Network Working Group
Request for Comments: 4505
Obsoletes: 2245
Category: Standards Track

K. Zeilenga, Ed.
OpenLDAP Foundation

June 2006

Механизм Anonymous в SASL

Anonymous Simple Authentication and Security Layer (SASL) Mechanism

Статус документа

В этом документе содержится спецификация стандарта для 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.

Авторские права

Аннотация

В сети Internet обычной практикой является предоставление анонимным пользователям доступа к различным сетевым службам. Обычно это организуется на основе механизма с открытыми паролями, использующего «anonymous» в качестве имени пользователя и, в некоторых случаях, - необязательную трассировочную информацию (типа адреса электронной почты) в качестве пароля. В новых протоколах IETF не допускаются команды регистрации в системе (login) в виде открытого текста, поэтому требуется новый метод предоставления доступа анонимным пользователям в контексте схемы SASL[1].

1. Введение

В этом документе определяется механизм анонимного доступа для схемы SASL [SASL]. Имя этого механизма «ANONYMOUS».

В отличие от многих других механизмов SASL, задачей которых является идентификация и аутентификация пользователя на сервере, задача данного механизма SASL состоит в предоставлении пользователю доступа к службам или ресурсам без раскрытия серверу своей идентификации. Т. е., данный механизм обеспечивает метод анонимной регистрации в системе.

Данный механизм не обеспечивает уровня защиты.

Этот документ заменяет собой RFC 2245. Изменения по отношению к RFC 2245 отражены в Приложении A.

2. Механизм Anonymous

Механизм состоит из простого сообщения, передаваемого клиентом серверу. Клиент может включить в это сообщение трассировочную информацию в форме строки символов Unicode [Unicode] с кодировкой UTF-8 [UTF-8] в соответствии с [StringPrep] и «трассировать» профиль stringprep, определенный в главе 3 данного документа. Трассировочную информацию, которая не имеет семантического значения, следует задавать в одной из двух возможных форм - адрес электронной почты Internet или «темная» (opaque) строка, не содержащая символов @ (U+0040), которая может быть интерпретирована системным администратором домена на стороне клиента. По причинам сохранения приватности адрес электронной почты или иные сведения, идентифицирующие пользователя, могут использоваться только с его разрешения.

Сервер, который позволяет анонимный доступ, будет анонсировать поддержку механизма ANONYMOUS и разрешать использование этого механизма любому желающему, обычно ограничивая права для анонимных пользователей.

Ниже приведен формальный синтаксис клиентского сообщения в формате ABNF [ABNF], как иллюстрация к данной технической спецификации.

```
message     = [ email / token ]        ;; готовится в соответствии с главой 3

UTF1        = %x00-3F / %x41-7F ;; less '@' (U+0040)
UTF2        = %xC2-DF UTF0
UTF3        = %xE0 %xA0-BF UTF0 / %xE1-EC 2(UTF0) / %xED %x80-9F UTF0 / %xEE-EF 2(UTF0)
UTF4        = %xF0 %x90-BF 2(UTF0) / %xF1-F3 3(UTF0) / %xF4 %x80-8F 2(UTF0)
UTF0        = %x80-BF

TCHAR       = UTF1 / UTF2 / UTF3 / UTF4
              ;; любые символы Unicode в кодировке UTF-8, за исключением @ (U+0040)

email       = addr-spec        ;; в соответствии с [IMAIL]
token       = 1*255TCHAR
```

Примечание для разработчиков:

> Размер маркера <token> ограничен 255 символами в кодировке UTF-8. Поскольку данная кодировка использует от 1 до 4 октетов на символ, размер маркера может достигать 1020 октетов.

[1] Simple Authentication and Security Layer - простой уровень аутентификации и защиты. *Прим. перев.*

3. «Трассировка» профиля «Stringprep»

В этой главе определена «трассировка» профиля [StringPrep]. Этот профиль разработан для использования с механизмом SASL ANONYMOUS. В частности, клиент готовит <message> в соответствии с этим профилем.

Набором символов для этого профиля является Unicode 3.2 [Unicode].

Для профиля не требуется отображения.

Для профиля не требуется нормализации Unicode.

Список невыделенных кодов для этого профиля определен в Приложении A к документу [StringPrep]. Невыделенные коды не являются запрещенными.

Запрещено использование символов из следующих таблиц [StringPrep]:

- C.2.1 (управляющие символы ASCII)
- C.2.2 (управляющие символы, отличные от ASCII)
- C.3 (символы для приватного использования)
- C.4 (не имеющие символов коды)
- C.5 (суррогатные коды)
- C.6 (неприемлемо для текста)
- C.8 (изменение свойств дисплея запрещено)
- C.9 (символы для тегов)

Других запрещенных символов нет.

Данный профиль требует двунаправленной проверки символов в соответствии с главой 6 документа [StringPrep].

4. Пример

Здесь рассмотрен простой пример использования механизма ANONYMOUS между клиентом и сервером IMAP. В примере префиксы «C:» и «S:» указывают строки, передаваемые клиентом и сервером, соответственно. Если следующая строка не содержит префикса «C:» или «S:», она является просто переносом предыдущей строки, сделанным для удобства чтения.

Отметим, что в этом примере используется профиль IMAP [IMAP4] для SASL. Кодирование base64 для запросов и откликов, а также префиксы «+ » в откликах являются частью профиля IMAP4 и не относятся непосредственно к SASL. Кроме того, протоколы с профилями SASL, разрешающими клиенту включать в запрос на организацию аутентификационной сессии начальный отклик, позволяют сэкономить один период кругового обхода для аутентификационного обмена (избежать показанного ниже отклика «+ » с пустой строкой).

В данном примере трассировочной информацией является строка «sirhc».

```
S: * OK IMAP4 server ready
C: A001 CAPABILITY
S: * CAPABILITY IMAP4 IMAP4rev1 AUTH=DIGEST-MD5 AUTH=ANONYMOUS
S: A001 OK done
C: A002 AUTHENTICATE ANONYMOUS
S: +
C: c2lyaGM=
S: A003 OK Welcome, trace information has been logged.
```

5. Вопросы безопасности

Механизм ANONYMOUS предоставляет доступ к службам и/или ресурсам любому желающему. По этой причине его следует отключать по умолчанию, предоставляя администратору возможность включения этого механизма при необходимости.

Если анонимному пользователю предоставляется право записи, возможна организация атаки на службу путем заполнения всего доступного для записи пространства. Для предотвращения таких атак можно запретить запись для анонимных пользователей.

Если анонимные пользователи имеют возможность чтения и записи в одну область, сервер можно будет использовать в качестве коммуникационного механизма анонимного обмена информацией. Серверам, разрешающим анонимным пользователям подачу информации, следует реализовать модель drop box, в которой анонимный доступ для чтения невозможен в областях, открытых анонимным пользователям для подачи информации.

Если анонимный пользователь может запускать множество ресурсоемких операций (например, команд IMAP SEARCH BODY), это позволяет организовать атаку на службу. Серверам настоятельно рекомендуется снижать приоритет для анонимных пользователей или ограничивать для них выделяемые ресурсы.

Хотя серверы могут вносить ограничения на число анонимных пользователей, такие ограничения открывают возможность атак на службы, поэтому ими следует пользоваться с осторожностью.

Трассировочная информация не проверяется и ее можно фальсифицировать. Это может использоваться для указания чужих данных при доступе к информации сомнительного свойства. Администраторам, исследующим факты недопустимого использования, следует принимать во внимание возможность фальсификации трассировочных данных.

Клиентские программы, использующие корректный адрес электронной почты в качестве трассировочной информации без явного на то разрешения пользователя, могут подвергать риску персональные данные пользователя. Любой, кто пользуется доступом к архивам специфического содержания с анонимным доступом (например, сексуальные

извращения), очевидно нуждается в скрытности. Клиентским программам не следует передавать почтовый адрес пользователя без явного разрешения и следует предлагать пользователю опцию отказа от передачи трассировочной информации, показывая только IP-адрес и время.

Прокси-серверы с анонимным доступом помогут защитить приватную информацию, но следует принимать во внимание возможность организации в таких случаях DoS-атак.

Анонимные соединения чувствительны к перехвату с участием человека (man-in-the-middle attack), при которых передаваемая информация может просматриваться и изменяться. Клиентам и серверам настоятельно рекомендуется использовать внешние средства защиты данных.

Протоколы, которые не могут обеспечить явную регистрацию в системе для анонимных пользователей, более уязвимы к вторжениям, связанным с некоторыми общепринятыми методами реализации. В частности, серверы Unix, которые предлагают пользователям регистрацию в системе, могут запускаться с правами пользователя root и переключаться на соответствующее значение user id после явной команды login. Обычно такие серверы отвергают все команды доступа к данным до явной регистрации в системе и могут создавать безопасную среду с ограниченными возможностями (например, с помощью chroot в Unix) для анонимных пользователей. Если анонимный доступ не запрашивается явно, вся система доступа к данным может подвергнуться внешним атакам без возможности явного использования защитных мер. Протоколам, предлагающим ограниченный доступ к данным для анонимных пользователей, не следует предоставлять такой доступ без этапа явной регистрации в системе.

Общие вопросы безопасности SASL [SASL] применимы и к данному механизму.

Вопросы безопасности StringPrep [StringPrep] и вопросы безопасности Unicode [Unicode], рассмотренные в [StringPrep], также применимы к этому механизму. Вопросы безопасности UTF-8 [UTF-8] также применимы к данному механизму.

6. Согласование с IANA

Реестр SASL Mechanism [IANA-SASL] содержит запись для механизма ANONYMOUS, которая была обновлена IANA с учетом данного документа, обеспечивающего техническую спецификацию механизма.

```
To: iana@iana.org
Subject: Updated Registration of SASL mechanism ANONYMOUS

SASL mechanism name: ANONYMOUS
Security considerations: See RFC 4505.
Published specification (optional, recommended): RFC 4505
Person & email address to contact for further information:
     Kurt Zeilenga <Kurt@OpenLDAP.org>
     Chris Newman <Chris.Newman@sun.com>
Intended usage: COMMON
Author/Change controller: IESG <iesg@ietf.org>
Note: Updates existing entry for ANONYMOUS
```

«Трассировка» профиля [StringPrep], определенная в данном RFC, была зарегистрирована:

```
To: iana@iana.org
Subject: Initial Registration of Stringprep "trace" profile

Stringprep profile: trace
Published specification: RFC 4505
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@openldap.org>
```

7. Благодарности

Этот документ является пересмотром документа RFC 2245, который подготовил Chris Newman. Фрагменты синтаксиса, определённого в главе 1, были заимствованы из RFC 3629, автором которого является Francois Yergeau.

Данный документ является результатом работы группы IETF SASL.

8. Нормативные документы

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

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

[SASL] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[StringPrep] Hoffman, P. and M. Blanchet, "Preparation of Internationalized Strings ('stringprep')", RFC 3454, December 2002.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" is defined by "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), as amended by the "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) and by the "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 3629 (also STD 63), November 2003.

9. Дополнительная литература

[IMAP4] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[IANA-SASL] IANA, "SIMPLE AUTHENTICATION AND SECURITY LAYER (SASL) MECHANISMS", <http://www.iana.org/assignments/sasl-mechanisms>.

Приложение A. Изменения по отношению к RFC 2245

Это приложение не является нормативным.

RFC 2245 позволяет клиенту включать необязательную трассировочную информацию в понятной человеку форме. RFC 2245 разрешает для этих строк только кодировку US-ASCII. В связи с интернационализацией сети Internet данный документ ограничивает такие строки набором символов Unicode в кодировке UTF-8. Определен профиль «stringprep» для точного указания символов Unicode, допустимых для включения в такие строки. Размер строки ограничен 255 символами, для кодирования каждого из которых может применяться от 1 до 4 октетов.

Кроме того, внесено множество редакторских правок.

Адрес редактора

Kurt D. Zeilenga

OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).