Автор:
05.11.14 07:21 -

Компания Google представила новый инструмент nogotofail для тестирования надёжности защищённых каналов связи на предмет использования некорректно настроенных соединений TLS/SSL, которые могут привести к применению известных видов атак или к непредвиденной передаче данных в открытом виде. По мнению разработчиков nogotofail, простого включения поддержки шифрования трафика недостаточно, так как неправильная настройка параметров защищённого соединения может свести безопасность на нет. Несмотря на предлагаемые в большинстве систем разумные настройки по умолчанию, присутствует обилие различных реализаций SSL/TLS и разработчики приложений часто необдуманно меняют настройки.

Nogotofail анализирует трафик между сервером и приложением, симулируя проведение MITM-атаки, для оценки наличия типовых пробоем с проверкой SSL-сертификатов, ошибок в библиотеках HTTPS и TLS/SSL, методов раскрытия данных в каналах SSL и STARTTLS. Nogotofail может быть запущен на транзитном узле или использован в качестве прокси. Код nogotofail написан на языке Python и распространяется под лицензией Apache.

Первичной задачей nogotofail является предоставление разработчикам приложений инструмента для удобной оценки защищённости каналов связи. Кроме того, вместе с nogotofail предлагается два клиентских приложения для Android и Linux, которые позволяют оценить общее состояние шифрования трафика на устройстве, изменить настройки и отследить возникновение проблем.

Read more http://www.opennet.ru/opennews/art.shtml?num=41005