

АНАЛИЗ УЯЗВИМОСТЕЙ СИСТЕМЫ ДОМЕННЫХ ИМЕН В СЕТЯХ ТСП/Р

Килипко С.В.

Науковий керівник – доц. каф. БИТ., к.т.н., Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. Безопасности информационных технологий, тел. (057) 702-14-25),
E-mail: jl.sergo@gmail.com; факс (057) 702-14-25

This report considers approach to describing the security issues for Domain Name System. Also author describes extensions to DNS that provide data integrity and authentication to security aware resolvers and applications thought the use of cryptographic digital signatures.

Глобальная сеть Internet, которая стала неотъемлемой частью деятельности современного общества, не является безопасной для работы средой. Существует множество атак, направленных как на потребителей информации, так и на ресурсы, которые ее предоставляют. В частности, существует целый класс атак, направленных на нарушение соответствия доменного имени реальному IP-адресу.

В докладе рассматриваются возможные атаки на протокол системы доменных имен а также методы их предотвращения, которые основываются на практической и теоретичной модели взаимодействия конечного пользователя и ресурса в сети Internet посредством ТСП\Р соединения.

При обращении к ресурсу происходит преобразование доменного имени к сетевому адресу, по которому этот ресурс находится. Это

преобразование является слабым звеном прикладных протоколов, какими бы защищенными они не были. Большинство угроз связаны с использованием протокола передачи информации UDP, который не гарантирует целостность полученной информации.

Улучшение защиты протокола DNS является актуальным на текущий момент вопросом. Первым шагом является использование более надежного протокола TCP. Следующим шагом является использование асимметрической криптографии, а в частности цифровой подписи, которая позволит гарантировать целостность и подлинность информации, то есть запрашивающая сторона может быть уверена, что она получила ответ на тот вопрос, который задавала.

Использование этих средств в комплексе позволит существенно уменьшить количество возможных угроз и обезопасить взаимодействие пользователя с глобальной сетью Internet.