Sigurnost operacijskih sustava i aplikacija

SGX - Intel® Software Guard Extensions

Matija Alojz Stuhne, 28.3.2025.

Pregled predavanja

1. Motivacija
2. Pitanja za ispit
3. Općenito
4. Ključni pojmovi
5. Primjer
6. Nedostatci
7. Zaključak

Pitanja za ispite

- Koji problem SGX pokušava riješiti (pojasnite)?
- Ukratko objasnite što je SGX.
- Zašto bismo SGX mogli opisati kao *reverse sandbox?*
- Objasnite što je to enklava te pomoću čega se potvrđuje njena ispravnost (izvršavanje predviđenog koda na predviđeni način); koji se podatak koristi u tom procesu?.
- Objasnite što je to udaljena atestacija te zašto je bitna.

Motivacija

- Javni *cloud* servisi sve su popularniji --> izvršavaju naše aplikacije
- Ne postoji garancija kako vlasnik *cloud* servisa nije zlonamjeran.
- Ne postoji garancija kako stroj na kojem se pokreće naša aplikacija nije kompromitiran.

- Rješenje postoji u obliku korištenja okruženje za povjerljivo izvršavanje (engl. *Trusted execution environment – TEE)*.
  - *TEE* --> Sigurno i izolirano okruženje unutar procesora u kojem se izvršava osjetljiv kod koji obrađuje osjetljive podatke; izolirano od ostatka sustava.
- Jedno od rješenja koje osigurava postojanje okruženja za povjerljivo izvršavanje jest SGX (*Software Guard Extensions*).

SGX - Općenito (1)

- Sigurnosna tehnologija dostupna na Intelovim procesorima.
  - Najraniji modeli koji podržavaju SGX: Intel Skylake linija (jesen 2015.)

- Predstavlja skup proširenja Intelove ahitekture kojem je cilj jamčiti integritet i povjerljivost, naših, aplikacija (i njihovih podataka) koje se izvršavaju na udaljenim računalima.

- Osigurava okruženje za povjerljivo izvršavanje (engl. *Trusted execution environment* - *TEE*).

SGX - Općenito (2)

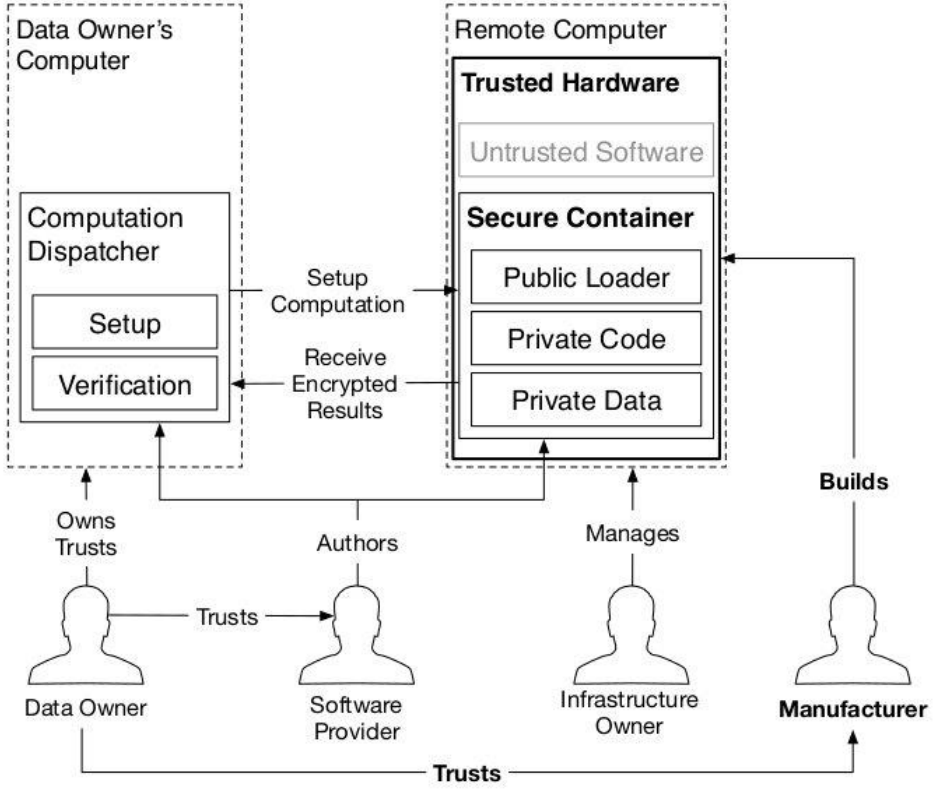
- SGX djeluje kao *reverse sandbox,* štiteći naše aplikacije (osjetljive dijelove) i korisničke podatke od operacijskog sustava (ili hipervizora), BIOS-a, firmvera, pogonitelja (engl. *driver*)…

- Glavna pretpostavka jest da je sve osim naše aplikacije, i procesora, nepouzdano te da se aplikacija i njeni podatci trebaju zaštititi.

- Naša aplikacija podijeljena je na "trusted" i "untrusted" dio.
  - Povjerljivi dio aplikacije je onaj koji obrađuje osjetljive podatke, a nepovjerljivim se smatram ostatak koda.
  - **SGX štiti povjerljivi dio stavljajući ga u izolaciju od ostatka sustava.**

SGX - Tko kome (ne)vjeruje?

- Korisnik vjeruje razvijatelju aplikacije te proizvođaču procesora (Intel).
- Razvijatelj vjeruje proizvođaču procesora.
- Korisnik i razvijatelj ne vjeruju pružatelju *cloud* usluga.



Osnovni prikaz koncepta izvedbe i povjerenja u SGX-u.

Ključni pojmovi - Uvod

- Za implementaciju SGX-a uveden je novi skup procesorskih instrukcija.
  - Sve su implementirane kroz mikrokod (za stvaranje, pristup i brisanje **enklava**).

- Uveden je koncept **enklava** (izoliranih kontejnera) čija se ispravnost provjerava procesom **udaljene atestacije** (dokaz identiteta).
  - Enklava predstavlja povjerljivi dio aplikacije koji obrađuje osjetljive podatke.

- Kako bi postigao izolaciju, SGX uvodi i koristi *Processor Reserved Memory* (**PRM**), izoliranu šifriranu memoriju, čiji se integritet i povjerljivost štite direktno od strane procesora.

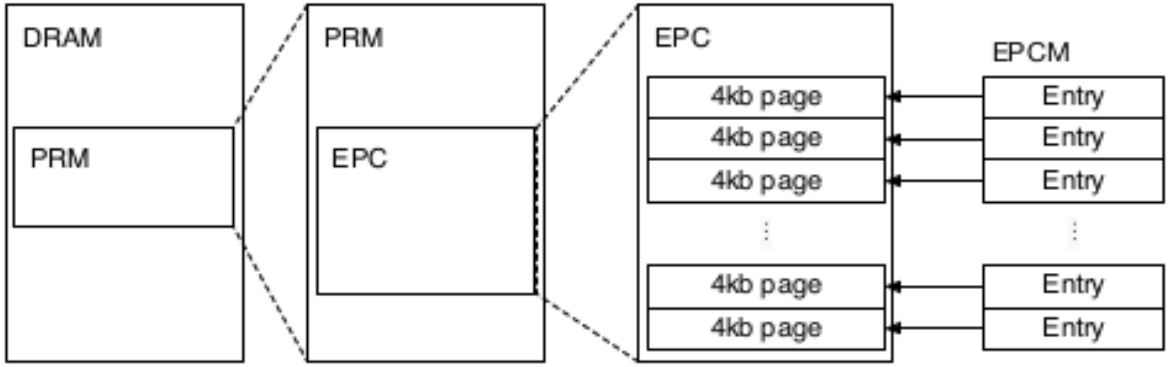
Ključni pojmovi - PRM / EPC / EPCM (1)

Sve navedeno omogućava izoliranost enklava.	**PRM** ***- Processor Reserved Memory -***	**EPC** ***- Enclave Page Cache -***	**EPCM** ***- Enclave Page Cache Map -***
Uloga	Dio memorije rezerviran isključivo za SGX.	Podskup PRM memorije koji koristi enklava.	Interna struktura koja prati koje stranice pripadaju kojoj enklavi.
Dodatno	• Fizički odvojeni dio RAM-a. • Pristup je dozvoljen samo SGX hardveru i aktivnim enklavama. • Uključuje EPC – memoriju koju koriste enklave.	• Sadrži memorijske stranice koda i podataka koje koriste aktivne enklave. • Podaci su automatski **šifriraju** pri pisanju u memoriju i dešifriraju pri čitanju.	• Evidentira kojoj enklavi pripadaju koje stranice, jesu li one valjane i šifrirane, te na kojoj se virtualnoj adresi povjerljivi dijelovi aplikacije moraju nalaziti. • Evidentira tip stranice ovisno o tome sadrži li aplikacija podatke (regularne stranice) ili pomoćne strukture vezane uz implementaciju SGX-a (special_type).

Ključni pojmovi - PRM / EPC / EPCM (2)

- Memorijske stranice enklavama dodjeljuje operacijski sustav, tj. kernel, koji je nepouzdan.

- Hardverske promjene uvedene implementacijom podrške za SGX brinu o tome da se enklavama dodjeljuju samo memorijske lokacije koje spadaju pod PRM, tj. da operacijski sustav ne može enklavi dodijeliti memorijske lokacije iz nepouzdanog RAM-a.



Prikaz podjele memorije kojoj mogu pristupiti samo SGX hardver i enklave.

- EPCM i *Memory Encryption Engine* (MEE) osiguravaju da pristup EPC stranicama može imati samo aktivna enklava kojoj te stranice pripadaju, a svi se drugi pristupi, uključujući druge enklave, BIOS, OS, hipervizora ili DMA (*Direct Memory Access*) blokiraju.

Ključni pojmovi - Enklava (1)

- **Enklava** je skupni naziv za osjetljivi programski odsječak koji se izvršava te podatke koje obrađuje, a kojima može pristupiti isključivo pouzdan Intelov procesor.

- Zaštićen i siguran kontejner koji izvršava naše aplikacije.
  - Vanjski softver ne može čitati niti mijenjati podatke u enklavi.

- Ispravnost enklave može se provjeriti procesom udaljene atestacije koristeći mjerni sažetak (engl. *measurement hash)*.

Ključni pojmovi - Enklava (2)

- Svaka enklava jednoznačno je identificirana koristeći ***mjerni sažetak***, tj. kriptografski sažetak koji jednoznačno predstavlja kod i podatke učitane u enklavu.

- Mjerni sažetak računa se tijekom faze učitavanja enklave (dodavanja memorijskih stranica u **PRM**, tj. **EPC**)**.**

- Odudaranje od specificiranih koraka izgradnje enklave (od strane udaljenog računala) rezultira krivim mjernim sažetkom.

Ključni pojmovi - Udaljena atestacija (1)

- **Udaljena atestacija** je proces koji udaljenim korisnicima dalje dokaz kako se unutar SGX enklave sigurno izvršava određeni kod.

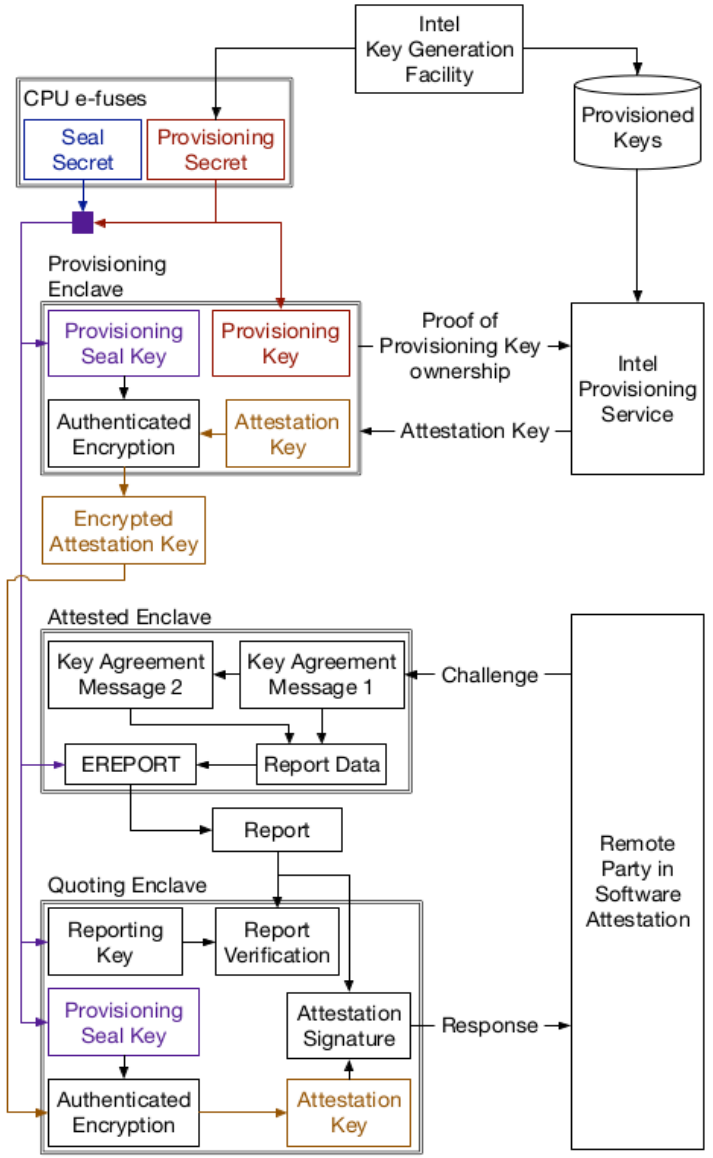
- Umjesto da vjerujemo operacijskom sustavu ili hipervizoru udaljenog računala i njegovim administratorima, vjerujemo samo Intelovom procesoru.

- Udaljena atestacija temelji se na provjeri mjernog sažetka enklave.

Ključni pojmovi - Udaljena atestacija (2)

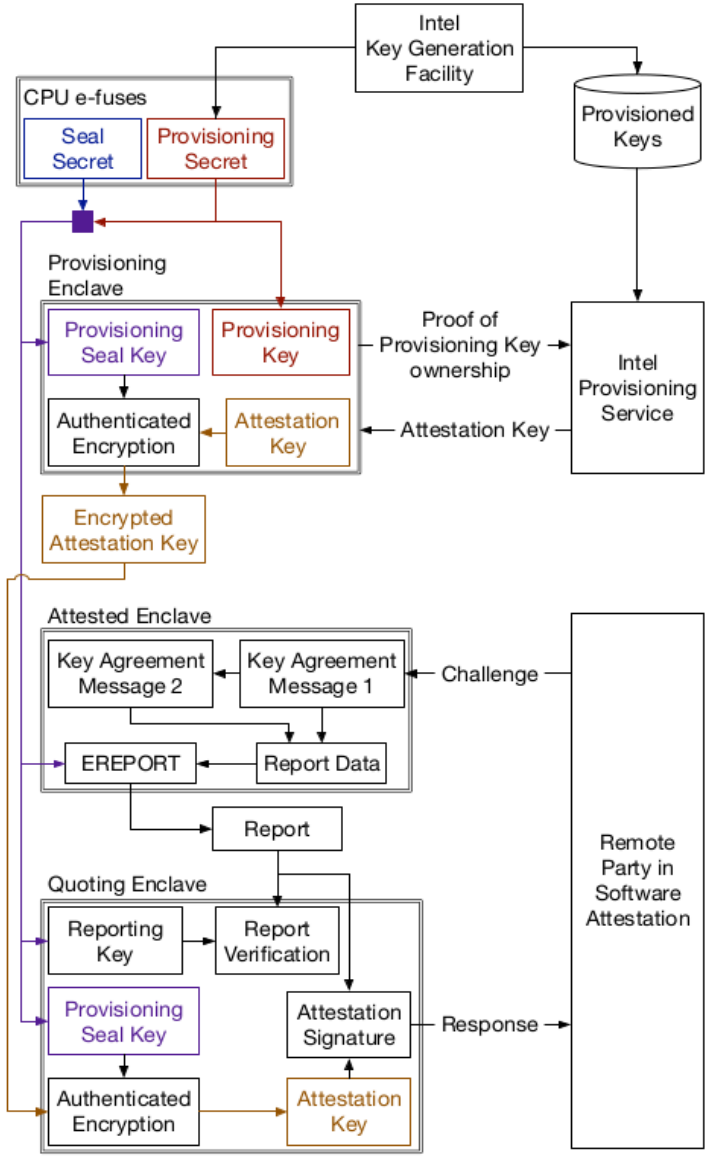
1. CPU sadrži dvije tajne (*Seal Secret*, *Provisioning Secret*).
   - *Seal Secret* --> izvedena iz fizičkih svojstava CPU-a
   - *Provisioning Secret* --> generira ju i upisuje, u CPU, Intel

2. *Provisioning* enklava koristi se kako bi Intel-ov udaljeni servis znao da komunicira sa sigurnim SGX procesorom.
   - Koristi *Provisioning Key* koji je izveden iz certificiranog identiteta enklave i *Provisioning Secret-a* kako bi Intel-u dokazao da komunicira sa sigurnom *Provisioning* enklavom. S obzirom da je ta enklava napravljena od strane Intel-a i prisutna u svakom SGX procesoru, Intel pohranjuje sve *Provisioning* ključeve.
   - Dokazom identiteta procesora, natrag se dobiva *Attestation Key* iz kojeg se izvodi enkriptirani *Attestation Key* koji služi za siguran prijenos atestacijskog ključa do *Quoting* enklave.

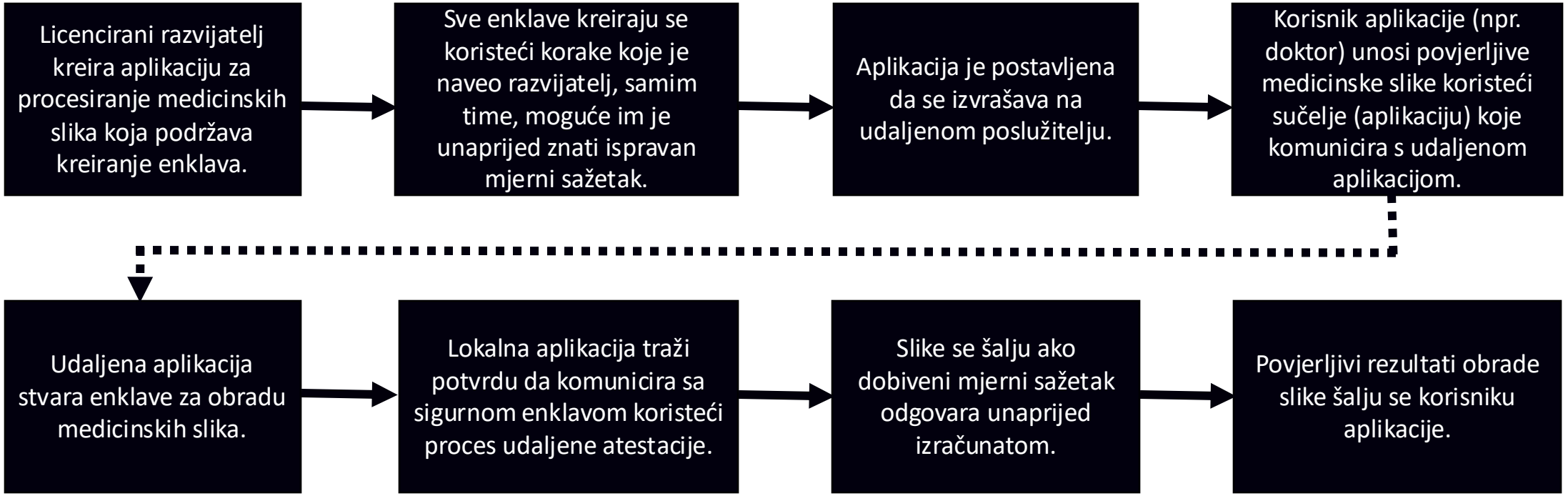


Ključni pojmovi - Udaljena atestacija (3)

3. Enklava za koju želimo provesti proces udaljene atestacije, procesom lokalne atestacije, potvrđuje svoj identitet *Quoting* enklavi koja zaprima i njen izvještaj koji, međuostalim, sadrži i mjerni sažetak .
4. *Quoting* enklava potpisuje taj izvještaj atestacijskim ključem te time kaže "enklava za koju se zatražila atestacija ima ove karakteristike, a njihov točan izračun je garantiran od strane Intela".
5. Korisnik koji je zatražio atestaciju za određenu enklavu, dobiva potpisani mjerni sažetak enklave te time (u usporedbi sa onim koji zna) provjerava identitet i ispravnost enklave.



SGX – Primjer (pojednostavljeno)



SGX - Nedostatci

1. Kompleksnost razvoja novih i refaktoriranja starih aplikacija.

   - Razvijatelj mora aplikaciju podijeliti na "*trusted*" i "*untrusted*" dio.
   - Prilikom korištenja u produkciji, razvijatelj mora biti licenciran od strane Intel-a.
   - Razvijatelj mora unaprijed odrediti na kojim virtualnim adresama unutar enklave će se određeni dijelovi aplikacije nalaziti --> statički se definira raspored u virtualnom adresnom prostoru --> o tome kasnije brine ECPM.

     Zašto?

     1. Funkcija koja računa mjerni sažetak uzima u obzir i lokaciju određenih dijelova koda.
     2. Sprječava napadača da proizvoljno remapira fizičke adrese na druge virtualne adrese, potencijalno mijenjajući tijek izvršavanja programa.

SGX - Nedostatci

2. Ograničenja SGX sigurnosnog modela

- SGX ne pruža zaštitu od pasivnih napada adresne translacije.*
  - Napadač može rekonstruirati redoslijed čitanja i pisanja stranica fizičke memorije te ih povezati sa virtualnim adresama unutar enklave, samim time i rekonstruirati logiku izvršavanja neke osjetljive aplikacije.
- SGX ne pruža zaštitu od *cache timing* napada.*
  - Napadač može mjeriti koliko se brzo i često pristupa određenoj memorijskoj lokaciji te iz toga razlučiti uzorak pristupa memoriji, a samim time potencijalno može razlučiti neke osjetljive informacije.
  - Dokumentirano od strane Intel-a.

- SGX ne pruža zaštitu ako razvijatelj na krivi način koristi predviđeni SDK.
  - S obzirom na kompleksnost razvijanja sigurnih aplikacija koje podržavaju enklave, ovo je velik problem.

**** Varijacije uspješno izvedenih napada vidljive su u materijalima iz literature.***

Tko koristi ili nudi podršku za SGX?

- Brojni pružatelji *cloud* usluga podržavaju korištenje SGX-a.
  - Microsoft Azure
  - IBM, CloudSigma, ...

- Kompanije koje razvijaju rješenja za zaštitu osobnih podataka prilikom obrade i/ili skladištenja podataka.
  - Aggregion
  - AMI, Anjuna, ...

Zaključak

- SGX predstavlja kompleksno rješenje koje štiti aplikacije (i korisničke podatke) koje se izvršavaju unutar nesigurnih (najčešće udaljenih) okolina.
- Korisno u današnjem vremenu kada se masovno koriste pružatelji *cloud* usluga.
- Postojanje dokumentiranih i uspješno iskorištenih ranjivosti stvara osjećaj nesigurnosti samog rješenja.

Literatura

- Aumasson, J. P., and Luis Merino. "SGX secure enclaves in practice: security and crypto review." Black Hat 2016 (2016): 10.
  - https://www.blackhat.com/docs/us-16/materials/us-16-Aumasson-SGX-Secure-Enclaves-In-Practice-Security-And-Crypto-Review-wp.pdf
- Nilsson, Alexander, Pegah Nikbakht Bideh, and Joakim Brorsson. "A survey of published attacks on Intel SGX." arXiv preprint arXiv:2006.13598 (2020).
  - https://www.researchgate.net/publication/342435947_A_Survey_of_Published_Attacks_on_Intel_SGX
- Costan, Victor, and Srinivas Devadas. "Intel SGX explained." Cryptology ePrint Archive (2016).
  - https://eprint.iacr.org/2016/086
- Zheng, Wei, et al. "A survey of Intel SGX and its applications." Frontiers of Computer Science 15 (2021): 1-15.
  - https://dl.acm.org/doi/10.1145/3456631

Dodatna literatura

- Intel® SGX Product Offerings
  - https://www.intel.com/content/www/us/en/architecture-and-technology/sgx-product-offerings.html

Hvala!