**ФИО**

Кузьмин С. С., Черакаев Я. А. (6114-100503D)

**Topic**

Key Agreement; User Authentication; Multi-Server

**Описание предметной области**

В данном топике рассматриваются темы аутентификации пользователей с помощью мульти-сервера и смарт-карт. Мульти-сервер – это набор программно-аппаратных и решений для получения, хранения, обработки, редактирования и передачи информации от источника к конечному получателю информации. Смарт-карта – это пластиковые карты со встроенной микросхемой. В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, управляющую устройством и контролирующую доступ к объектам в его памяти.

**Недостаток(Gap)**

Создание таких методов аутентификации является долгим процессом. Технологии в данной сфере, хоть и имеют широкое применение, но до сих пор не являются совершенными, к примеру, они не могут защитить от brute-force атаки. Более того, эти схемы обеспечивают условную анонимность, которая предполагает, что, если злоумышленник обнаружит закрытый ключ пользователя, его личность можно легко восстановить и использовать не по назначению.

**Идея**

Решить проблему безопасности многочисленных аутентификаций для разных серверов, совместив метод биометрии и hash-функций, делая brute-force атаку бессмысленной из-за затрачиваемого времени.

**Краткий текст обзора**

При аутентификации на сервер у пользователей всегда могли возникнуть проблемы с сохранением анонимности. Для решения этой проблемы был предложен метод аутентификации с помощью использования мульти-сервера.[1] Наибольший всплеск исследований на эту тему пришёлся на период с 2014 на 2019 года. Возможно также использование смарт-карты из-за присущей им защиты от помех.[2], [3] Такая схема аутентификации является упрощённой, так как использует только одноразовый номер и хэш-функцию.[4]

Продолжительное исследование данной темы показывает, что это точный долгий и трудоёмкий процесс - создание схем аутентификаций.[5] На сегодняшний день проблема безопасности не решена полностью, например, существует угроза в виде brute-force атак. Также предложенный способ обеспечивает лишь условную анонимность, которая предполагает, что злоумышленника от доступа к личности пользователя отделяет только закрытый ключ.

Недавно была предложена биометрическая аутентификация с протоколом согласования ключей для многосерверной среды и было заявлено, что этот протокол эффективен и устойчив к заметным атакам безопасности.[1], [5] Тщательные исследования показывают, что пользователи протокола передают личную информацию серверам приложений во время процесса регистрации и аутентификации. Подобный характер раскрытия учетных данных приводит к серьезным угрозам, в частности, к внутренним атакам, атакам с выдачей себя за пользователя и атакам за выдачу себя за сервер.[5] В качестве решения вышеупомянутых проблем предлагаются новые протоколы согласования ключей с взаимной аутентификацией на основе биометрических данных для многосерверной архитектуры, основанные на криптографии с эллиптическими кривыми.[1], [7], [8] Это позволяет пользователю получать доступ к сервисам разных поставщиков без необходимости проходить многократную регистрацию. Конфиденциальность того, кто желает получить доступ к этим услугам, часто имеет решающее значение. Чтобы получить доступ к этой услуге таким образом, чтобы обеспечить конфиденциальность пользователя, пользователь должен пройти анонимную аутентификацию, независимую от услуг поставщиков.[9] Однако существующие анонимные схемы на основе идентификации подходят только для домена клиент-сервер.[8], [10] Более того, эти схемы обеспечивают условную анонимность, которая предполагает, что, если злоумышленник обнаружит закрытый ключ пользователя, его личность можно легко восстановить и использовать не по назначению.[10] Чтобы избежать этой ситуации, в этом документе представлена ​​новая схема соглашения о ключах, которые хранятся на отдельном сервере в виде hash-функций с применением соли, аутентифицированных пользователем на основе безусловной анонимности, для многосерверной среды Интернета вещей.[4], [6], [9]

**References**

[1] R. Amin и G. P. Biswas, «Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment», *Wirel. Pers. Commun.*, т. 84, вып. 1, сс. 439–462, сен. 2015, doi: 10.1007/s11277-015-2616-7.

[2] H. Zhu, X. Hao, Y. Zhang, и M. Jiang, «A Biometrics-based Multi-server Key Agreement Scheme on Chaotic Maps Cryptosystem», 2013.

[3] 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», *J. Comput. Syst. Sci.*, т. 80, вып. 1, сс. 195–206, фев. 2014, doi: 10.1016/j.jcss.2013.07.004.

[4] M.-C. Chuang и M. C. Chen, «An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics», *Expert Syst. Appl.*, т. 41, вып. 4, сс. 1411–1418, мар. 2014, doi: 10.1016/j.eswa.2013.08.040.

[5] D. He, «Security flaws in a biometrics-based multi- server authentication with key agreement scheme», *J. Supercomput.*, т. 63, вып. 1, сс. 235–255, 2011, doi: 10.1007/s11227-010-0512-1.

[6] M. A. Akram, Z. Ghaffar, K. Mahmood, S. Kumari, K. Agarwal, и C.-M. Chen, «An anonymous authenticated key-agreement scheme for multi-server infrastructure», *Hum.-Centric Comput. Inf. Sci.*, т. 10, вып. 1, с. 22, май 2020, doi: 10.1186/s13673-020-00227-9.

[7] A. Hassan, A. A. Omala, M. Ali, C. Jin, и F. Li, «Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity», *Mob. Netw. Appl.*, т. 24, вып. 3, сс. 890–902, июн. 2019, doi: 10.1007/s11036-018-1145-5.

[8] A. G. Reddy, E.-J. Yoon, A. K. Das, V. Odelu, и K.-Y. Yoo, «Design of Mutually Authenticated Key Agreement Protocol Resistant to Impersonation Attacks for Multi-Server Environment», *IEEE Access*, т. 5, сс. 3622–3639, 2017, doi: 10.1109/ACCESS.2017.2666258.

[9] A. Irshad, M. Sher, S. A. Chaudhary, H. Naqvi, и M. S. Farash, «An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre», *J. Supercomput.*, т. 72, вып. 4, сс. 1623–1644, апр. 2016, doi: 10.1007/s11227-016-1688-9.

[10] H. Lin, F. Wen, и C. Du, «An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics», *Wirel. Pers. Commun.*, т. 84, вып. 4, сс. 2351–2362, окт. 2015, doi: 10.1007/s11277-015-2708-4.