным компьютерным ресурсам (например, путём создания крупных сетей специально инфицированных компьютеров - зомби), которые могут позволять организацию атак методом грубой силы (brute-force attack);

4. возможность прослушивания трафика (например, из беспроводных сетей).

Любой из двух первых механизмов может использоваться для того, чтобы отрицательные персонажи могли организовать атаки с участием человека (man-in-the-middle) на пути от отправителя к получателю, если такая атака потребуется.

2.3. Местоположение

Отрицательные персонажи или их посредники (proxy) могут располагаться в любой части сети Internet. Некоторые атаки, возможные прежде всего в пределах административной единицы домена заявленного источника и/или получателя, предоставляют отрицательным персонажам возможности, не доступные в других условиях, как описано ниже. Отрицательные персонажи могут также сговариваться между собой, действуя из множества мест (“распределенный отрицательный персонаж”).

Следует также отметить, что при использовании зомби и иных посредников внешние отрицательные персонажи могут получить доступ к некоторым возможностям, реализованным внутри административной единицы заявленного отправителя или получателя. Это повышает роль мер безопасности (таких, как аутентификация при подаче сообщений) даже внутри административной единицы.

2.3.1. Внешние отрицательные персонажи

DKIM фокусируется прежде всего на отрицательных персонажах, расположенных за пределами административных единиц заявленного источника и получателя. Эти административные единицы часто соответствуют защищённым частям сетей вблизи источника и получателя. В таких областях обычно не существует доверительных отношений, требуемых для подачи сообщения. Напротив, в таких административных единицах существуют другие механизмы типа аутентификации при подаче сообщений, которые проще в реализации и, очевидно, используются более широко, нежели DKIM.

Внешние отрицательные персонажи обычно пытаются воспользоваться природой электронной почты, позволяющей передавать сообщения от любого отправителя к любому получателю, в соответствии с которой многие агенты MTA принимают сообщения от кого угодно для доставки в свой локальный домен. Сообщения могут создаваться без подписей, с некорректными подписями или с корректными подписями сложных в трассировке доменов. Сообщения могут также принимать вид рассылок по спискам (mailing list), поздравительных открыток и других писем от систем, легитимно передающих и пересылающих почту от имени другого отправителя.

2.3.2. Внутри административной единицы заявленного источника

Отрицательные персонажи в виде злонамеренных и не имеющих полномочий пользователей или заражённых вредоносными программами (malware-infected) компьютеров могут присутствовать внутри административной единицы, соответствующей адресу отправителя. Поскольку операция подачи сообщения (submission) в таких областях обычно происходит до включения сигнатуры в сообщение, DKIM не обеспечивает эффективной защиты от внутренних отрицательных персонажей. Защита от них определяется другими мерами (подобающее использование межсетевых экранов, агенты подачи сообщений MSA с аутентификацией автора).

В тех случаях, когда административная единица не представляет собой неразрывную область (например, компания, в которой связь между филиалами осуществляется через Internet), подписи DKIM могут использоваться для того, чтобы отличать легитимные сообщения извне от попыток использования подставных адресов в локальном домене.

2.3.3. Внутри административной единицы получателя

Отрицательные персонажи могут также находиться внутри административной единицы получателя сообщения. Они могут пытаться использовать доверительные отношения, существующие внутри административной единицы. Поскольку сообщения обычно проходят проверку DKIM только на границе административных единиц, DKIM не обеспечит эффективной защиты против сообщений, поданных внутри административной единицы.

Например, отрицательный персонаж может попытаться использовать подмену полей заголовка, показывающих результат проверки. Это поле обычно добавляется проверяющей стороной, которая будет также детектировать подставные поля в проверяемых сообщениях. Данное поле может использоваться для фиктивной индикации позитивного результата проверки.

Как и в случае нахождения на стороне источника отрицательные персонажи могут работать на уровне контроля системы подачи сообщений внутри административной единицы. Поскольку DKIM разрешает верификацию в любой точке административной единицы получателя, влияние таких угроз можно минимизировать путём переноса проверки ближе к получателю (например, выполнять её на уровне агента доставки MDA[1] или пользовательского почтового агента MUA).

3. Примеры негативных действий

Одним из наиболее фундаментальных примеров негативных действий являются попытки доставить сообщения, которые не передавались из указанного домена отправителя. Как было сказано выше, такие сообщения могут быть просто нежелательными для получателя или могут являться частью системы доставки вредоносных программ.

[1]Mail Delivery Agent

3.1. Использование подложной идентификации отправителя

Этот класс включает передачу сообщений с целью скрыть истинного автора. В некоторых случаях реальный отправитель может сам быть отрицательным персонажем, а в других он может являться посторонним лицом, находящимся под контролем отрицательного персонажа (например, захваченный компьютер).

В комбинации с практикой подписывания всех сообщений DKIM может служить эффективной мерой против злоупотребления адресами, не контролируемыми отрицательными персонажами. Однако DKIM не помогает против использования адресов, контролируемых отрицательными персонажами. Иными словами, присутствие корректной сигнатуры DKIM не гарантирует того, что отправителем не является отрицательный персонаж. Не гарантируется также учёт подписавшей сообщение стороны, поскольку DKIM не пытается идентифицировать конкретный подписавший сообщение узел, а указывает лишь контролируемый подписавшим домен. Системы аккредитации подтверждения репутации, а также поддерживаемые локально «белые» и «чёрные» списки могут служить для учёта проверенных с помощью DKIM адресов и вероятности того, что подписанное сообщение является легитимным.

3.2. Использование конкретной идентификации

Вторым из основных классов негативных действий является указание в сообщениях конкретной идентификации.

Отметим, что некоторые из негативных действий, включающих конкретную идентификацию, могут совершенствоваться (хотя иной раз и со сниженной эффективностью) путём использования похожих внешне идентификаторов, которые могут обмануть некоторых получателей. Например, если отрицательный персонаж может контролировать домен examp1e.com (между буквами p и e находится цифра 1), он может убедить некоторых получателей, что сообщение с адреса admin@examp1e.com реально отправлено с адреса admin@example.com. Подобные типы атак с использованием символов других языков могут оказаться весьма затруднительными в силу одинакового написания части символов в распространённых шрифтах. Подобно сказанному выше, если отрицательный персонаж контролирует домен example2.com, он может подписывать сообщения от bigbank.example2.com, способные ввести в заблуждение некоторых получателей. DKIM не обеспечивает защиты от таких атак, хотя этот протокол поддерживает возможность использования систем аккредитации и/или учёта репутации, помогающих пользователю идентифицировать эти атаки.

DKIM обеспечивает эффективную защиту от использования конкретной идентификации только в тех случаях, когда ожидается, что такие сообщения будут подписаны. Основным способом реализации такого подхода является использование практики подписывания сообщений отправителем (SSP), спецификация которой разрабатывается группой IETF DKIM.

3.2.1. Использование социальных аспектов

Одной из причин использования конкретной идентификации отправителя является стремление заставить получателя прочесть сообщение за счёт того, что сообщение покажется знакомым или полученным или будет указывать на предыдущее сообщение, которому получатель доверяет. Такая тактика используется вредоносными программами рассылки электронной почты, рассылающими саму эту программу по адресам из адресной книги заражённого хоста. В этом случае однако адрес автора может не фальсифицироваться, поэтому использование DKIM может оказаться неэффективным в таких случаях.

Возможно также использование захваченной адресной книги для рассылки атакующим почты от произвольного имени. В этом случае DKIM может обеспечивать эффективную защиту путём ограничения набора адресов, для которых может быть получена корректная подпись при использовании адресной книги для рассылки почты из другого места.

3.2.2. Связанное с идентификацией мошенничество

Негативные действия, связанные с использованием электронной почты для мошенничества, часто (но не всегда) включают передачу сообщений, использующих адрес отправителя, принадлежащий другому лицу, как часть мошеннической операции. Использование определённого адреса отправителя иной раз обеспечивает мошенникам успех, способствуя тому, что получатель поверит, будто сообщение действительно пришло от указанного автора.

Для проведения таких мошеннических операций у отрицательных персонажей может присутствовать серьёзная финансовая мотивация или ресурсы, позволяющие обмануть любые меры по защите от недопустимого использования конкретного адреса.

Когда получатель проверяет сигнатуры (сам или с помощью других), DKIM обеспечивает эффективную защиту от использования подставных адресов в подписанных сообщениях. Когда публикуемая отправителем практика подписывания сообщений говорит, что все сообщения с данного адреса должны быть подписаны, DKIM дополнительно повышает защиту от недобросовестного использования адреса источника в неподписанных сообщениях.

3.2.3. Атаки на репутацию

Другим мотивом использования конкретного адреса в сообщении может служить намерение подорвать репутацию другого лица (такие действия часто называют joe-job[1]). Например, компания, желая подорвать репутацию своего конкурента, может разослать в большом количестве незапрошенную электронную почту (спам) от имени конкурента. По этой причине системы оценки репутации должны создаваться лишь на безусловно надёжной базе.

3.2.4. Атаки с отражением

Среди отрицательных персонажей достаточно широко используется практика преднамеренной отправки сообщений по ошибочным адресам, вызывающая их возврат по указанному в заголовках адресу (адрес envelope-from в соответствии с RFC 2821). В этом случае конкретный идентификатор отправителя, указанный в исходном сообщении, является реальной целью, поскольку именно по этому адресу возвращается сообщение.

DKIM в общем случае не пытается проверить корректность адреса возврата RFC2821.mailfrom в сообщениях, указанного непосредственно (отметим, что адрес mailfrom является элементом протокола SMTP, а не сообщения, с которым работает DKIM), или в необязательном поле заголовка Return-Path. Более того, как отмечено в параграфе 4.4

[1]Происходит от имени Joe Doll - владельца службы Joe's CyberPost, которая одной из первых столкнулась с крупномасштабной акцией описанного здесь типа. См. также http://www.joes.com/spammed.html. *Прим. перев.*

документа RFC 2821 [RFC2821], допустимо и рекомендуется указывать в сообщения различные адреса в поле отправителя и поле возврата. По этой причине DKIM не обеспечивает защиты против атак с отражением.

4. Атаки на системы подписывания сообщений

Можно ожидать, что отрицательные персонажи станут пытаться использовать все ограничения системы аутентификации сообщений. Очевидно также, что они будут заинтересованы в снижении эффективности системы аутентификации сообщений, чтобы воспрепятствовать её развёртыванию. Предполагается, что целями атак будут как механизмы сигнатур, так и декларации по использованию подписей в сообщениях (в этом документе такие декларации называются “практикой подписывания сообщений” или SSP).

4.1. Атаки против сигнатур в сообщениях

Ниже приведён список предполагаемых атак, нацеленных на сигнатуры DKIM.

Название	***Влияние***	***Вероятность***
Кража секретных ключей домена	Сильное	Низкая
Кража делегированных секретных ключей	Среднее	Средняя
Восстановление секретных ключей путём атаки на канал	Сильное	Низкая
Повтор избранных сообщений	Слабое	Средняя/высокая
Повтор подписанных сообщений	Слабое	Высокая
DoS-атаки на проверяющих	Сильное	Средняя
DoS-атаки на службы ключей	Сильное	Средняя
Злоупотребление канонизацией имён	Слабое	Средняя
Злоупотребление размером сообщения	Среднее	Средняя
Использование вышедших из употребления ключей	Среднее	Низкая
Захват серверов ключей	Сильное	Низкая
Фальсификация откликов службы ключей	Среднее	Средняя
Публикация некорректно сформированных ключей и подписей	Сильное	Низкая
Криптографическая слабость генерации подписей	Сильное	Низкая
Злоупотребление отображаемыми именами	Среднее	Низкая
Захваченные системы в сети отправителя	Сильное	Средняя
Атаки с пробной верификацией	Среднее	Средняя
Публикация ключей доменом верхнего уровня	Сильное	Низкая

4.1.1. Кража секретных ключей домена

Технологии подписывания сообщений (такие, как DKIM) уязвимы к кражам закрытых ключей, используемых при создании подписей. Сюда входят кражи через сеть (взлом сети или хоста для получения доступа к ключам) или иными способами (насильственное вторжение в помещения, получение ключей за взятку, насильственное изъятие и т. п.).

Ключи, применяемые для всех адресов домена, обычно находятся вместе с агентами MTA, которые следует помещать в хорошо защищённых местах (например, в вычислительных центрах). Следует применять различные меры по ограничению доступа к закрытым ключам (такие, как невозможность просмотра ключа с помощью той или иной команды), хотя в конечном итоге просмотр содержимого памяти может позволить найти значения ключа. Поскольку агенты MTA обычно работают без непосредственного обслуживания[1], защитные меры типа блокировки паролем доступа к клавиатуре на практике используются редко. Весьма эффективны будут такие меры защиты, как использование специализированного оборудования для хранения закрытых ключей и выполнения криптографических операций по созданию подписей - они позволят предотвратить экспорт закрытых ключей без получения физического доступа к устройству. Такие устройства позволят практически сразу заметить кражу ключей и принять адекватные меры (отмену действия украденных ключей) в случае кражи.

4.1.2. Кража делегированных секретных ключей

В некоторых ситуациях владелец домена может передать (делегировать) полномочия подписывания сообщений для домена отдельному пользователю или третьей стороне, предоставляющей услуги аутсорсинга (например, крупная компания по администрированию или маркетинговая компания). Поскольку в этом случае ключи могут храниться в менее защищённых устройствах, нежели корпоративные агенты MTA, во многих случаях эти ключи будут более уязвимы к кражам.

Для того, чтобы снизить уровень риска, возможности ключей, используемых для подписывания сообщений, владелец домена может ограничить лишь подписыванием сообщений от имени конкретных адресов в данном домене. Это обеспечивает защиту для большинства адресов домена.

Угрозу могут представлять и недостатки самого процесса передачи полномочий. Уменьшить уровень таких угроз можно путём использования обычных мер предотвращения кражи ключей и фальсификации передаваемых открытых ключей. Например, возможность кражи можно минимизировать, если сторона, которой передаются полномочия, генерирует пары ключей для использования и передаёт открытый ключ владельцу домена. Возможность фальсификации (подстановки другого открытого ключа) может быть снижена, если передача этого ключа подписывается получившей полномочия стороной и подпись проверяется владельцем домена.

4.1.3. Восстановление секретных ключей путём атаки на канал

Все популярные алгоритмы создания цифровых подписей являются объектами широкого спектра атак на каналы передачи. К наиболее распространенным относятся Timing Attack [Kocher96], Differential Power Analysis [Kocher99] и Cache Timing Attack [Bernstein04]. Большинство таких атак требует физического доступа к машине или возможности запуска процессов непосредственно на целевой машине (адресат). Защита от таких атак не входит в задачи DKIM.

Однако возможно удалённое выполнение временного анализа (по крайней мере в локальных сетях) [Boneh03], в частности, на платформах серверного типа, где атакующий может вставлять трафик, который будет непосредственно подвергнут интересующим криптографическим операциям. При наличии достаточного числа образцов этот метод можно использовать для восстановления закрытых ключей даже при наличии значительного шума во временных измерениях.

[1]Отсутствует физический доступ персонала. *Прим. перев.*

Ниже перечислены три наиболее распространённых меры против временного анализа.

1. Сделать операции используемыми в фиксированное время. На практике это может оказаться достаточно сложным.
2. Сделать время независимым от входных данных. Это может оказаться сложнее, но в работе [Boneh03] приведены детальные рекомендации.
3. Использовать «затемнение». Эта мера обычно считается наиболее практичной и, хотя и не обеспечивает общей защиты, является мерой против Timing-атак. Использование этого метода на 2-10% повышает стоимость операций, а сам метод реализован в большинстве современных криптографических библиотек. К сожалению алгоритмы DSA[1] и ECDSA[2] не имеют стандартных методов, хотя некоторые средства защиты могут поддерживаться.

Отметим, что добавление случайной задержки в работе является лишь полумерой. Поскольку шум в общем случае имеет однородное распределение, можно использовать достаточно большое число образцов для получения точного временного сигнала.

4.1.4. Повтор избранных сообщений

Повтором избранных сообщений называют сценарии, когда атакующий создаёт сообщение и получает для него сигнатуру передавая сообщение через агент MTA, уполномоченный доменом-отправителем, самому себе или своему сообщнику. После этого подписанное сообщение передаётся снова с использованием других адресов в конверте множеству (обычно весьма значительному) других получателей.

В силу того, что созданное атакующим сообщение должно быть сначала подписано, с этим типом атак чаще всего будут сталкиваться ISP, работающие с конечными пользователями, и организации, предоставляющие клиентам почтовые услуги, особенно в тех случаях, когда нет учёта работы клиента (в данном случае, атакующего) или он достаточно слабый. Одним из способов решения этой проблемы для домена может быть подписывание сообщений только для клиентов, прошедших процесс проверки для обеспечения трассировки почты в случаях злоупотреблений. В настоящее время низкие цены (зачастую отсутствие платы) на предоставление услуг электронной почты не позволяют реализовать такую проверку на практике. По сути дела используются лишь две модели - подписывание всей почты или подписывание лишь почты доверенных клиентов.

Вариантом такой атаки является передача атакующим сообщения с целью получить на него подписанный ответ, содержащий исходное сообщение. Ответ может быть получен от непричастного пользователя или это может быть автоматически создаваемое сообщение об отсутствии пользователя (user unknown). В некоторых случаях такой подписанный ответ может способствовать атакующему при повторе полученного ответа. Использование этого варианта можно усложнить, ограничивая размер исходного сообщения, возвращаемого в автоматических откликах и использование дополнительных механизмов типа фильтрации содержимого исходящей почты.

Может помочь также отзыв подписи или связанного с ней ключа. Однако высокая скорость повторной передачи сообщения (особенно в случаях использования армии зомбированных компьютеров) с учётом времени, требуемого для детектирования атаки и отзыва подписи, делает такое решение весьма проблематичным. Связанная с этим проблема заключается в достаточно высокой вероятности того, что домены будут использовать небольшое число ключей подписи для множества своих пользователей, что создаёт удобства для кэширования, но с высокой вероятностью может приводить к побочному ущербу (в виде отказов при проверке подписей) в случае внезапного отзыва ключа.

Отзыв подписи решает проблему сопутствующего ущерба ценой высоких требований к масштабируемости. В крайнем случае может потребоваться специальная проверка (проверяющие) для каждой отзываемой подписи, что приведёт к весьма значительному частоты транзакций. В качестве альтернативы были предложены «идентификаторы отзыва» (revocation identifier), которые будут позволять отзыв на промежуточном уровне детализации (возможно по учётным записям). Сообщения, содержащие такие идентификаторы, будут приводить к запросам в базу данных об отзывах, которая может быть представлена в DNS.

Требуется дополнительное исследование для сравнения преимуществ отзыва (на основе возможной скорости replay-атак) и издержек на запросы к базе данных об отзывах.

4.1.5. Повтор подписанных сообщений

Повторным использованием подписанного сообщения считается передача уже подписанного сообщения другому получателю, не предусмотренному автором или исходным отправителем сообщения. Атакующий добивается получения сообщения от жертвы, а затем рассылает его без изменения, но с другими адресами в конвертах. Это может использоваться, например, для того, чтобы прикинуться легитимным отправителем сообщений при передаче спама. Это может нанести ущерб репутации автора или даже всего домена.

Жертвами повторного использования подписанных сообщений может стать большее число доменов, нежели при повторе выбранного сообщения, поскольку в первом случае атакующему не требуется возможности отправлять сообщения из домена-жертвы. Однако в этом случае возможностей у атакующего существенно меньше. Без использования вместе с другой атакой типа нарушения ограничений на размер сообщения атакующий не сможет воспользоваться этим, например, для рекламы.

Многие списки рассылок (особенно те, где не меняется содержимое сообщения и подписанные поля заголовка, а следовательно, действие подписи сохраняется) оказываются вовлечёнными в такое повторное использование подписанных сообщений. Ограничения на размер тела сообщения и другие механизмы повышения «уровня живучести» сообщений эффективно усиливают такую возможность. Единственным, что отличает эту форму нежелательного повторного использования подписанных сообщений, является намерение рассылающего, которое не может быть определено сетью.

4.1.6. DoS-атаки на проверяющих

Хотя для генерации и проверки подписей требуются некоторые вычислительные ресурсы, создание непригодных подписей не требует много ресурсов. Поэтому злоумышленник может организовать атаку против проверяющей

[1]Digital Signature Algorithm - алгоритм цифровой подписи.
[2]Elliptic Curve DSA

подписи стороны, просто передавая ей большое число сообщений с непригодными подписями и даже с множеством подписей в одном сообщении. Проверка такого числа подписей может оказаться трудной задачей.

Воздействие таких атак можно значительно ослабить выбором поведения проверяющей стороны. Например, можно ограничиться восприятием лишь некоторого числа подписей в сообщении, ограничить размер воспринимаемых ключей (для предотвращения слишком длинных подписей) и проверять подписи в нужном порядке. Проверяющий может также поддерживать состояние, представляющее частоту отказов при проверке подписей для защиты во время атак.

4.1.7. DoS-атаки на службы ключей

Атакующий может также попытаться снизить доступность службы ключей отправителя, чтобы сделать его сообщения непроверяемыми. Одним из способов является быстрая передача большого числа сообщений с подписями, ссылающимися на определённый ключ, приводящая к значительному росту нагрузки на сервер ключей. Возможны и другие типы DoS-атак на сервер ключей или обслуживающую его сетевую инфраструктуру.

Лучшей защитой от таких атак является наличие избыточных серверов ключей, предпочтительно в разнесённых географически частях Internet. Кэширование также сильно помогает, снижая нагрузку на полномочные серверы ключей при наличии множества одновременных запросов. Предпочтительно также использовать протокол обслуживания ключей, минимизирующий «стоимость» транзакции поиска ключа. Отмечено, что такими свойствами обладает система доменных имён DNS (Domain Name System).

4.1.8. Злоупотребление канонизацией имён

Алгоритмы канонизации являются компромиссом между сохранением пригодности подписи сообщения и желанием не допустить несанкционированных изменений сообщения. В прошлом предлагались алгоритмы канонизации, которые в некоторых случаях позволяли атакующему менять смысл сообщения.

Подписи, поддерживающие множество алгоритмов канонизации, дают подписывающему возможность указать ожидаемую живучесть подписи и устойчивость к изменению содержимого. Если в алгоритме канонизации общего пользования будут обнаружены неожиданные уязвимости, можно развернуть новые алгоритмы, хотя этот процесс будет медленным, поскольку подписывающая сторона никогда не имеет уверенности, какой алгоритм поддерживает проверяющая сторона. По этой причине алгоритмы канонизации, подобно алгоритмам шифрования, должны проходить широкую и тщательную проверку.

4.1.9. Злоупотребление размером сообщения

Ограничение размера тела служит необязательной индикацией от подписывающей стороны, сколько данных было подписано. Проверяющий может игнорировать это ограничение, проверить указанную часть сообщения или отсечь сообщение до указанного размера и проверить его. Мотивацией этой функции послужило поведение многих списков рассылки, добавляющих трейлер (например, указание списка) в конце сообщения.

При ограничении размера тела сообщения атакующий имеет возможность добавить содержимое в сообщение. Было показано, что это содержимое, хоть оно и расположено в конце, может влиять на остальную часть, особенно в случае сообщений в формате HTML.

Если размер тела не задан или проверяющая сторона игнорирует его, ограничения не оказывают влияния. Если проверяющий или получатель отсекает сообщение по границе подписи, атакующий не может ничего добавить.

Если проверяющий соблюдает заданное ограничение размера, существует вероятность того, что атакующий может сделать нежелательное содержимое видимым для получателя. Размер добавленного сообщения не имеет большого значения, поскольку это может быть просто URL с указанием на фактическое содержимое. Принимающий агент MUA может ослабить влияние этой угрозы, как минимум, идентифицируя неподписанное содержимое в сообщении.

4.1.10. Использование вышедших из употребления ключей

Преимущества, получаемые путём кэширования записей с ключами, открывают возможность использования отозванных ключей в течение некоторого времени после отзыва. Ярким примером является случай, когда у владельца ключа, предоставленного администратором домена, должны быть неожиданно отозваны полномочия отправки почты с одного или нескольких адресов в домене.

Кэшированная запись с ключом обычно имеет короткий срок действия от нескольких часов до нескольких дней. Во многих случаях угрозу можно смягчить установкой времени жизни (TTL) для ключей, не находящихся под непосредственным контролем администратора домена (при условии возможности установки TTL для каждой записи, как это может DNS). В некоторых случаях, например, при восстановлении после кражи секретного ключа, относящегося к одному из MTA домена, при выборе значения TTL следует учитывать возможность кражи и усилия, требуемые для отзыва ключа. Выбранное значение TTL должно быть достаточно велико, чтобы смягчить атаки на отказ в обслуживании и обеспечить разумную эффективность транзакций, но не следует делать его слишком большим.

4.1.11. Захват серверов ключей

Вместо попытки получить секретный ключ атакующий может сосредоточить усилия на сервере, используемом для публикации открытых ключей домена. Как и в случае с кражей ключей мотивом может быть возможность подписывать сообщения от имени домена. Такая атака позволяет злоумышленнику дополнительную возможность блокировать публикацию легитимных ключей, лишая домен способности проверять подписи в почте.

Чтобы предоставить возможность подписывать сообщения лишь уполномоченным владельцем подписывающего домена лицам, нужно организовать связь между адресом подписи и местом, из которого получается открытый ключ для проверки сообщения. DKIM делает это путём публикации открытого ключа или ссылки на него в иерархии DNS подписывающего домена. Проверяющий определяет местоположение открытого ключа по адресу или домену подписи. Поэтому защита процесса проверки зависит от безопасности иерархии DNS подписывающего домена.

Атакующий может скомпрометировать хост, являющийся основным сервером ключей для подписывающего домена, например первичный сервер DNS для домена. Другим вариантом может быть компрометация сервера DNS вышележащего уровня и изменение делегирования серверов имён для подписывающего домена на серверы, находящиеся под контролем злоумышленника.

Такие атаки можно несколько смягчить независимым мониторингом службы ключей. Аудит службы ключей следует выполнять путём переноса зон, а не запросов к первичному серверу зоны, чтобы можно было обнаружить добавление записей в зону.

4.1.12. Фальсификация откликов службы ключей

Отклики службы ключей атакующий с подходящим местоположением может подделать. Для DNS одним из способов является «отравление кэша» (cache poisoning), когда атакующий предоставляет ненужную (и неверную) дополнительную информацию в отклики DNS и эта информация кэшируется.

DNSSEC [RFC4033] является предпочтительным способом смягчения этой угрозы, но скорость внедрения DNSSEC достаточно мала, поэтому не хотелось бы попадать в зависимость от развёртывания этой системы. В случае атаки с отравлением кэша создаваемые уязвимости локализованы и имеют ограниченную длительность, хотя записи со сравнительно большим значением TTL могут сохраняться за пределами самой атаки.

4.1.13. Публикация некорректно сформированных ключей и подписей

В такой атаке злоумышленник публикует специально созданные ключевые записи или отправляет почту с намеренно искажёнными подписями, пытаясь запутать проверяющего и, возможно, совсем отключить проверку. Эта атака на практике связана с уязвимостью реализации, переполнением буфера или отсутствием проверки границ, а не с самим механизмом подписи. Угрозу лучше всего устранить путём аккуратной реализации и создания тестовых наборов для процесса проверки.

4.1.14. Криптографическая слабость генерации подписей

Криптографические алгоритмы, применяемые для создания подписей сообщений, в частности, алгоритм хэширования и операции создания и проверки подписей могут со временем подвергаться математическим исследованиям, снижающим уровень защиты. На момент написания документа алгоритм SHA-1 был подвергнут широкому математическому анализу, который значительно сократил время, потребное для создания двух сообщений с одинаковым хэш-значением. Можно ожидать сохранения этой тенденции.

Одним из следствий слабости алгоритма хэширования являются атаки с конфликтом хэш-значений. Такие атаки на систему подписи включают человека, создающего два разных сообщения с совпадающими хэш-значениями, из которых нормальным способом подписывается лишь одно сообщение. Атака основана на втором сообщении, наследующем подпись первого. Для DKIM это означает, что отправитель может создать «хорошее» и «плохое», а некий фильтр на подписывающей стороне будет подписывать хорошее сообщение, а не плохое. Атакующий получает подписанное хорошее сообщение и помещает его подпись в плохое сообщение. Этот вариант не распространён, но может встречаться, например, на сайте, где содержимое анализируется сообщений перед их подписыванием.

Известные в настоящее время атаки на SHA-1 делают такую возможность чрезвычайно трудно осуществимой, но по мере роста вычислительных возможностей она может стать реальной.

Система подписи сообщений должны создаваться с поддержкой множества алгоритмов подписи и хэширования, а подписывающий домен должен быть способен задать используемые для подписей алгоритмы. Выбор алгоритмов должен публиковаться в записях ключей, а не только в самой подписи, чтобы атакующий не могу создавать подписи с более слабым алгоритмом, нежели домен готов разрешить.

Поскольку подписывающий и проверяющий почту обычно не взаимодействуют, согласование применяемых для подписи алгоритмов невозможно. Иными словами, подписывающий не может узнать, какие алгоритмы поддерживает проверяющий (в результате пересылки почты) и где проверяющий размещён. По этой причине ожидается, что после широкого распространения систем подписывания сообщений смена алгоритмов будет происходить достаточно медленно, а устаревшие алгоритмы будут поддерживаться в течение продолжительного срока. Поэтому алгоритмы подписи должны быть защищены от ожидаемых криптографических разработок на несколько лет.

4.1.15. Злоупотребление отображаемыми именами

Подписи сообщений связаны лишь непосредственно с адресом электронной почты (без имени отправителя), а некоторые MUA отображают (или некоторые получатели воспринимают) лишь имя отправителя. Эта несогласованность может приводить к атакам с использованием поля From: в заголовке, как показано ниже.

```
From: "Dudley DoRight" <whiplash@example.org>
```

В этом примере атакующий whiplash@example.org может подписать сообщение и все же убедить некоторых получателей, что его отправил Dudley DoRight, которому получатель доверяет. При использовании «мусорных» доменов и/или адресов привлечь атакующего к ответственности за указание чужого имени может быть сложно.

Такие атаки должны отражаться агентом MUA у получателя. Одним из вариантов является отображение адреса отправителя, а не только указанного в заголовке имени.

4.1.16. Захваченные системы в сети отправителя

Во многих случаях MTA могут быть настроены на восприятие и подписание сообщений, исходящих из топологических границ сети отправителя (например, за межсетевым экраном). Ширящееся применение скомпрометированных систем для отправки электронной почты создаёт проблему в таких случаях, поскольку атакующий, применяя скомпрометированную систему в качестве посредника, может создавать подписанные сообщения.

Имеется несколько методов ослабления таких атак. Использование аутентифицированного представления почты даже внутри сети позволяет ограничить набор адресов, которые атакующий может применять для получения подписи. Это также поможет быстрее обнаружить взломанную систему, являющуюся источником сообщений. Анализ исходящей почты для обнаружения нежелательного и вредоносного содержимого, а также мониторинг объёма сообщений, отправляемых пользователями, также препятствуют отправке и подписыванию произвольных сообщений.

4.1.17. Атаки с пробной верификацией

Как отмечено выше, злоумышленники (атакующие) могут подписывать сообщения от имени контролируемого ими домена. Поскольку они могут контролировать и службу ключей (например, полномочные серверы DNS для субдомена _domainkey), они могут наблюдать поиск открытых ключей и их источник при проверке сообщений.

Одна из таких атак, которую назовём «пробой проверки» (verification probe) заключается в отправке сообщения с подписью DKIM по каждому из множества адресов в списке рассылки. Сообщениям не нужны действительные подписи и каждый экземпляр обычно будет использовать свой селектор. Затем атакующий может отследить запросы к службе ключей и определить, какие селекторы были запрашивались и, соответственно, для каких адресатов использовалась проверка DKIM. Это может использоваться для нацеливания будущих сообщений получателям, которые не применяют проверку DKIM, при условии, что эти адресаты с высокой вероятностью будут влиять на содержимое сообщения.

4.1.18. Публикация ключей доменом верхнего уровня

Для поддержки способности домена подписывать субдомены, административно контролируемые им, DKIM разрешает домены подписей (тег d=) быть доменом более высокого уровня, нежели подписываемый адрес (i= или эквивалент). Однако по причине отсутствия механизма определения общего административного контроля над субдоменом, родитель может публиковать ключи, которые действительны для любого домена, расположенного ниже в иерархии DNS. Иными словами, почта из домена example.anytown.ny.us может быть подписана с использованием ключей доменов anytown.ny.us, ny.us или us в дополнение к ключам самого домена.

Работа домена всегда требует доверительных отношений с доменами более высокого уровня. Эти домена уже имеют полную власть над своими субдоменами - они могут менять делегирование серверов имён для домена или полностью лишать его прав. Поэтому маловероятно, что домен более высокого уровня станет намеренно компрометировать свой субдомен таким образом. Однако, если домены более высокого уровня передают почту от своего имени, они могут захотеть публиковать ключи на своём уровне. Эти домены должны проявлять особую осторожность при делегировании публикуемых ключей, чтобы предотвратить компрометацию субдоменов за счёт неправомерного применения ключей.

4.2. Атаки на методы подписывания сообщений

Ниже представлен список предполагаемых атак на методы подписания сообщений.

Название атаки	*Степень воздействия*	*Вероятность*
Похожие имена доменов	Высокая	Высокая
Неправомерное использование доменных имён на других языках	Высокая	Высокая
Атака на отказ в обслуживании при подписи	Средняя	Средняя
Использование множества адресов From:	Слабая	Средняя
Неправомерное использование подписей третьей стороны	Средняя	Высокая
Фальсификация откликов SSP[1]	Средняя	Средняя

4.2.1. Похожие имена доменов

Атакующие могут попытаться обойти методы подписания в домене, используя имя, близкое по написанию к имени домена, но отличающееся от имени домена подписи (например, заменить example.com на examp1e.com). Если сообщение не должно быть подписано, DKIM не будет требовать реального существования домена (хотя это могут требовать другие механизмы). Существуют службы мониторинга регистрации доменов для обнаружения возможных злоупотреблений именами, но они не могут заметить использование незарегистрированных доменных имён.

Похожие атаки возможны в тех случаях, когда MUA не выводит имя домена в легко узнаваемом формате. Если, например, китайский домен отображается в punycode как xn--cjsp26b3obxw7f.com, его легко подменить другим столь же малопонятным доменным именем.

Пользователи, не знакомые с соглашениями об именовании доменов в Internet, также могут ошибаться при восприятии некоторых имён. Например, они могут спутать online.example.com и online-example.com.

4.2.2. Неправомерное использование доменных имён на других языках

Интернационализация доменных имён открывает возможность для дополнительных атак с использованием схожих имён, как описано выше. Внешнее сходство многих символов Unicode позволяет создавать домена, имена которых в текстовом представлении будут неотличимы (особенно при использовании символов из разных групп) от других, возможно, более значимых имён. Этот вопрос подробно рассмотрен в Unicode Technical Report 36 [UTR36].

Наблюдение за процедурами регистрации доменов поможет раскрыть такие имена, но возможных совпадений много. Как и для схожие домены интернационализация имён может служить для обмана систем подписания в других доменах.

4.2.3. Атака на отказ в обслуживании при подписи

Подобно тому, как публикация открытых ключей домена может использоваться атакующим, так и публикация правил SSP может способствовать атакам. В случае SSP передача большого объёма неподписанной почты, предназначенной для выхода из домена, будет приводить к множеству транзакций, запрашивающих записи SSP. Возможны также DoS-атаки более общего типа на серверы, поддерживающие записи SSP. Особенно важно это в тех случаях, когда по умолчанию применяется правило «мы не подписываем все подряд», означающее, что отказ SSP ведёт к тому, что проверяющий не обязан применять более строгие правила подписания.

Как и для защиты от DoS-атак на серверы ключей, лучшим способом является создание резервных серверов, предпочтительно в территориально разнесённых частях Internet. Кэширование тоже помогает, поскольку методы подписывания меняются редко и значения TTL могут быть достаточно велики.

4.2.4. Использование множества адресов отправителя

Хотя большинство получателей никогда с этим не сталкивается, RFC 2822 [RFC2822] позволяет указывать в поле From: множество спецификаций адресов. Поиск SSP основан на адресах From:, поэтому при наличии здесь адресов из разных доменов возникает вопрос о выборе методов подписания. Можно задать правило (например, использовать первый адрес), но тогда атакующий может указать «проходной» (одноразовый) адрес перед адресом значимого домена. SSP может просматривать все адреса и выбирать правило с максимальными ограничениями, но это требует дальнейшего изучения.

4.2.5. Неправомерное использование чужих подписей

В ряде случаев, включая списки рассылки, приглашения на мероприятия и услуги «отправь статью другу», подпись DKIM в сообщении может быть не связана с доменом исходного отправителя. Поэтому «сторонние» подписи,

[1]Sender Signing Practices - практика подписания в домене.

добавляемые списками рассылки или службами приглашений, зачастую должны считаться в той или иной мере действительными. Поскольку это фактически позволяет любому домену подписывать любое сообщение, отправляющий домен может публиковать SSP с указанием того, что он не применяет подобные службы, поэтому проверяющие должны с подозрением относиться к таким подписям.

Однако ограничения, создаваемые публикацией практики подписания «без сторонних» доменов, фактически запрещают многие варианты использования электронной почты. Для большинства доменов, которые не могут принять эти методы, атакующий может с той или иной вероятностью подписать сообщения, предназначенные для выхода из домена. Поэтому службы аккредитации и репутации, а также поддерживаемые локально «чёрные» и «белые» списки должны будут играть важную роль при оценке сообщений, подписанных сторонними организациями.

4.2.6. Фальсификация откликов SSP

По аналогии с фальсификацией откликов службы ключей (параграф 4.1.12) могут фальсифицироваться и отклики на запросы SSP. Одной из таких атак будет ослабление практики подписывания, делающей неподписанные сообщения (предположительно из данного домена) менее подозрительными. В другой атаке на домен жертвы, который не подписывает сообщения, может быть предпринята попытка сделать сообщения из такого домена более подозрительными, чтобы помешать их доставке.

Как и для случая фальсификации откликов службы ключей, предпочтительным способом ослабления атак является DNSSEC. Но даже при отсутствии DNSSEC уязвимости, связанные с отравлением кэша, будет локальными.

4.3. Прочие атаки

В этом параграфе рассмотрена другая атака на инфраструктуру Internet, которая возможна при развёртывании DKIM.

Название атаки	***Степень воздействия***	***Вероятность***
«Усиление» пакетов через DNS	-	Средняя

4.3.1. Атаки с усилением через DNS

В последнее время возросло число атак на отказ в обслуживании, включающих передачу фиктивных запросов UDP DNS к открытым для доступа серверам доменных имён [US-CERT-DNS]. Если отклик от сервера имён по размеру превышает запрос, сервер имён позволяет усилить такую атаку.

DKIM вносит косвенный вклад в такие атаки за счёт требования публикации достаточно больших записей DNS для распространения открытых ключей. Имена таких записей можно узнать путём проверки корректно подписанных сообщений. Такие атаки не оказывают влияния на DKIM, Следует отметить, DKIM не является единственным приложением, использующим большие записи DNS, поэтому следует искать решение этой проблемы на уровне DNS.

5. Производные требования

Здесь приведены требования к DKIM, не указанные в явной форме выше. Эти требования включают:

- хранилище ключей и записей SSP должно поддерживать территориально распределенные серверы;
- записи ключей и SSP должны быть кэшируемыми проверяющей стороной или иной инфраструктурой;
- время жизни записей в кэше ключей должно быть настраиваемым на уровне записи;
- идентификатор алгоритма подписи в сообщении должен быть указан в записи ключа для домена;
- алгоритмы, используемые для подписывания сообщений, должны быть устойчивы к развитию криптографии на несколько лет вперёд.

6. Вопросы безопасности

Этот документ описаны угрозы безопасности, в которых применение DKIM может обеспечивать определённые преимущества, а также представлены некоторые атаки, связанные с развёртыванием механизма.

7. Литература

[Bernstein04] Bernstein, D., "Cache Timing Attacks on AES", April 2004.

[Boneh03] Boneh, D. and D. Brumley, "Remote Timing Attacks are Practical", Proc. 12th USENIX Security Symposium, 2003.

[DKIM-BASE] Allman, E., "DomainKeys Identified Mail (DKIM) Signatures", Work in Progress, August 2006.

[DKIM-SSP] Allman, E., "DKIM Sender Signing Practices", Work in Progress, August 2006.

[Kocher96] Kocher, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, and other Cryptosystems", Advances in Cryptology, pages 104-113, 1996.

[Kocher99] Kocher, P., Joffe, J., and B. Yun, "Differential Power Analysis: Leaking Secrets", Crypto '99, pages 388-397, 1999.

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[US-CERT-DNS] US-CERT, "The Continuing Denial of Service Threat Posed by DNS Recursion".

[UTR36] Davis, M. and M. Suignard, "Unicode Technical Report #36: Unicode Security Considerations", UTR 36, July 2005.

Приложение A. Благодарности

Автор благодарит Phillip Hallam-Baker, Eliot Lear, Tony Finch, Dave Crocker, Barry Leiba, Arvel Hathcock, Eric Allman, Jon Callas, Stephen Farrell, Doug Otis, Frank Ellermann, Eric Rescorla, Paul Hoffman, Hector Santos и множество других участников почтовой конференции ietf-dkim за полезные предложения и конструктивную критику ранних версий документа.

Адрес автора

Jim Fenton

Cisco Systems, Inc.

MS SJ-9/2

170 W. Tasman Drive

San Jose, CA 95134-1706

USA

Phone: +1 408 526 5914

EMail: fenton@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor в настоящее время обеспечивается IETF Administrative Support Activity (IASA).