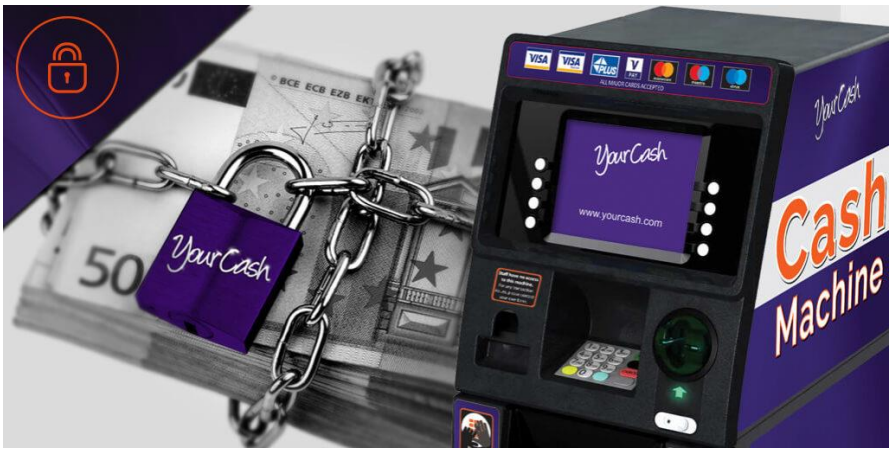


BEVEILIGINGS-ADVIESRAPPORT

Project 3/4

NAMEN

- Bryan Chung (0990458)
- Jia-jie Yeh (0992427)
- Jurgen van den Berg (1000875)
- Wouter van Huut (1018984)

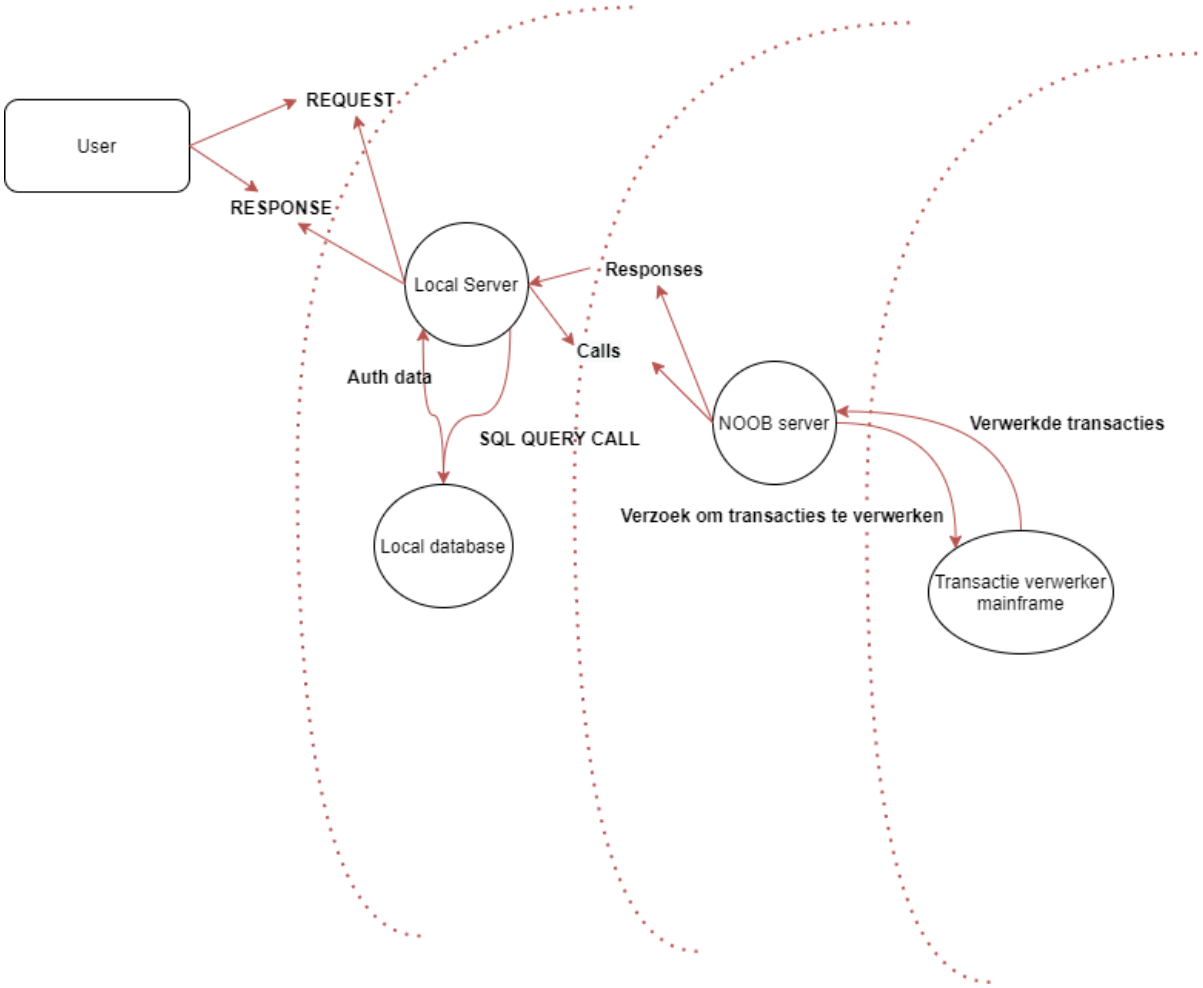
Groep :B4 / Klas :TI1B

Inleverdatum 30-04-2021
Versie 1

Inhoudsopgave

Hst 1. Beveiliging rapport

1.1 Data Flow Diagram (DFD)



1.2 Risicoanalyse

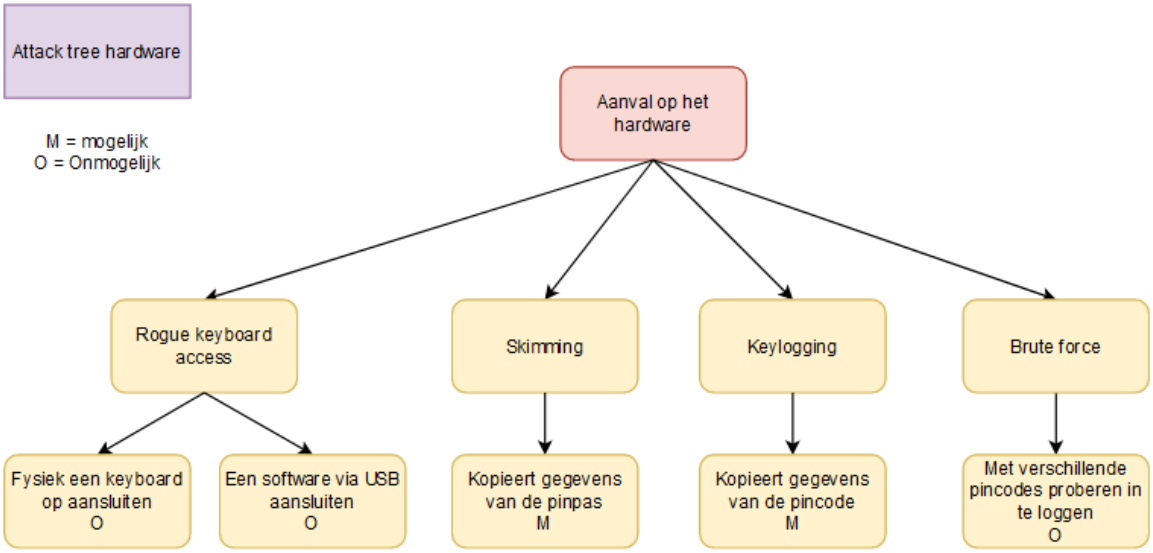
	Soorten risico aanvallen	Uitvoering
1	Rogue keyboard access	Dit is een fysiek toetsenbord koppelen aan een pinautomaat en vervolgens een stukje code of een SQL – injectie executeren. De aanvaller kan de pinautomaat dan controleren.
2	Skimming	Met deze methode dupliceer je de gegevens van een pinpas. Dit gebeurd door een replica te maken van een pinautomaat en dat plaatsen ze aanvallers op het pin sectie.
3	Keylogging	Dit is het zelfde geval van skimming, maar dan voor de gebruiker zijn pincode. Er wordt dan een replica keypad over het standaard pin keypad gelegd, waardoor de gebruiker zijn pincode wordt gestolen.
4	Dataverbinding	Als er iemand tussen de dataverbinding van het systeem komt, dan is het systeem is niet versleuteld. Hierdoor zijn de onderdelen bijvoorbeeld; de informatie van de keypad en de gui zeer gevoelig.
5	SQL	De gui moet beveiligd worden voor aanvallen, zoals SQL-injectie. Hierdoor krijgt de aanvaller gebruik tot je data in je database. Dit kan vernietigd of gestolen worden.
6	Brute force	De aanvaller kan ook via brute force aanvallen op meerdere onderdelen van het systeem. Hierbij kunnen de data zoals; pincodes en wachtwoorden van de gebruiker te verkrijgen.

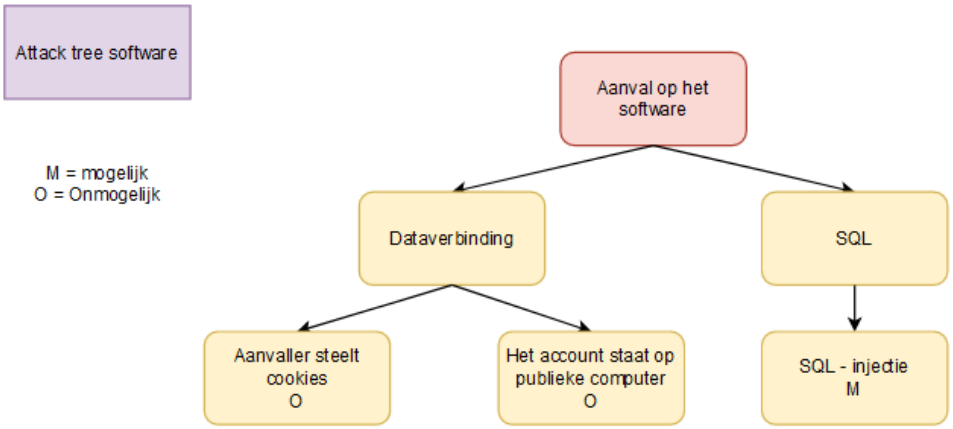
1.3 Maatregelen

	Soorten risico aanvallen	Oplossingen
1	Rogue keyboard access	Dit is een van de makkelijkste aanvalssoort op de ATM, waardoor het ook gelijk makkelijk te detecteren is. Hierdoor kan je als een nieuw apparaat wordt toegevoegd dan wordt het ATM stop gezet. Je kan ook speciale karakters accepteren.
2	Skimming	Dit kan je oplossen om door een elektromagnetische puls. Dit geeft een korte schok aan de skimmer. De schok verstoort of beschadigd de skimmer.
3	Keylogging	De aanvaller is moeilijk te detecteren, want tegenwoordig niet altijd een keypad replica gebruikt, maar ook een USB-stick. Eerst was de oplossing voelen aan de toetsenbord en kijken of het nep is. Dit is het zelfde geval bij het gebruik van de rogue keyboard.
4	Dataverbinding	Dit valt op te lossen om beveiliging te maken door middel van SHA-3^15 hash of encryptie. Hierdoor krijgt de aanvaller onleesbare data.
5	SQL	Deze aanval kan je voorkomen om de input validatie te gebruiken.
6	Brute force	Om het systeem te beschermen tegen DDoS aanvallen van de aanvaller kan je bijvoorbeeld een Anti DDoS systeem gebruiken. In Nederland is een bekende zogenaamd NaWas. Er is ook een Nationale Anti-DDoS coalitie.

1.4 Attack tree

Om een helder beeld te krijgen van een beveiligingssysteem wordt er een attack tree gemaakt. Deze attack tree geeft een beeld over de situaties van de risico aanvallen op het systeem en hoe het systeem op reageert.





Beveiligingsbronnen

1. https://www.kaspersky.com/blog/atm-attacks-2/15160/
   https://jarnobaselier.nl/rogue-access-point-easy-wifi-hacking/

2. https://www.lookingglasscyber.com/blog/atm-hacking-you-dont-have-to-pay-to-play/
   https://www.tpsworldwide.com/atm-skimming-preventing-bank-card-hacks/
   https://mens-en-samenleving.infonu.nl/diversen/22626-hoe-skimmers-skimmen.html

3. https://www.pandasecurity.com/en/mediacenter/security/keyloggers-be-careful-what-you-type/
   https://ecobank.com/personal-banking/security-centre/scams/keyloggers
   https://www.malwarebytes.com/keylogger/

4. https://www.vpngids.nl/veilig-internet/surfen/wat-is-encryptie/

5. https://kinsta.com/nl/blog/sql-injecties/
   https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

6. https://www.ncsc.nl/onderwerpen/ddos/het-nederlandse-anti-ddos-initiatief
   https://www.nbip.nl/nawas/

Hst 2. Advies rapport

2.1 onderzoeksvragen

- Is het ontwerp compleet, of mist het nog informatie?
  Nee, het mist geen informatie en ziet er compleet uit. Het bevat alle standpunten en bij de literatuurlijst zijn alle belangrijke bronnen vermeld en door een website link verbonden.

- Kan er iets kapot gaan en verbeterd worden?
  Ja, de dispenser uitgang kan ingebroken worden. Maar door een verbetering is het bedekt met een plaat, waardoor de aanvaller niet meer in kan komen.

- Zie je nog blinden vlekken die de peergroep gemist heeft?
  Nee, we konden geen open plekken vinden. Waarbij aanvallen mogelijk zijn op de pinautomaat.

- Zijn de maatregelingen sterk genoeg?
  Ja, de maatregelingen bedekken grotendeels de belangrijke zwakke punten van de bank. Zelfs heeft de peercoach groep meer dan 1 maatregelingen kunnen vinden voor 1 risico.

- Zijn de informatiebronnen uitgebreid genoeg?
  De literatuurlijst is goed uitgebreid en verwerkt de standpunten van de bronnen die gebruikt zijn. Dit geeft een goed zicht waar het informatie vandaan komt.

- Ziet de attack tree van de peergroep goed uit?
  De attack tree van de peergroep is ook in 2 delen verdeeld. In een hardware -en software gedeelte. Het hardware gedeelte is verdeeld hoe het fysiek ingebroken wordt, hoe moeilijk de hardware componenten betast worden en hoe de bank bescherming van de gelddispenser. Het software gedeelte is verdeeld in database hacken, datastroom onderscheppen, de GUI en pinpas stelen. Hier worden de moeilijkheidsgraden van de aanvallen gemankeerd met een ‘P van possible’ en ‘I van impossible’. Dit zorgt ervoor een gedetailleerde overzicht over de aanvallen op de bank.

- Is de DFD compleet?
  Alle standpunten van de bank zijn er in verwerkt. De gebruiker heeft dan een laag voor het invoeren van zijn data dus de pincode, balans en card ID. Dit wordt dan verstuurd naar de volgende laag en dat is de ATM laag. Hier wordt de data van de gebruiker verstuurd naar de landelijke server. Dit wordt dan vergeleken met de banken die er allemaal verbonden zijn aan de landelijke server via een Iban id. Anders gaat het via de Noob server als het uit een andere land komt. Hier wordt dan de data terug gestuurd.

2.2 beveiligingsadvies

In het geheel is het beveiligingsrapport goed bedekt. De zwakke punten waar de bank overvallen kan worden zijn goed bedekt met maatregelen die het aanval proef maakt. Voor de rest ziet het er goed uit. De feedback zal ervoor zorgen dat de beveiligingsrapport verbeterd wordt. De bronnen zijn duidelijk met goeie standpunten ernaast en de attack tree/DFD geven een goed geheel over het ontwerp.

2.3 Advies landbank

- De communicatie tussen de banken wordt gedaan door een landelijke server op te zetten. Alle banken met de zelfde land verbinden hier dan aan. Als een persoon met een bankpas wilt gaan pinnen van een bank in het zelfde land dan is dit mogelijk.
  Als de comminactieprotocol wordt er met een GET en POST request gewerkt. Deze request zijn dan onderdeel van een communicatie via HTTP verbinding. Hiermee wordt het veiliger gemaakt en gebruikt gemaakt van SSL. Dit protocol wordt dan HTTPS.

  Dus wat ons peergroep down is een landelijke communicatie op te stellen en helpen opstellen met andere peergroepen. Hiermee worden de beveiliging van de verbinding tussen de pinautomaten, landelijke server en databases gemaakt. Door het besluit van de communicatie tussen banken in ons land hebben we een het onderwerp gelijk verdeeld met elkaar. Iedereen heeft dan evenveel te doen.