Groepsonderzoeksrapport

De beveiliging van pinautomaten

MLB INC.

Auteurs: Stephan de Jonge, 0901653@hr.nl

Chinji Hoe, 0891747@hr.nl

Niek Eichner, 0889076@hr.nl

Gun Coban, 0895664@hr.nl

Datum: 24-04-15

Contents

Inleiding

Dit artikel probeert antwoord te geven op de volgende vragen: Hoe vindt betalingsverkeer tussen banken plaats. Wat houden de internationale standaarden voor banken in. Waarvoor dienen de standaarden. Op welk deel van het betalingsverkeer zijn deze standaarden van toepassing en welke nadelen hebben de standaarden. Dit rapport is geschreven voor een project van de Hogeschool Rotterdam waarin een pinautomaat gerealiseerd moet worden. Dit rapport dient als indicatie over hoe goed er over de beveiliging is nagedacht.

Kern

Banken maken geld naar elkaar over via onderlinge afspraken of via een gestandaardiseerd platform zoals SWIFT of IBAN. Deze platformen beschrijven stap voor stap hoe de communicatie plaats vindt met behulp van standaarden en afspraken. IBAN bepaald voornamelijk hoe de rekeningnummers eruit zien. IBAN nummers bevatten informatie over het land van herkomst, het soort rekening en een regulier rekeningnummer. Op deze wijze is IBAN een handige specificatie voor het beheren van internationale rekeningnummers. SWIFT bevat vele standaarden en is erg compleet. SWIFT bevat onder andere de volgende ISO standaarden: ISO 9362 (bankieren en bankiers telecommunicatie berichten plus bank identificatie codes). ISO 10383 (markt identificatie codes, zekerheden en financiële instrumenten). ISO 13616 (IBAN registratie). ISO 15022 (zekerheden en schema's voor berichtgeving). ISO 20022-1 (financiële services en universeel financieel berichtgevingsschema). RFC 3615 (definitie van uniforme bron benamingen). SWIFT verwerkt trouwens ook betalingen. Dit gebeurt via SWIFT secure messaging waarvan één datacenter in Amerika staat en de andere in Nederland. De datacenters zijn zo goed als realtime up to date met met elkaar. PCI SSC is een data security standaard dat een raamwerk biedt om de beveiliging van betaalkaarten the complimenteren en the verbeteren door standaarden en tools te leveren. ISO 27002 is de welbekende informatie beveiliging standaard voor initiërend, implementerend en onderhoudend personeel van informatie beveiligingsmanagement systemen. De context draait voornamelijk om de C.I.A. driehoek. IPSEC oftewel internet protocol security dient er voor om het IP (internet) protocol te voorzien van gestandaardiseerde mogelijkheden om de transmissie te beschermen. Voornamelijk via de implementatie van encryptie en authenticatie vanaf de IP laag in het OSI model. SSL en TLS zijn applicatie laag protocollen waarmee een beveiligde transmissie opgesteld kan worden tussen een client en een server. Door het uitgeven van publieke encryptiesleutels aan clienten en door het geheimhouden van de privésleutel die de content van publieke sleutels kan ontcijferen wordt de veiligheid van de transmissie gewaarborgd. SSL en TLS werken dus met encryptie door eerst een handshake (initialisatie) te doen en daarna geeft het een sleutel uit die gebruikt kan worden om data te versleutelen. ISO 7198 staat in onze modulewijzer als een standaard die behandelt moet worden in dit rapport. Helaas zien wij echter niet in waarom wij cardiovasculaire implantaten zouden moeten behandelen voor de beveiliging van pinautomaten. ISO 7198 laten wij daarom verder buiten beschouwing. 3DES, AES en RSA zijn veelgebruikte en bewezen encryptie methodes dit betekent echter niet dat ze waterdicht zijn. We zouden een heel rapport per encryptie methode kunnen schrijven van daar kiezen wij ervoor om de drie bovenstaande methodes kort te introduceren. RSA werkt via een public en private key principe net zoals SSL/TLS sterker nog SSL en TLS maken gebruik van RSA, 3DES of AES sleutels AES sleutels kunnen maximaal 256 bits lang zijn. RSA sleutels maximaal 4096 bits en 3DES sleutels maar maximaal 168 bits. Elke encryptie methode is uniek en heeft zijn eigen sequentie voor het versleutelen en ont sleutelen van data.

Standaarden zoals IBAN hebben voornamelijk effect op het organisatorische gedeelte van het betalingsverkeer. Het is immers belangrijk dat mensen belangrijke data direct kunnen begrijpen. Dit voorkomt fouten en onduidelijkheden. IBAN is van groot belang om de zaken voor onze voorstellingen begrijpelijk en duidelijk te houden.

Cryptografische standaarden zijn ervoor bedoelt men te assisteren met het correct versleutelen en ont sleutelen van data. In feite zou ieder zijn eigen cryptografische standaard kunnen ontwikkelen. Helaas zou dat niet gewenst zijn, aangezien men de zelf ontwikkelde standaard ook aan andere entiteiten zou moeten leveren die met hem of haar zouden willen communiceren. Door een gestandaardiseerde encryptie suite te gebruiken kan men gemakkelijk veilig met elkaar communiceren en kunnen problemen van het protocol vanuit één centraal punt opgelost worden waardoor na een revisie men alleen nog maar hoeft over te stappen op de nieuwe versie. Het is ook erg gemakkelijk zaken over het hoofd te zien met encryptie. Het gebruiken van een standaard geeft een gevoel van betrouwbaarheid aangezien de kennis gebundeld is. We mogen hiermee nog steeds niet aannemen dat de standaard 100% foutloos en betrouwbaar is want er kunnen later altijd nog fouten ontdekt worden in de implementatie die achteraf weer gerepareerd moeten worden. Gelukkig biedt het gestandaardiseerde model hier ruimte voor.

IPSEC, SSL/TLS kunnen worden gebruikt in de netwerk communicatie tussen banken. IPSEC leent zich hier beter voor aangezien er complete vertrouwelijke data tunnels opgezet kunnen worden tussen 2 locaties. SSL/TLS lijkt ons meer geschikt voor cliënten die de bank benaderen via een TCP/IP netwerk. Uiteraard spelen de encryptiemethodes hier ook een rol in. Men zou een IPSEC tunnel op kunnen zetten waarbij er gebruik wordt gemaakt van RSA sleutels.

ISO 15022, 20022-2, 10838 en RFC 3615 dienen er voornamelijk voor om data correct, inzichtelijk en verantwoordelijk op te slaan in informatie systemen. Ze beschrijven wat er nodig is voor transfers, boekingen, stortingen etc. Voornamelijk financieel verantwoordelijke richtlijnen. ISO 9362 definieert dan weer erg specifiek hoe data zich voortbeweegt door de informatie systemen voor banken.

Het grote probleem met standaarden is dat ze publiek beschikbaar zijn voor iedereen en dat iedereen ze mag en kan implementeren. Vanuit een security experts oogpunt is het niet wenselijk om de encryptie methodes te delen met de hele wereld. Waarom zou men überhaupt geen andere richtlijn mogen hebben? Het is niet alsof één of meerdere standaarden alle eisen van een entiteit kunnen en zullen dekken. Bovendien wat moet een entiteit doen als zij het niet met de standaard eens zijn? Er zijn tal van manieren om een probleem op te lossen standaarden zijn hard nodig om het overzicht te houden maar men hun eigen inzicht is onmisbaar voor de evolutie van onze digitale samenleving.

Conclusie

Implementeer en gebruik standaarden zo werkt de wereld nou eenmaal. En er zijn genoeg goede redenen om beveiligingsstandaarden toe te passen op diens netwerk of applicatie. Laten we er echter rekening mee houden dat standaarden ook exploiteerbaar zijn en dat men er van alles aan

kan doen om standaarden te saboteren zolang zij profijt hebben van hun gedane moeite. Gebruik standaarden om iets veilig genoeg te maken. Want compleet waterdicht bestaat niet. We kunnen de kans zo klein mogelijk maken door bestaande standaarden correct te implementeren immers moeten we dan ook de juiste standaarden voor ons doel kiezen.

Wij zullen dus gebruik gaan maken van SSL/TLS met RSA sleutels voor een beveiligde data transmissie tussen de pinautomaat en de database server. De database server wordt via een API aangesproken. De API maakt gebruik van het HTTPS protocol (http + SSL/TLS). Ook gebruiken we de CIA driehoek om onze acties te controleren. Het feit dat het bankrekeningnummer en de pincode versleutelt op de betaalpas staan is ook gestandaardiseerd. De pinautomaat verstuurt geen pincodes alleen bankrekeningnummers van de pas. De pincode is dus ook niet bekend bij de bank de bank geeft hem één keer uit en kan hem indien wijzigen maar de code zwerft niet in de database van de bank. Onze pinautomaat accepteert geen passen die hij niet kent. Als er een onzinnig getal op de positie van het rekening nummer of de pincode staat dan negeert hij dit. De automaat neemt alleen pincodes van 4 getallen lang. Lokale gebruikersvariabelen worden direct geleegd wanneer de klant klaar is met de automaat. Dus na het printen van de bon worden automatisch gebruikersvariabelen gewist. De pinautomaat heeft een privé decryptie sleutel deze bevindt zich in de microcontrollers NVRAM is niet gemakkelijk te onderscheppen tenzij iemand een redelijk tot erg capabele elektrotechnische of technische informatica ingenieur is. De microcontroller die wij gebruikt hebben is vele malen meer kwetsbaar dan iets wat praktisch verantwoord is. Zoals boven al vermeld werd is het niet mogelijk de database server direct aan te spreken als pinautomaat. Elke pinautomaat moet via de API de database aanspreken. Dit geeft aanzienlijk meer controle over de transmissie. En het maakt het maken van betrouwbare logboeken veel makkelijker. Als de tijd het toelaat kunnen we al het HTTPS verkeer ook nog door een IPSEC tunnel laten lopen zodat de data dubbel versleuteld is tijdens transmissie.

Bronnen

Wikipedia 2015. Online dictionary. Geraadpleegd April 2015. URL: http://en.wikipedia.org.

ACM DL Digital Library 2015. Geraadpleegd April 2015. URL: http://dl.acm.org.

ACM DL Digital Library 2010. Towards understanding ATM security: a field study of real world ATM use. Geraadpleegd April 2015. http://dl.acm.org.

ACM DL Digital Library 1999. Security issues in ATM networks. Geraadpleegd April 2015. URL: http://dl.acm.org.

ISO 2015. Geraadpleegd in April 2015. URL: http://www.iso.org/iso.

PCI 2015. Geraadpleegd in April 2015. URL: https://www.pcisecuritystandards.org.