Network Working Group C. Newman
Request for Comments: 2444 Innosoft
Updates: 2222 October 1998
Category: Standards Track

# Механизм SASL с однократными паролями

The One-Time-Password SASL Mechanism

**Статус документа**

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа "Internet Official Protocol Standards" (STD 1). Документ может распространяться без ограничений.



**Тезисы**

OTP[1] [OTP] обеспечивает полезный механизм аутентификации для случаев с ограниченным доверием к клиенту или серверу. В настоящее время OTP добавляется к протоколам специально подготовленным способом с эвристическим анализом. Данная спецификация определяет механизм OTP SASL [SASL], который обеспечивает простую и формализованную интеграцию со многими прикладными протоколами.

## 1. Как работать с документом

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY) в данном документе должны интерпретироваться в соответствии с документом Key words for use in RFCs to Indicate Requirement Levels [KEYWORDS].

Данный документ предполагает знакомство читателя с OTP [OTP], расширенными откликами OTP [OTP-EXT] и SASL [SASL].

## 2. Использование

Механизм OTP SASL используется взамен механизма SKEY SASL [SASL]. OTP является хорошим выбором для ситуаций работы с клиентами, которые не вызывают доверия (например, при подключении из Internet-кафе[2]), поскольку одноразовый пароль предоставляет клиенту лишь однократную возможность подключения от имени пользователя. Удобно использовать OTP и в тех случаях, когда используется интерактивная система входа на сервер (login), поскольку скомпрометированная аутентификационная база OTP может быть использована только для атак по словарю (dictionary attack) в отличии от аутентификационных баз других простых механизмов типа CRAM-MD5 [CRAM-MD5].

Важно отметить, что при каждом использовании механизма OTP запись базы данных аутентификации для пользователя обновляется.

Данный механизм SASL обеспечивает формальный способ интеграции OTP с поддерживающими SASL протоколами, включая IMAP [IMAP4], ACAP [ACAP], POP3 [POP-AUTH] и LDAPv3 [LDAPv3].

## 3. Создание профиля OTP для SASL

OTP [OTP] и расширенные отклики OTP [OTP-EXT] поддерживают множество опций. Однако для выполнения аутентификации требуется использование клиентом и сервером совместимых наборов опций. Данная спецификация определяет один механизм SASL - OTP. Для этого механизма применимы перечисленные ниже правила.

- **Должен** использоваться расширенный синтаксис откликов.
- Серверы **должны** поддерживать следующие 4 расширенных отклика OTP: hex, word, init-hex и init-word. Серверы **должны** поддерживать отклики word и init-word для стандартного словаря; **следует** также поддерживать дополнительные словари. Для серверов **недопустимо** требовать от клиента поддержки любых дополнительных расширений или опций OTP.
- Клиентам **следует** поддерживать вывод для пользователя запросов (challenge) OTP и вводить записи OTP в формате multi-word. Клиенты также **могут** поддерживать прямой ввод парольных фраз и расчет откликов hex или word.

[1] One-Time-Password – одноразовый пароль.
[2] В оригинале - kiosk client. Прим. перев.

- Клиенты **должны** индицировать отказы при аутентификации вследствие слишком малого значения полученного порядкового номера. Пользователю **следует** предлагать возможность сброса последовательности с использованием отклика init-hex или init-word.

**Требуется** поддержка алгоритма MD5 и **рекомендуется** поддержка SHA1.

## *4. Механизм аутентификации OTP*

Этот механизм не обеспечивает никакого уровня защиты.

Клиент начинает с передачи серверу сообщения, содержащего указанную ниже информацию.

(1) **Идентификация полномочий** (authorization identity). По умолчанию используется пустая строка идентификации. Это используется системными администраторами или прокси-серверами для входа с чужой идентификацией. Поле идентификации может включать до 255 и завершается октетом NUL (0). Предпочтительно использовать символы US-ASCII, хотя допускается и использование символов UTF-8 [UTF-8] для поддержки имен на отличных от английского языках. Использование других наборов символов кроме US-ASCII и UTF-8 запрещено.

(2) **Идентификация подлинности** (authentication identity). Идентификация личности, чья парольная фраза будет использоваться. Это поле может содержать до 255 октетов. Предпочтительно использовать символы US-ASCII, хотя допускается и использование символов UTF-8 [UTF-8] для поддержки имен на отличных от английского языках. Использование других наборов символов кроме US-ASCII и UTF-8 запрещено.

Сервер отвечает, передавая сообщение, содержащее запрос (challenge) OTP, как описано в спецификации OTP [OTP] и расширенных откликов OTP [OTP-EXT].

Если клиент видит имя неизвестного ему алгоритма хэширования, он не сможет обработать парольную фразу, введенную пользователем. В такой ситуации клиент **может** запросить использование формата six-word, ввести последовательность прерывания, указанную в профиле SASL для используемого протокола, и попробовать другой механизм SASL или закрыть соединение и прервать аутентификацию. В результате такого поведения сервер ограничивается одни алгоритмом хэширования OTP на пользователя.

В случае успеха клиент генерирует расширенный отклик в формате hex, word, init-hex или init-word. Клиенту не требуется завершать отклик пробелом или символами перевода строки и **не следует** включать ненужные пробельные символы.

Сервер **должен** быть устойчив к получению данных произвольной длины, но **может** прервать аутентификацию если размер введенных пользователем данных превышает разумное значение.

## *5. Примеры*

В приведенных здесь примерах "C:" указывает строки, которые клиент передает серверы, а "S:" представляет строки, передаваемые сервером клиенту. "<NUL>" указывает нуль-символ ASCII (NUL).

Первый пример иллюстрирует использование механизма OTP с ACAP-профилем [ACAP] в SASL. В качестве парольной фразы используется This is a test.

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "hex:5bf075d9959d036f"
S: a001 OK "AUTHENTICATE completed"
```

Следующий пример отличается от первого лишь использованием отклика в формате six-words.

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "word:BOND FOGY DRAB NE RISE MART"
S: a001 OK "AUTHENTICATE completed"
```

В следующем примере для той же ситуации используется механизм OTP-SHA1.

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-sha1 499 ke1234 ext"
C: "hex:c90fc02cc488df5e"
S: a001 OK "AUTHENTICATE completed"
```

Приведенный ниже пример отличается от предыдущего лишь использованием расширенного отклика в формате init-hex.

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "init-hex:5bf075d9959d036f:md5 499 ke1235:3712dcb4aa5316c1"
S: a001 OK "OTP sequence reset, authentication complete"
```

Далее приведен пример использования механизма OTP с IMAP-профилем [IMAP4] в SASL. Парольная фраза - this is a test.

```
C: a001 AUTHENTICATE OTP
S: +
C: AHRpbQ==
S: + b3RwLW1kNSAxMjMga2UxMjM0IGV4dA==
C: aGV4OjExZDRjMTQ3ZTIyN2MxZjE=
S: a001 OK AUTHENTICATE completed
```

Отметим, что отсутствие изначального отклика клиента и кодирование base64 являются характеристиками IMAP-профиля SASL. Запрос сервера имеет вид «otp-md5 123 ke1234 ext», а отклик клиента - «hex:11d4c147e227c1f1».

## 6. Вопросы безопасности

Данная спецификация не связана с вопросами безопасности за исключением тех, которые рассмотрены в спецификациях SASL [SASL], OTP [OTP] и расширенных откликов OTP [OTP-EXT]. Краткое повторение этих вопросов приводится ниже.

Данный механизм не обеспечивает конфиденциальности сессий, аутентификации серверов и защиты от активных атак.

Данный механизм может быть подвергнут пассивным атак с использованием словаря. Для снижения вероятности успеха таких атак следует правильно выбирать парольные фразы.

Аутентификационная база данных сервера, требуемая для использования с OTP не должна содержать открытого текста или его эквивалентов.

Реализация сервера должна быть защищена от race-атак [OTP].

## 7. Поддержка символов других языков

Удаленный доступ является важным сервером и пользователей следует побуждать к применению в именах и парольных фразах только символов US-ASCII. Однако, если в именах или парольных фразах присутствуют символы, отличные от US-ASCII, их следует интерпретировать в соответствии с кодировкой UTF-8 [UTF-8].

Серверам, поддерживающим дополнительные словари, настоятель **рекомендуется** разрешать использование формата six-word со словами отличных от английского языков.

## 8. Согласование с IANA

Ниже приведен регистрационный шаблон для механизма OTP SASL.

**SASL mechanism name**: OTP

**Security Considerations**: см. раздел 6 данного документа

**Published specification**: данный документ

**Person & email address to contact for futher information**: см. список авторов ниже

**Intended usage**: общего назначения

**Author/Change controller**: см. список авторов ниже

Этот документ также изменяет статус регистрации механизма SKEY SASL [SASL], меняя его на OBSOLETE (отменен).

## 9. Литература


[ACAP] Newman, C. and J. Myers, "ACAP – Application Configuration Access Protocol", RFC 2244, November 1997.

[CRAM-MD5] Klensin, J., Catoe, R. and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.

[IMAP4] Crispin, M., "Internet Message Access Protocol – Version 4rev1", RFC 2060[1], December 1996.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[1], March 1997.

[LDAPv3] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[MD5] Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321[1], April 1992.

[OTP] Haller, N., Metz, C., Nesser, P. and M. Straw, "A One-Time Password System", RFC 2289, February 1998.

[OTP-EXT] Metz, C., "OTP Extended Responses", RFC 2243, November 1997.

[POP-AUTH] Myers, J., "POP3 AUTHentication command", RFC 1734, December 1994.

[SASL] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222[1], October 1997.

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.


## 10. Адрес автора


**Chris Newman**

Innosoft International, Inc.

1050 Lakes Drive

West Covina, CA 91790 USA

EMail: chris.newman@innosoft.com


**Перевод на русский язык**

Николай Малых

[1]Перевод этого документа имеется на сайте http://www.protocols.ru. *Прим. перев.*

nmalykh@gmail.com

## *11. Полное заявление авторских прав*