Развој безбедног софтвера

Дизајн безбедног софтвера

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

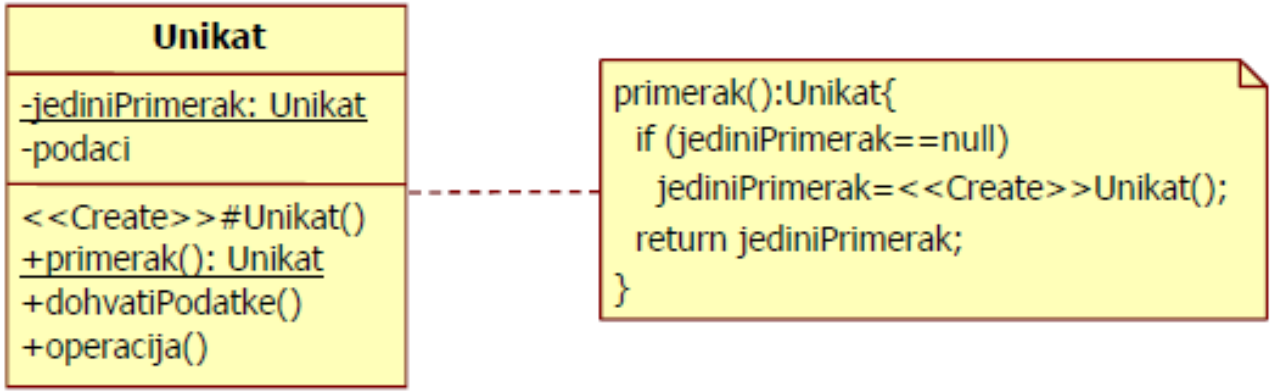
Садржај

- Безбедносни пројектни узорци
- Каталог безбедносних узорака
- Принципи безбедног дизајна

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Безбедносни узорци

- Софтверски пројектни узорак (*software design pattern*) је генерално, реупотребљиво решење проблема који се често јавља у одређеном контексту приликом дизајнирања софтвера



- https://rti.etf.bg.ac.rs/ir4ps

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Безбедносни узорци

- Безбедносни узорак (*security pattern*) описује решење за проблем контролисања (заустављања или избегавања) скупа специфичних претњи кроз неки сигурносни механизам дефинисан у одређеном контексту
- Безбедносни узорци помажу софтверским инжењерима који нису стручњаци у области безбедности да додају безбедносни аспект у свој дизајн

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Безбедносни пројектни узорци

- Безбедносни узорци могу бити архитектурални узорци (*architectural patterns*) када описују глобалне софтверске архитектуралне концепте (нпр., PKI, мрежна сегрегација, итд.)
- Безбедносни узорци могу бити пројектни узорци (*design patterns*) када описују структуре на нивоу кода апликације (нпр., валидација уноса, логовање, управљање изузецима, итд.)
- Безбедносни узорци могу обухватати и оба нивоа: архитектурални и пројектни (нпр., домен контролер и др.)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Анатомија безбедносног узорка

Проблем

- Контекст у коме проблем постоји и у коме је решење из узорка применљиво
- Опис безбедносног проблема у идентификованом контексту
- Примери сценарија

Решење

- Идеја узорка
- Структура решења из узорка
- Динамички аспекти решења
- Упутство за имплементацију
- Примери решавања сценарија
- Последице
- Познате примене

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Каталог безбедносних узорака

Тајност

- Симетрично шифровање
- Асиметрично шифровање

Интегритет

- Хеш функције
- Дигитални потписи
- Валидација уноса
- Сигурни бафер података

Доступност

- Дизајн високе доступности
- Мерачи перформанси
- Филтери

Аутентикација

- Аутентикатор

Ауторизација

- Контрола приступа помоћу улога
- Листе за контролу приступа

Одговорност

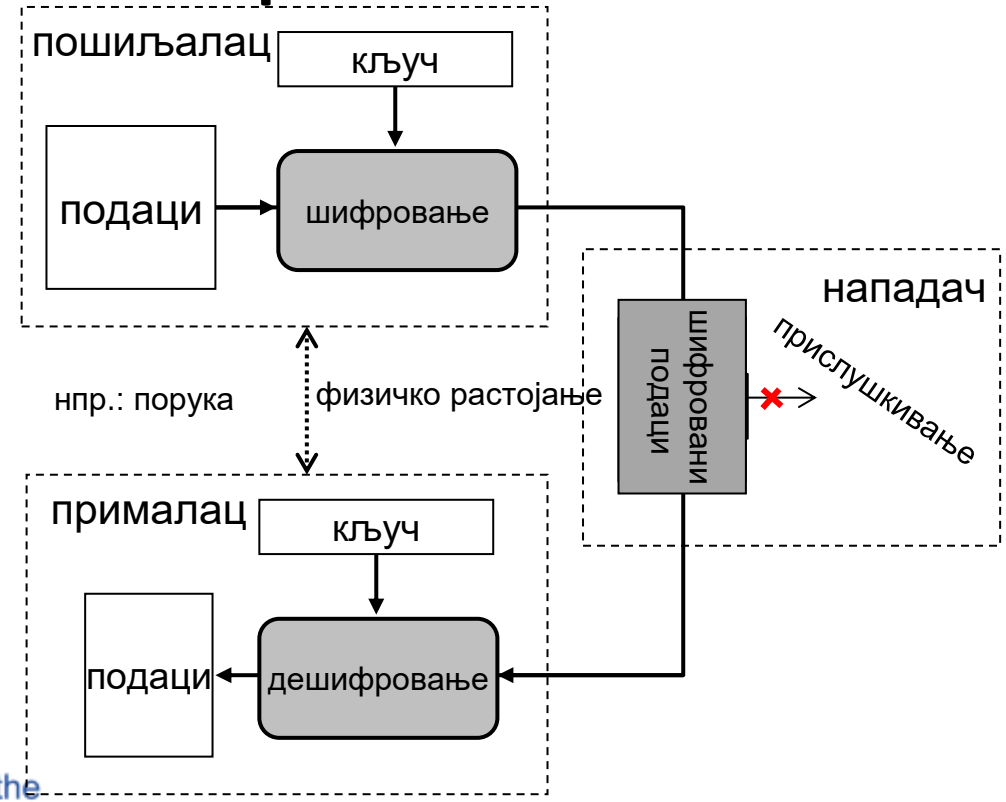
- Логер

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Тајност – опис проблема

Проблем

- Два учесника у комуникацији (нпр., претраживач и сервер) желе да размене тајну вредност
- Без потпуне контроле над комуникационом инфраструктуром претпоставка је да тајна вредност може бити пресретнута и прочитана од стране нападача
- Нпр. WiFi приступна тачка у ресторану логује саобраћај и сакупља креденцијале корисника за различите сервисе



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Тајност - идеја

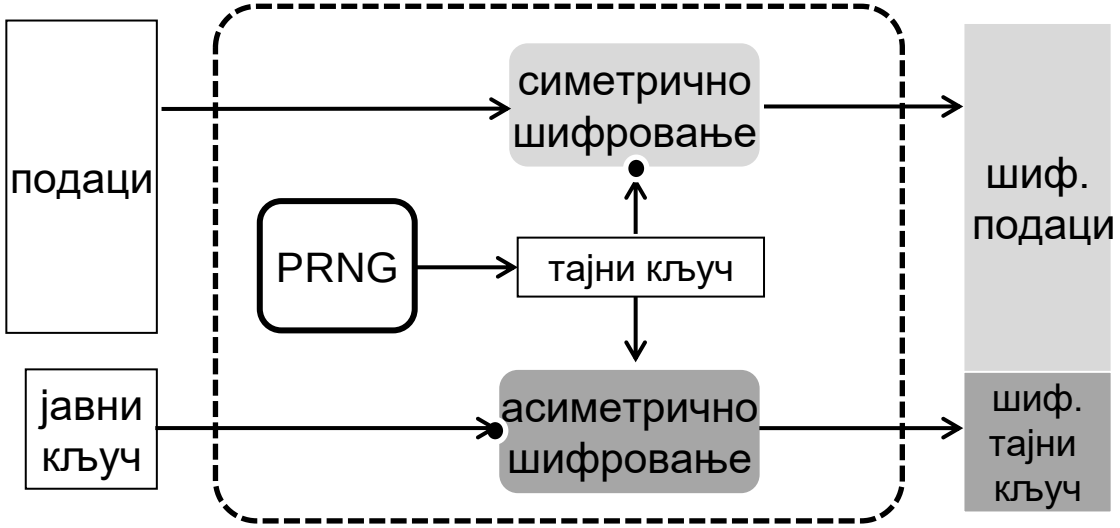
- Шифровање трансформише обичан текст (*plaintext*) у шифровани текст (*cyphertext*) уз помоћ кључа (*key*)
- Докле год је кључ тајни и користе се безбедни алгоритми, нападач не може да открије оригинални обичан текст
- **Симетрично шифровање** – исти кључ за шифровање и дешифровање
  - Предности и недостаци?
- **Асиметрично шифровање** – једна кључ за шифровање, други за дешифровање
  - Предности и недостаци?

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Тајност – хибридна шема

- Асиметрично шифровање је спорије и захтева кључеве веће дужине
- Проблем брзине могуће је решити хибридном шемом



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Шифровање – проблеми у пракси?

Проблеми са управљањем кључевима

- Кључеви генерисани слабим алгоритмима
- Кључеви нису складиштени и преношени на безбедан начин

Слабости протокола

- Користе се небезбедни алгоритми
- Користи се небезбедна конфигурација (мод рада, допуна, дужина кључа)

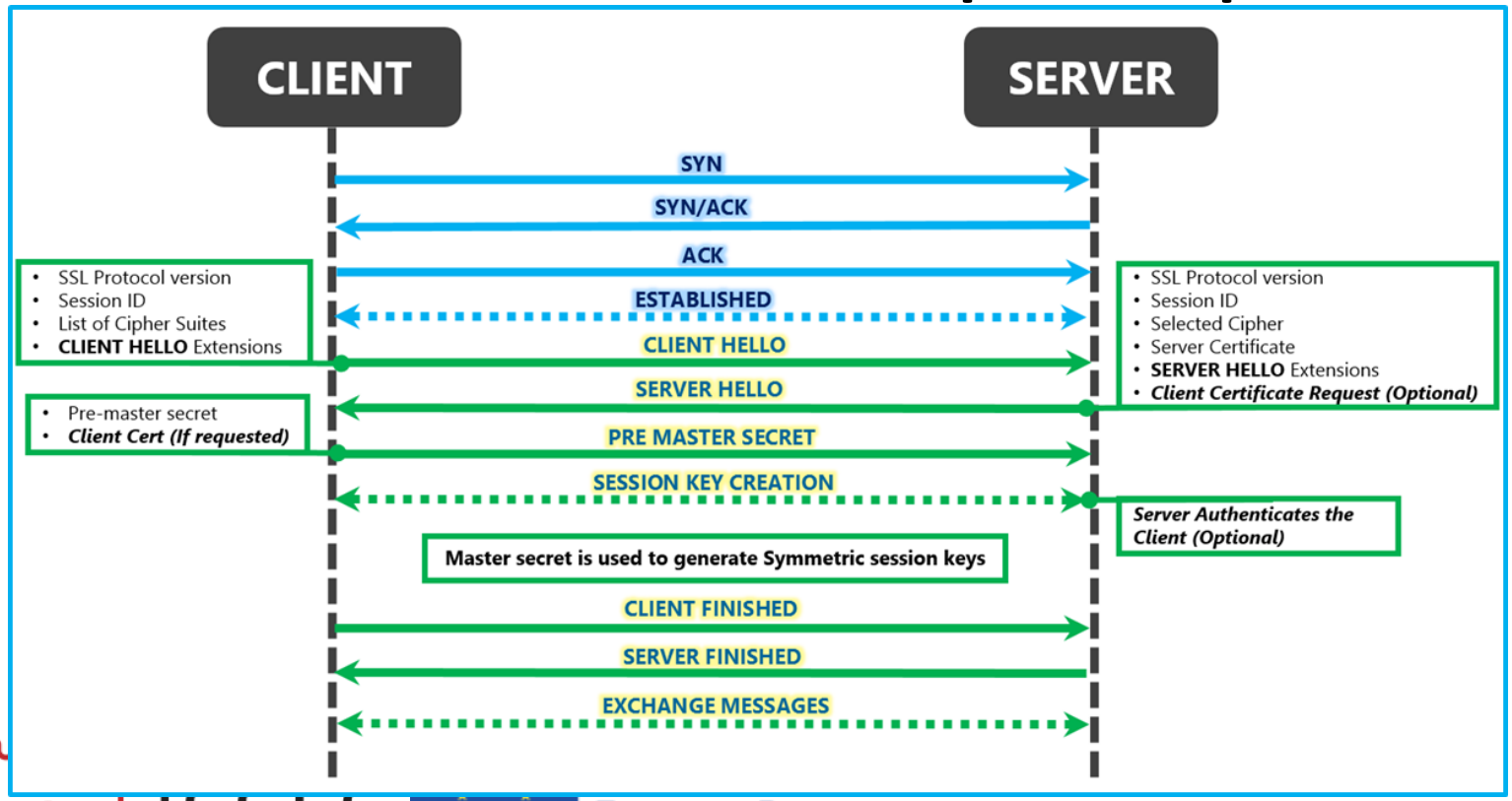
Имплементациони проблеми

- Грешке у имплементацији
- Бочни напади (нпр. временски напади, диференцијална анализа, итд.)

Људске грешке

ISSES
Co-funded by the Erasmus+ Programme of the European Union

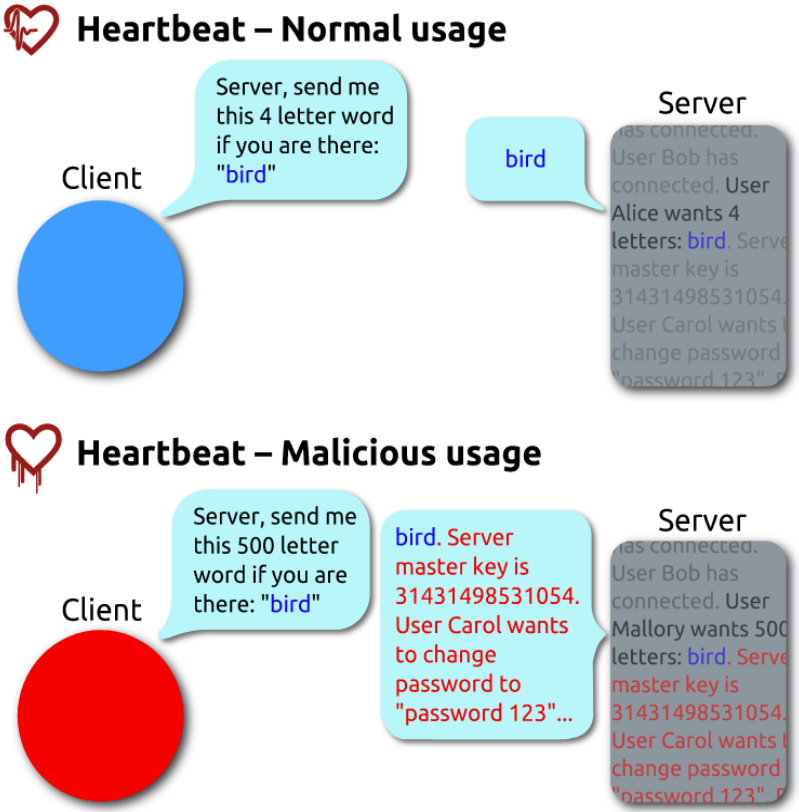
HTTPS - пример



TLS протокол

Heartbleed

- OpenSSL имплементација TLS протокола имала је сигурносни пропуст (*buffer underflow*) чак две године
- Пример имплементационог пропуста

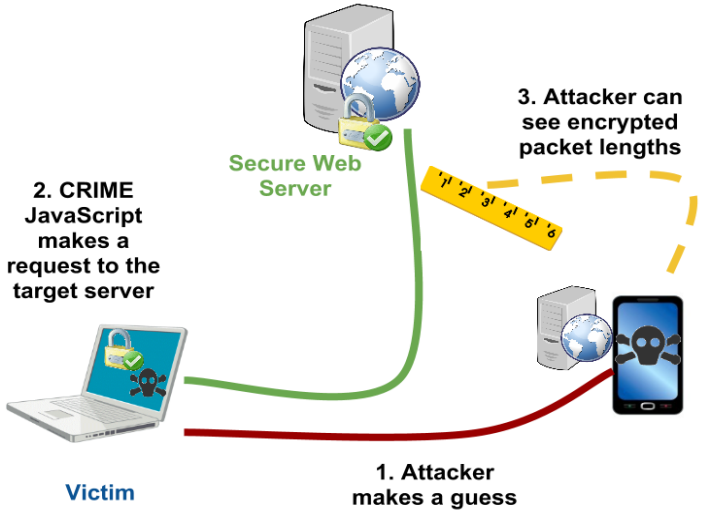


ISSES
Co-funded by the Erasmus+ Programme of the European Union

Compression Ratio Info-leak Made Easy

GET /twid=0
Host: twitter.com
User-Agent: Chrome
Cookie: twid=71bc3e...

- На основу TLS компресије и чињенице да нападач може да види дужину захтева
- **len(encrypt(compress(input + public + secret)**
  - input – URL
  - public – Known headers
  - secret – Cookie
- Нападач мора бити у могућности да прислушкује саобраћај и да упути велики број захтева у име жртве
- Пример слабости протокола



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Тајност - закључак

- Чак и добро познате сигурносне контроле имају слабости
- Укључивањем сигурносне контроле посао није завршен
- За све сигурносне контроле треба:
    - Разумети шта им је сврха – избећи пропусте у дизајну
    - Истражити која је добра пракса за конфигурацију – избећи лошу конфигурацију
    - Истражити који су поуздани пружаоци услуге – избећи имплементационе проблеме
    - Бити у току са променама

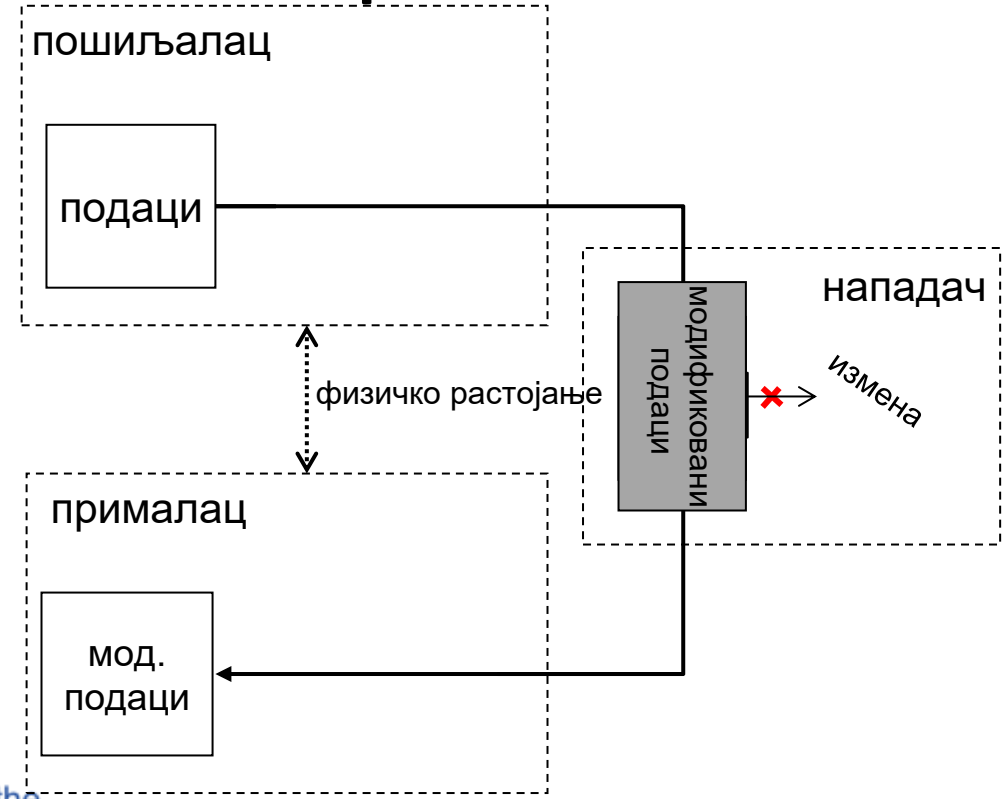
ISSES

Co-funded by the Erasmus+ Programme of the European Union

Интегритет – опис проблема

Проблем

- Два учесника у комуникацији (нпр. претраживач и сервер) желе да размене податке
- Без потпуне контроле над комуникационом инфраструктуром претпоставка је да подаци могу бити измењени од стране нападача
- Нпр. WiFi приступна тачка у ресторану мења све захтеве за плаћањем тако да измени примаоца средстава



ISSES
Co-funded by the Erasmus+ Programme of the European Union

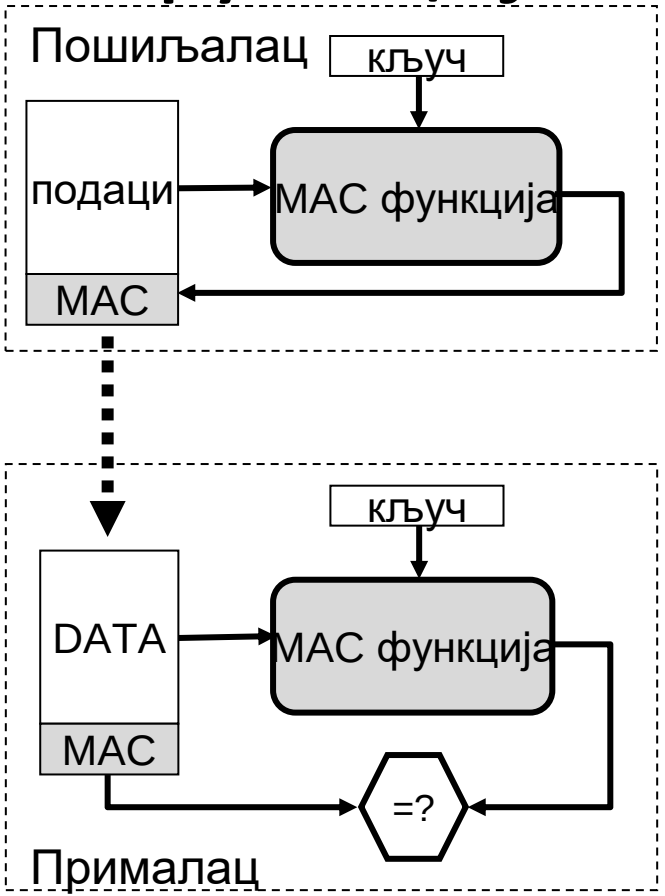
Интегритет - идеја

- Криптографске хеш функције мапирају податке произвољне дужине у излаз фиксне дужине
- Хеш функција треба да задовољи следеће особине:
  - Да је детерминистичка, како би иста порука увек произвела исту хеш вредност
  - Брзо се израчунава хеш вредност за било коју поруку
  - Није замисливо да је могуће реконструисати поруку од њене хеш вредности
  - Мала промена у поруци мења хеш вредност тако да нема корелације са претходном
  - Није замисливо да је могуће пронаћи две различите поруке са истом хеш вредношћу

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Интегритет – MAC функције

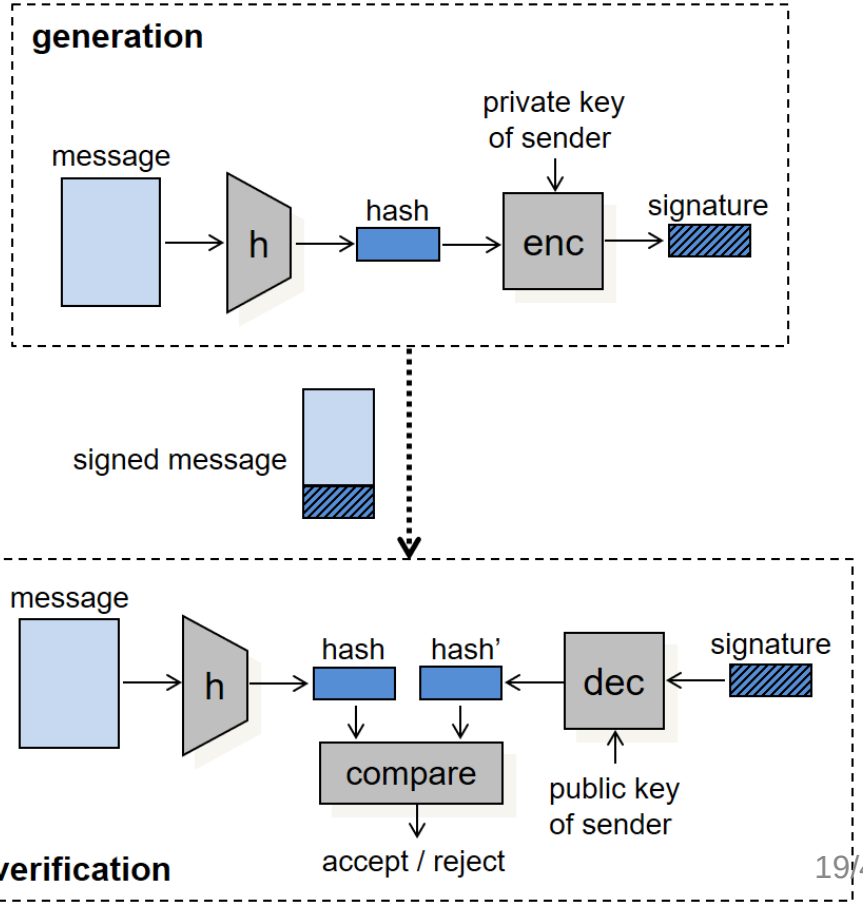
- Сличне као хеш функције, али користе симетрични кључ као додатни улазни параметар
- Користе се за заштиту интегритета поруке и аутентикацију порекла поруке



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Интегритет – дигитални потписи

- Слично као MAC функције, али се користе асиметрични клучеви
- Поред интегритета и порекла, штити се и непорецивост



Интегритет – валидација уноса

Проблем

- Апликација прихвата податке од екстерних извора (нпр. корисника преко интернета, фајл система, екстерних сервиса трећих страна)
- Улазни подаци могу утицати на извршавање наредби (нпр. SQL базе података, XML парсери, OS наредбе)
- Софтверски инжењери тестирају производ како би утврдили да ради исправно (функционално тестирање)
- Шта се дешава уколико се пошаљу бесмислени подаци? Шта се дешава уколико се пошаљу пажљиво осмишљени подаци за напад извршавањем наредби?
- Нпр. нападач жели да обрише базу података апликације

ISSES
Co-funded by the Erasmus+ Programme of the European Union

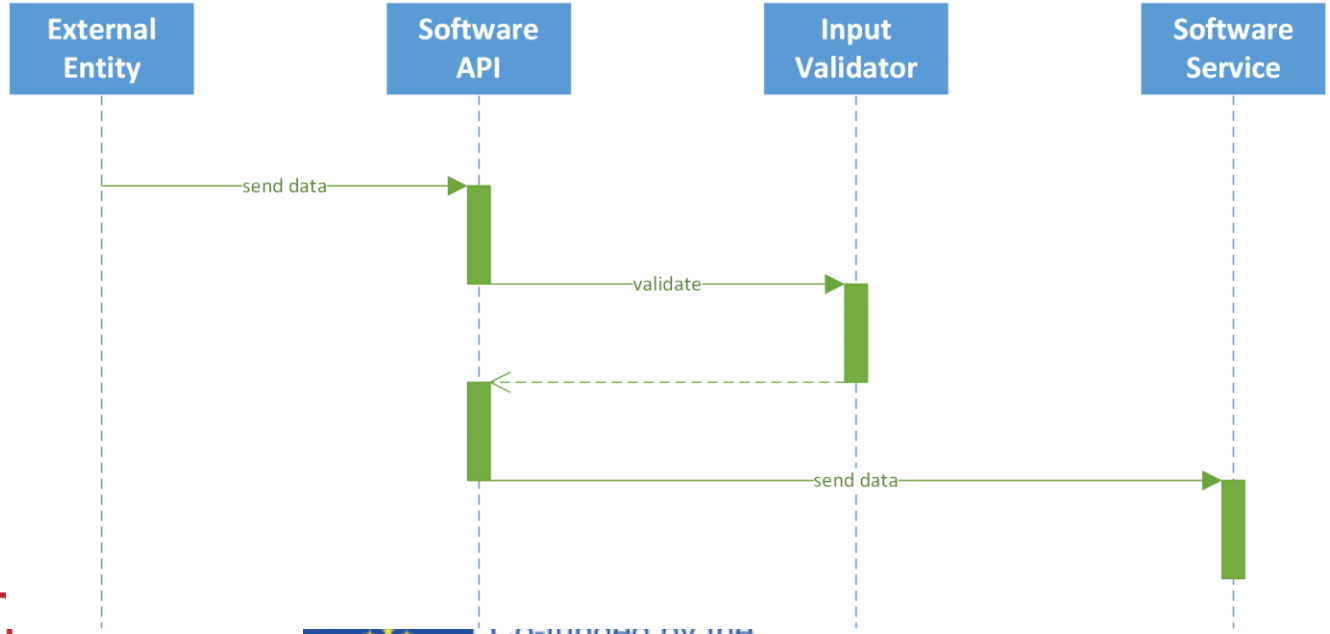
Интегритет – валидација уноса (2)

- Тестирање сваког уноса који долази од спољног извора (нпр. корисника, апликације)
- Спречавање неправилно формираних података од уласка у систем
- Улазни подаци треба да буду проверени на правила која увек морају бити испоштована (нпр. Поље је стринг од максимално 20 карактера или број који није већи од 1000)
- Стандардни улазни типови (нпр. JSON, XML, упит базе података) имају испробане и тестиране механизме за валидацију уноса (нпр. XSD шеме, припремљени упити (*prepared statements*))

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Интегритет - валидација уноса (3)

- Као и са многим другим сигурносним контролама може се дефинисати као један аспект у објектно-оријентисаним језицима



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Интегритет – сигурни бафер података

Проблем

- У питању су програмски језици који немају уграђену проверу граница низа.
- Дешава се прекорачење бафера када процес упише податке иза границе бафера фиксне дужине.
- Проблем је имплементационе природе и може се решити провером дужине низа и границе низа приликом уписа.
- Нападач који искористи овај пропуст може да изврши произвољни код и преузме контролу над ОС.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Интегритет – сигурни бафер података

Решење

- Представити бафер као структуру података која укључује информације о дужини и алоцираној меморији.
- Када се ради са бафером проверавати дужину и доступну меморију пре уписивања.
- (qmail) Пример у језику C за рад са стринговима уместо коришћења терминалног карактера користити структуру `stralloc`:

```
typedef struct stralloc{
        char *s;          //pokazivac na string ili 0
        unsigned int len; //duzina u bajtovima
        unsigned int a;   //broj alociranih bajtova u stringu
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Доступност – опис проблема

Проблем

- Оптерећење (*workload*) апликације у фази развоја представља само делић оптеречења у продукцији
- Одбијање услуге (*denial of service*) може се догодити уколико се не обезбеди довољно ресурса за захтеве легитимних корисника
- Постоји и напади коришћењем мреже ботова који могу да изведу DDoS напад како би “угасили” одређени сервис
- Хардверски проблем или природна катастрофа може уништити машину на којој је покренут неки сервис

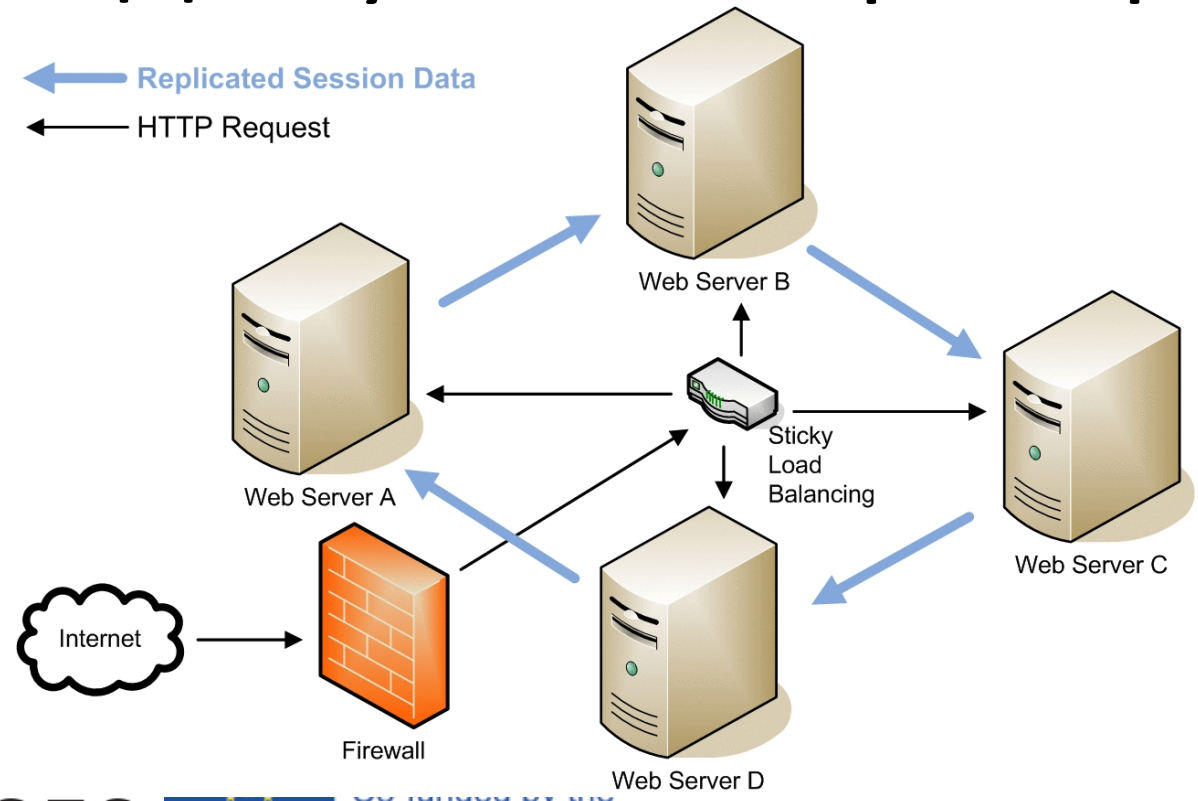
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Доступност – идеја

- Као што се безбедност заснива на заштити најслабије карике, тако се и доступност заснива на откривању и решавању уских грла у систему
- Мерачи перформанси могу да помогну инжењерима да детектују места у апликацији која се често користе и захтевају доста ресурса
- Редудантне инсталације апликације (*application deployments*) значајно повећавају доступност система (нпр. кластери са балансером оптерећења)
- Редудантне инсталације система помажу у очувању доступности када је читава локација угрожена (нпр. локације са инсталацијом система у случају катастрофе - *disaster recovery site*)
- Фајервол помаже у филтрирању саобраћаја и може заштитити апликацију у случају DDoS напада

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Доступност – пример



ISSES
Erasmus+ Programme
of the European Union

Аутентикација – опис проблема

Проблем

- Екстерни субјекат (нпр. корисник, сервис) жели да приступи подацима или позове функцију апликације
- Власник апликације жели да има контролу ко може да приступи подацима и функцијама
- Апликација мора да пружи могућност идентификације, тј. Да има листу дигиталних идентитета за сваког регистрованог екстерног субјекта
- Шта се дешава када један екстерни субјекат тврди да је други екстерни субјекат пружајући одговарајући идентификатор?

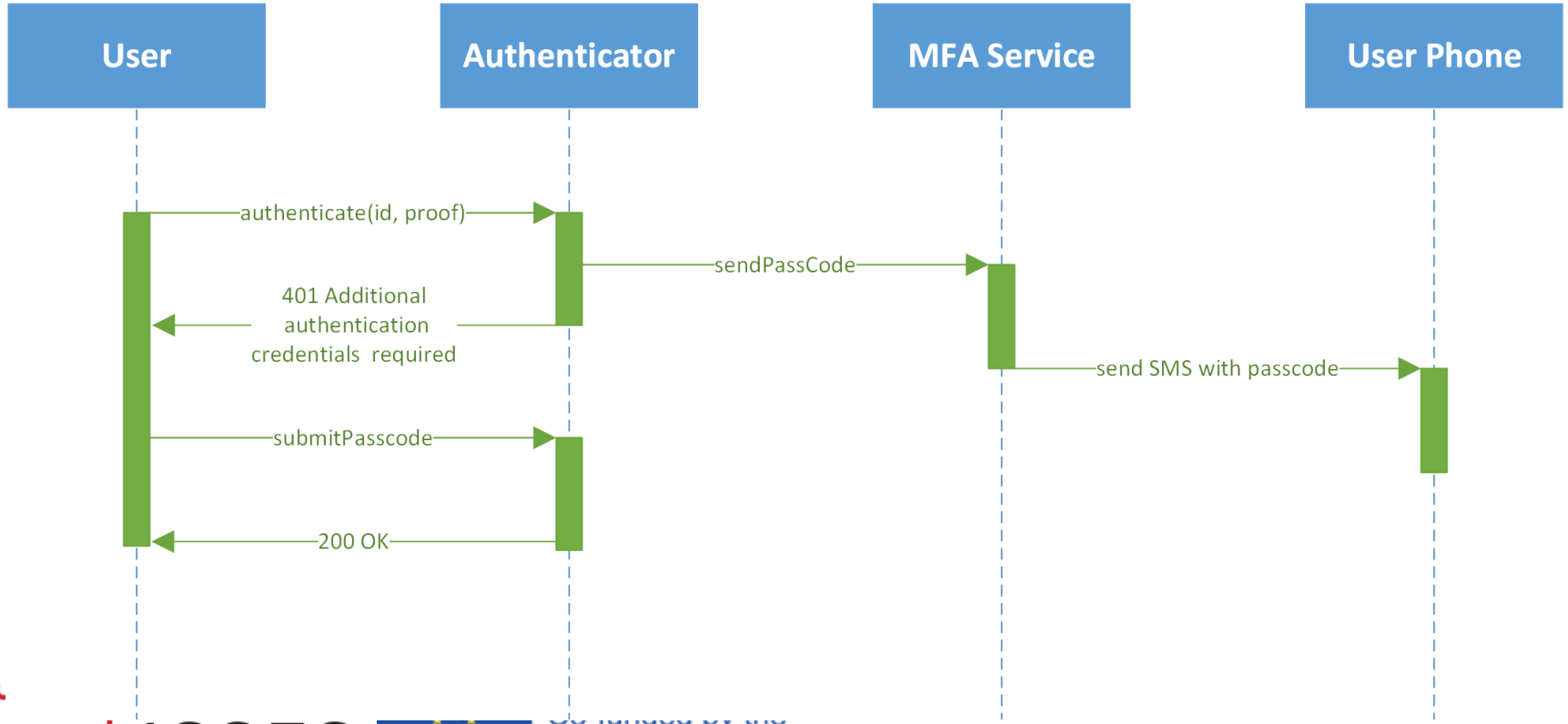
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Аутентикација – идеја

- Аутентикација је процес доказивања тачности тврдње као што је идентитет субјекта
- Нешто што корисник зна – лозинка, PIN
- Нешто што корисник има – PKI, токен
- Нешто што корисник јесте – биометрија
- Вишефакторска

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Аутентикација – пример



ISSES
Erasmus+ Programme of the European Union

Ауторизација – опис проблема

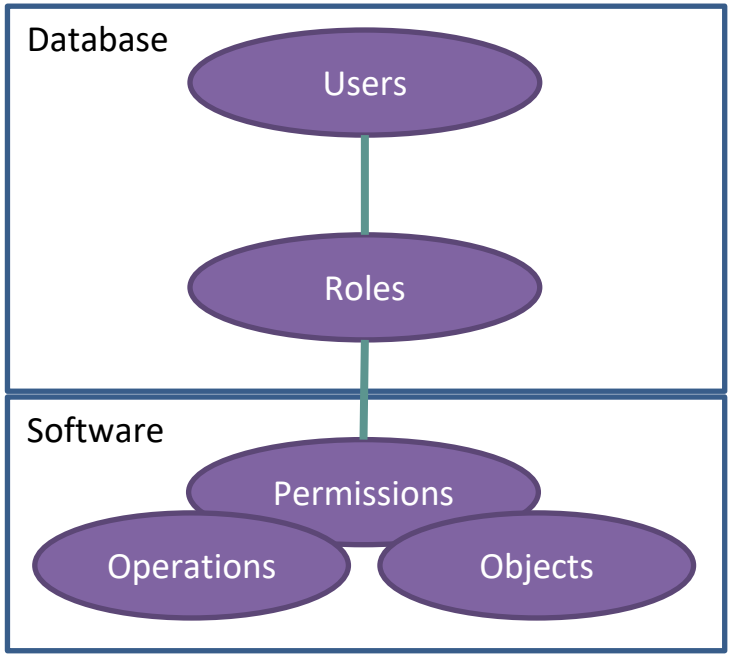
Проблем

- Аутентификовани субјекат (нпр. корисник, сервис) жели да приступи подацима или позове функцију апликације
- Апликација садржи осетљиве податке и функције које не би требало да буду доступне свим корисницима
- Контрола приступа треба да буде примењена за све субјекте и објекте узимајући у обзир:
  - Да субјекти и објекти могу бити додавани, модификовани и уклањани из система
  - Додељивање права приступа треба да буде реализовано на једноставан начин

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Контрола приступа помоћу улога

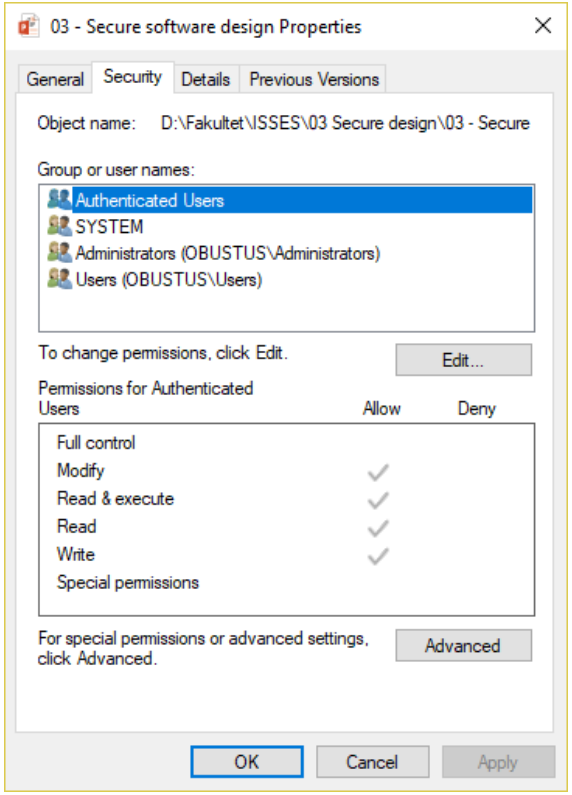
- Већина организација има широк дијапазон улога (позиција) у организацији – инжењер, контрола квалитета, менаџер, администратор
- Свака улога носи са собом различите одговорности – писање кода, извршавање тестова, управљање логовима, одржавање инфраструктуре
- RBAC модел се базира на организационој структури и нуди флексибилан централизовани начин администрације



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Листе за контролу приступа

- RBAC модел је погодан када можемо одредити класе корисника и објеката
- Оперативни систем може имати произвољно велики број корисника од којих сваки има свој засебни фајл систем
- У том случају RBAC матрица би била превелика
- ACL разрешава овај проблем дистрибуирајући права приступа на објекте, чиме се отежава управљање, али повећава ефикасност



Одговорност

Проблем

- Субјекат може да тврди да се нешто догодило када заправо није
- Субјекат може да тврди да се нешто није догодило када заправо јесте
- Порецивост је озбиљна претња у сваком систему

Идеја

- Дигитални потписи обезбеђују непорецивост поруке
- Шта се дешава ако је PKI превише скуп или непрактичан да би био примењен?
- Систем за логовање догађаја може бити дизајниран да разреш овај проблем

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Принципи безбедног дизајна

Доделити најмање потребне привилегије

Раздвојити одговорности

Опрезно додељивати поверење

Користити једноставна решења

Бележити осетљиве догађаје

Обезбедити грешке и користити сигурне подразумеване акције

Не ослањати се на нејасност

Имплементирати одбрану у дубину

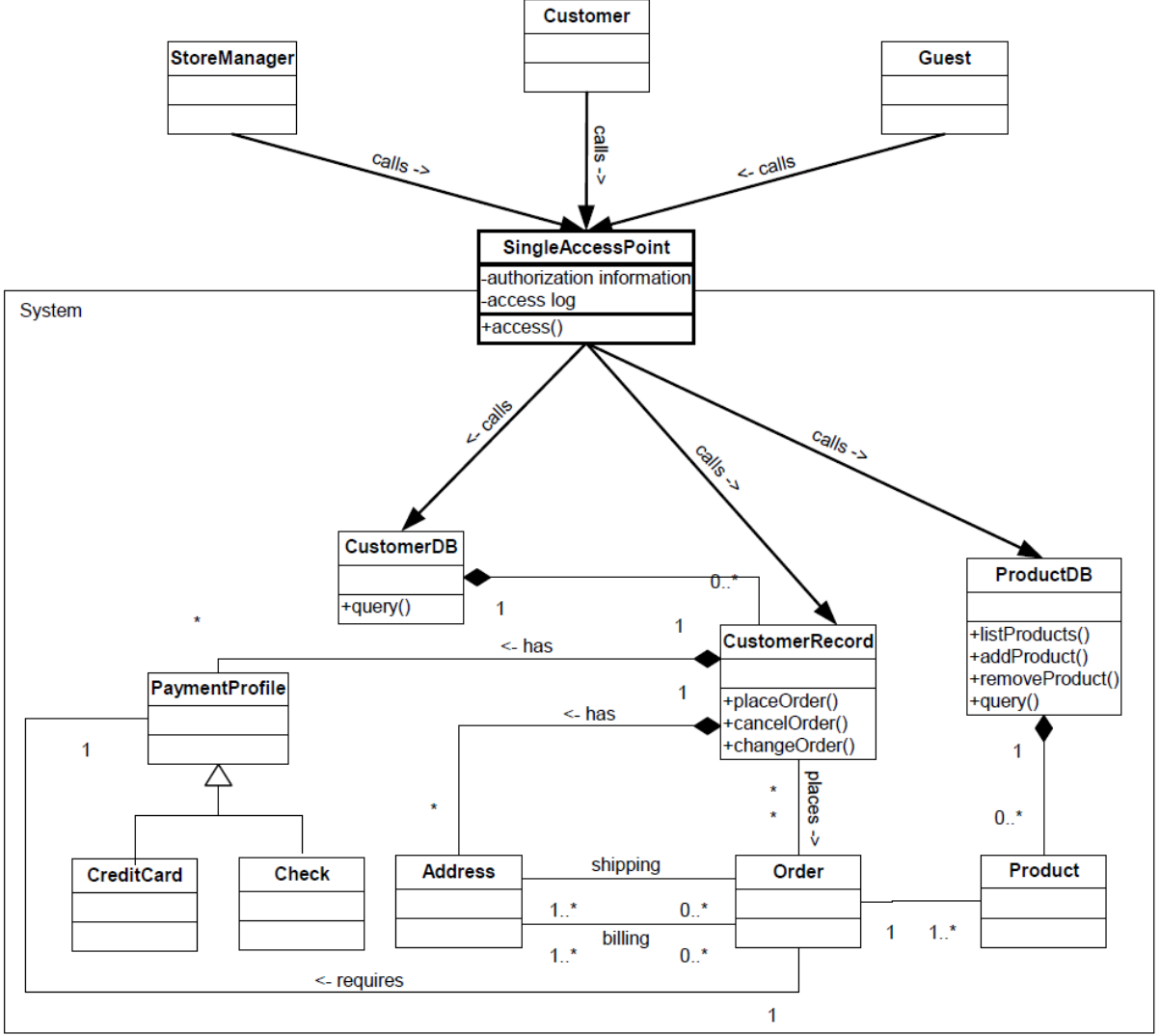
Не измишљати безбедоносну технологију

Осигурати најслабију карику

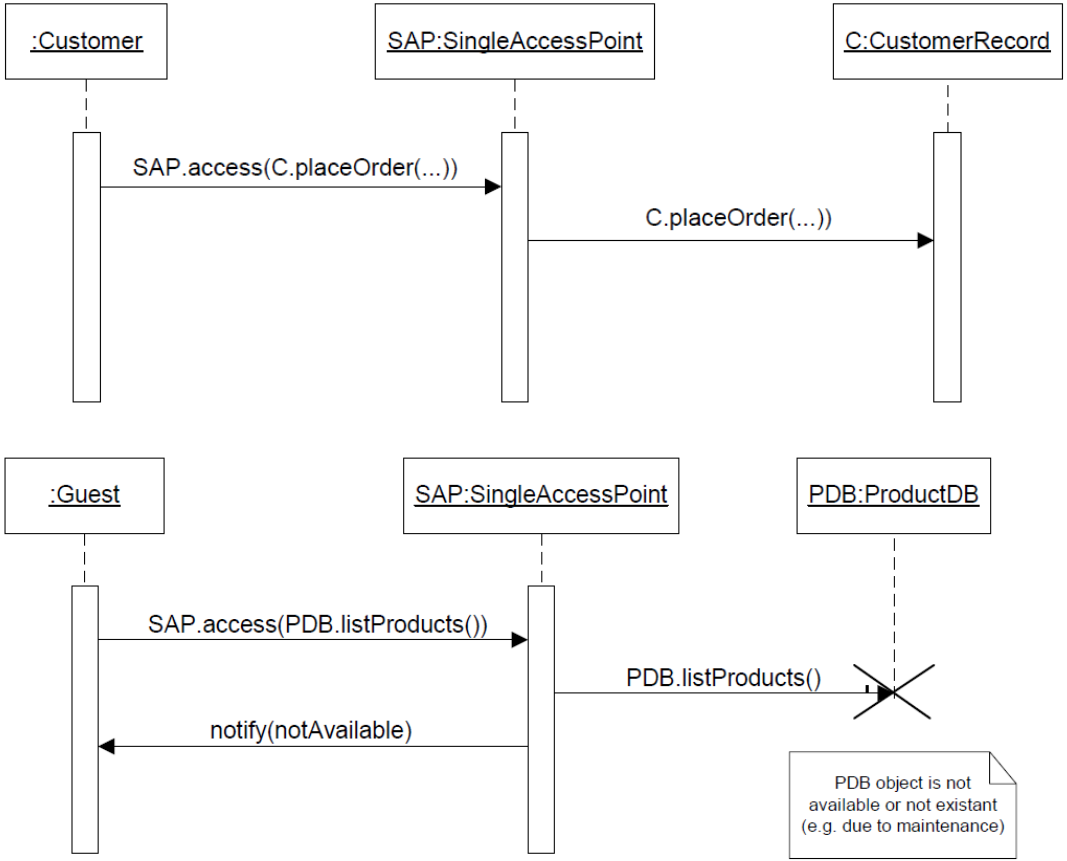
ISSES

Co-funded by the Erasmus+ Programme of the European Union

Пример безбедносног узорка – Single Access Point



Пример безбедносног узорка – Single Access Point



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Пример безбедносног узорка – Single Access Point

Доделити најмање потребне привилегије

Раздвојити одговорности

Опрезно додељивати поверење

Користити једноставна решења

Бележити осетљиве догађаје

Обезбедити грешке и користити сигурне подразумеване акције

Не ослањати се на нејасност

Имплементирати одбрану у дубину

Не измишљати безбедоносну технологију

Осигурати најслабију карику

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Сигурна размена порука

Вежба – осмислити решење

Ана шаље поруку Петру:

- Трећа страна не сме видети поруку
- Петар зна да је порука стигла од Ане
- Ана не може порећи да је послала поруку
- У поруци нема злонамерног садржаја
- Минимална количина пропусног опсега се користи

1. Које операције треба спровести?
2. Којим редоследом?
3. Који су предуслови?
4. Које су претпоставке о окружењу?

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Једноставна контрола приступа

Вежба – осмислити решење

- Систем има 5 објеката и 5 субјеката
- Систем има 5000 објеката и 5 субјеката
- Систем има 5 објеката и 5000 субјеката
- Систем има 5000 објеката и 5000 субјеката

Колико је тешко променити мапирање права приступа?

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Механизам логовања

Вежба – осмислити решење

- Потпуност – улази садрже довољно података и сви догађаји који су битни за непорецивост су забележени
- Поузданост – обезбедити доступност механизма и интегритет логова
- Тачност – улази у оквиру система имају прецизно забележено време
- Употребљивост – догађаји везани за безбедност се лако могу извући из логова
- Минимализам – креирати минималну количину логова потребних да испуне сврху

ISSES
Co-funded by the Erasmus+ Programme of the European Union

ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Развој безбедног софтвера подразумева изучавање различитих механизама којима се нарушава информациона безбедност и врше напади на интернет апликације и софтверске системе.
- Примена ових механизама када се извршавају према системима физичких и правних лица која нису упозната и сагласна са активностима на провери рањивости и тестирању упада у њихове системе је кажњива према Кривичном законику Републике Србије (Чланови 298 до 304а).
- Студенти на предмету Развој безбедног софтвера могу ове методе за потребе изучавања да користе искључиво у оквиру затвореног лабораторијског окружења које је обезбеђено за наставу на предмету Развој безбедног софтвера.
- Студенти не могу да подразумевају да су на било који начин охрабрени од стране наставника или да им се препоручује да користе ове методе који се изучавају према другим апликацијама Електротехничког факултета или апликацијама било ког трећег правног или физичког лица.
- Свака евентуална активност коју би предузео неки студент коришћењем ових метода и механизама према апликацијама које нису у оквиру лабораторије на предмету искључива је одговорност студента.

ISSES
Co-funded by the Erasmus+ Programme of the European Union