

Заштита података у употреби помоћу хардвера од поверења

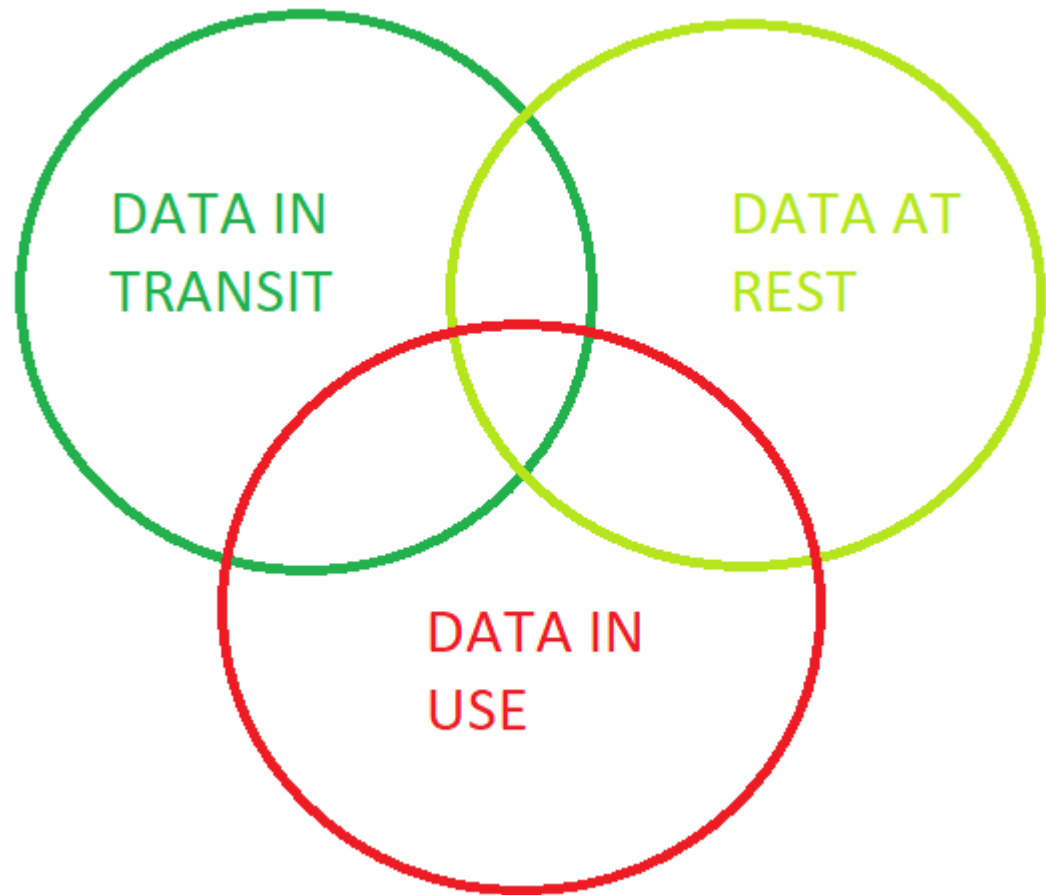
др Жарко Станисављевић
ванредни професор
Катедра за рачунарску технику и информатику
Електротехнички факултет
Универзитет у Београду

Садржај

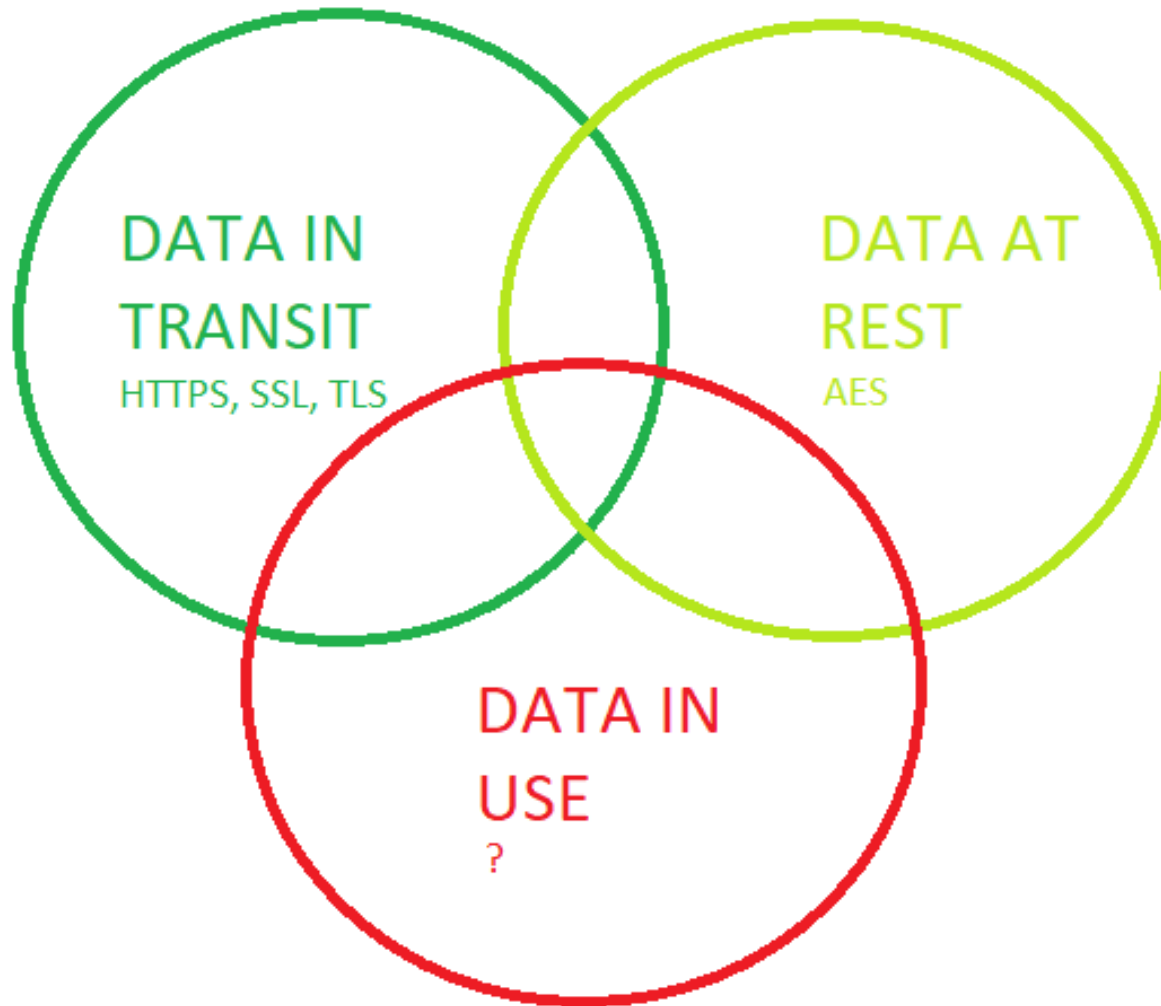
- ▶ Заштита података
- ▶ Заштита података у употреби
- ▶ Хардвер од поверења
- ▶ Пример употребе
- ▶ *CoCoS.ai* пројекат

Заштита података – проблем

- Поверљиво израчунавање (енг. Confidential computing) [1]
- Конзорцијум за поверљиво израчунавање (енг. Confidential Computing Consortium)



Заштита података – решење



Заштита података у употреби – FHE

- ▶ Хомоморфна енкрипција (енг. Fully Homomorphic Encryption – FHE)[2]
 - Решење засновано на математици
 - Проблем дефинисан 1978.
 - Омогућава произвољна израчунавања над шифрованим подацима без познавања кључа за декрипцију
 - Није још увек довољно ефикасна за практичну примену [3]

Заштита података у употреби – TEE

- ▶ Хардвер од поверења (енг. Trusted Execution Environment – TEE) [4]
 - Криптографија + хардвер од поверења
 - Окружење заштићено од злонамерног манипулисања (енг. Tamper resistant)
 - Гарантује:
 - аутентичност извршног кода,
 - интегритет извршног стања и
 - тајност кода, података и стања.
 - Пружа:
 - удаљену атестацију
 - Отпоран на нападе

Хардвер од поверења – ARM

▶ ARM TrustZone [5]

- Постоји од Cortex–А серије процесора из 2004.
- Првенствено се користи у IoT уређајима
- Хардверски раздваја:
 - Заштићени свет и
 - Нормални свет
- Тек однедавно је доступан за треће стране

Хардвер од поверења – Intel

▶ Intel SGX [6]

- Појавио се 2016. као проширење Intel-ове архитектуре процесора (енг. Software Guard Extensions – SGX) са задатком да обезбеди тајност и интегритет код сигурносно осетљивих израчунавања
- Поставља се хардверски заштићени контејнер на удаљеном рачунару у који се постављају поверљиви подаци и код
- Процесно базирано решење

▶ Intel TDX [7]

- Решење базирано на виртуелној машини
- Најављен 2020. као ново проширење архитектуре (енг. Trusted Domain Extensions – TDX)

Хардвер од поверења – AMD

▶ AMD SEV [8]

- Шифрује се виртуелна машина јединственим кључем који је познат само процесору (Secure Encrypted Virtualization – SEV)
- Доступан API
- Јасан механизам успостављања поверења у окружење
- Погодан за израчунавања високих перформанси (енг. High Performance Computing – HPC) [9]

▶ AMD SEV–SNP [10]

- Исправља примећене слабости претходних верзија (Secure Nested Paging – SNP)
 - Појачана контрола интегритета меморије
 - Атестација могућа у произвољном тренутку

Хардвер од поверења – удаљена атестација

- ▶ Када се користи TEE корисник се мора уверити у исправност окружења
- ▶ Још увек не постоји стандард
- ▶ IETF је формирао RATS (Remote ATtestation ProcedureS) радну групу
- ▶ Различити начини имплементације
 - Увид у атестациони извештај
 - Атестациони прокси
 - Атестациони протоколи произвођача хардвера
 - Решења отвореног кода

Пример употребе

- ▶ Безбедно израчунавање више страна (енг. Secure Multi-Party Computation – SMPC)
- ▶ Омогућава да више учесника изведе неко израчунавање и добије резултат без откривања осетљивих информација било које стране
- ▶ Посебно интересно код примене алгоритама вештачке интелигенције и машинског учења
 - Здравство
 - Банкарство

CoCoS.ai пројекат

- ▶ <https://cocos.ai>
- ▶ Финансиран од стране Фонда за иновациону делатност кроз Програм сарадње науке и привреде
- ▶ Реализују га Ultraviolet Consult и Електротехнички факултет
- ▶ Представља платформу која омогућава SMPC
- ▶ Користи се AMD EPYC треће генерације
- ▶ Проблеми?

Коришћена литература

1. Rashid, Fahmida Y. "The rise of confidential computing: Big tech companies are adopting a new security model to protect data while it's in use-[news]." *IEEE Spectrum* 57.6 (2020): 8–9.
2. Craig Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
3. Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan. Can homomorphic encryption be practical? In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pages 113–124. ACM, 2011.
4. Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: what it is, and what it is not." 2015 *IEEE Trustcom/BigDataSE/ISPA*. Vol. 1. IEEE, 2015.
5. Pinto, Sandro, and Nuno Santos. "Demystifying arm trustzone: A comprehensive survey." *ACM Computing Surveys (CSUR)* 51.6 (2019): 1–36.
6. Costan, Victor, and Srinivas Devadas. "Intel SGX explained." *Cryptology ePrint Archive* (2016).
7. Sardar, Muhammad Usama, Saidgani Musaev, and Christof Fetzer. "Demystifying attestation in intel trust domain extensions via formal verification." *IEEE Access* 9 (2021): 83067–83079.
8. https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf
9. Akram, Ayaz, et al. "Performance analysis of scientific computing workloads on general purpose TEEs." *2021 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*. IEEE, 2021.
10. SEV-SNP, A. M. D. "Strengthening VM isolation with integrity protection and more." White Paper, January (2020).

Хвала на пажњи

Питања