УДК 004.7

Защита DNS

Белова С.В.
Белорусский национальный технический университет

На сегодняшний день сообщество пользователей Интернет достигло немыслимых размеров, и далеко не все его члены заслуживают доверия.

Служба DNS является достаточно критичным и важным компонентом, который используется каждый раз при отправке сообщения электронной почты или доступе к Web-странице. Она предназначена для преобразования символьных доменных имен, удобных для пользователей, в IP-адреса и представляет собой иерархически организованную распределенную базу данных, рассеянную по многим серверам имен.

Однако при разработке DNS защита была отнюдь не главной целью. Фактически DNS представляет собой незащищенный протокол. Служба DNS не проверяет, поступил ли ответ от аутентичного источника и содержит ли он аутентичные данные.

По причинам все большего распространения протокола IPv6, доступ к компьютерам через DNS имена станет еще более важным.

Одним из решений, которые можно использовать для защиты DNS среды, является применение протокола DNSSEC, представляющего собой собрание расширений, повышающих надежность DNS.

DNS клиент позволяет DNS серверу выполнять проверку от своего имени, при этом DNS клиент способен принимать DNSSEC ответы, возвращаемые с DNS сервера. Сам DNS клиент настроен на использование таблицы политики разрешения имен (Name Resolution Policy Table – NRPT) для определения того, как ему взаимодействовать с DNS сервером.

Для аутентификации DNS сервера используется протокол IPsec. DNSSEC использует SSL для подтверждения того, что подключение защищено. DNS сервер проходит проверку подлинности с помощью сертификата, подписанного доверенным издателем.

Таким образом, DNSSEC предоставляет новые функции, которые помогут сделать DNS инфраструктуру безопаснее, посредством совместного использования подписанных DNS зон, SSL защищенных подключений к доверенным DNS серверам и IPsec аутентификации и шифрования.