EMBEDDED SISTEMI
BEZBEDNOST, SECURE BOOT I AXIADO PRINCIPI

Uloga embedded inženjera u savremenoj industriji

- Embedded sistemi u industriji danas više nisu ograničeni na jednostavne mikrokontrolere sa GPIO pinovima i tajmerima.
- Savremeni embedded inženjer mora razumeti ceo životni ciklus uređaja, počev od trenutka uključenja napajanja, preko inicijalnog boot procesa, pa sve do bezbednog ažuriranja firmware-a na terenu.

Uloga embedded inženjera u savremenoj industriji

- U industrijskom okruženju, embedded inženjer je odgovoran ne samo za funkcionalnost sistema, već i za njegovu bezbednost, pouzdanost i otpornost na napade.
- Od njega se očekuje razumevanje integriteta firmware-a, zaštite od neautorizovanog pristupa i pravilnog upravljanja bezbednosnim mehanizmima tokom celog životnog veka uređaja.

Embedded sistemi i bezbednosni zahtevi

- Embedded sistemi se danas koriste u kritičnim oblastima kao što su mrežna infrastruktura, automobilska industrija, IoT uređaji, industrijska automatizacija i medicinska oprema.
- U tim oblastima, kompromitovanje sistema može dovesti do ozbiljnih posledica, uključujući finansijske gubitke, bezbednosne incidente ili ugrožavanje ljudskih života.

Embedded sistemi i bezbednosni zahtevi

Osnovni bezbednosni zahtevi uključuju:

- zaštitu firmware-a od neovlašćenih izmena,
- sprečavanje izvršavanja neautorizovanog koda,
- kontrolu debug i servisnih interfejsa,
- sigurno i verifikovano ažuriranje softvera.

Boot proces – osnova svakog embedded sistema

- Boot proces predstavlja niz jasno definisanih koraka koji se izvršavaju od trenutka uključenja napajanja do pokretanja glavne aplikacije ili operativnog sistema.
- Razumevanje boot procesa je jedno od najčešćih pitanja na tehničkim intervjuima za embedded pozicije.

Boot proces – osnova svakog embedded sistema

Tipičan redosled boot procesa je:

Power On → ROM Bootloader → Secondary Bootloader → Operativni sistem ili aplikacija

Svaka naredna faza zavisi od poverenja u prethodnu.

ROM Bootloader

ROM bootloader se nalazi u nepromenljivoj memoriji samog čipa (ROM ili mask ROM) i ne može se ažurirati. On predstavlja prvi i osnovni pouzdani deo sistema.

Njegova osnovna uloga je:

- inicijalizacija minimalnog hardvera,
- pronalaženje sledeće faze boot procesa,
- verifikacija integriteta i autentičnosti sledećeg bootloader-a.

Zbog toga se ROM bootloader često smatra početkom lanca poverenja.

Problem poverenja u firmware

- Ako napadač uspe da zameni ili izmeni firmware, ceo sistem postaje kompromitovan, bez obzira na kvalitet aplikativnog koda.
- Zato se uvodi koncept provere integriteta firmware-a pre njegovog izvršavanja.

Ovaj problem je osnovni motiv za uvođenje Secure Boot mehanizama u savremene embedded sisteme.

Secure Boot – osnovni koncept

Secure Boot je mehanizam koji obezbeđuje da se na uređaju izvršava isključivo autentifikovan i neizmenjen firmware.

Važno je naglasiti:

- Secure Boot ne štiti poverljivost koda,
- Secure Boot štiti integritet i autentičnost koda,
- Ako verifikacija ne uspe, sistem se ne pokreće ili ulazi u bezbedan režim.

Hash funkcije i integritet podataka

Hash funkcije se koriste za proveru integriteta podataka.
One mapiraju ulaz proizvoljne dužine u izlaz fiksne dužine.

Osnovne karakteristike:

- isti ulaz uvek daje isti hash,
- mala promena ulaza drastično menja hash,
- iz hash vrednosti se ne može rekonstruisati originalni podatak.
- Najčešće korišćeni algoritmi su SHA-256 i SHA-384.

Digitalni potpis i autentifikacija firmware-a

Digitalni potpis koristi asimetričnu kriptografiju.
Firmware se potpisuje privatnim ključem proizvođača, dok uređaj koristi javni ključ za verifikaciju potpisa.

Na ovaj način se:

- proverava integritet firmware-a,
- proverava identitet proizvođača,
- sprečava učitavanje neautorizovanog softvera.

Root of Trust (RoT)

- Root of Trust predstavlja minimalni deo sistema koji je implicitno pouzdan.
- On je početna tačka poverenja za ceo sistem.
- Ako Root of Trust nije kompromitovan, moguće je verifikovati sve ostale komponente sistema.

Šta se nalazi u Root of Trust-u

Root of Trust obično sadrži:

- javne kriptografske ključeve,
- sertifikate,
- hardversku logiku za verifikaciju potpisa.

- Najčešće je implementiran u hardveru i fizički izolovan od ostatka sistema.

Hardverska bezbednost kao temelj sistema

Hardverska bezbednost je ključna jer softver uvek može biti zamenjen ili modifikovan.
Zbog toga se bezbednosni mehanizmi implementiraju na hardverskom nivou.

Primeri hardverskih bezbednosnih tehnologija uključuju:

Secure Element,

TPM (Trusted Platform Module),

ARM TrustZone.

Secure Element i TPM

- Secure Element je poseban čip ili hardverski blok unutar SoC-a namenjen sigurnom čuvanju kriptografskih ključeva i izvršavanju kriptografskih operacija.

- TPM se najčešće koristi u računarima i serverima, ali principi njegovog rada su direktno primenljivi i u embedded sistemima.

Axiado – konceptualni pristup bezbednosti

- Axiado predstavlja industrijsko rešenje za bezbedno upravljanje sistemom.
  - Ne radi se o klasičnom mikrokontroleru, već o nezavisnom bezbednosnom kontroleru koji nadgleda rad celog sistema.

Uloga Axiado sistema u praksi

Axiado:

- nadgleda boot proces,
- proverava integritet firmware-a,
- sprovodi bezbednosne politike,
- deluje nezavisno od glavnog CPU-a.

- Ova nezavisnost značajno povećava otpornost sistema na napade.

Firmware lifecycle

Firmware prolazi kroz sledeće faze:

razvoj,

testiranje,

proizvodnju,

rad na terenu (field).

Svaka faza ima različite bezbednosne zahteve i nivoe dozvola.

Secure firmware update i rollback protection

Firmware update mora biti:

- kriptografski autentifikovan,
- zaštićen od neovlašćenih izmena,
- zaštićen od downgrade (rollback) napada.

- Rollback protection sprečava vraćanje sistema na staru, ranjivu verziju firmware-a.

Debug interfejsi i bezbednost

Debug interfejsi kao što su JTAG i SWD omogućavaju dubok pristup sistemu i predstavljaju potencijalni bezbednosni rizik.

U produkcionoj fazi:

- debug pristup mora biti ograničen ili potpuno onemogućen,
- često se dozvoljava samo uz autentifikaciju.

Secure lifecycle uređaja

Embedded uređaji obično imaju više bezbednosnih režima:

- development režim,
- production režim,
- field (operativni) režim.

Svaki režim ima jasno definisana prava i ograničenja.

Embedded Linux i Secure Boot

Kod Embedded Linux sistema koriste se bootloader-i kao što je U-Boot.
Secure Boot se primenjuje kroz:

- verifikaciju bootloader-a,
- verifikaciju kernela,
- verifikaciju device tree-ja i root filesystem-a.

Jetson Nano kao praktičan primer

Jetson Nano je dobar primer platforme na kojoj se može analizirati kompletan boot lanac i razlika između softverskih i hardverskih bezbednosnih mehanizama.

Kako ovo prezentovati na tehničkom intervjuu

Na intervjuu je važno pokazati razumevanje principa, a ne samo poznavanje konkretnih proizvoda.

Poseban naglasak treba staviti na:

- Secure Boot,
- Root of Trust,
- integritet firmware-a,
- hardversku osnovu bezbednosti.

Axiado (kratko)

Axiado je nezavisni bezbednosni koncept kontrolera koji deluje kao eksterni Root of Trust. On nadgleda boot proces, proverava integritet firmware-a i sprovodi bezbednosne politike nezavisno od glavnog procesora.

Zašto je Axiado bolji od Secure Boot-a implementiranog samo u CPU-u?

Zato što Secure Boot unutar CPU-a pretpostavlja da je CPU pouzdan. Axiado uklanja tu pretpostavku, jer je nezavisan hardverski entitet koji nadgleda CPU i može da spreči boot čak i ako je CPU kompromitovan.

Gde se nalazi Root of Trust kod Axiado sistema?

Root of Trust je implementiran u Axiado kontroleru, a ne u glavnom SoC-u, što omogućava nezavisnu verifikaciju i enforcement bezbednosnih politika!

Šta Axiado radi tokom boot-a?

- aktivira se odmah po uključenju napajanja,
- proverava firmware u flash memoriji,
- verifikuje digitalni potpis,
- odlučuje da li CPU može da se pokrene.

Kako Axiado povećava otpornost sistema?

Razdvajanjem bezbednosne logike od glavnog procesora i uvođenjem nezavisnog nadzora nad boot procesom i firmware lifecycle-om.

Da li Axiado zamenjuje TPM ili Secure Element?

Ne nužno!
Axiado može da ih dopuni ili integriše njihove funkcije, ali njegova ključna vrednost je nezavisni nadzor i kontrola celog sistema, a ne samo čuvanje ključeva.
Bezbednost embedded sistema nije funkcija, već arhitektura – a Axiado upravo adresira arhitekturni problem poverenja.

Šta nikako NE!

Axiado je samo još jedan mikrokontroler!

Secure Boot je softverska funkcija!

Root of Trust može da se implementira bilo gde!

AXIADO CASE STUDY
Boot Failure, Attack Scenario i Recovery mehanizmi

Sistem se koristi u mrežnoj infrastrukturi, gde je neautorizovano izvršavanje koda neprihvatljivo.

Axiado je konfigurisan kao eksterni Root of Trust i ima potpunu kontrolu nad boot procesom.

Da li Axiado zamenjuje TPM ili Secure Element?

Ne nužno!
Axiado može da ih dopuni ili integriše njihove funkcije, ali njegova ključna vrednost je nezavisni nadzor i kontrola celog sistema, a ne samo čuvanje ključeva.
Bezbednost embedded sistema nije funkcija, već arhitektura – a Axiado upravo adresira arhitekturni problem poverenja.

Normalan boot scenario (referentni slučaj)

Power ON
|
Axiado Controller aktivan
|
Axiado čita firmware iz flash-a
|
Digital Signature Verification
|
PASS
|
Dozvoljen boot glavnog CPU-a
|
OS / Application start

Glavni CPU nema kontrolu nad odlukom da li se sistem pokreće.

Attack scenario – kompromitovan firmware

Scenario napada:

Napadač:

dobija fizički ili logički pristup uređaju,

menja firmware u flash memoriji,

pokušava da ubaci zlonamerni kod ili modifikovanu verziju bootloader-a.

Bez Axiado sistema, CPU bi izvršio kompromitovani firmware.

Attack scenario – kompromitovan firmware

Power ON
|
Axiado Controller aktivan
|
Axiado čita firmware iz flash-a
|
Digital Signature Verification
|
PASS
|
Dozvoljen boot glavnog CPU-a
|
OS / Application start

Glavni CPU nema kontrolu nad odlukom da li se sistem pokreće.

Detekcija napada od strane Axiado sistema
Šta Axiado radi pri sledećem resetu:

Power ON
|
Axiado aktivan
|
Čitanje firmware-a
|
Hash izračunavanje
|
Upoređivanje sa potpisom
|
FAIL

Razlog:

Digitalni potpis ne odgovara sadržaju firmware-a.

Boot failure – ponašanje sistema

Reakcija Axiado kontrolera:

glavni CPU ne dobija dozvolu za boot,

reset linija CPU-a ostaje aktivna ili se CPU drži u halt stanju,

kompromitovani kod se nikada ne izvršava.

Napad je zaustavljen pre izvršavanja prvog instrukcijskog ciklusa CPU-a.

Recovery scenario – bezbedan oporavak sistema
Secure recovery firmware

Boot FAIL
|
Axiado aktivira recovery režim
|
Učitavanje trusted recovery image-a
|
Minimalni servisni OS

Recovery scenario – bezbedan oporavak sistema
Secure recovery firmware

Recovery image:

je potpisan,

smešten u zaštićenoj memoriji,

služi za bezbedno ponovno programiranje firmware-a.

Recovery scenario – daljinsko ažuriranje
Ako sistem ima mrežnu konekciju:

Recovery Mode
|
Secure Channel (TLS)
|
Download signed firmware
|
Verification (Axiado)
|
Install + Update version counter

Axiado proverava firmware pre i posle instalacije.

Rollback protection u praksi

Napadač pokušava da:

instalira staru, ranjivu verziju firmware-a.

Axiado:

čuva monotoni brojač verzije,

odbija instalaciju firmware-a sa nižim brojem verzije.

Bez Axiado vs. sa Axiado

Bez Axiado:

kompromitovani firmware se izvršava,

sistem je trajno ugrožen.

Sa Axiado:

napad je detektovan u boot fazi,

CPU se nikada ne pokreće,

sistem se oporavlja kroz kontrolisani recovery.