Pitanja za ispite

1. Nabrojite najmanje tri namjene za koje možemo koristiti TPM.
2. Kako TPM osigurava integritet podataka tijekom pokretanja sustava?
3. Koje su glavne značajke TPM-a kojima se štite kriptografski ključevi?
4. Kako TPM omogućuje sigurnu autentifikaciju uređaja i korisnika, te gdje je to korisno?
5. Opišite scenarij u kojem bi TPM mogao spriječiti neovlašteni pristup osjetljivim podacima na računalu.

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.

Pitanja za ispite

- Koji su osnovni principi sigurnosnog modela Androida?
- Kako višestrana suglasnost poboljšava sigurnost platforme?
- Što je pohrana s ograničenim pristupom i zašto je uvedena?
- Kako Android postiže sigurnost međukomponentne komunikacije?
- Koji su glavni sigurnosni izazovi Android platforme?
- Koje su najčešće prijetnje Android aplikacijama?

Pitanja za ispite

- Kako se postiže izolacija procesa između kontejnera?
- Koja je uloga opcije *nodev* prilikom montiranja datotečnog sustava kontejnera?
- Kako se ostvaruje mrežna veza između Docker kontejnera i koje je njezino sigurnosno ograničenje?
- Koje dvije vrste sustava za dodatnu zaštitu jezgre postoje i na koji način oni pružaju zaštitu?
- Objasnite način rada sigurnosnog modela AppArmour.

Pitanja

- Što je modeliranje prijetnji?
- Koji je glavni razlog korištenja modeliranja prijetnji?
- Koji su zadaci eksperta modeliranja prijetnji?
- Koji su koraci tipičnog projekta modeliranja prijetnji?
- O čemu govori manifest modeliranja prijetnji?

Pitanja za ispite

- Nabrojite i ukratko opišite svaku kategoriju modela prijetnji STRIDE.
- Koji su koraci projekta metodom modeliranja prijetnji STRIDE.
- Navedite prednosti i mane metode modeliranja prijetnji STRIDE.
- Kako napadači koriste *Spoofing* i *Denial of Service* te koje su metode zaštite?
- Zašto su granice povjerenja važne u dijagramima protoka podataka i kako one pomažu u identificiranju prijetnji?

Pitanja za ispite

- Što je stablo napada i po čemu se razlikuje od grafa napada
- Nabrojite prednosti modela stabla napada nad drugim modelima prijetnja
- Objasnite strukturu stabla napada
- Opišite načine definiranja metrika napada u stablu napada
- Napravite primjer jednostavnog stabla napada koristeći kontinuirane vrijednosti čvorova te označite najefektivniji put po tim svojstvima

Pitanja za ispite

- Navedite i objasnite tri sigurnosna zahtjeva koja bi trebao implementirati svaki sustav
- Zašto je bitno da se razmišlja o sigurnosti u samom početku SDLC-a
- Koja je razlika između bug-a i ranjivosti u arhitekturi
- Objasnite prednosti i mane korištenja eksternih komponenti
- Objasnite Tactic-Oriented Architectural Analysis (ToAA)

Pitanja za ispite

- Zašto mikroservisi imaju veće sigurnosne izazove od monolita?
- Objasnite što je *API Gateway* i navedite njegov značaj u sigurnosti
- Navedite neke metode autentifikacije u mikroservisnoj arhitekturi
- Objasnite princip najmanjih privilegija
- Objasnite kako se sigurnost uklapa u DevSecOps

Pitanja za ispite

- Objasnite od kojih vrsta grešaka štiti Rust?
- Objasnite situacije u kojima je Rust potencijalno dobar odabir jezika?
- Objasnite vlasništvo (eng. *Ownership*) u kontekstu Rusta?
- Koje dozvole imaju varijable i reference unutar *borrow checkerovih* pravila u programskom jeziku Rust?
- Što se događa s varijablom u Rustu kada se u funkciju pošalje izmjenjiva referenca na tu varijablu?