Развој безбедног софтвера

Сигурносни захтеви

ISSES

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

Садржај

- Смишљање сигурносних захтева
- Експлицитни сигурносни захтеви
  - PCI DSS
- Квалитативни сигурносни захтеви
  - Случајеви злоупотребе
  - Нападачка стабла

ISSES

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

Пословни захтеви насупрот софтверским захтевима

- Пословни захтеви (*Business requirements*) се односе на пословне циљеве и дефинишу оквир потребе или проблема који треба решавати кроз конкретну активност или пројекат

- Софтверски захтеви (*Software requirements*) треба да установе кораке специфичне за софтвер који су потребни како би се испунили пословни захтеви

- Пословни захтеви одговарају на питање ***зашто?*** се неки пројекат реализује, док софтверски захтеви одговарају на питање ***шта?*** треба радити на пројекту

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

Прикупљање захтева

- Софтверски захтев представља функционалност софтвера која је потребна кориснику да реши неки проблем или да испуни неки циљ
- Смишљање захтева (*Requirement engineering*) представља процес дефинисања корисничких очекивања приликом развоја новог софтвера или модификовања постојећег
- Велики изазов за софтверске инжењере је да усагласе своју визију производа који развијају са визијом корисника – све заинтересоване стране у пројекту морају имати заједничко виђење шта ће финални производ представљати
- Да би решили овај изазов потребни су начини да се прецизно забележе, разумеју и представе потребе корисника приликом дефинисања спецификације софтверског производа

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

Прикупљање захтева (2)

- Потребно је да захтеви буду конкретни (***S**pecific*), прецизно дефинисани, са довољно детаља потребних за дизајнирање софтвера
- Захтеви треба да буду мерљиви (***M**easurable*), достижни (***A**ttainable*) и разумни (***R**easonable*)
- Потребно је да је захтеве могуће пратити кроз процес развоја (***T**raceable*)
- Смишљање захтева укључује три врсте активности:
  - Конструисање захтева (*Eliciting requirements*) – у комуникацији са корисницима утврдити њихове потребе
  - Анализа захтева (*Analyzing requirements*) – утврђивање да ли су конструисани захтеви нејасни, некомплетни, двосмислени или контрадикторни и исправљање уочених недостатака
  - Моделовање захтева (*Requirements modeling*) – захтеви се могу приказати на различите начине, нпр. текстуалним описом, случајевима коришћења, корисничким причама, спецификацијом процеса, итд.

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

Конструисање сигурносних захтева

- Корисник углавном не поседује довољно знања да би дефинисао конкретан сигурносни захтев за софтвер
  - Корисник ће умети да искаже да жели да се функција X изврши када притисне дугме Y
  - Корисник неће исказати да функција X треба да буде отпорна на напад убацивањем наредби (*command injection attack*)
- Корисник углавном уме да искаже сигурносне захтеве на високом нивоу апстракције
  - Потребно је испоштовати све законске одредбе везане за информациону безбедност (избећи казне)
  - Потребно је обезбедити неометан рад система
  - Потребно је очувати поверење корисника
  - Потребно је заштитити бренд

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

Анализа сигурносних захтева

- Анализа сигурносних захтева подразумева декомпоновање пословних сигурносних захтева у одлуке приликом дизајнирања и имплементационе задатке приликом развоја производа
- Потребно је утврдити шта је потребно заштитити и како то урадити
  - Како знати да ли је нешто заштићено?
- Сигурносне захтеве можемо анализирати из две перспективе:
  - Грануларност
  - Извор

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

Грануларност сигурносних захтева

- Висок ниво апстракције
  - На основу *CIA (confidentiality, integrity, availability)* и *AAA (authentication, authorization, auditing)*
  - Очувати тајност поверљивих података (*personally identifiable information – PII)*
  - Контрола приступа до поверљивих података
- Низак ниво апстракције
  - Везан за конкретан програмски код и конфигурацију
  - Уградити проверу контроле приступа у функције које читају поверљиве податке; користити принцип најмањих потребних привилегија
  - Шифровати поверљиве податке приликом транспорта између сервиса А и сервиса В
  - Уградити валидацију корисничког уноса за све податке који се шаљу до базе у којој се налазе поверљиви подаци

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

Извор сигурносних захтева

- Експлицитни сигурносни захтеви
  - Повезани са званичним регулативама (закони, регулативе, стандарди, правилници)
  - Могу бити високог нивоа апстракције (нпр. заштитити приступ медицинским подацима) или ниског нивоа апстракције (нпр. корисничке лозинке би требале да имају барем 8 карактера)
  - Обично је овакве захтеве једноставније идентификовавати, имплементирати, тестирати и пратити
- Квалитативни сигурносни захтеви
  - Изведени на основу посматрања система из перспективе нападача (нпр. моделовање претњи, примери злоупотребе система, итд.)
  - Грануларност зависи од циља анализе (нпр. висок ниво апстракције за дефинисање архитектуре система, низак ниво апстракције за случајеве коришћења)
  - Идентификација и анализа оваквих захтева се у великој мери ослања на стручност сигурносног аналитичара

Експлицитни сигурносни захтеви

- Стандард у области информационе безбедности је документ који је одобрен од стране признатог и препознатог тела за стандардизацију, који описује правила, даје смернице и описује карактеристике за заштиту производа од напада; усаглашеност са стандардом није обавезна
  - ISO 27001, NIST 800-53
- Регулатива у области информационе безбедности садржи директиве за заштиту информационих технологија и рачунарских система, као и инструкције за компаније и организације за заштиту њихових система и информација од напада; усаглашеност са регулативом је обавезна
  - GDPR, NERC CIP

Пример: PCI DSS

- *Payment Card Industry Data Security Standard - PCI DSS*
- Технички стандард чији је циљ да се заштити тајност података са кредитних и дебитних картица (*cardholder data - CHD*)
- Задатак је да се спрече преваре са кредитним картицама тако што би приступ CHD подацима био омогућен само организацијама које прихватају уплате и обрађују ове податке на легалан начин
- Састоји се од 12 секција са захтевима који обухватају:
  - Људске ресурсе и процесе у оквиру организације (документа, процедуре, свест запослених)
  - ИКТ инфраструктуру (мрежа, фајервол, оперативни систем, антивирус)
  - Техничке детаље апликативног софтвера

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

PCI DSS - преглед

Захтеви	Одговорност
1. Инсталирати и одржавати фајервол конфигурацију	ТП
2. Не користити подразумеване лозинке и друге сигурносне параметре	ТП
3. Заштитити сачуване податке власника картице (*CHD*)	ТП, Развојни тим
4. Шифровати *CHD* приликом преноса кроз отворене јавне мреже	ТП, Развојни тим
5. Користити и редовно ажурирати антивирусне програме	ТП
6. Развијати и одржавати сигурне системе и апликације	Развојни тим
7. Ограничити приступ до CHD само по пословним потребама (need to know)	ТП, Развојни тим
8. Доделити јединствен идентификатор свакој особи са приступом рачунару	ТП
9. Ограничити физички приступ до CHD	ТП
10. Пратити и надзирати све приступе мрежним ресурсима и CHD	ТП, Развојни тим
11. Редовно тестирати сигурносне системе и процедуре	ТП, Контрола квалитета
12. Одржавати полису која описује сигурносне аспекте за сво особље	Менаџмент

Заштитити сачуване податке власника картице (з.3)

3.1 Обезбедити да се CHD подаци чувају минимално колико је потребно; успоставити процедуру складиштења података и уклањања непотребних података

3.2 Не треба складиштити осетљиве аутентикационе податке након аутентикације

3.3 Маскирати PAN (*payment card number*) када се приказује неовлашћеним корисницима

3.4 Учинити PAN нечитљивим на свим местима где је сачуван

3.5 Заштитити све криптографске кључеве коришћене за шифровање CHD

3.6 Документовати и имплементирати процедуре за управљање криптографским кључевима

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

Шифровати *CHD* приликом преноса кроз отворене јавне мреже (з.4)

4.1 Користити јаке криптографске и сигурносне протоколе за заштиту CHD током преноса кроз отворене јавне мреже

4.2 Никада се не сме слати PAN технологијама за размену порука са корисницима (*e-mail, instant messaging, SMS, chat*, итд.)

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

Развијати и одржавати сигурне системе и апликације (з.6)

6.1 Обезбедити да су сви делови система заштићени од познатих сигурносних пропуста тако што ће се редовно инсталирати сви сигурносни додаци које обезбеђују произвођачи софтвера

6.2 Установити процес којим ће се идентификовати и рангирати идентификовани сигурносни пропусти

6.3 Развијати сигурне интерне и екстерне апликације

6.4 Пратити процедуре за измену за све промене у свим компонентама

6.5 Поштовати смернице за развој безбедног софтвера и радити сигурносне ревизије кода

6.6 Све јавно доступне веб апликације треба да буду заштићене од познатих напада

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

Ограничити приступ до CHD (з.7)

7.1 Ограничити приступ до CHD само на оне кориснике којима је у опису посла баратање са тим подацима

7.2 Успоставити систем за контролу приступа који ограничава присуп кориснику на бази минималног скупа података који му је неопходан и подесити систем тако да одбија сваки приступ осим уколико није експлицитно дозвољен (*deny all*)

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

Пратити и надзирати све приступе мрежним ресурсима и CHD (з.10)

10.1 Успоставити процес којим би се могао повезати сваки приступ компоненти система са појединачним корисником који је приступио

10.2 Имплементирати аутоматизовано прављење ревизионих трагова (*audit trails*) за реконструисање значајних догађаја у систему

10.3 Дизајнирати скуп параметара које сваки улаз у ревизионом трагу треба да има

10.4 Синхронизовати све системске часовнике

10.5 Заштитити ревизионе трагове од измена

10.6 Прегледати логове на дневном нивоу

10.7 Чувати историјат ревизионих трагова

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

PCI DSS - закључак

- PCI DSS је стандард који покрива искључиво заштиту података са дебитних и кредитних картица
- Не може се користити да покрије читаву сигурносну полису неке организације
- Већина препорука које се могу наћи у PCI DSS могу се наћи и у другим водећим индустријским стандардима, као и у приручницима са добрим праксама
- Већина захтева који су у домену развоја софтвера се могу испунити коришћењем базичних сигурносних концепата – криптографије, контроле приступа, провере уноса корисника, логовања

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

Квалитативни сигурносни захтеви

- Квалитативни сигурносни захтеви дефинишу се кроз моделовање претњи
- Моделовање претњи подразумева скуп техника сигурносне анализе дизајнираних да би се разумело:
  - шта нападач жели да постигне (претње)
  - како може да покуша да то постигне (напади)
  - како систем може да га у томе спречи (противмере)
- Квалитет моделовања претњи зависи од стручности онога ко га прави и правилног разумевања система
- Моделовање претњи може се извести за било који систем и на различитим нивоима грануларности

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

Моделовање претњи

- Постоји велики број различитих техника, али већина се састоји из сличног скупа корака који обухвата:

1. Идентификовање критичних ресурса (нпр. информација, опреме, функција)
2. Дефинисање сигурносних циљева за сваки ресурс (нпр. поверљивост, интегритет, доступност)
3. Идентификовање и декомпоновање претњи за сваки сигурносни циљ
4. Идентификовање и анализа ризика
5. Дефинисање сигурносних захтева за избегавање претњи

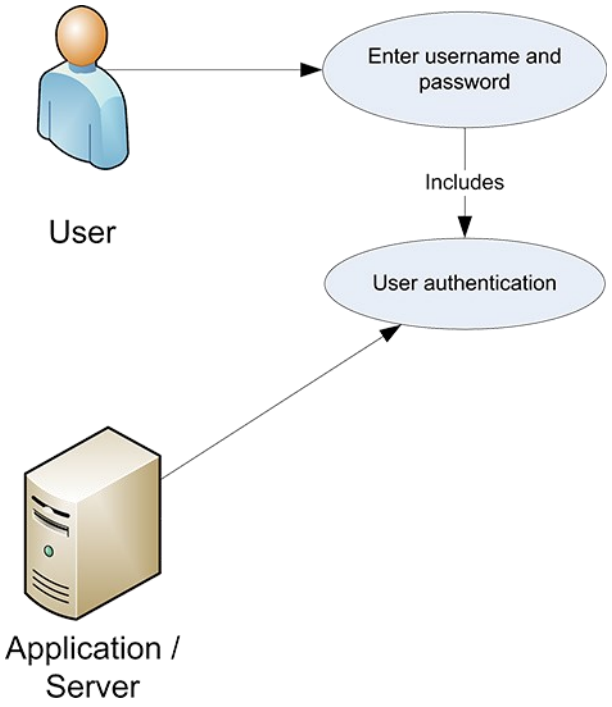
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Пример: случајеви коришћења

- Случајеви коришћења (*use cases*) представљају начин за смишљање, представљање, прецизирање и документовање софтверских захтева

- Случај коришћења представља листу акција или корака који дефинишу интеракцију између улоге у систему и система да би се остварио зацртани циљ

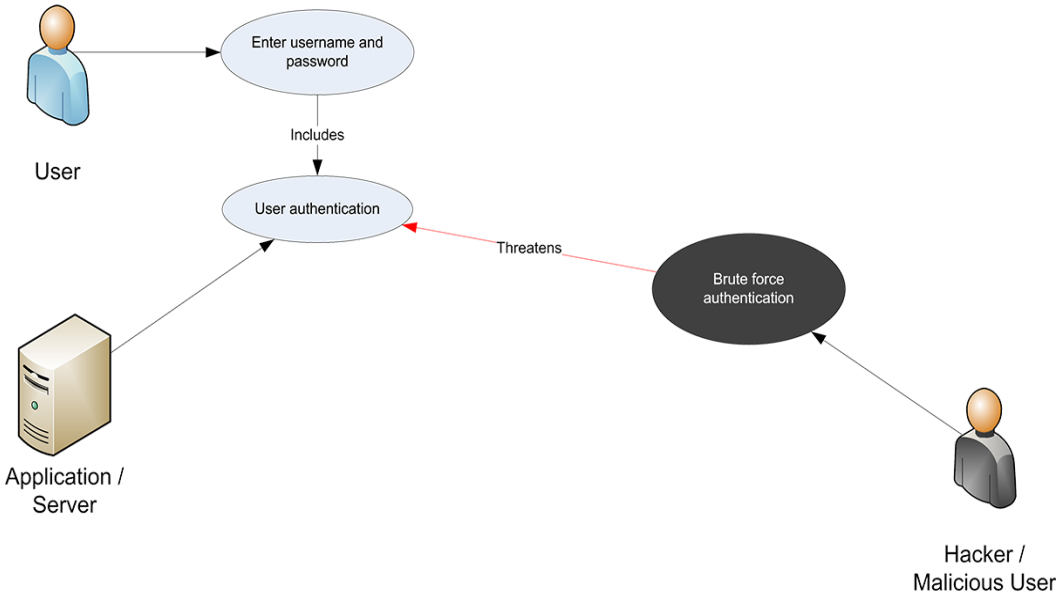
- Заинтересоване стране су задовољније са визуелним приказом секвенце оперативних акција него са декларативном спецификацијом софтверских захтева



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

Случајеви злоупотребе

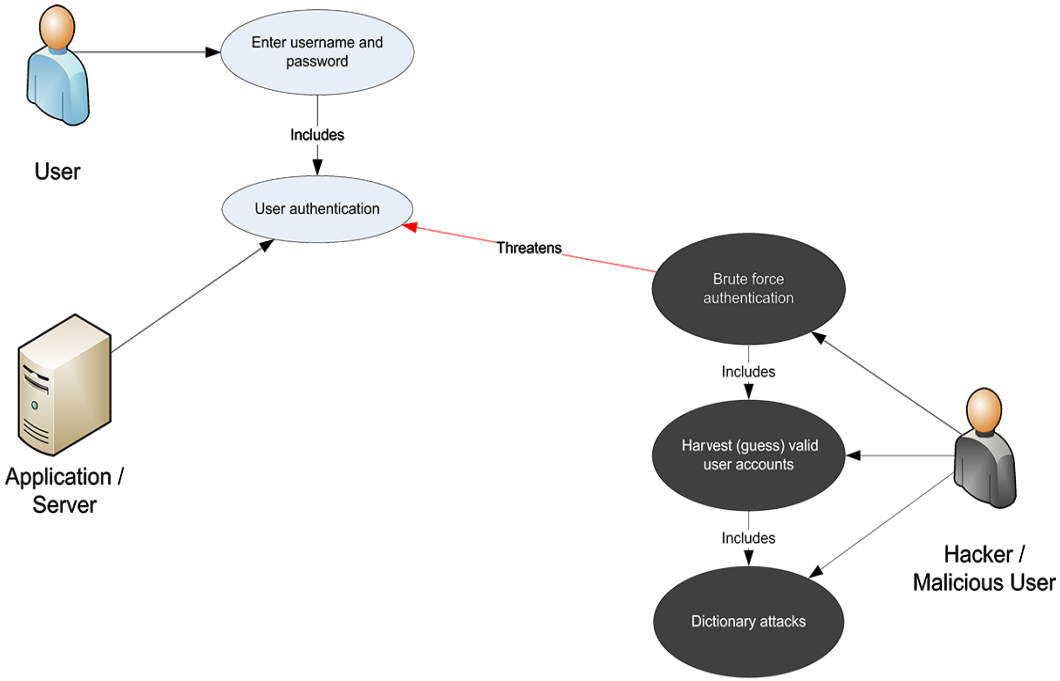
- Случај злоупотребе (*misuse case*) представља секвенцу акција које систем или други ентитет може да изврши у интеракцији са нападачем и на тај начин произведе штету заинтересованим странама уколико је секвенца успешна



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

Случајеви злоупотребе - релације

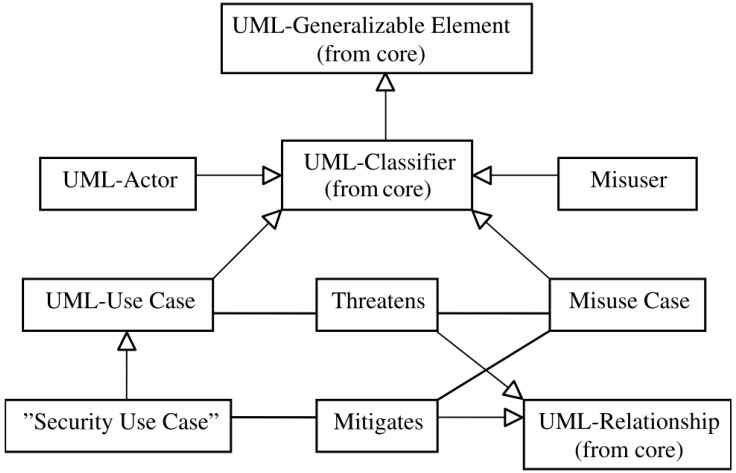
- Користе се асоцијације за повезивање нападача са случајем злоупотребе
- Уобичајене релације за случајеве коришћења, као што су укључује, проширује и генерализује могу се користити и за случајеве злоупотребе

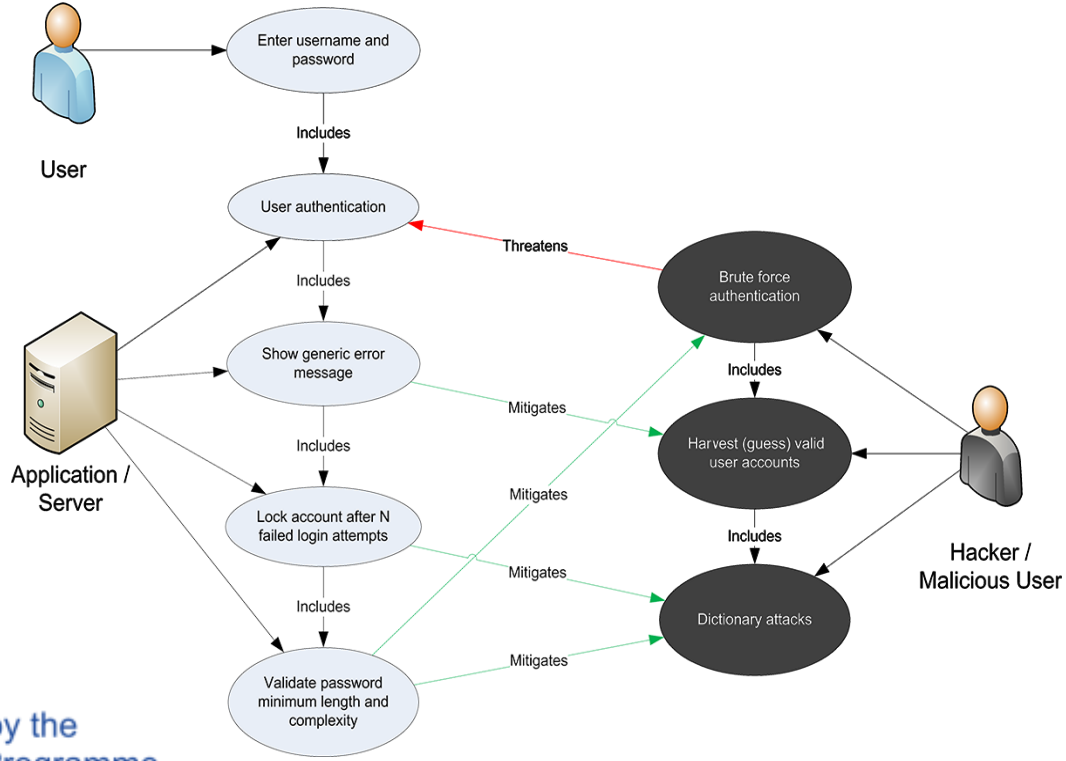


ISSES
Co-funded by the Erasmus+ Programme of the European Union

Случајеви злоупотребе - избегавање

- Случај коришћења може да избегне случајеве злоупотребе смањивањем његове могућности за успех





ISSES
d by the
Erasmus+ Programme
of the European Union

Пример

1. Који су случајеви коришћења?
   a) Шта су ресурси?
   b) Који су њихови сигурносни циљеви?
2. Који су случајеви злоупотребе?
   a) Ко су нападачи?
3. Који су сигурносни случајеви коришћења?

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

Нападачке приче (*Abuser Stories*)

- Нападачке приче представљају исто за корисничке приче, као што случајеви злоупотребе представљају за случајеве коришћења
- Корисничке приче су кратки неформални описи захтева написани од стране корисника система – изражавају функционалност система која доноси вредност
- Нападачке приче идентификују на који начин нападачи могу злоупотребити систем – изражавају сигурносне захтеве система
- Нпр. *Као нападач желим да украдем информације о кредитној картици како бих направио лажирану потрошњу*

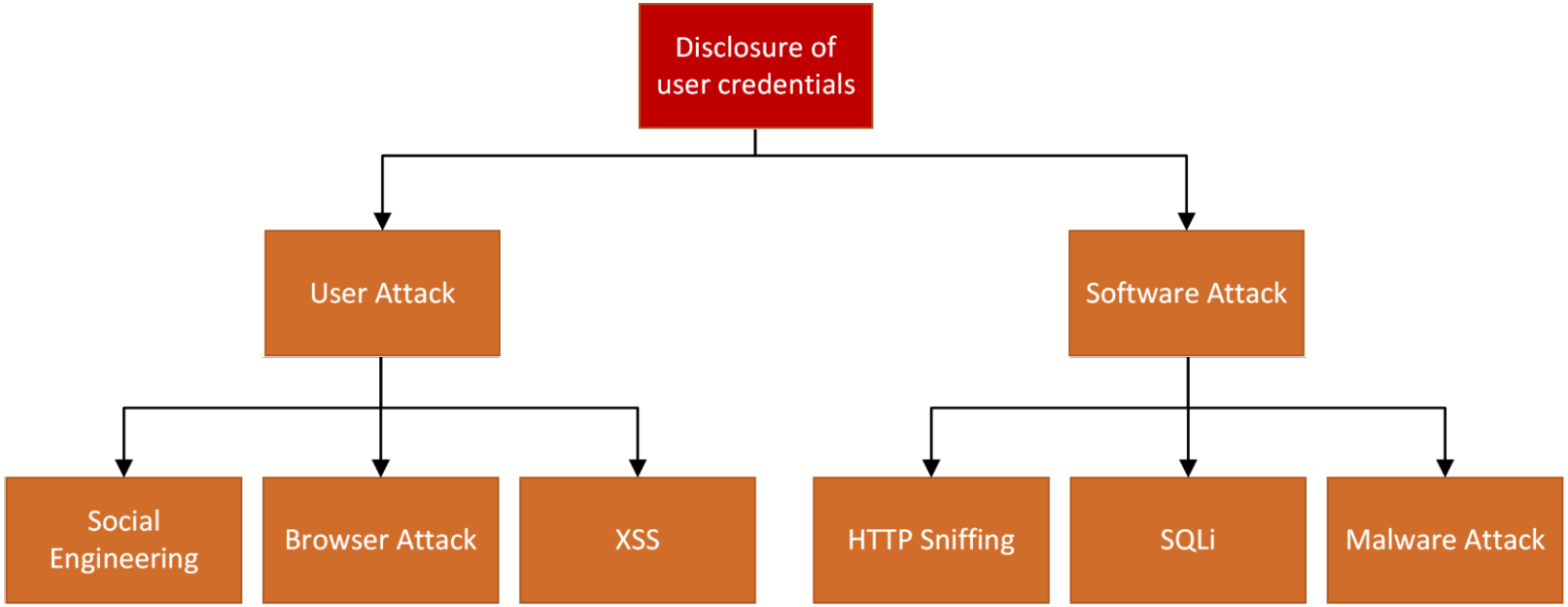
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Нападачка стабла (*Attack trees*) - преглед

- Нападачка стабла служе да се илуструје на које начине неки ресурс може бити нападнут, које контрамере су успостављене и како могу бити заобиђене
- Корен стабла је претња која се истражује
- Родитељски чворови се могу декомпоновати у више чворова који представљају нападе или претње који могу бити у логичким И или ИЛИ релацијама
- Претња се остварује ако се:
  - остваре сви чворови деца у логичкој И релацији;
  - оствари било који чвор дете у логичкој ИЛИ релацији;

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

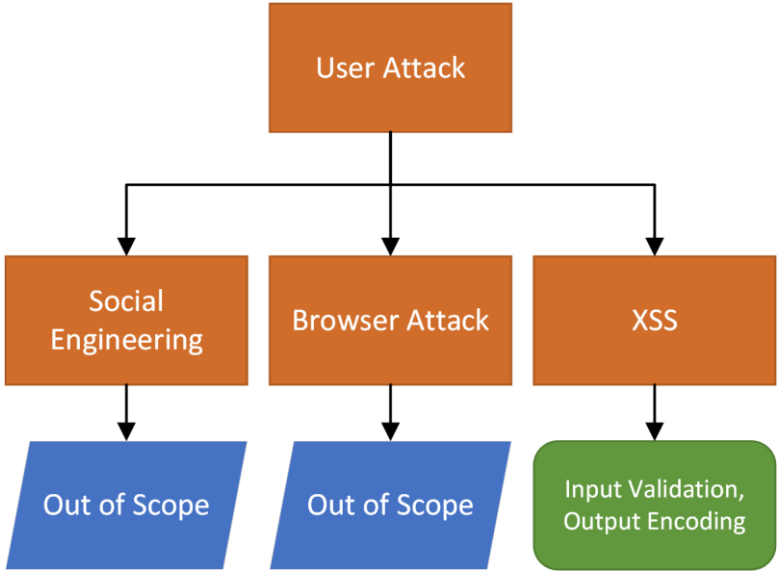
Пример нападачког стабла



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

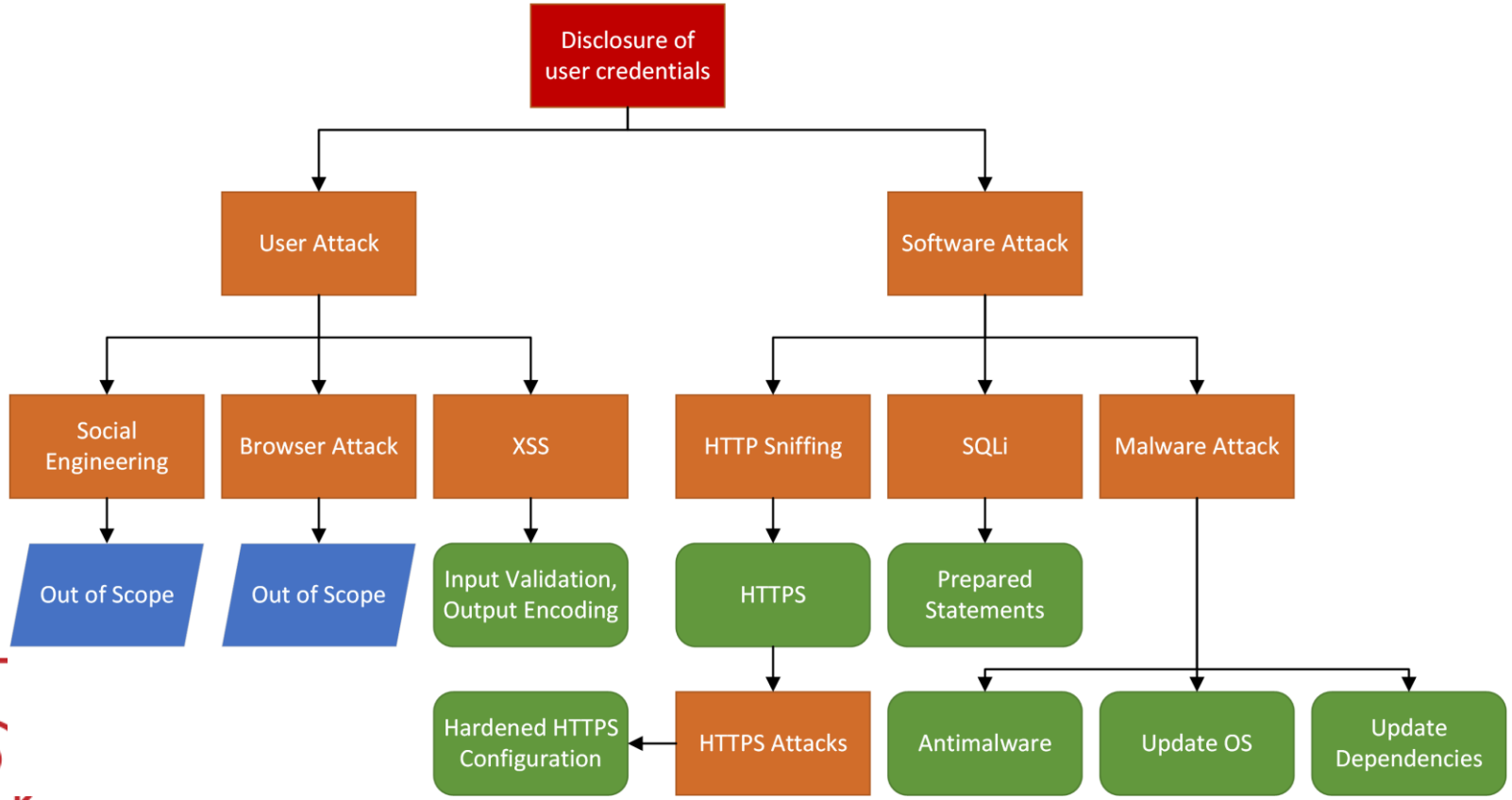
Проширена нападачка стабла

- Може се означити да су напади изван опсега (*out of scope*)
- Нападачка стабла се могу проширити да укључе и контрамере
- Контрамере се могу заобићи новим нападима
- Листови стабла треба да садрже чворове:
  - изван опсега
  - контрамере
  - није избегнут напад



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

Пример проширеног нападачког стабла



Пример: Напад на сеф

- Нацртати нападачко стабло

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

Случајеви злоупотребе и нападачка стабла - закључак

- Случајеви злоупотребе и нападачка стабла представљају корисне технике за развијање напдачког начина размишљања
- Ове технике нису практичне за примену приликом развоја софтвера
  - Превисока је цена развоја и одржавања
  - Тешко се интегришу у агилне методе развоја
  - Ретко су неопходне за сигурносну процену

ISSES

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

Смишљање сигурносних захтева

- Најчешће руководство компаније која развија софтвер (у договору са клијентом) дефинише сигурносне захтеве на високом нивоу апстракције
- Софтверски инжењер има задатак да разуме сигурносне захтеве на високом нивоу апстракције и преведе их у имплементационе одлуке и задатке на ниском нивоу апстракције

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