

Основы системного администрирования и сетевых технологий

УРОК №10

Проверка подлинности пакетов

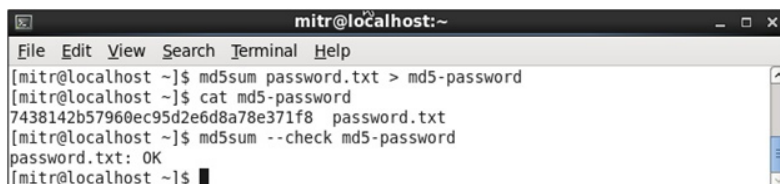
Перед инсталляцией пакета необходимо выполнить проверку его подлинности, поскольку злоумышленник может изменить содержимое пакета, например, добавив в него вирус. Особенно важно осуществлять проверку при получении пакетов из непроверенных источников. Проверку подлинности пакетов можно осуществлять несколькими способами.

Проверка подлинности с помощью функции хэширования

Основная форма проверки подлинности пакетов подразумевает использование функции хэширования. Величина, получаемая с помощью функции хэширования, называется хэшем. Хэш характеризует набор данных произвольного размера посредством фрагмента данных фиксированной длины. В отличие от контрольной суммы, вывод хэша трудно предсказуем, то есть очень сложно модифицировать данные, а затем сгенерировать идентичный хэш. Большинство алгоритмов используют длинный ключ (например, 128 битный), то есть вероятность сгенерировать аналогичный ключ чрезвычайно мала. Если загружается файл из незнакомого источника, но есть ключ из доверенного источника, то можно быть уверенным, что:

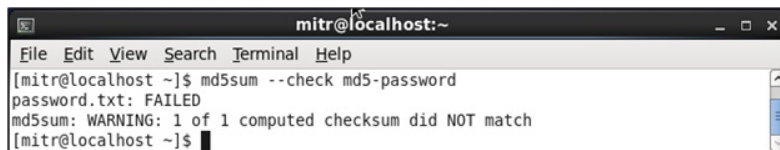
- шансы получить модифицированный файл с идентичным хэшем очень невелики;
- вероятность того, что злоумышленник может взять файл, модифицировать его и сгенерировать идентичный хэш, бесконечно мала.

Проверка подлинности с помощью функции хэширования



```
mitr@localhost:~  
File Edit View Search Terminal Help  
[mitr@localhost ~]$ md5sum password.txt > md5-password  
[mitr@localhost ~]$ cat md5-password  
7438142b57960ec95d2e6d8a78e371f8 password.txt  
[mitr@localhost ~]$ md5sum --check md5-password  
password.txt: OK  
[mitr@localhost ~]$
```

Рисунок 1.
Создание и проверка хэша
с помощью md5sum



```
mitr@localhost:~  
File Edit View Search Terminal Help  
[mitr@localhost ~]$ md5sum --check md5-password  
password.txt: FAILED  
md5sum: WARNING: 1 of 1 computed checksum did NOT match  
[mitr@localhost ~]$
```

Рисунок 2.
Результат проверки
с помощью md5sum измененного файла

Популярным инструментом генерирования хэшей является программа md5sum на основе алгоритма MD5 (Message Digest номер 5). Программа md5sum может создавать хэши и проверять их. Для того, чтобы сгенерировать хэш, нужно после имени программы указать имя файла (или файлов), для которого хэш генерируется.

Хэш имеет вид шестнадцатиричного числа, состоящего из 32 цифр (каждое шестнадцатиричное число – 4 бита). Хэш можно проверить, сравнив его с значением из доверенного источника и убедившись, что данные корректны. Если хэши совпадают, то можно быть уверенным, что файл не подвергался изменению с момента создания хэша.

Пример создания и проверки хэша файла приведен на рис 1.

Если теперь изменить файл password.txt то проверка даст результаты, показанные на рис. 2.

Проверка подлинности с использованием цифровой подписи

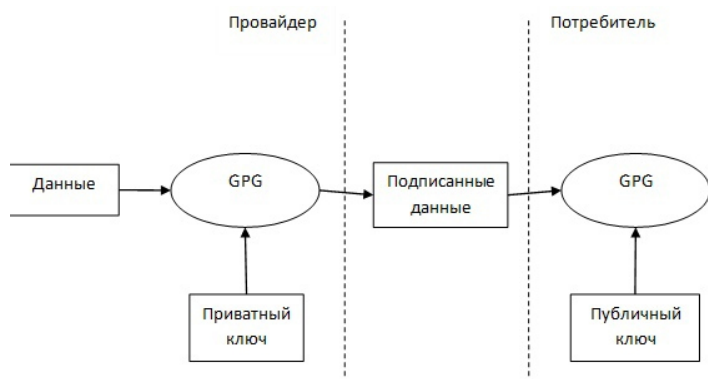


Рисунок 3.
Использование GPG при работе
с электронной подписью

Цифровая подпись – некоторая разновидность хэша, которая, однако, не требует никаких уникальных сведений о данных, подвергающихся проверке подлинности. Для проверки подлинности цифровой подписи нужен только публичный ключ, предоставляемый лицом или организацией, которую необходимо аутентифицировать. Имея публичный ключ можно подвергать проверке любые данные, подписанные таким лицом или организацией.

Лицо, которое желает подписать данные, генерирует два ключа: публичный и приватный. В основе ключей лежит пароль, который известен только создателю ключей. Создатель лежит пароль и приватный ключ в секрете, а публичный ключ доступен для всех желающих.

При работе с цифровыми подписями в сфере свободного программного обеспечения наиболее популярен инструмент GNU Privacy Guard (GPG). Процесс подписи данных с использованием PGP показан на рис. 3.

Менеджер пакетов `rpm` позволяет подписывать пакеты электронной подписью для последующей проверки их подлинности.

Общая форма команды проверки подлинности `rpm`:

`rpm -checksig имя_пакетного_файла`

Проверка подлинности с использованием цифровой подписи

Очевидно (рис. 3), чтобы произвести проверку, нужен публичный ключ. Дистрибутивы Linux могут содержать несколько публичных ключей, которые использованы для подписи пакетов, входящих в состав дистрибутива. Если необходимого публичного ключа нет, то его можно постараться получить на сайте производителя пакета. Если публичный ключ PGP доступен в текстовом виде, то нужно сохранить его в файле и импортировать с помощью команды

```
rpm --import имя_файла_с_ключем_GPG
```

Проверка пакетов

Проверку содержимого пакета можно выполнить до его установки. Например, содержимое екоторого rpm-файла можно запросить с помощью команды

```
rpm -qip имя_файла.rpm
```

Часто используемые запросы к файлу, содержащему пакет, приведены в табл. 1.

Проверка пакетов

Таблица 1. Часто используемые запросы к файлу пакета

| | |
|---|-------------------------------|
| Запрос | rpm |
| Базовые сведения о пакете | rpm -qri имя_файла |
| Список файлов для установки | rpm -qpl имя_файла |
| Сценарии установки и удаления | rpm -qp -scripts имя_файла |
| Показать пакеты, необходимые для данного пакета | Rpm -qp - -requires имя_файла |
| Показать, какой пакет представляет этот файл | rpm -qp - -provides имя_файла |

Основы системного администрирования и сетевых технологий
