Sigurnost programske podrške

- Inženjerstvo softvera koji će pri napadu nastaviti ispravno raditi

Sigurnosna programska podrška

- Računalni programi i knjižnice za potporu sigurnosti računala ili mreže

Osiguranje softvera

- Razina pouzdanosti da softver nema ranjivosti

Sigurnost aplikacije

Mjere poduzete tijekom životnog ciklusa aplikacije radi prevencije iznimki u odnosu na politiku sigurnosti aplikacije ili sustava uslijed pogrešaka u projektiranju, razvoju, ugradnji, nadogradnji ili održavanju aplikacije

Kada je sigurnost softverski problem ?

- zahtijeva promjenu implementacije ili dizajna (softvera)

Uzroci problema softverske sigurnosti

- nedostatak svijesti, značaja
- nedostatak znanja
- Sigurnost kao sekundarna briga

Sigurnosni ciljevi : CIA

1. **C**onfidentiality (povjerljivost, tajnost)
2. **I**ntegrity (integritet, cjelovitost)
3. **A**vailability (dostupnost)

Realizacija ciljeva: AAAA

- Autentifikacija (**a**uthentication)
- Autorizacija (**a**uthorization)
- Nadzor, praćenje (**a**uditing)
- Djelovanje (**a**ction)

Životni ciklus sigurnog softvera

Analiza: sigurnosni zahtjevi, procjena rizika, …

Dizajn: modeliranje prijetnji, analiza površine napada, …

Implementacija: statička analiza, …

Verifikacija: dinamička analiza, fuzz testiranje, …

Isporuka: plan odgovora na incidente, finalni pregled
*ispitno pitanje

Prije početka rada:

- poduka svih članova da bi znali osnove i ostali u trendu
- barem jedan tečaj godišnje

1. Analiza

- rano postavljanje pouzdanih (trustworthiness) zahtjeva
- specifikacija minimalnih zahtjeva na sigurnost aplikacija
- uspostava minimalno prihvatljivih razina kvalitete sigurnosti i privatnosti
- tim dokazuje sukladnost kroz Final Security Review (FSR)
- procjena rizika

2. Dizajn

- što ranije uklanjanje problema sigurnosti i privatnosti
- izbjegavati „dodavanje“sigurnosti na kraju razvoja
- opisati kako sigurno ugraditi funkcionalnost
- redukcija rizika smanjenjem prostora za napad
    - isključenjem ili restrikcijom pristupa na sistemske resurse
    - primjenom principa najmanjeg prava
    - uslojavanjem
- modeliranje prijetnje - **glavna aktivnost dizajna**

sigurne mogućnosti – opća funkcionalnost koju treba osigurati (npr. unos, robusnost)

sigurnosne mogućnosti – funkcionalnost koja se odnosi na sigurnost (npr. autentifikacija)

3. Implementacija

- odabir alata i okruženja
- analiza korištenih funkcija i API-ja s obzirom na sigurnost
- statička analiza - osigurava inspekciju programskog koda, ali ju ne može zamijeniti!!

4. Verifikacija

- dinamička analiza
- *fuzz testing* - nastoji se izazvati zastoj unosom neispravnih ili pseudoslučajnih podataka
- ponovni pregled modela prijetnji i mjerenje površine napada

5. Isporuka

- definiranje plana odziva na incidente
- Final Security Review (FSR) - promišljena provjera svih sigurnosnih aktivnosti, prije objave
    - ishodi: passed FSR | passed FSR with exceptions | FSR with escalation
- **security advisor** potvrđuje (temeljem FSR i šire) da su zahtjevi zadovoljeni
- zasebno se potvrđuju komponente utjecaja na privatnost
- arhiviranje

Opcionalne aktivnosti

- Nadzor, ručna inspekcija koda (code review)
- Penetracijsko testiranje
- Analiza povredivosti sličnih aplikacija

RACI tablica

akronim (Responsable, Accountable, Consulted, Informed)

Sigurnosni zahtjevi

nefunkcionalni

- Procjene vrijednosti sustava – vrijednost sustava i podataka
- Zahtjevi za kontrolu pristupa – ograničenje na pristup podacima
- Zahtjevi za enkripcijom i autentifikacijom – kako, gdje i kada
- Zahtjevi za kontrolom virusa

Neki mogu *zahtijevati funkcionalnost*, npr.: duljina korisničkog unosa, validacija podataka

Izvori zahtjeva

- Korisnici
- Sigurnosna implikacija funkcionalnosti
- Regulatorna sukladnost

Alati za softversku sigurnost (ne mrežnu)

Microsoft SDL i derivati

- Attack Surface Analyzer – smanjenje površine napada
- Microsoft Threat Modeling Tool – modeliranje prijetnji
- MiniFuzz basic file fuzzing tool – fuzz testiranje
- Regular expression file fuzzing tool – testiranje potencijalnih DoS ranjivosti

Statička analiza

- StyleCop https://stylecop.codeplex.com/ # slično, FxCop
- CodeSmart http://www.axtools.com/
- NDepend http://www.ndepend.com/
- PMD Java, Checkstyle, FindBugs+Find Security Bugs