Prof. Vincent Naessens

Gedistribueerde systemen 2

Report horeca registratie systeem

Caliskan Mikail
Lefevre Cedric

https://github.com/hv2r55g/HORECA-registration-system.git

Academiejaar 2020 - 2021

1 Relevante design beslissingen

De voornaamste design keuzes zijn de keuzes die te maken hebben met de gekozen crypto protocollen en hashfuncties. De registrar gaat maandelijks (efficiëntie) een set van pseudoniemen gaan doorsturen naar de catering facilities (CF). De set is 30 pseudoniemen groot wat overeenkomt met het aantal dagen in een maand. De pseudoniemen zijn het resultaat van een cryptografische hashfunctie die een secret key, business nummer en de datum van de betreffende dag als input had. Er werd geopteerd voor de SHA256 hashfunctie aangezien dit resulteert in een langere hash dan de SHA1. Door de langere hash is het nog moeilijker om te reverse engineeren. Ook is de SHA-familie de meest gebruikelijke tegenover andere cryptografische hashfuncties. Per pseudoniem wordt er ook een secret key gegenereerd op basis van de master key, business nummer en de datum van de betreffende dag. De secret key werd gecreëerd met het symmetrisch encryptie protocol AES. Aangezien die tegenover asymmetrische protocollen relevant sneller is. De tradeoff die symmetrische protocollen maken is dat de sleutel dan via een secure channel gedeeld moet worden, maar aangezien deze secret keys nooit gedecrypteerd moeten worden kunnen we deze tradeoff maken.

De registrar deelt niet enkel de pseudoniemen uit aan de verschillende CF's, maar gaat ook de tokens gaan genereren en signen voor de verschillende gebruikers. Aangezien de tokens geverifieerd moeten worden door een andere server opteren we hier voor asymmetrische encryptie protocollen. Op deze manier moeten er geen secure channels opgezet worden. Tussen de asymmetrische protocollen onderling werd geopteerd voor het DSA protocol (snel signen, trager verifiëren, RSA omgekeerd) om het werk van de registrar te verlichten en deels te verschuiven naar de mixing proxy. De mixing proxy zal namelijk bij het ontvangen van een token checks moeten uitvoeren, waaronder het controleren dat de token effectief door de registrar gemaakt is. Wanneer de token geldig blijkt te zijn wordt er een bevestiging gestuurd naar de gebruiker. De bevestiging bestaat uit een logo die de gebruiker kan tonen aan de eigenaar van de CF om aan te tonen dat hij/zij geregistreerd is.

Steeds wanneer een CF de deuren opent zal die van de mixing proxy een logo toegewezen krijgen die alle klanten eveneens ontvangen indien ze bij de betreffende CF een aankoop doen. De mixing proxy bevat 27 logo's: 26 voor iedere letter in het alfabet en 1 voor alle andere karakters. Dagelijks na het sluiten van alle CF's gaat de mixing proxy de mapping van de logo's en de karakters gaan shuffelen voor een extra beveiliging in het systeem. De mixing proxy gaat op basis van het tiende karakter van de sign van de hash van de CF het juiste logo gaan bepalen. Voor het signen wordt het RSA protocol gebruikt aangezien de sign voor identieke data gelijk moet zijn. DSA zal namelijk bij het signen steeds een nieuwe random waarde in zijn berekening nemen waardoor er voor dezelfde data steeds verschillende signs zijn.

2 SWOT-Analyse

2.1 Sterktes

- Simpele GUI die duidelijk de nodige functionaliteiten visualiseert.
- Decentralisatie van de verschillende server side componenten zorgt voor een zeer privacy vriendelijk systeem.
- Het introduceren van de verschillende protocollen zorgt ervoor dat klanten geen valse info meer kunnen achterlaten na het bezoeken van een horecazaak. Dit was wel mogelijk bij de traditionele contact tracing.

- Doordat het contacteren van de bezoekers automatisch gebeurd, worden de contactpersonen veel sneller geïnformeerd dan met de traditionele contact tracing.

2.2 Zwaktes

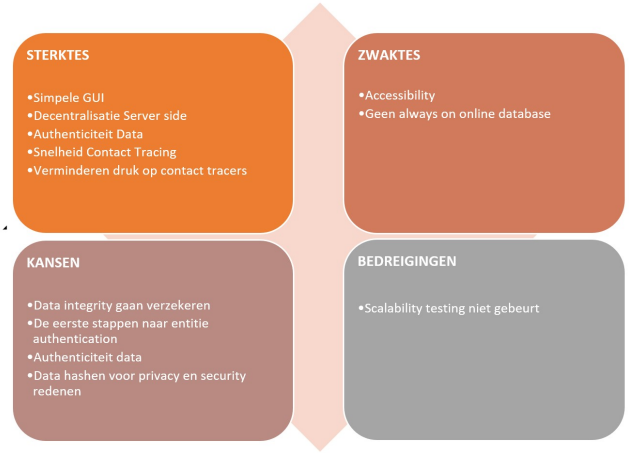
- Niet iedereen is in het bezit van een smartphone, wat gedaan met de mensen die dit niet hebben? Dit systeem kan dus geen complete vervanger zijn voor het huidige systeem.
- De RMI verbindingen zijn op dit moment niet beveiligd, waardoor er gemakkelijk communicatie kan afgeluisterd worden.
- De data wordt op dit moment niet gecapteerd in een online database, waardoor de mogelijkheid bestaat dat er data verloren gaat wanneer de server uitvalt. Het is echter wel een eenvoudige stap om van deze zwakte en sterkte te maken.

2.3 Kansen

- Data integrity: de tokens die de klanten gebruiken worden gecheckt of het geen vervalste tokens zijn.
- We hebben de kans genomen om de gevoelige data van de gebruikers telkens onherkenbaar te gaan maken zodat wanneer er een databreach zou zijn, de evil entity niet veel met de verkregen data kan doen.
- Het implementeren van sms verificatie voor de gebruikers of via het its me platform is een uitbreiding die makkelijk kan worden toegevoegd.
- Er kon voor de gebruiker een native app worden gecreëerd maar door tijdsgebrek was dit niet mogelijk.

2.4 Bedreigingen

- Scalability is zeer belangrijk voor een project als dit maar is iets wat we niet hebben kunnen testen in de mate dat het zou gebruikt worden in de buitenwereld. We weten hierdoor niet hoe ons systeem zou reageren op dergelijke input.



Figuur 1: Samenvatting van de hierboven beschreven SWOT analyse