How Do You Achieve Secure Remote Computing for the Healthcare Industry?

By Eddie DeMars

Based on my paper: An Exploration of Using Intel SGX for Remote Computing In Healthcare

Problems with Computing in Healthcare

- Healthcare industry has several issues that cause computing to be difficult
- Budget
  - Remote Computing
- HIPAA
  - Privacy
- Any remote computing must protect patient privacy first and foremost

How Do You Achieve Secure Remote Computing for the Healthcare Industry?

Intel SGX

- Trusted Execution Environment (TEE) for certain Intel processors
- Allows for the creation of “enclaves”
- Protects data within from hardware and software attacks

How is This Helpful?

- Intel SGX can be used to allow for secure remote computing
- Steps:
  - Both sides create enclaves with code to be run
  - Perform attestation
  - Send encrypted data to be processed
  - Enclave decrypts data, processes it, encrypts it and sends it back
- Data gets processed but the third party never sees it

Recommendations

- Solves a lot of issues, but brings a lot of baggage
  - Hard to program in, vulnerable to side channel attacks, and ethical concerns around Intel
- Interested? Further research:
  - Paper, slides, and example program on GitHub: https://github.com/edwardwdemars/
  - GWAS: DyPS and SAFETY
    - https://orbilu.uni.lu/handle/10993/44966
    - https://arxiv.org/abs/1703.02577
  - Intel SGX Explained by Victor Costan and Srinivas Devadas
    - http://www.css.csail.mit.edu/6.858/2020/readings/costan-sgx.pdf

Sources from Paper

- [1] Journal, H. (2022, February 12). Why is HIPAA Important? Updated 2022. *HIPAA Journal*. https://www.hipaajournal.com/why-is-hipaa-important/
- [2] HIPAA History. (n.d.). *HIPAA Journal*. Retrieved November 28, 2022, from https://www.hipaajournal.com/hipaa-history/
- [3] Rights (OCR), O. for C. (2008, May 7). *Summary of the HIPAA Privacy Rule* [Text]. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- [4] Rights (OCR), O. for C. (2009, November 20). *Summary of the HIPAA Security Rule* [Text]. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- [5] Confidential Computing Consortium. (2021, January). *Confidential Computing: Hardware-Based Trusted Execution for Applications and Data*. https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/11/CCC_outreach_whitepaper_updated_2022-11-02.pdf
- [6] Costan, V., & Devadas, S. (2016). *Intel SGX Explained*. https://eprint.iacr.org/2016/086
- [7] Sadat, M. N., Aziz, M. M. A., Mohammed, N., Chen, F., Wang, S., & Jiang, X. (2017). *SAFETY: Secure gwAs in Federated Environment Through a hYbrid solution with Intel SGX and Homomorphic Encryption* (arXiv:1703.02577). arXiv. https://doi.org/10.48550/arXiv.1703.02577
- [8] Rights (OCR), O. for C. (2007, March 28). *Does the HIPAA Privacy Rule protect genetic information?* [Text]. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/faq/354/does-hipaa-protect-genetic-information/index.html
- [9] Pascoal, T., Decouchant, J., Boutet, A., & Esteves-Verissimo, P. (2021). DyPS: Dynamic, Private and Secure GWAS. *Proceedings on Privacy Enhancing Technologies*. https://doi.org/10.2478/popets-2021-0025
- [10] *Confidential Computing Consortium—Open Source Community*. (n.d.). Confidential Computing Consortium. Retrieved November 30, 2022, from https://confidentialcomputing.io/