november 2009 nummer 7

INFORMATIEBEVEILIGING

Internationale normen voor IT beveiligingstechnieken

De juridische aspecten van digitaal onderzoek

Hoe veilig is PassWindow?

De kwetsbaarheden van browser plugins

PvIB
Platform voor InformatieBeveiliging

ib

Is PassWindow wel echt zo veilig als de maker claimt?

Auteur: Andor Demarteau > Andor Demarteau is Security Consultant bij CapGemini en is bereikbaar via andor@nl.linux.org.

In dit artikel introduceert de auteur het authenticatiesysteem PassWindow en verdiept hij zich in de toepasbaarheid en de veiligheid ervan. Maar eerst wordt de achtergrond uitgelegd: wat is nu precies 1, 2 en 3 factor authenticatie en hoe doen we het nu? Daarna gaat Andor Demarteau in op PassWindow en analyseert het verschil tussen het product enerzijds en RSA-tokens en one-time pads anderzijds. Tot slot worden de toepassingsmogelijkheden van PassWindow beschreven.

Factor authenticatie

Je hebt drie verschillende authentiserende factoren nodig voor 3-factor authenticatie: De categorisatie gaat als volgt:

- iets dat je hebt: smartcard, token, PassWindow, et cetera.
- iets dat je weet: passwords, pincodes, andere geheime teksten en combinaties
- iets dat je zelf bent: een biometrisch kenmerk, bijvoorbeeld een vingerafdruk

Wat maakt een 2- of 3-factor authenticatie nu sterker dan één van deze drie factoren op zichzelf? Eén van de basisprincipes in de IT security is hoe meer verschillende gegevens je over iemand hebt en kunt gebruiken om diegene te identificeren, des te zekerder ben je ervan dat hij of zij het ook echt is. Daarop volgt dan de authenticatie van die persoon aan de hand van diezelfde gegevens. Overigens geldt dit ook voor fysieke beveiliging en toegangscontrole. Meer authentiserende gegevens maakt het lastiger voor hackers om in te breken door zich voor te doen als een geautoriseerde gebruiker.

Alleen een wachtwoord of pincode is niet veilig genoeg. Beide kun je aan iedereen vertellen en (wat natuurlijk vaak genoeg gebeurd) opschrijven en ergens onder plakken. Denk maar aan de Post-its onder toetsenborden en bureaus.

Maar wat nu als je naast dat gegeven ook een smartcard nodig hebt? Als je dan je wachtwoord opschrijft en ergens achterlaat, hebben kwaadwillenden er nog niets aan. Ze moeten je ook nog je smartcard afpakken. Het omgekeerde gaat natuurlijk ook op: als je toegang hebt met alleen een badge zonder pincode, dan is het verliezen ervan voldoende voor de vinder om zichzelf toegang te verschaffen. Maar als er ook nog een pincode bij nodig is, dan moet je beide hebben wil je toegang kunnen verkrijgen.

En ja, ik weet dat een aantal lezers nu direct denkt aan het skimmen van bankpassen. Vaak lezen fraudeurs een pincode af door middel van een camera boven het keypad, waarmee ze de toetsaanslagen vastleggen. Een effectieve maatregel om dit te voorkomen is je hand af te dekken met bijvoorbeeld je portemonnee, zodat de camera niet kan zien welke knoppen in welke volgorde worden indrukt. Oké, het is een 'security through obscurity' maatregel, maar het is beter dan niets. Want als het hele apparaat gecompromitteerd is, kun je doen wat je wilt, dan helpt niets.

Iets dat je hebt

Zoals gezegd gaat dit puur om iets dat je bij je hebt (een bezit), waarmee je identificeerbaar bent. Dat kan een toegangsbadge, een paspoort, een nationale ID-card, maar ook een gewone sleutel zijn. Hoewel je met een sleutel bij je eigen voordeur of je auto niet uniek identificeerbaar bent (tenzij het de enige sleutel is), krijg je met die sleutel wel toegang tot je woning of je auto. Letterlijk gezien authenticeer je jezelf als legitieme gebruiker door het slot te openen.
Niet veilig genoeg? Dat klopt, als je wel eens een sleutel bent kwijtgeraakt, weet je daar alles van. Maar een toegangsbadge voor je werk is wat dat betreft net zo onbetrouwbaar als de sleutel van je woning. Dit op zichzelf is dus zeker geen sterke vorm van authenticatie.

Iets dat je weet

Die onbetrouwbaarheid geldt overigens voor alle drie de vormen als je ze op zichzelf staand gebruikt. Maar helemaal voor wachtwoorden! Sommige mensen ruilen hun gebruikersnaam en wachtwoord gewoon in voor een chocoladereep. In een artikel getiteld Passwords revealed by sweet deal, rapporteerde de BBC in april 2004 dat bij een onderzoek onder willekeurige reizigers in Liverpool Street zeventig procent bereid was hun inlog gegevens af te geven in ruil voor een chocoladereep. Erger nog; vierendertig procent gaf de inlog gegevens zelfs zonder het aanbieden van de chocolade af. Puur en alleen doordat de onderzoekers vroegen of hun wachtwoord iets te doen had met huisdieren, achternaam of favoriete voetbalclub.
Hoewel dit artikel ruim vijf jaar oud is, vermoed ik dat er wat dat betreft niet veel is veranderd. Een tweede onderzoek wees uit dat ruim negenenzeventig procent van de ondervraagden ongewild informatie gaf, waarmee identiteitsdiefstal mogelijk is. Tachtig procent van de ondervraagden heeft een hekel aan wachtwoorden en vraagt zich af of het niet anders kan *(bron: http://news.bbc.co.uk/2/hi/technology/3639679.stm)*.

Iets dat je bent

Biometrie, het meten van biologische kenmerken, wordt tegenwoordig veel gezien als dé oplossing voor alle authenticatie

alex_lee2001, via Flickr.com

problemen. De vraag is of dat zo is. Kijk bijvoorbeeld naar vingerafdrukken, een veelgebruikte biometrisch kenmerk dat gevoelig blijkt te zijn voor fraude. Dat werd pijnlijk duidelijk in april 2008 toen het Duitse hackerscollectief, Chaos Computer Club, de vingerafdruk van een minister op een folie meestuurde met het clubblad Datenschleuder. Het was hun protest tegen het opnemen van een vingerafdruk in het nieuwe paspoort, zo valt ondermeer te lezen op de site van Bruce Sneier onder de titel German Minister's Fingerprint Published *(bron: http://www.schneier.com/blog/archives/2008/04/german_minister.html)*.

Daarbij toonde het hackerscollectief twee belangrijke feiten aan:
- vingerafdrukken zijn te gemakkelijk te kopiëren.
- en, nog veel belangrijker, als dat is gebeurd, is het originele biometrische gegeven volledig onbruikbaar geworden voor de rest van het leven van de eigenaar.

Een ander interessant voorbeeld, wat dichter bij huis en ook van vorig jaar, is natuurlijk Albert Heijn met zijn vingerafdrukbetalingssysteem. Ook hier bleek het kinderlijk eenvoudig om de vingerafdruk van deelnemers aan deze vorm van betaling te kopiëren en op hun kosten vervolgens boodschappen te doen. Dat blijkt uit een artikel in het Algemeen Dagblad: AH opgelicht met rubberen vingerafdruk *(bron: http://www.ad.nl/binnenland/2410057/AH_opgelicht_met_rubberen_vingerafdruk.html)*.

En dan nog iets: biometrische gegevens veranderen door de tijd. Ook kleine dingen kunnen invloed hebben. Denk hierbij bijvoorbeeld aan een sneetje in de vinger, waar al dan niet een pleister overheen zit en een verkoudheid die invloed heeft op stemherkenning. Zo zijn er voor bijvoorbeeld irisscans, gezichtsherkenning en andere biometrische kenmerken ook vele veranderingen te bedenken. Toegegeven, een biometrisch kenmerk kun je niet kwijtraken, zoals een badge, of vergeten, zoals een toegangscode. Maar je kunt het wel kwijtraken als betrouwbaar gegeven als het gekopieerd en vervolgens misbruikt wordt.

Dat geldt in hoge mate voor vingerafdrukken. Je laat ze overal achter en daarmee is een vingerafdruk vele malen beroerder als authenticatiemethode dan het geeltje onder het bureau. Irisscans, handprintscans en andere, meer geavanceerde, biometrische methodes zijn navenant ook minder goed te kopiëren en daarmee bruikbaarder. Het nadeel is dat de apparatuur daarvoor weer duurder is en het daardoor niet of nauwelijks wordt gebruikt.

Biometrie is geenszins volledig slecht, kopieerbaar en dus onbruikbaar. Echter; bij gebruik ervan zal heel goed moeten worden gekeken naar de toepasbaarheid, de kosten, de mogelijke afwijkingen in de metingen en kopieerbaarheid van het biometrische gegeven.

Tokens en one-time pads

De meeste tokens zijn eigenlijk een digitale vorm van een one-time pad of OTP. Ze genereren namelijk een pseudorandom combinatie van cijfers of een combinatie van cijfers en letters die je slechts eenmalig kunt gebruiken voor het authenticatieproces.
De meeste tokens, RSA tokens of die van de

PassWindow

Is PassWindow wel echt zo veilig als de maker claimt?

banken, hebben een 2-factor authenticatie. Je hebt het token en een bijbehorende pincode nodig of, voor banken, je pas en pincode omdat die tokens universeel zijn. De voormalige Postbank (inmiddels ING) gebruikte voorheen papieren TANcode lijsten, die konden kwijtraken. Ook hier was een tweede authentiserende factor in de vorm van een wachtwoord nodig. Over de sms'jes van nu; meer dan een challenge/ response systeem is het niet. Het enige dat de bank eigenlijk weet, is dat de persoon die de gsm in handen heeft, de persoon is die de transactie wil doen.

De kracht van OTP zit in de eenmalige geldigheid van de code: mocht je authenticatiepoging in verkeerde handen terechtkomen, dan kunnen die gegevens niet zonder meer misbruikt worden om onrechtmatig toegang te verkrijgen.
Een zogenaamde 'replay attack' noemen is dus niet mogelijk.

De beveiliging van een OTP-systeem berust dus op twee principes: het niet herbruikbaar zijn van de logingegevens en, als een token met 2-factor authenticatie word gebruikt, op de betrouwbaarheid van het apparaat dat de OTP-code genereert.

Wat is PassWindow?
PassWindow is een systeem waarbij een transparant (deel van een) pasje op het beeldscherm wordt gelegd. In dit transparante deel is een 'onzichtbaar' patroon geprint. Doordat er op het scherm ook een patroon wordt getoond dat elke keer anders is, komt er in het transparante deel van het pasje een vier- tot zescijferige code tevoorschijn. Deze code kan voor online authenticatie worden gebruikt, bijvoorbeeld bij het online betalen met een creditcard.

Voordelen
De Australiër Matthew Walker bedacht PassWindow uit frustratie met alle moeilijke, dure en technische oplossingen, die wij als security professionals kennen. De basis voor zijn drive om een ander systeem te bedenken, kwam vooral voort uit het feit dat hij slachtoffer is geweest van online creditcardfraude. De afgelopen twee jaar is hij bezig geweest deze oplossing voor online authenticatie uit te werken. Volgens Walker's site (www.passwindow.com) is zijn systeem de beste oplossing voor online authenticatie.

De belangrijkste voordelen volgens hem:
- beveiliging tegen keyloggers en phishing-aanvallen, het systeem bereikt dat op dezelfde wijze als een OTP-systeem dat doet.
- gebruikers hoeven geen wachtwoorden meer te onthouden.
- beveiliging tegen social engineering, omdat het patroon niet via mail of telefoon overdraagbaar is.
- het is gemakkelijk patronen te vervangen bij verlies of diefstal, onder andere per post of per mail.
- de kaart is veilig in je portemonnee in plaats van een token die in het zicht aan een sleutelbos hangt.
- het is veiliger dan een sms omdat de patronen via SSL worden verzonden en niet over de onbetrouwbare lijnen van derden.

Op zijn site geeft hij er nog meer voordelen, maar voor dit artikel zijn dit de meest belangrijke punten. Andere voordelen, zoals de prijs van het systeem en het feit dat er geen cryptografie wordt gebruikt, wat weleens handig zou kunnen zijn in verband met bepaalde internationale wetgeving, zijn natuurlijk waar, maar zeggen niet zoveel over de beveiligingswaarde van het systeem. Cryptografie natuurlijk wel, maar niet vanwege de reden die de site opgeeft. Hoewel er dan wel weer SSL wordt gebruikt voor de verbinding. Wat verder opvalt, is dat de punten over social engineering en het makkelijk vervangbaar zijn van patronen elkaar tegenspreken.

PassWindow versus tokens
Ten opzichte van tokens heeft Walker eigenlijk maar één belangrijk voordeel: PassWindow is goedkoper en makkelijker te vervangen. Zeker als je gebruikers op afstand hun nieuwe patroon zelf laat printen en op de kaart laat plakken. Maar juist dat punt geeft ook een probleem: e-mail is nu niet bepaald het meest veilige

communicatiemiddel. En als je voor de e-mail optie kiest, dan is Walkers anti-phishing argument ook meteen om zeep geholpen.

Inderdaad, als je het goed doet zou SSL veiliger moeten zijn dan een sms-bericht. Aan de andere kant: sms een OTP, gebruik die eenmalig en je hebt in essentie hetzelfde bereikt.
En als je gebruikers inderdaad hun hardware token in het zicht aan hun sleutelbos laat dragen, dan ben je als bedrijf op het gebied van security awareness toch iets te kort geschoten. Maar grote kans dit soort gebruikers hun PassWindow pasje ook zo naast hun laptop leggen of in hun borstzakje stoppen, want elke keer die portemonnee opvissen en het pasje eruit halen en terugstoppen is ook zo'n gedoe.

In principe is er maar één reden waarom PassWindow nooit een vervanger van de token kan zijn: 1- versus 2-factor authenticatie. De PassWindow oplossing valt slechts in de categorie 'iets dat je hebt', terwijl tokens ook nog een pincode hebben en dus in de categorie 'iets dat je weet' zijn onder te brengen. Kortom; security technisch gezien is een token met pincode gewoonweg veiliger dan PassWindow.

PassWindow, waneer dan wel?
Maar is PassWindow dan onbruikbaar? Nee, dat niet. Als onderdeel van de categorie 'iets dat je hebt' is het zeker een revolutionaire en unieke oplossing, waar bijvoorbeeld de ING zijn voordeel mee zou kunnen doen als vervanger van die tancodelijsten of sms'jes.
Verder is het overduidelijk waar deze oplossing een flinke meerwaarde zal bieden. Namelijk precies op het gebied waar die frustratie van Walker is ontstaan: het voorkomen van creditcardfraude op internet. Huidige creditcards hebben een extra code op de achterkant ter verificatie dat je de echte kaarthouder bent. Helaas vragen tegenwoordig vrijwel alle online winkels die creditcards accepteren om deze code. Hiermee is het veiligheidsaspect waarvoor die code was ingevoerd volledig teniet gedaan, aangezien de winkelier nu het creditcardnummer plus verificatiecode heeft.

Als je de kaart zou uitrusten met een PassWindow die deze verificatiecode vervangt, heb je dat probleem simpel, efficiënt en goedkoop opgelost. Enige nadeel is dat bij elke transactie de online winkel aan de creditcardmaatschappij een patroon moet opvragen waarbij de kaarthouder zich kan identificeren als de legitieme eigenaar ervan (of in ieder geval diegene die de fysieke kaart op dat moment heeft). Maar aangezien er toch een verificatiestap wordt gedaan voordat de transactie door de online shop wordt goedgekeurd, is dat slechts trivaal.

Grote creditcardgegevens diefstal, zoals die van meer dan honderddertig miljoen kaarten *(bron: http://news.bbc.co.uk/2/hi/americas/8206305.stm)*, zijn daarmee redelijk nutteloos geworden. Zonder de fysieke kaart en dus het PassWindow, waarmee de verificatiecode gegenereerd wordt, is het kaartnummer en de vervaldatum niet meer voldoende voor gebruik. Dit moet dan wel altijd en bij elke transactie gebruikt worden.

Eén van de andere punten die de maker aangeeft, namelijk ter vervanging van security vragen op sites als je je password vergeten bent, is eveneens een relevante toepassing. Het enige nadeel is wel dat je voor elke site een unieke en separate pas moet hebben met dat patroon erop. Dat werkt pas echt als een initiatief als OpenID (een unieke online ID per persoon, dat bruikbaar is voor alle daarbij aangesloten sites) echt van de grond komt.

PassWindow mark II
Een inherente zwakheid van dit systeem zal echter altijd het statische patroon blijven dat op de kaart zit. Je kunt dit vervangen natuurlijk, wat vooral per e-mail onveilig is, maar het blijft een kritiek punt. Hoe zouden we dit kunnen oplossen zonder het systeem te duur, te onhandig en gewoon weer een token te maken? Meest ideaal is dat ook het patroon op de pas wijzigt per transactie. Dat kan door een nieuw patroon op basis van tijd en een basispatroon te genereren. Dan ben je ook direct af van het (foto)kopiëren van de kaart en heb je elke keer een unieke oplossing. De kaart heeft dan natuurlijk wel een chip nodig. Nu hebben de meeste smartcards die tegenwoordig al, dus ook dat is niet echt een beperkende factor. Maar hoe de chip van stroom te voorzien, is wel een struikelpunt. De techniek staat nog in de kinderschoenen, maar er zijn ontwikkelingen gaande, waarmee stroom uit de radiogolven van wifi-accesspoints gegenereerd kan worden. En aangezien de meeste gadgets tegenwoordig zowel wifi, als bluetooth hebben en er weinig stroom nodig is, lijkt dit een goede oplossing voor de toekomst. Dat we daarmee het internet weer een stuk visueler maken en een deel van onze bevolking daarmee wederom een stap achteruit doet (inclusief mijzelf), daar gaat dit artikel niet over.

Conclusie
PassWindow is een uniek en nuttig systeem, maar vooral voor beperkt gebruik, waarbij een zwakkere vorm van authenticatie voldoet. Voor vervanging van authenticatie voor systemen waar nu tokens worden gebruikt met een pincode, of generieke met een smartcard met pincode, is het geen oplossing. Als je echter een oplossing zoekt om je huidige OTP-systeem op basis van lijsten of sms-berichten te vervangen, dan is PassWindow een goede keuze.
Het is en blijft echter een 1-factor authenticatie en als je het voor 2-factor wilt gebruiken, zal er altijd een wachtwoord, een pincode of een ander te onthouden gegeven aan moeten worden toegevoegd. Of biometrie natuurlijk: Albert Heijn zou de vingerafdrukbetalingen al een stuk veiliger kunnen maken door niet alleen de vingerafdruk te gebruiken, maar tegelijkertijd een PassWindow in de bonuskaart als extra authenticatie.