Network Working Group
Request for Comments: 2577
Category: Informational

M. Allman
NASA Glenn/Sterling Software
S. Ostermann
Ohio University

May 1999

Вопросы безопасности FTP

FTP Security Considerations

Статус документа

В этом документе приведена информация для сообщества Internet. Документ не содержит каких-либо стандартов Internet. Разрешается свободное распространение документа.

Тезисы

Спецификация протокола FTP[1] содержит множество механизмов, которые могут использоваться для компрометации системы сетевой безопасности. Спецификация FTP позволяет клиентам передавать серверу команды копирования файлов на третью машину. Такой “трехсторонний” механизм, получивший название proxy FTP, связан с хорошо известной проблемой защиты. Спецификация FTP также разрешает неограниченное число попыток ввода пользовательского пароля, что дает злоумышленникам возможность организации атак путем тупого перебора паролей (brute force). В этом документе приводятся рекомендации для системных администраторов и тех, кто поддерживает серверы FTP, по снижению риска, связанного с использованием FTP.

1 Введение

Спецификация протокола FTP [PR85] обеспечивает механизм, позволяющий клиентам организовать управляющее соединение и передавать файлы между двумя серверами FTP. Этот механизм получил название "proxy FTP" и может использоваться для снижения уровня трафика в сети – клиент просто говорит серверу о необходимости копирования файла на другой сервер вместо того, чтобы копировать файл сначала с первого сервера на клиентский хост, а потом от клиента на второй сервер. Такой механизм полезен, в частности, для тех случаев, когда клиент подключается к сети по медленному каналу (например, с помощью модема). Однако механизм proxy FTP имеет и негативную сторону, открывая возможность организации bounce-атак [CERT97:27]. Кроме организации bounce-атак этот метод позволяет также отгадывать пользовательские пароли методом “грубой силы” (brute force[2]).

В этом документе не обсуждается использование протокола FTP совместно с протоколами обеспечения безопасности типа IP Security. Эти вопросы также следует рассмотреть, но они выходят за пределы данного документа.

В документе приводится информация для разработчиков серверов FTP и системных администраторов. В главе 2 описывается bounce-атака на FTP. Глава 3 содержит рекомендации по предотвращению таких атак. В главе 4 даны рекомендации для серверов, ограничивающих доступ по сетевым адресам, а в главе 5 – рекомендации по предотвращению возможности подбора паролей клиентами (brute force "password guessing"). Глава 6 содержит краткое обсуждение механизмов повышения “секретности”, а в главе 7 рассматривается механизм предотвращения подбора имен пользователей. В главе 8 обсуждается вопрос захвата портов (port stealing). И, наконец, глава 9 содержит обзор вопросов безопасности FTP, связанных с программными ошибками, а не протоколом, как таковым.

2 Bounce-атака

Версия протокола FTP, описанная в стандарте [PR85], позволяет атаковать хорошо известные сетевые службы, причем проследить действия злоумышленников достаточно сложно. Атака включает передачу серверу FTP команды PORT, содержащей сетевой адрес атакуемой машины и номер порта атакуемой службы. Такая команда позволяет клиенту отдать серверу FTP команду передачи на атакуемую станцию файла, который может содержать команды для атакуемой службы (SMTP, NNTP и т. п.). Использование промежуточного сервера для организации атаки осложняет идентификацию атакующего хоста и может обмануть системы ограничения доступа по сетевым адресам.

Например, клиент загружает на сервер FTP файл, содержащий команды SMTP и после этого, используя подходящую команду PORT, дает этому серверу команду на соединение с портом SMTP атакуемой машины. Далее клиент дает серверу команду на передачу загруженного ранее файла с командами SMTP атакуемому хосту. Это может позволить атакующему передать обманным путем почту без прямого подключения к почтовому серверу. Атакующего в этом случае отследить достаточно сложно.

[1] File Transfer Protocol – протокол передачи файлов. *Прим. перев.*

[2] По-русски лучше будет назвать этот метод «тупым перебором». *Прим. перев.*

3 Защита от Bounce-атак

Спецификация протокола FTP [PR85] предполагает, что соединения для передачи данных организуются на основе протокола TCP[3] [Pos81]. Порты TCP с номерами от 0 до 1023 зарегистрированы для распространенных (well known) служб типа электронной почты, новостей и управляющих соединений FTP [RP94]. Спецификация протокола FTP не ограничивает диапазон номеров портов, используемых для передачи данных. Следовательно, используя proxy FTP, клиент может с помощью сервера FTP организовать атаку на известные службы любой машины.

Для предотвращения подобных атак предлагается, чтобы серверы не открывали для передачи данных соединений с портами TCP, номера которых меньше 1024. если сервер получает команду PORT, содержащую порт TCP с номером меньше 1024, предлагается возвращать отклик с кодом 504 (определен как "Command not implemented for that parameter" - “Команда для данного параметра не реализована” в спецификации [PR85]). Отметим, что такое решение не спасает от атак службы, связанные с портами, номера которых превышают 1023.

Имеются предложения (например, [AOM98] и [Pis94]) по обеспечению механизма, который бы позволил организовать передачу данных с использованием транспортного протокола, отличного от TCP. В этом случае также потребуются предосторожности для защиты распространенных служб, использующих соответствующий транспортный протокол.

Отметим также, что для организации bounce-атаки злоумышленнику требуется возможность записи файлов на сервер FTP (upload) и последующая возможность загрузки (download) этих файлов на атакуемый хост. Использование надлежащей защиты для файлов на сервере не позволяет организовать полнофункциональную атаку. Однако злоумышленники все равно смогут атаковать службы, передавая с удаленного сервера FTP произвольные данные, которые могут осложнить работу некоторых служб.

Запрет команды PORT также помогает предотвратить bounce-атаки. Большинство операций по копированию файлов можно выполнить, используя лишь команду PASV [Bel94]. Отрицательной стороной запрета на использование команды PORT является утрата возможности использования proxy FTP, но эта функция во многих случаях просто не требуется.

4 Ограничение доступа

Для некоторых серверов FTP желательно ограничение доступа по сетевым адресам. Например, сервер может ограничивать доступ к некоторым файлам из отдельных мест сети (например, тот или иной файл недоступен из сети определенной организации). В таких случаях серверу следует проверять принадлежность адресов удаленного хоста для управляющего соединения и соединения, используемого для передачи данных прежде, чем предоставлять возможность копирования файла с ограниченным доступом. Проверяя принадлежность адресов для обоих соединений, можно предотвратить несанкционированный доступ к файлу путем организации управляющего соединения из доверенной сети, а соединения для передачи данных из другого места. Точно так же клиенту следует проверять IP-адрес удаленного хоста после того, как будет принят запрос на организацию соединения для передачи данных, чтобы удостовериться, что данные будут получены от нужного сервера.

Отметим, что ограничение доступа по сетевым адресам не предотвращает уязвимость серверов FTP для атак с подменой адресов ("spoof" attack). В таких атаках злоумышленник может использовать подставной адрес из внутренней сети организации для получения доступа к файлам, недоступным извне. Для предотвращения подобных атак следует использовать защищенные механизмы аутентификации типа tex, что описаны в [HL97].

5 Защита паролей

Для минимизации риска тупого подбора паролей с использованием сервера FTP предлагается ограничивать на серверах число попыток, которые могут использоваться для ввода корректного пароля. После небольшого (3 – 5) количества неудачных попыток серверу следует закрыть управляющее соединение для данного клиента. Перед закрытием управляющего соединения сервер должен передать клиенту отклик с кодом 421 ("Service not available, closing control connection." - “Сервис недоступен, управляющее соединение закрывается” [PR85]). В дополнение к этому предлагается вводить на сервере 5-секундную задержку отклика на некорректные команды "PASS" для снижения эффективности атак с подбором пароля (brute force attack). По возможности для реализации этих предложений следует использовать механизмы операционной системы.

Злоумышленник может обойти описанные выше механизмы путем организации множества параллельных управляющих соединений с сервером. Для предотвращения таких ситуаций сервер может ограничивать общее число управляющих соединений или попытаться обнаружить подозрительные действия и блокировать организацию новых соединений с атакующего хоста. Однако обе эти механизма открывают дверь для DoS-атаки, когда атакующий просто создает множество соединений, блокируя доступ легитимных пользователей.

В соответствии со стандартом FTP [PR85] пароли передаются в открытом виде с использованием команды "PASS". Предлагается использовать на клиентах и серверах FTP дополнительный механизм аутентификации, который не был бы открыт для подслушивания (такие механизмы разработаны группой IETF Common Authentication Technology [HL97]).

6 Конфиденциальность

В соответствии со стандартом FTP [PR85] все данные и управляющая информация (включая пароли) передаются через сеть в незашифрованном виде. Для обеспечения конфиденциальности передаваемой через сеть информации следует использовать (по возможности) схемы шифрования. Один из таких механизмов описан в документе [HL97].

7 Защита имен пользователей

Стандарт FTP [PR85] задает передачу отклика с кодом 530 в ответ на команду USER, если имя пользователя отвергнуто сервером. Если имя пользователя корректно и требуется пароль, серверу следует возвращать код 331. Для предотвращения сбора информации о корректных именах пользователей сервера предлагается в ответ на команду USER всегда возвращать код 331 и отвергать комбинацию имени и пароля при вводе некорректного имени пользователя[2].

[3] Transmission Control Protocol.

[2] В этом случае не злоумышленнику определить, что было неверным – имя или пароль. *Прим. перев.*

8 Захват портов (Port Stealing)

Многие операционные системы при динамическом выделении портов просто последовательно увеличивают номера портов. Организовав корректную операцию копирования файла, злоумышленник может определить текущий номер выделенного порта и предсказать номер, который будет использован при следующем выделении порта. После этого атакующий может организовать соединение с этим портом, не позволяя легитимному пользователю осуществить копирование файлов. Кроме того, таким путем атакующий может даже захватить файл, предназначенный легитимному пользователю. Возможна также передача подложного файла в поток данных от легитимного клиента. Остроту этой проблемы можно снизить путем использования в клиентах и серверах FTP случайных значений для номера локального порта (случайный порт запрашивается у ОС или для его определения используется предоставляемый ОС механизм.

9 Проблемы безопасности, связанные с программами

Этот документ посвящен вопросам безопасности протокола FTP. Существует также ряд проблем, связанных с конкретными реализациями протокола FTP. Детальное рассмотрение этих вопросов выходит за пределы данного документа, однако следует обозначить проблемы, которые были обнаружены и должны быть учтены в будущих реализациях программ:

Anonymous FTP (анонимный доступ)

Анонимный доступ означает возможность подключения клиентов к серверу FTP с минимальной аутентификацией и предоставление доступа к некоторым файлам (public). Проблемы безопасности возникают в тех случаях, когда анонимным пользователям доступны для чтения все файлы или предоставлена возможность создания файлов [CERT92:09] [CERT93:06].

Remote Command Execution (удаленное исполнение команд)

Расширение протокола FTP "SITE EXEC" позволяет клиентам выполнять на сервере произвольные команды. Эту возможность следует реализовать с большой осторожностью. Известно несколько случаев использования команды SITE EXEC для обхода средств обеспечения безопасности серверов FTP [CERT94:08] [CERT95:16]

Debug Code (отладочный код)

Некоторые из упомянутых выше случаев компрометации серверов FTP были связаны с использованием программ, в которых не были отключены средства отладки [CERT88:01].

Данный документ рекомендует разработчикам серверов FTP с поддержкой перечисленных здесь возможностей, внимательно ознакомится с бюллетенями CERT, посвященными атакам на эти или похожие механизмы.

10 Заключение

Использование рассмотренных выше предложений может снизить риск, связанный с использованием серверов FTP без ущерба для их функциональности.

11 Вопросы безопасности

Весь документ посвящен вопросам безопасности.

Благодарности

Мы благодарим Alex Belits, Jim Bound, William Curtin, Robert Elz, Paul Hethmon, Alun Jones и Stephen Tihor за их комментарии, оказавшие помощь при подготовке документа. Мы также благодарны членам группы FTPEXT, которые внесли много полезных предложений на конференции IETF в Мемфисе.

Литература

[AOM98] Allman, M., Ostermann, S. and C. Metz, "FTP Extensions for IPv6 and NATs", RFC 2428, September 1998.

[Bel94] Bellovin. S., "Firewall-Friendly FTP", RFC 1579, February 1994.

[CERT88:01] CERT Advisory CA-88:01. ftpd Vulnerability. December, 1988 ftp://info.cert.org/pub/cert_advisories/

[CERT92:09] CERT Advisory CA-92:09. AIX Anonymous FTP Vulnerability. April 27, 1992. ftp://info.cert.org/pub/cert_advisories/

[CERT93:06] CERT Advisory CA-93:06. Wuarchive ftpd Vulnerability. September 19,1997 ftp://info.cert.org/pub/cert_advisories/

[CERT94:08] CERT Advisory CA-94:08. ftpd Vulnerabilities. September 23, 1997. ftp://info.cert.org/pub/cert_advisories/

[CERT95:16] CERT Advisory CA-95:16. wu-ftpd Misconfiguration Vulnerability. September 23, 1997 ftp://info.cert.org/pub/cert_advisories/

[CERT97:27] CERT Advisory CA-97.27. FTP Bounce. January 8, 1998. ftp://info.cert.org/pub/cert_advisories/

[HL97] Horowitz, M. and S. Lunt, "FTP Security Extensions", RFC 2228, October 1997.

[Pis94] Piscitello, D., "FTP Operation Over Big Address Records (FOOBAR), RFC 1639, June 1994.

[Pos81] Postel, J., "Transmission Control Protocol", STD 7, RFC 793[1], September 1981.

[PR85] Postel, J. and J. Reynolds, "File Transfer Protocol (FTP)", STD 9, RFC 959, October 1985.

[RP94] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700[2], October 1994. См. также: http://www.iana.org/numbers.html

[1]На сайте www.protocols.ru имеется перевод этого документа на русский язык. *Прим. перев.*

Адреса авторов

Mark Allman

NASA Glenn Research Center/Sterling Software

21000 Brookpark Rd. MS 54-2

Cleveland, OH 44135

EMail: mallman@grc.nasa.gov

Shawn Ostermann

School of Electrical Engineering and Computer Science

Ohio University

416 Morton Hall

Athens, OH 45701

EMail: ostermann@cs.ohiou.edu

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

[2]В соответствии с RFC 3232 документ “Assigned Numbers” признан утратившим силу. Выделенные значения можно посмотреть в базе данных на сайте www.iana.org. *Прим. перев.*