**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. Наибольший всплеск исследований на эту тему пришёлся на период с 2014 на 2019 года.[[1]](#footnote-2) Возможно также использование смарт-карты из-за присущей им защиты от помех.[[2]](#footnote-3) Такая схема аутентификации является упрощённой, так как использует только одноразовый номер и хэш-функцию.[[3]](#footnote-4)

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.[[4]](#footnote-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]](#footnote-6) В качестве решения вышеупомянутых проблемпредлагаются новые протоколы согласования ключей с взаимной аутентификацией на основе биометрических данных для многосерверной архитектуры, основанные на криптографии с эллиптическими кривыми.[[6]](#footnote-7)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.[[7]](#footnote-8) Однако существующие анонимные схемы на основе идентификации подходят только для домена клиент-сервер.[[8]](#footnote-9) 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.[[9]](#footnote-10) Чтобы избежать этой ситуации, в этом документе представлена ​​новая схема соглашения о ключах, аутентифицированных пользователем на основе безусловной анонимности, для многосерверной среды Интернета вещей.[[10]](#footnote-11)

**References**

Akram, Muhammad Arslan, ZahidGhaffar, Khalid Mahmood, SaruKumari, Kadambri Agarwal, иChien-Ming Chen. «An anonymous authenticated key-agreement scheme for multi-server infrastructure». *Human-centric Computing and Information Sciences* 10, вып. 1 (15 май 2020 г.): 22. https://doi.org/10.1186/s13673-020-00227-9.

Amin, Ruhul, и G. P. Biswas. «Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-Server Environment». *Wireless Personal Communications* 84, вып. 1 (сентябрь 2015 г.): 439–62. https://doi.org/10.1007/s11277-015-2616-7.

Chuang, Ming-Chin, иMeng Chang Chen. «An Anonymous Multi-Server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Cards and Biometrics». *Expert Systems with Applications* 41, вып. 4 (март 2014 г.): 1411–18. https://doi.org/10.1016/j.eswa.2013.08.040.

Hassan, Alzubair, Anyembe Andrew Omala, Mohamed Ali, ChunhuaJin, иFagen Li. «Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity». *Mobile Networks and Applications* 24, вып. 3 (июнь 2019 г.): 890–902. https://doi.org/10.1007/s11036-018-1145-5.

He, Debiao. «Security Flaws in a Biometrics-Based Multi- Server Authentication with Key Agreement Scheme». *The Journal of Supercomputing* 63, вып. 1 (2011 г.): 235–55. https://doi.org/10.1007/s11227-010-0512-1.

Lin, Hao, Fengtong Wen, иChunxia Du. «An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics». *Wireless Personal Communications* 84, вып. 4 (октябрь 2015 г.): 2351–62. https://doi.org/10.1007/s11277-015-2708-4.

Xue, Kaiping, Peilin Hong, и Changsha 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* 80, вып. 1 (1 февраль 2014 г.): 195–206. https://doi.org/10.1016/j.jcss.2013.07.004.

Zhu, Hongfeng, Xin Hao, Yifeng Zhang, и Man Jiang. «A Biometrics-Based Multi-Server Key Agreement Scheme on Chaotic Maps Cryptosystem», 2013 г.

1. Amin и Biswas, «Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-Server Environment». [↑](#footnote-ref-2)
2. Zhu идр., «A Biometrics-Based Multi-Server Key Agreement Scheme on Chaotic Maps Cryptosystem». [↑](#footnote-ref-3)
3. Chuang и Chen, «An Anonymous Multi-Server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Cards and Biometrics». [↑](#footnote-ref-4)
4. Amin и Biswas, «Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-Server Environment». [↑](#footnote-ref-5)
5. He, «Security Flaws in a Biometrics-Based Multi- Server Authentication with Key Agreement Scheme». [↑](#footnote-ref-6)
6. Amin и Biswas, «Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-Server Environment». [↑](#footnote-ref-7)
7. Xue, Hong, и Ma, «A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture». [↑](#footnote-ref-8)
8. Akramидр., «An anonymous authenticated key-agreement scheme for multi-server infrastructure». [↑](#footnote-ref-9)
9. Lin, Wen, и Du, «An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics». [↑](#footnote-ref-10)
10. Hassan идр., «Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity». [↑](#footnote-ref-11)