Автор:
30.09.14 09:17 -

Ted Unangst опубликовал интересную статью, в которой рассказал о причинах создания проекта LibreSSL , привёл ретроспективу первого месяца разработки и поделился информацией о последних достижениях и планах на будущее.

Из особенностей разработки LibreSSL отмечается большая работа по развитию переносимой версии, которая разрабатывается одновременно с вариантом для OpenBSD и выпущена раньше нативной редакции для OpenBSD, которая будет представлена 1 ноября в составе OpenBSD 5.6. При этом код LibreSSL завязан на генераторе псевдослучайных чисел arc4random , реализация которого для FreeBSD и NetBSD оставляет желать лучшего и находится в заброшенном виде.

Из планов и текущих задач отмечается работа по созданию API ressl, который позиционируется в качестве замены API OpenSSL. Главными задачами при проектировании новго API является обеспечение непротиворечивости и простоты. По словам разработчика, новый API разрабатывается с оглядкой на то, что требуется пользователю, а не на то что позволяет сделать протокол TLS. Например, пользователю необходимо установить защищённое соединение с сервером, обеспечить работу защищённого сервера и организовать отправку и приём данных через установленное соединение. API будет абстрагирован от внутренностей и будет скрывать низкоуровневые манипуляции с сертификатами X.509 или ASN.1, и по сути близок к описанию защищённого транспорта поверх SSH-туннелей, предоставляя средства для установки защищённых соединений без лишних усложнений.

Абстрагирование программного интерфейса позволит подготовить варианты API ressl, реализованные поверх OpenSSL и других реализаций. Ранее предпринимаемые попытки создания замены OpenSSL как правило ограничивались созданием прокладок, воспроизводящих API OpenSSL. В задачи же LibreSSL входит создание нового универсального API, достаточно абстрактного для подготовки реализаций поверх различных библиотек, не ограничивающихся API OpenSSL.

Из особенностей ressl API отмечается такая возможность, как верификация имени хоста. TLS-соединение выглядит малополезным, если оно устанавливается с хостом, достоверность которого не гарантируется. При установке TLS-соединения осуществляется проверка сертификатов и связанной с ним цепочки доверия. Затем следует убедиться, что имя хоста, к которому осуществляется соединение,

соответствует имени, указанному в сертификате. OpenSSL не выполняет данное сопоставление, перенося его на плечи разработчиков приложения, которые часто игнорируют данную проверку или забывают её добавить. Выполнение проверки требует от разработчика знакомства с такими элементами, как CommonNames и SubjectAltNames, а также умение правильно организовать сопоставление масок. В итоге, в разных приложениях периодически всплывают уязвимости , связанные с неверной обработкой масок и нулевых байтов. В ressl API проверка имени хоста выполняется по умолчанию.

Read more http://www.opennet.ru/opennews/art.shtml?num=40710