Безбедносно инжењерство

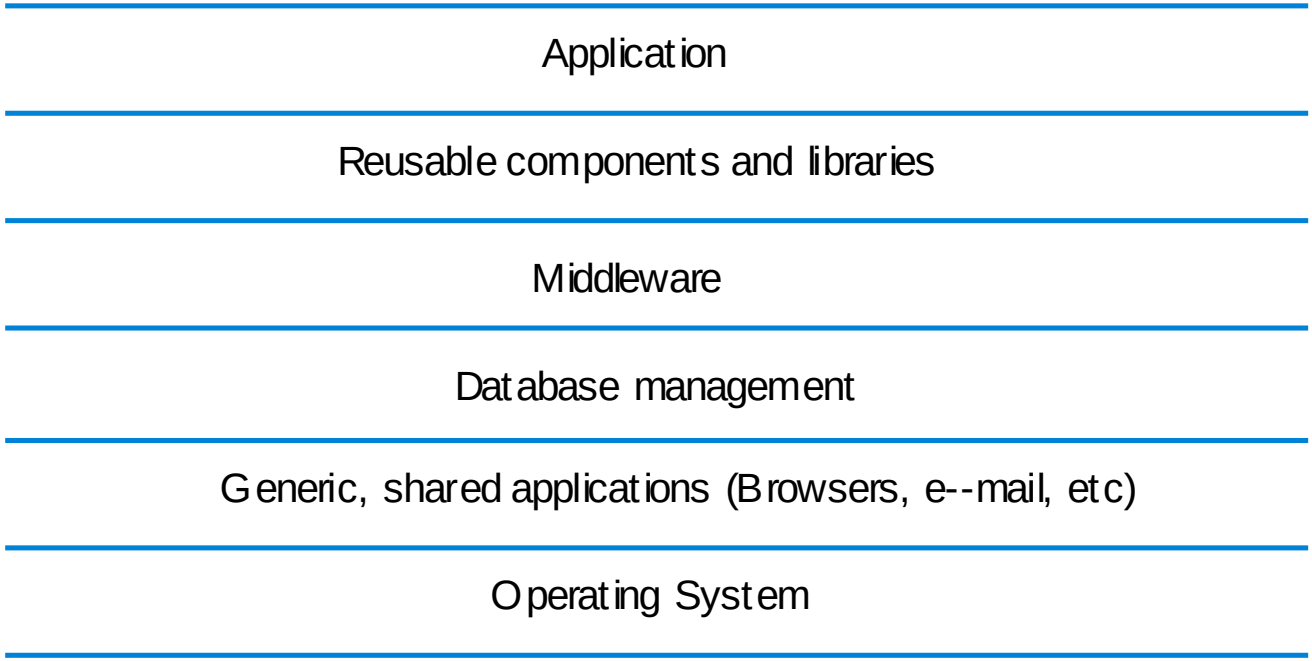
Циљеви

- Представљање питања и проблема који се могу јавити приликом дизајнирања сигурносних апликација система.
- Управљање безбедносним ризицима и извођење захтева безбедности из анализе ризика.
- Описати добар дизајн за сигуран развој система.
- Објаснити појам система преживљавања и методе анализе преживљавања.

Безбедносно инжењерство

- Алати, технике и методе које подржавају развој и одржавање система који може одолети злонамерним нападима који имају за циљ оштећење компјутерског система или његових података.
- Подпоље шире области безбедности рачунара.

Слојеви система



Апликација/инфраструктура безбедности

- Безбедносна апликација је проблем софтверског инжењерства где се систем дизајнира тако да се одупре нападима.
- Безбедностна инфраструктура је проблем управљања системом где инфраструктура има за циљ да се одупре нападима.
- Фокус овог поглавља је безбедносна апликација.

Концепти безбедности

Израз	Дефиниција
Asset (средство)	Системски извор који има вредност и потребно га је заштитити.
Exposure (излагање)	Могућ губитак који би био резултат успешног напада. Ово може бити губирак или оштећење података, или времена и труда које је неопходно уложити након нарушавања безбедности.
Vulnerability (рањивост)	Слабост у компјутерском систему која се може искористити за проузроковање губитка.
Attack (напад)	Коришћење рањивости система. Генерално, ради се из спољашности и представља намеран покушај да се проузрокује одређена штета.
Threats (претње)	Последице које носи са собом потенцијални напад. Ово се може посматрати као рањивост система која је повезана са једним нападом.
Control (контрола)	Мере заштитет које смањују рањивост система. Енкрипција би била један пример.

Примери концепта сигурности

Term	Definition
Asset (средство)	Подаци о сваком пацијенту који је примио или прима одређену терапију.
Exposure (излагање)	Потенцијални финансијски губитак од будућих пацијената који не желе да се подвргну терапији јер немају поверења у клинику и сигурност својих података. Финансијски губитак услед судских спорова. Губитак репутације.
Vulnerability (рањивост)	Слаба лозинка која омогућава нападачима да је лако погоде. Корисничка имена иста као и стварна имена.
Attack (напад)	Упад неовлашћеног корисника.
Threat (претња)	Неовлашћени корисник ће имати приступ систему уколико погоди корисничко име и шифру овлашћеног корисника.
Control (контрола)	Систем за проверу лозинки који онемогућује постављање неке речи која постоји у речнику за лозинку.

Безбедносне контроле

- Контроле које су намењене да осигурају да напади буду безуспешни. Ово је аналогно избегавању грешака.
- Контроле које су намењене откривању и сузбијању напада. Ово је аналогно детекцији грешака и толеранцији.
- Контроле које су намењене опоравку од проблема. Ово је аналогно грешци опоравка.

Безбедносни захтеви

- Пацијент информације
  - морају бити преузете на почетку седнице клинике на сигурном месту системског клијента који користи клиничко особље.
  - не смеју бити одржаване на системским клијентима након што је клиничка седница завршена.
- Дневник на посебном рачунару са сервером базе података морају се одржавати у свим изменама система базе података.

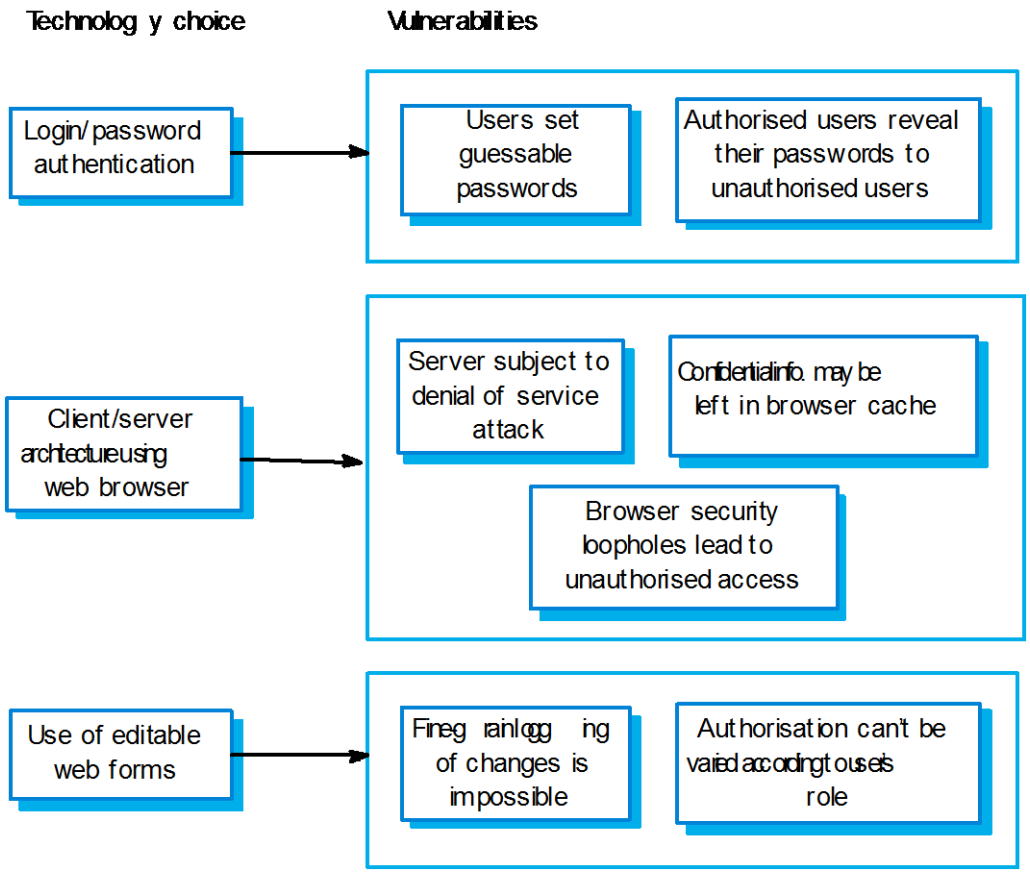
Животни циклус процене ризика

- Процена ризика док се систем развија и након прављења плана и распореда.
- Више података је доступно – системска платформа, посредничке и архитектуре система, и организација података.
- Рањивост која произилази из дизајна би требало да буде препозната.

Примери одлука дизајна

- Корисници система се идентификују коришћењем корисничког имена/лозинке.
- Архитектура система је клијент/сервер са клијентима који приступају систему преко уобичајног прегледача.
- Информације су представљене као веб форме које се могу мењати.

Технологија рањивости



Дизајн за безбедност

- Архитектонски дизајн – како овај дизајн утиче на безбедност система?
- Добра пракса – шта је прихваћено као добра пракса приликом дизајнирања безбедних система?
- Дизајн за распоређивање – какву би подршку требало пројектовати у систем како би се избегла рањивост приликом употребе?

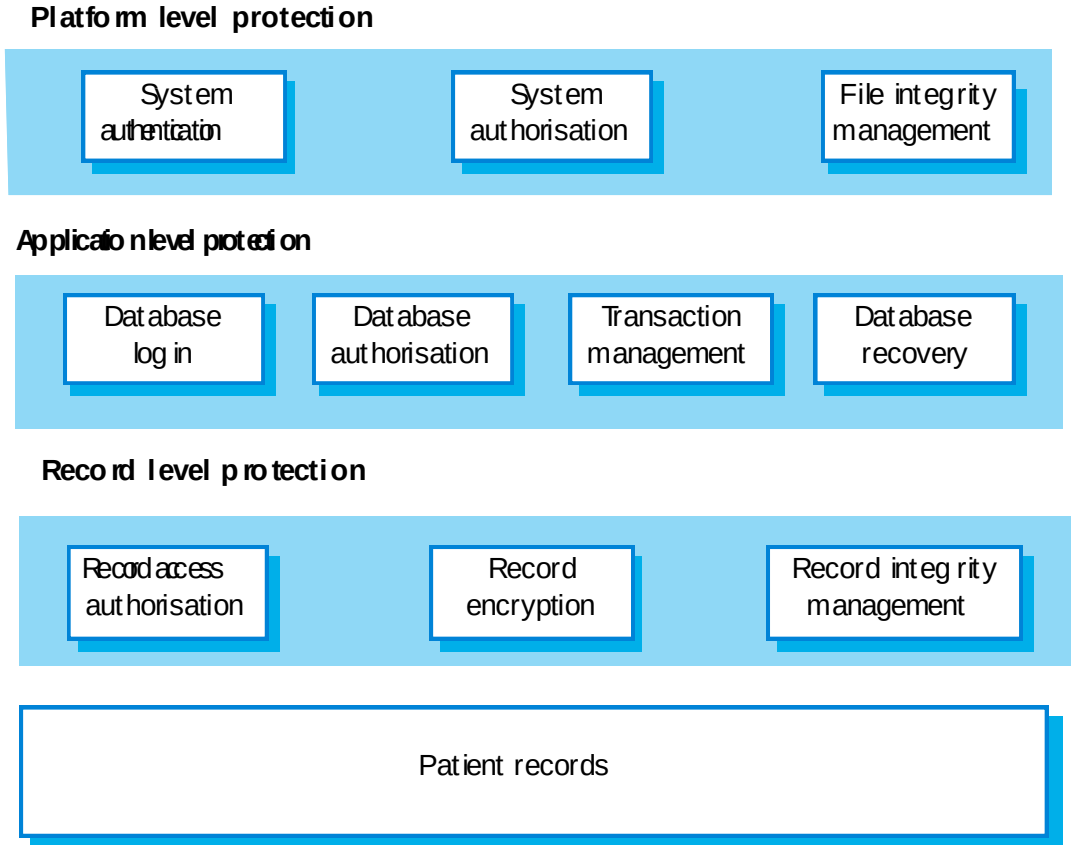
Архитектонски дизајн

- Заштита
  - Како би требало организовати систем тако да критични подаци буду заштићени од спољних напада?
- Дистрибуција
  - Како би требало распоредити средства система у складу са тим да се минимизују ефекти успешног напада?
- Потенцијални конфликт
  - Што више распоредимо средства, скупља је заштита.

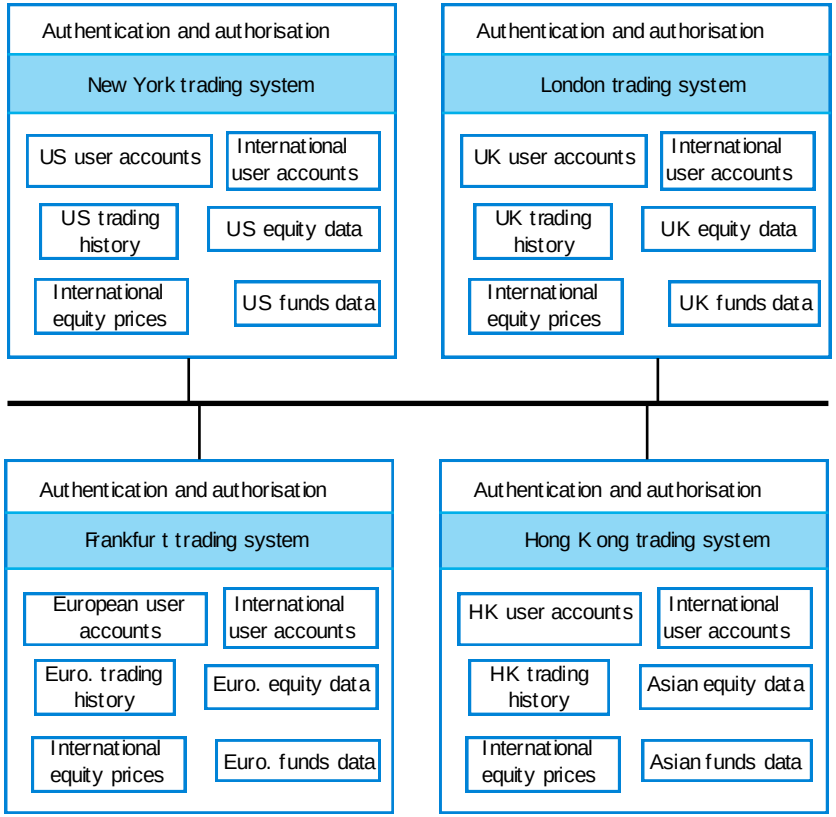
Заштита

- Заштита на нивоу платформе
- Заштита на нивоу апликације
- Заштита на нивоу података

Слојна заштита



Дистрибуирана једнакост система



Дизајн смернице

- Дизајн смернице обухватају добру праксу у безбедном дизајну система имају два циља:
  - Подижу свест о питањима безбедности у тиму софтверског инжењерства.
  - Могу се користити као основа за ревизију листи која се примењује током процеса провере система.

Дизајн смернице 1

- Основне безбедносне одлуке о експлицитној безбедносној политици.
- Избегавајте једну тачку неуспеха.
- Безбедни неуспех.
- Баланс безбедности и употребљивости.
- Будите свесни могућности друштвеног инжењеринга.

Дизајн смернице 2

- Користите редундантност и разноликост да смањите ризик.
- Проверите све улазе.
- Дизајн за распоређивање.
- Дизајн за опоравак способности.

Закључак

- СЕ брине о безбедности система и брани систем од злонамерних напада.
- Безбедносне претње могу бити претња поверљивости или доступности система или његових података.
- Дизајн за безбедност подразумева архитектонско пројектовање, уз праћење добре праксе дизајна и минимизирања увођења система рањивости.
- Кључна питања код пројектовања сигурне архитектуре укључује организовање структуре за заштиту имовине и расподела средстава да се смање губитци.
- Опште безбедносне смернице наводе дизајнера на безбедносна питања и да корсити као ревизију контролне листе.

Key points

- Security engineering is concerned with how to develop systems that can resist malicious attacks
- Security threats can be threats to confidentiality, integrity or availability of a system or its data
- Design for security involves architectural design, following good design practice and minimising the introduction of system vulnerabilities
- Key issues when designing a secure architecture include organising the structure to protect assets and distributing assets to minimise losses
- General security guidelines sensitise designers to security issues and serve as review checklists