**Лаба 1**

**ФИО**

Абрамов И. В и Горин Д. В.

**Topic**

Authenticated Key Exchange; Key Agreement Protocol; Password

**Описание предметной области**

Данный топик охватывает исследования в области защиты информации, а именно Обмен ключами аутентификации (Authenticated Key Exchange), который представляет собой процесс в ходе которого 2 или более стороны могут установить безопасно общий ключ. Протоколы обмена ключами (Key Agreement Protocol) представляющий собой способы согласования общего ключа между сторонами и технология пароля (Password) – это секретная комбинация символов, используемая для аутентификации пользователя или для защит доступа к информации.

**Недостаток**

Аутентификация по ключам и протоколы согласования ключей могут быть подвержены атакам типа "человек посередине", где злоумышленник перехватывает и изменяет коммуникацию между участниками.

**Идея**

Для исправления выявленного недостатка мы предлагаем метод доступа к ключам аутентификации посредством приватного ключа, которым будут обладать только пользователи, которые совершают обмен ключами.

**Краткий текст обзора:**

Задачи защиты информации встают перед людьми каждый день, поэтому возник такой метод, как защита информации посредством протокола обмена ключами аутентификации (Authenticated Key Exchange), с помощью которого 2 или более стороны могут установить общий безопасный ключ для доступа к данным и обмениваться им. В связи с этим в данной исследуемой области предлагаются такие методы, как EKE (более безопасный протокол обмена ключами между тремя сторонами)[1], [2].Также в работе Chen и Lee [3], [4] предложен метод 3PAKE, который стал работать более быстро, так как проходил в меньшее количество этапов, позже предложили простое усовершенствование S-3PAKE, чтобы противостоять атакам, которые применялись к более ранним версиям 3PAKE [5]. Ещё были созданы 2 метода, которые описываются в работах Chong и Zhang [6], [7]: QKA и AKA, которые являлись улучшением алгоритма KA, что позволило двум пользователям устанавливать секретный ключ совместно, чтобы в этом не участвовала только одна сторона. Ещё были предложены методы, защита которых основана на использовании криптосистем и динамических псевдонимов [8], [9]. К сожалению, представленные методы обладают существенным недостатком: все протоколы подвержены атакам типа «человек посредине» [10], при которых может происходить утечка данных при обмене ключами доступа. В нашей статье мы предлагаем решение, способное устранить этот недостаток. По-нашему мнению для безопасного обмена ключами аутентификации, необходимо, чтобы обе стороны имели 2 вида ключей: публичный и приватный. Тогда при обмене ключами, одна сторона передаёт зашифрованный публичный ключ, и расшифровать его может только человек, который обладает приватным ключом, таким образом будет существовать гарантия защита от атаки типа «человек посредине».

References:

[1] C.-L. Lin и T. Hwang, «A password authentication scheme with secure password updating», *Computers & Security*, т. 22, вып. 1, Art. вып. 1, 2003, doi: 10.1016/S0167-4048(03)00114-7.

[2] H.-M. Sun, B.-C. Chen, и T. Hwang, «Secure key agreement protocols for three-party against guessing attacks», *Journal of Systems and Software*, т. 75, вып. 1, Art. вып. 1, 2005, doi: 10.1016/j.jss.2003.11.017.

[3] T.-H. Chen, W.-B. Lee, и H.-B. Chen, «A round- and computation-efficient three-party authenticated key exchange protocol», *Journal of Systems and Software*, т. 81, вып. 9, Art. вып. 9, 2008, doi: 10.1016/j.jss.2007.11.720.

[4] T.-F. Lee и T. Hwang, «Simple password-based three-party authenticated key exchange without server public keys», *Information Sciences*, т. 180, вып. 9, Art. вып. 9, 2010, doi: 10.1016/j.ins.2010.01.005.

[5] R. C.-W. Phan, W.-C. Yau, и B.-M. Goi, «Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)», *Information Sciences*, т. 178, вып. 13, Art. вып. 13, 2008, doi: 10.1016/j.ins.2008.02.008.

[6] S.-K. Chong и T. Hwang, «Quantum key agreement protocol based on BB84», *Optics Communications*, т. 283, вып. 6, Art. вып. 6, 2010, doi: 10.1016/j.optcom.2009.11.007.

[7] L. Zhang, F. Zhang, Q. Wu, и J. Domingo-Ferrer, «Simulatable certificateless two-party authenticated key agreement protocol», *Information Sciences*, т. 180, вып. 6, Art. вып. 6, 2010, doi: 10.1016/j.ins.2009.11.036.

[8] T.-Y. Chang, M.-S. Hwang, и W.-P. Yang, «A communication-efficient three-party password authenticated key exchange protocol», *Information Sciences*, т. 181, вып. 1, Art. вып. 1, 2011, doi: 10.1016/j.ins.2010.08.032.

[9] K. Xue, P. Hong, и C. Ma, «A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture», *Journal of Computer and System Sciences*, т. 80, вып. 1, Art. вып. 1, 2014, doi: 10.1016/j.jcss.2013.07.004.

[10] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. (Belin) Tai, J. Cook, и E. Eugene Schultz, «Improving password security and memorability to protect personal and organizational information», *International Journal of Human-Computer Studies*, т. 65, вып. 8, Art. вып. 8, 2007, doi: 10.1016/j.ijhcs.2007.03.007.