Лаба 1

# ФИО

Наумов И.Е. Ильин Д.Р. (6112-100503D)

# Topic

Attestation; Trusted Computing; Hardware Security

# Описание предметной области

Область Attestation, Trusted Computing и Hardware Security занимается разработкой и обеспечением безопасности аппаратного обеспечения, проверкой подлинности и целостности программного обеспечения, а также защитой от угроз в области информационной безопасности.

# Недостаток (Gap)

Интегрирования Hardware Security и Trusted Computing недостаточно для безопасного функционирования устройств Интернета вещей (IoT). Некоторые устройства и системы могут не быть полностью совместимы с технологиями Trusted Computing или Hardware Security, что может создавать сложности при их интеграции.

# Идея

Комплексное интегрирование механизмов аттестации (Attestation), Trusted Computing и аппаратной безопасности (Hardware Security) для обеспечения надежной защиты устройств IoT от потенциальных киберугроз.

# Краткий текст обзора

Цифровая безопасность в сети Интернета вещей (IoT) становится все более актуальной и приобретает все большее значение в современном мире, где устройства IoT становятся неотъемлемой частью повседневной жизни людей. Как результат, происходит бурное развитие технологий и методов обеспечения безопасности в этой области.

Изучение и разделение результатов исследований, представленных во всех статьях, позволяет выделить несколько ключевых факторов, которые играют важную роль в обеспечении цифровой безопасности в сети IoT. Первым из них является интегрирование механизмов аттестации (Attestation) и Trusted Computing, которые обеспечивают защиту от подделки и обеспечивают повышенную безопасность системы,[1],[2], но могут привести к ограничениям в гибкости настройки и управления системой.

Важным аспектом является дополнительное применение механизмов аппаратной безопастности,[3], [4] для проверки и подтверждения идентичности устройств и целостности их программного обеспечения , [2], [5]. Такие меры помогают предотвратить внедрение вредоносного программного обеспечения. обеспечивают надежную защиту от внешних киберугроз и решают проблему совместимости.

Для дополнительного усиления безопасности устройств IoT важно использовать дополнительные методы, такие как биометрические данные,[6], [7]. Это позволяет создать более надежную систему аутентификации и обеспечивает высокий уровень защиты личных данных и конфиденциальной информации.

Важным направлением является также постоянное обновление и совершенствование мер безопасности в соответствии с возрастающими угрозами и развивающимися технологиями. Стратегии защиты устройств IoT должны быть адаптированы к новым вызовам и угрозам в киберпространстве,[8], [9], [10].

В своей статье мы предлагем решение данной проблемы путем комлексного интегрирования механизмов аттестации (Attestation), Trusted Computing и аппаратной безопасности (Hardware Security). Данный подход помогает создать устойчивую и надежную защиту, необходимую для сохранения конфиденциальности данных, обеспечения целостности устройств в динамичной цифровой среде и решение проблемы совместимости систем с технологиями.

[1] Dilsun Kaynar, Deepak Garg, Jason Franklin, и Anupam Datta, «A Logic of Secure Systems and its Application to Trusted Computing | IEEE Conference Publication | IEEE Xplore». Просмотрено: 14 март 2024 г. [Онлайн]. Доступно на: https://ieeexplore.ieee.org/abstract/document/5207647

[2] Y. Yu, H. Wang, B. Liu, и G. Yin, «A Trusted Remote Attestation Model Based on Trusted Computing», в *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, сс. 1504–1509. doi: 10.1109/TrustCom.2013.183.

[3] W. Ozga, «Hardening High-Assurance Security Systems with Trusted Computing», 2021.

[4] Vivek Haldar, Deepak Chandra, и Michael Franz, «VM ’04 — Technical Paper». Просмотрено: 14 март 2024 г. [Онлайн]. Доступно на: https://www.usenix.org/legacy/events/vm04/tech/haldar/haldar\_html/

[5] W. Ozga, R. Faqeh, D. L. Quoc, F. Gregor, S. Dragone, и C. Fetzer, «CHORS: hardening high-assurance security systems with trusted computing», в *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, в SAC ’22. New York, NY, USA: Association for Computing Machinery, 2022, сс. 1626–1635. doi: 10.1145/3477314.3506961.

[6] A. Mpanti, S. D. Nikolopoulos, и I. Polenakis, «Defending Hardware-based Attacks on Trusted Computing using a Hardware-Integrity Attestation Protocol», в *Proceedings of the 18th International Conference on Computer Systems and Technologies*, в CompSysTech ’17. New York, NY, USA: Association for Computing Machinery, 2017, сс. 155–162. doi: 10.1145/3134302.3134320.

[7] Georgios Keramidas и Apostolos P.Fournaris, «From Hardware Security Tokens to Trusted Computing and Trusted Systems | SpringerLink». Просмотрено: 14 март 2024 г. [Онлайн]. Доступно на: https://link.springer.com/chapter/10.1007/978-3-319-00663-5\_6

[8] A. Nagarajan, V. Varadharajan, M. Hitchens, и E. Gallery, «Property Based Attestation and Trusted Computing: Analysis and Challenges», в *2009 Third International Conference on Network and System Security*, 2009, сс. 278–285. doi: 10.1109/NSS.2009.83.

[9] J. F. Reid, «Enhancing security in distributed systems with trusted computing hardware», phd, Queensland University of Technology, 2007. Просмотрено: 14 март 2024 г. [Онлайн]. Доступно на: https://eprints.qut.edu.au/16379/

[10] E. G. Sirer *и др.*, «Logical attestation: an authorization architecture for trustworthy computing», в *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, в SOSP ’11. New York, NY, USA: Association for Computing Machinery, 2011, сс. 249–264. doi: 10.1145/2043556.2043580.