Úvod do počítačovej bezpečnosti - Zadanie 1

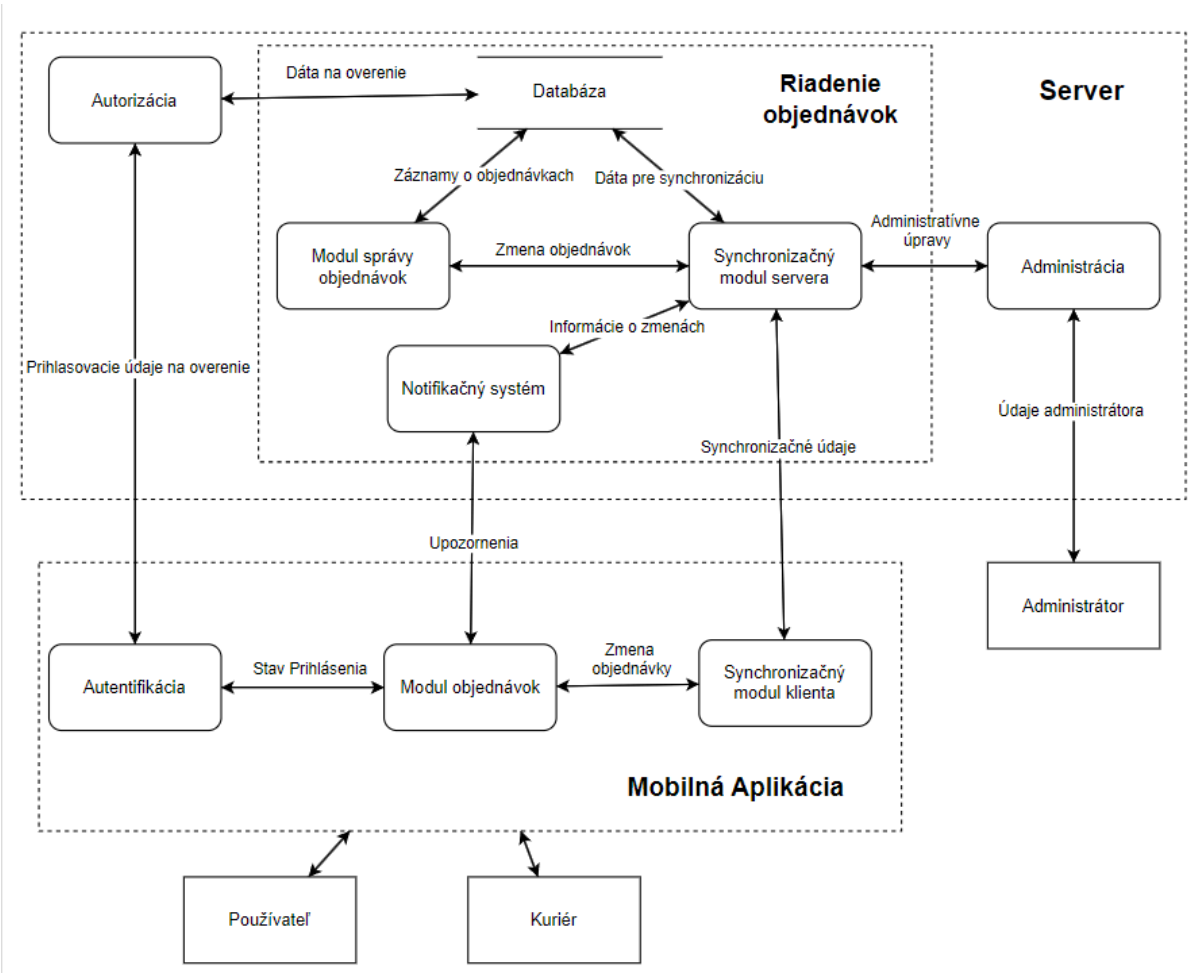
Doručovací systém

1. Návrh architektúry

Hlavné funkcie systému:

1. **Zadávanie a správa objednávok**
    - Zákazníci môžu vytvoriť objednávku prostredníctvom mobilnej aplikácie. Zadajú adresu doručenia, výber dopravcu (v prípade externého dopravcu), typ doručenia a ďalšie údaje.
    - Každá objednávka je uložená v databáze s jedinečným identifikátorom (číslo objednávky), ktorý zákazníci môžu použiť na sledovanie zásielky.
2. **Sledovanie zásielok v reálnom čase**
    - Zákazníci môžu sledovať aktuálny stav svojej objednávky cez aplikáciu (web/mobil). Sledovanie zahŕňa informácie o tom, kde sa zásielka nachádza, kedy bola odoslaná a odhadovaný čas doručenia.
    - Kuriéri poskytujú aktuálne informácie o stave zásielky (vyzdvihnuté, doručované, doručené), ktoré sú synchronizované do systému.
3. **Komunikácia medzi zákazníkmi a kuriérmi**
    - Kuriéri majú prístup k mobilnej aplikácii, v ktorej vidia pridelené objednávky a potrebné informácie o doručení.
    - Zákazníci môžu byť informovaní cez push notifikácie, e-maily alebo SMS o stave zásielky (odovzdaná kuriérovi, blížiace sa doručenie).
4. **Notifikačný systém**
    - Systém je navrhnutý tak, aby aktívne upozorňoval zákazníkov na zmeny stavu ich zásielky. Napríklad, keď je objednávka pripravená na vyzdvihnutie, je doručovaná alebo už bola doručená.
    - Notifikácie môžu byť zasielané cez e-mail, SMS alebo push notifikácie v mobilnej aplikácii.
5. **Administrácia a správa objednávok**
    - Administrátori systému majú prístup k backoffice systému, kde môžu monitorovať objednávky, meniť ich stav, prípadne manuálne zasiahnuť pri problémoch.
    - Administrátori môžu tiež generovať prehľady o doručovacích výkonoch, problémoch, úspešnosti doručenia a ďalších metrikách.
6. **Bezpečnosť a autentifikácia**
    - Všetci používatelia (zákazníci, kuriéri, administrátori) musia byť autentifikovaní cez zabezpečené prihlásenie. Používa sa dvojfaktorová autentifikácia (2FA) pre kuriérov a administrátorov.
    - Prístupy sú riadené na základe rolí (zákazník, kuriér, administrátor), aby sa zabezpečilo, že každý používateľ má prístup len k relevantným informáciám a funkciám.

2. Data Flow Diagram



3. Identifikácia hrozieb podľa metódy STRIDE

Externé entity

	Spoofing	Repudiation
Používateľ	Hrozba, že útočník môže použiť ukradnuté prihlasovacie údaje používateľa na prístup do mobilnej aplikácie.	Používateľ môže poprieť, že vykonal určité akcie, napríklad zadanie alebo zrušenie objednávky, ak sa nevedie riadny záznam (audit trail).
Kuriér	Útočník sa môže vydávať za kuriéra, aby získal prístup k objednávkam a ich detailom, čo by umožnilo neoprávnený prístup k informáciám o doručovaní.	Kuriér by mohol poprieť, že vykonal určité akcie (napríklad doručenie alebo nedoručenie objednávky), ak sa nevedú záznamy o týchto akciách (napr. digitálny podpis alebo sledovanie akcií).
Administrátor	Útočník môže získať prihlasovacie údaje administrátora a získať prístup k citlivým nastaveniam a operáciám v systéme.	Ak nie sú záznamy akcií (audit trail) správne implementované, administrátor môže poprieť, že vykonal zmeny, ktoré by mohli ovplyvniť systém alebo dáta.

Procesy

Autorizácia

- **Spoofing**: Útočník sa môže pokúsiť oklamať autorizačný proces a získať prístup do systému vydávaním sa za oprávneného používateľa.
- **Tampering**: Útočník môže zmeniť autorizačné pravidlá alebo politiky, čo mu môže umožniť získanie prístupu alebo zníženie oprávnení iných používateľov.
- **Repudiation**: Chýbajúci audit môže viesť k popretiu prístupu, čo znamená, že nie je možné určiť, kto k systému pristupoval.
- **Information Disclosure**: Ak je implementácia autorizačného systému slabá, môže útočník získať citlivé informácie o používateľoch alebo ich oprávneniach.
- **Denial of Service**: Útoky môžu byť zamerané na preťaženie autorizačného modulu, čím sa naruší proces autorizácie a zablokuje prístup pre legitímnych používateľov.
- **Elevation of Privilege**: Zraniteľnosť môže umožniť bežnému používateľovi získať privilegované oprávnenia prostredníctvom manipulácie s autorizačnými údajmi.

Modul správy objednávok

- **Spoofing**: Útočník môže použiť kompromitované poverenia, aby sa vydával za legitímneho používateľa alebo administrátora a manipuloval s objednávkami.
- **Tampering**: Manipulácia s údajmi objednávok (napr. zmena množstva alebo ceny) môže spôsobiť finančné straty alebo poškodiť dôveryhodnosť systému.

- **Repudiation**: Bez správneho auditu môže útočník poprieť, že zmenil objednávku alebo ju vymazal.
- **Information Disclosure**: Nedostatočná ochrana objednávkových údajov môže viesť k úniku citlivých informácií, ako sú údaje o zákazníkoch alebo ich objednávky.
- **Denial of Service**: Modul môže byť zahltený požiadavkami na vytváranie, upravovanie alebo mazanie objednávok, čo spôsobí, že nebude možné spracovať ďalšie požiadavky.
- **Elevation of Privilege**: Zneužitie chyby v module môže umožniť používateľovi získať práva na vykonanie administratívnych akcií, ako je úprava všetkých objednávok.

Synchronizačný modul servera

- **Spoofing**: Útočník sa môže pokúsiť vydávať sa za legitímny synchronizačný klient, čím môže pristupovať k citlivým údajom.
- **Tampering**: Môže dôjsť k manipulácii s údajmi počas synchronizácie (napr. zmena objednávok alebo ich statusov).
- **Repudiation**: Bez záznamu synchronizačných akcií môže byť problém spätne zistiť, či došlo k neoprávnenej synchronizácii alebo úprave údajov.
- **Information Disclosure**: Nedostatočne zabezpečený prenos môže viesť k úniku citlivých informácií, ak sa údaje počas synchronizácie prenášajú bez šifrovania.
- **Denial of Service**: Útočník môže zaplaviť server veľkým množstvom synchronizačných požiadaviek, čo by mohlo preťažiť systém.
- **Elevation of Privilege**: Ak synchronizačný modul neoveruje správne povolenia, môže útočník získať prístup k dátam, na ktoré nemá nárok.

Notifikačný systém

- **Spoofing**: Útočník môže predstierať, že je oprávnený zdroj a posielať falošné notifikácie.
- **Tampering**: Útočník môže manipulovať s notifikáciami, čo môže viesť k tomu, že používatelia dostanú nesprávne alebo škodlivé informácie.
- **Repudiation**: Používatelia môžu poprieť, že prijali konkrétne notifikácie, ak nie sú riadne uchované logy.
- **Information Disclosure**: Notifikácie môžu obsahovať citlivé informácie (napr. o objednávkach), ktoré by mohli byť odhalené tretím stranám.
- **Denial of Service**: Útok na notifikačný systém môže zahŕňať zasielanie veľkého počtu notifikácií, čo by mohlo viesť k zahlteniu systému a zneprístupneniu legitímnych upozornení.
- **Elevation of Privilege**: Ak má útočník prístup k úpravám notifikačných nastavení, môže získať prístup k citlivým informáciám alebo manipulovať so spôsobom ich doručenia.

Autentifikácia (Mobilná aplikácia)

- **Spoofing**: Útočník sa môže pokúsiť vydávať za legitímneho používateľa prostredníctvom ukradnutých prihlasovacích údajov.
- **Tampering**: Manipulácia s autentifikačným modulom by mohla umožniť neoprávnený prístup do systému.

- **Repudiation**: Používatelia môžu poprieť, že sa prihlásili, ak autentifikačný proces nezaznamenáva logy.
- **Information Disclosure**: Autentifikačné údaje môžu byť zraniteľné voči úniku, ak nie sú riadne zabezpečené.
- **Denial of Service**: Útoky na autentifikačný proces, napríklad prostredníctvom opakovaných pokusov o prihlásenie, môžu spôsobiť jeho preťaženie.
- **Elevation of Privilege**: Ak má autentifikačný modul chyby, útočník môže získať vyššie oprávnenia (napr. prístup ako administrátor).

Modul objednávok (Mobilná aplikácia)

- **Spoofing**: Útočník sa môže pokúsiť napodobniť používateľa alebo kuriéra a získať prístup k objednávkam.
- **Tampering**: Útočník môže zmeniť obsah objednávky, čo môže viesť k zmene jej hodnoty alebo podvodným transakciám.
- **Repudiation**: Používateľ môže poprieť zadanie objednávky, ak neexistuje dôkaz o jeho akciách.
- **Information Disclosure**: Únik údajov o objednávkach, napríklad meno používateľa alebo detaily objednávky, môže viesť k zneužitiu týchto informácií.
- **Denial of Service**: Neoprávnené žiadosti môžu preťažiť modul objednávok a zablokovať službu.
- **Elevation of Privilege**: Útočník môže nájsť chyby v module objednávok, ktoré mu umožnia získať oprávnenia administrátora.

Synchronizačný modul klienta (Mobilná aplikácia)

- **Spoofing**: Neoprávnený klient sa môže pokúsiť synchronizovať údaje bez povolenia.
- **Tampering**: Synchronizované údaje môžu byť počas prenosu zmenené útočníkom.
- **Repudiation**: Používateľ môže poprieť, že upravoval objednávky, ak synchronizačné akcie nie sú logované.
- **Information Disclosure**: Únik údajov počas synchronizácie môže viesť k odhaleniu citlivých informácií tretím stranám.
- **Denial of Service**: Modul môže byť preťažený synchronizačnými požiadavkami, čo znemožní legitímnym používateľom synchronizáciu dát.
- **Elevation of Privilege**: Ak synchronizačný modul obsahuje chyby, útočník môže získať vyššie oprávnenia a prístup k dátam, ktoré by mal ma

Administrácia

- **Spoofing**: Útočník môže získať prístupové údaje administrátora a vydávať sa za neho, čo mu umožní prístup k citlivým funkciám.
- **Tampering**: Manipulácia s kritickými údajmi (napr. objednávky, nastavenia), čo môže poškodiť systém alebo spôsobiť finančné škody.
- **Repudiation**: Bez podrobného logovania môže administrátor poprieť, že vykonal určité akcie.
- **Information Disclosure**: Únik citlivých údajov (napr. cez SQL injection), ak administrátorské rozhranie nie je dostatočne zabezpečené.

- **Denial of Service**: Opakované požiadavky môžu preťažiť administrátorské rozhranie a zneprístupniť systém.
- **Elevation of Privilege**: Využitie chýb v module môže útočníkovi umožniť získať administrátorské oprávnenia a úplnú kontrolu nad systémom.

Dátové toky

Dátový tok medzi Autorizáciou a Autentifikáciou

- **Tampering**: Útočník môže manipulovať s autentifikačnými údajmi pri ich prenose, napríklad pozmeniť identifikačné údaje alebo oprávnenia.
- **Information Disclosure**: Únik údajov pri autentifikácii môže viesť k tomu, že útočník získa prihlasovacie údaje alebo tokeny.
- **Denial of Service**: Útoky na dátový tok medzi autentifikáciou a autorizáciou môžu spôsobiť jeho preťaženie a tým znemožniť legitímne prihlásenia.

Dátový tok medzi Synchronizačným modulom servera a Synchronizačným modulom klienta

- **Tampering**: Útočník môže modifikovať synchronizované údaje, napríklad zmeniť detaily objednávok počas prenosu medzi serverom a klientom.
- **Information Disclosure**: Ak nie je komunikácia šifrovaná, útočník môže odpočúvať dátový tok a získať citlivé informácie, ako sú údaje objednávok alebo informácie o používateľoch.
- **Denial of Service**: Útokom na dátový tok medzi serverom a klientom, napríklad zasielaním opakovaných synchronizačných požiadaviek, môže útočník spôsobiť preťaženie a znefunkčniť synchronizáciu.

Dátový tok medzi Modulom správy objednávok a Notifikačným systémom

- **Tampering**: Môže dôjsť k zmene obsahu notifikácie, napríklad k odosielaniu nepravdivých informácií používateľom.
- **Information Disclosure**: Nedostatočne zabezpečený dátový tok môže viesť k úniku informácií o objednávkach, ktoré notifikačný systém zasiela.
- **Denial of Service**: Útočník môže opakovane žiadať notifikácie, čím zahlcuje systém a bráni legitímnym notifikáciám.

Dátový tok medzi Modulom objednávok a Používateľom/Kuriérom (Mobilná aplikácia)

- **Tampering**: Útok na dátový tok môže viesť k manipulácii s údajmi objednávok, napríklad zmeniť množstvo, cenu alebo adresu doručenia.
- **Information Disclosure**: Ak nie sú dáta šifrované, môže dôjsť k úniku informácií o objednávkach alebo detailoch používateľa.
- **Denial of Service**: Neoprávnený prístup alebo úmyselné preťaženie toku požiadaviek môže narušiť komunikáciu medzi používateľom/kuriérom a modulom objednávok.

Dátové úložisko (databáza)

Tampering: Útočník môže pozmeniť dáta uložené v databáze, ako sú informácie o používateľoch, objednávkach alebo nastaveniach, čo môže spôsobiť neplatnosť údajov alebo porušiť funkčnosť systému.
Information Disclosure: Únik citlivých informácií, ako sú údaje o používateľoch a objednávkach, môže nastať, ak je komunikácia s databázou nezabezpečená alebo ak úložisko nie je riadne chránené (napr. cez SQL injection).
Denial of Service: Útoky na databázu (napr. zahlcovanie žiadosťami) môžu spôsobiť jej preťaženie a znížiť dostupnosť systému.

4. Mitigácia hrozieb

Spoofing

Identifikovaná hrozba:

Útočník sa pokúša vydávať za legitímneho používateľa (napr. zákazníka alebo kuriéra), aby získal prístup k citlivým informáciám alebo vykonal neoprávnené akcie.

Mitigácia:

- **Viacfaktorová autentifikácia (MFA)**: Zabezpečenie prihlasovania viacfaktorovou autentifikáciou, kde sa pri prihlasovaní vyžaduje nie len heslo, ale aj ďalší autentifikačný faktor (napr. kód zaslaný na telefón alebo biometria).
- **Silná autentifikácia heslom**: Používanie silných hesiel s minimálnou dĺžkou a komplexnosťou. Zavedenie pravidiel pre zmenu hesiel, ktoré zabezpečia, že heslá nebudú ľahko predvídateľné.

Tampering

Identifikovaná hrozba:

Manipulácia s údajmi počas prenosu medzi frontendom a backendom. Útočník môže meniť požiadavky, ako napríklad adresu doručenia alebo status objednávky.

Mitigácia:

- **Šifrovaná komunikácia (TLS/SSL)**: Zabezpečenie všetkej komunikácie medzi klientom (web alebo mobilná aplikácia) a serverom pomocou protokolu TLS/SSL. Tým sa zabezpečí, že prenášané údaje sú šifrované a nemôžu byť ľahko zmenené alebo odpočúvané.
- **Digitálne podpisy**: Pre niektoré kľúčové dáta (napr. detaily objednávok) by sme mohli používať digitálne podpisy, aby bolo možné overiť ich integritu. Ak by údaje boli zmenené, digitálny podpis by sa stal neplatným.

Repudiation

Identifikovaná hrozba:

Používateľ môže poprieť, že vykonal objednávku alebo platbu, ak sa nerealizuje vhodné logovanie akcií a neexistuje digitálny dôkaz o transakciách.

Mitigácia:

- **Logovanie a auditné záznamy**: Implementovať robustné logovanie všetkých dôležitých akcií (napr. vytvorenie objednávky, úprava údajov, potvrdenie doručenia). Logy by mali obsahovať dátum, čas, IP adresu, identifikáciu používateľa a detail akcie. Tieto logy by mali byť bezpečne uložené a pravidelne kontrolované.
- **Digitálne podpisy**: Na potvrdenie kritických operácií (napríklad potvrdenie doručenia zásielky) by sme mohli používať digitálne podpisy alebo biometrické údaje, aby sme zabezpečili, že tieto akcie vykonal práve ten používateľ, ktorý má právo na takúto operáciu.
- **Záznam potvrdení:** Pre dôležité operácie, ako je zadanie objednávky alebo jej doručenie, by systém mohol generovať potvrdenia (napr. e-maily alebo SMS), ktoré by slúžili ako dôkaz, že daná akcia bola vykonaná.

Information Disclosure

Identifikovaná hrozba:

Nešifrovaná komunikácia môže viesť k úniku citlivých údajov, ako sú osobné údaje o zákazníkoch alebo objednávky, ak útočník zachytí komunikáciu.

Mitigácia:

- **End-to-End šifrovanie**: Všetka komunikácia medzi frontendom a backendom by mala byť šifrovaná pomocou protokolu TLS/SSL, aby sa zabezpečilo, že údaje sú počas prenosu chránené pred odpočúvaním.
- **Šifrovanie údajov v databáze**: Citlivé údaje, ako sú osobné informácie zákazníkov alebo údaje o zásielkach, by mali byť uložené šifrované. Tým sa zabezpečí, že aj v prípade neoprávneného prístupu k databáze útočník nebude môcť tieto údaje použiť.
- **Access Control**: Prístup k citlivým údajom by mal byť riadený na základe oprávnení. Zákazníci by mali mať prístup len k svojim údajom a administrátori len k relevantným častiam systému, kde je ich prístup oprávnený.

Denial of Service (DoS)

Identifikovaná hrozba:

Útočníci môžu zahlcovať systém množstvom požiadaviek, čo vedie k jeho nedostupnosti pre legitímnych používateľov.

Mitigácia:

- **Rate Limiting**: Implementácia obmedzení pre počet požiadaviek z jednej IP adresy v určitom časovom intervale. Tým sa zabráni tomu, aby jeden používateľ alebo útočník zahlcoval systém.
- **CDN a Web Application Firewall (WAF)**: Použitie CDN s WAF môže pomôcť blokovať škodlivé požiadavky ešte predtým, ako sa dostanú do systému. CDN dokáže aj efektívne rozložiť záťaž, aby sa znížil dopad útoku.
- **Load Balancing**: Použitie load balancera na rozloženie záťaže medzi viaceré servery znižuje riziko, že jeden server bude preťažený.

Elevation of Privilege

Identifikovaná hrozba:

Používateľ s nižšími oprávneniami (napr. zákazník) sa môže pokúsiť získať prístup k privilegovaným funkciám, napríklad do administrátorského rozhrania.

Mitigácia:

- **Role-Based Access Control (RBAC)**: Implementovať systém kontroly prístupu na základe rolí, kde každá rola (zákazník, kuriér, administrátor) má jasne definované oprávnenia a prístupové práva. Používatelia by mali mať prístup len k tým funkciám, ktoré sú relevantné pre ich rolu.
- **Minimization of Privilege**: Používať princíp minimálneho oprávnenia, kde každý používateľ alebo proces má len také oprávnenia, ktoré sú potrebné na vykonávanie jeho práce. To znamená, že aj keby útočník získal kontrolu nad účtom používateľa, jeho možnosti sú obmedzené.
- **Security Testing a Penetračné Testy**: Pravidelné bezpečnostné testovanie a penetračné testy môžu odhaliť zraniteľnosti súvisiace s kontrolou prístupu. Tieto testy by mali byť vykonávané na odhalenie možných zraniteľností, kde by mohol používateľ získať vyššie oprávnenia.

5. Attack Tree