Автор:
07.10.14 16:06 -

Доступен выпуск OpenSSH 6.7 , открытой реализации клиента и сервера для работы по протоколам SSH (1.3, 1.5 и 2.0) и SFTP. Из наиболее важных улучшений можно отметить поддержку сборки с LibreSSL, возможность проброса Unix domain сокетов, начало выноса функциональности OpenSSH в отдельную библиотеку, прекращение поддержки tcpwrapper, возможность возобновления прерванных загрузок в sftp.

Основные улучшения:

- В ssh и sshd добавлена поддержка проброса Unix domain сокетов через SSH-туннель, что позволяет перенаправить обращение к удалённому TCP-порту на локальный Unix domain сокет и наоборот, или соединить через ssh-туннель два Unix domain сокета. Например, для соединения СУБД PostgreSQL через SSH-туннель к локальному Unix domain сокету можно использовать команду "ssh -L/tmp/.s.PGSQL.5432:mydatabase.net:5432 someserver.com" или можно пробросить соединения клиентов к удалённому серверу на локальный сервер - "ssh -R/var/run/mysql.sock:/var/run/mysql.sock -R127.0.0.1:3306:/var/run/mysql.sock somehost";
- Началась значительная внутренняя переработка, целью которой является вынос частей OpenSSH в отдельную библиотеку. В настоящее время уже проведён рефакторинг кода, связанного с парсингом, обработкой ключей и KRL. Так как API ещё не стабилизирован библиотека не поставляется в обособленном виде, но после завершения работы её можно будет использовать для задействования функциональности OpenSSH в других продуктах;
- Прекращена поддержка запуска с использованием tcpwrapper-ов и libwrap, так как конфигурации с лишними прослойками потенциально могут быть подвежены атаке ShellShock ;
- Предлагаемый в sshd по умолчанию набор шифров и MAC переработан в плане удаления небезопасных алгоритмов. В частности, по умолчанию теперь отключены шифры CBC и arcfour, при этом их поддержку можно вернуть путём явного указания через директивы Ciphers и MACs в sshd_config;
- В sftp добавлена поддержка возобновления прерванных загрузок;
- В ssh и ssh-keygen для ключей ED25519 добавлена поддержка DNS-записей SSHFP;
- В sshd_config добавлена опция PermitUserRC для управления запуском ~/.ssh/rc, повторяющая опцию no-user-rc из файла authorized_keys;
- В ssh для директив LocalCommand и ControlPath добавлена новая escape-последовательность %C, которая раскрывается в утикальный идентификатор, формируемый как хэш из имени локального хоста, удалённого пользователя, удалённого хоста и номера порта;
- При выводе ошибки "Too many authentication failures" теперь указывается информация о пользователей, адресах, портах и протоколе;

- Для подвергнутого рефакторингу кода добавлены unit и fuzz тесты, которые автоматически запускаются при выволнении "make tests" для переносимой версии OpenSSH;
- Улучшения, специфичные для переносимой версии OpenSSH:
- Добавлена поддержка сборки с использованием переносимой версии LibreSSL ;
- При сборке с OpenSSL в качестве минимально поддерживаемой версии теперь используется openssl 0.9.8f;
- В скрипт инициализации openssshd.init добавлена поддержка генерации ключей ed25519;
- В sftp-server добавлена возможность использования prctl() для блокирования доступа к /proc/self/{mem,maps}.

Read more http://www.opennet.ru/opennews/art.shtml?num=40767