CHRONA – программно-аппаратный менеджер паролей

В современном мире технологии очень быстро развиваются. Это приводит к их усложнению. В свою очередь, усложнение технических систем требует изменения механизма предоставления прав доступа. Проверка должна быть:

* Жестче (чтобы исключить возможность нелегитимного воздействия)
* Быстрее (помимо безопасности, система должна быть удобной)
* Независимой от человека (пользователь не знает пароль и не сможет его скомпрометировать)

Одним из вариантов повышения безопасности является комбинация нескольких факторов аутентификации. Мы решили реализовать систему многофакторной аутентификации на основе факторов знания и обладания.

В нашем проекте пользователь имеет различные криптостойкие пароли ко всем сервисам. Однако он их не знает. Он может использовать их только тем способом и только для тех целей, которые определены вектором контроля.

Мы используем только проверенные алгоритмы, чтобы максимально защитить секретные данные. Вся система основана на разделении секрета. Для этого используется модифицированный алгоритм ассиметричного шифрования RSA. Также мы подвергаем обфускации связи идентификатор-ключ в базе данных с помощью SHA256/384. Для обмена ключами – протокол Диффи-Хеллмана. В настоящее время это одни из самых защищенных алгоритмов обеспечения конфиденциальности данных.

По сравнению с аналогами (например, eToken), наш менеджер паролей способен работать на любой платформе, поддерживающей считывание данных с USB-порта, без установленного специального программного обеспечения.

// Вторая страница – наброски для будущего

Мы предлагаем программно-аппаратный менеджер паролей. Он представляет собой совокупность девайса в виде USB-устройства и программного обеспечения, установленного на смартфоне пользователя.