

Account veiligheid vanuit het perspectief van de gebruiker

Sjors Gielen

Studentnummer: 500765899

Klas: IG 101

Leerjaar: 2016/2017

Blok: 3

Docent: Alexander Bonnee

Inhoudsopgave

Samenvatting	2
1. Inleiding	3
1.1 Terminology	3
1.1.1 MyBB	3
1.1.2 HTTPS	3
1.1.3 IP address	3
1.1.4 Hashing algoritme	4
1.1.5 Kraken van wachtwoorden	4
2. Wachtwoorden	5
2.1 Opslag van wachtwoorden	5
2.1.1 Brute force attacks	6
2.1.2 Brute force prevention rules	6
2.1.3 Dictionary attacks	6
2.1.4 Dictionary attacks prevention rules	7
2.2 Password managers	7
3. Extra security stappen	8
3.1 Two factor authentication	8
3.1.1 Sim kaart two factor authentication	8
3.1.2 Google authenticator	9
3.2 Activity alerts	9
4. Bedreigingen	10
4.1 Phishing	10
4.2 Keyloggers	11
4.3 Man in the middle attacks	12
Conclusie	14
Bronnenlijst	15
Peer reviews	17

Samenvatting

Wachtwoorden worden vaak opgeslagen in een database met behulp van een hashing algoritme. Dit hashing algoritme zorgt ervoor dat het wat tijd kost om te achterhalen wat het wachtwoord is voor een aanvaller, maar dit is heel erg afhankelijk van de kwaliteit van het wachtwoord. Dus is het vaak beter om jezelf extra te beschermen door middel van two factor authentication, deze extra stap zal het extra lastig maken om in je account te komen. Maar hier ook zijn er voor en nadelen, naast het feit dat two factor authentication niet altijd wordt aangeboden.

Als de gebruiker eenmaal de stappen heeft genomen om zichzelf te verdedigen zou het erg jammer zijn als de veel voorkomende bedreiging alsnog langs deze beveiligingen komen. Hiervoor worden drie veel voorkomende aanvallen behandeld, in de meeste van deze gevallen komt het neer op, als het er niet betrouwbaar uitziet, doe er dan niks mee.

1. Inleiding

Zelfs nu nog komen cryptoanalisten er nog steeds achter dat een schokkend groot aantal van de wachtwoorden die wordt gebruikt door gebruikers dermate zwakke wachtwoorden zijn. In een lijst die Matt Weir aan het kraken was, was de gemiddelde lengte van een wachtwoord 7.2 karakters, maar 6% van deze wachtwoorden hadden een hoofdletter en maar 1% had een speciaal karakter. Nog erger 51% van de wachtwoorden bestond uit exclusief kleine letters.(Weir, 2011). In deze paper wordt kort behandeld hoe wachtwoorden worden opgeslagen en gecommuniceerd met servers. Met constant informatie voor de gebruikers om een wachtwoord strategie te formuleren. De focus hier is niet hoe de cryptoanalisten en programmeurs de security van de gebruikers kunnen verbeteren, maar juist hoe kunnen de gebruikers hun risico minimaliseren voor onrechtmatig gebruik van hun accounts.

Hieruit volgt: hoe kunnen gebruikers zichzelf beter beschermen tegen onrechtmatig toegang tot hun accounts?

Startend met het hoofdstuk over wachtwoorden zelf waarin kort word behandeld hoe de wachtwoord opslag vaak wordt afgehandeld. Vervolgens hoe een aanvaller hier alsnog doorheen kan breken. Hierdoor worden al een paar simpele maatregelen voor een wachtwoord strategie geformuleerd.

Voor dit paper had ik persoonlijk al veel voorkennis en de DEFCON talk van Weir had mij zeer gemotiveerd tot het maken van dit paper. Vervolgens heb ik op google.scholar gezocht naar papers omtrent het onderwerp, met name papers die het hebben over de hoofdstukken of één van hun subhoofdstukken.

1.1 Terminology

In dit paper behandel ik meerdere termen uit de computer industry. Voor alle duidelijkheid wordt voor alle termen waar geen special kopje voor is opgenomen in het document hier de uitleg geplaatst.

1.1.1 MyBB

MyBB is gratis en open source, community-based software die wordt bijgehouden door vrijwilligers.(MyBB, 2017)

1.1.2 HTTPS

HTTPS is een netwerkprotocol dat bestaat op de rug van Hypertext transfer protocol(HTTP) met een toegevoegde encryptie transportlaag en/of beveiligde Sockets laag.

1.1.3 IP adres

Een IP adres(afkorting van Internet Protocol adres) is een identifier dat elk device (Computer, router, mobiele telefoon, printer, ect) van een netwerk aangereikt krijgt. Dit adres wordt gebruikt om over de correcte lijnen te communiceren met het device.

1.1.4 Hashing algoritme

Een hashing algoritme verandert een arbitraire quantiteit van data naar een vaste quantiteit. Als er data door een hashing algoritme wordt gestuurd dan komt er aan de andere kant een hash value uit. In sommige gevallen geven de zelfde datasets hetzelfde resultaat, de kans dat dit gebeurt is afhankelijk van de grootte van de hashings values.

1.1.5 Kraken van wachtwoorden

Het kraken van een wachtwoord in dit paper wordt behandeld als dat de aanvaller een manier heeft om het hashing algoritme dat wordt gebruikt na te bootsen en op die manier het wachtwoord van de gebruiker te vinden.

2. Wachtwoorden

De originele authenticatie factor. De gebruikersnaam en wachtwoord. Een combinatie al jaren lang in gebruik. Helaas door de constant gebeurende hacks en kleine fouten die we zien zoals “Cloudblood”(Cloudflare, 2017) wordt de eerste factor onder veel vuur gelegd.

Het is bekend dat het verdedigend team niet perfect is, daarom moet de gebruiker zichzelf oriënteren zodat hij/zij weet hoe groot zijn/haar risico is.

2.1 Opslag van wachtwoorden

In bijna alle gevallen worden wachtwoorden opgeslagen in een database, bijvoorbeeld een MySQL database. Dit word gedaan door middel van een simpele database query tijdens het aanmaken van het account. In sommige gevallen zijn er nog websites die geen encryptie doen op het ingevulde wachtwoord, maar in meeste gevallen worden wachtwoorden niet meer zonder encryptie opgeslagen.

Meest populair huidig is meerdere rondes van MD5 gecombineerd met een salt. Dit komt door hoe snel het is om MD5 uit te voeren. MD5 is een hashing functie die gemaakt is om zeer snel te draaien op een 32 bit machine. Bij MD5 is er wel het risico dat het proces wordt omgedraaid of op een zeer snelle manier wordt getest of een wachtwoord hetzelfde is als een ge-hashd wachtwoord. (tools.ietf, 2017)

Een wachtwoord salt is meestal uniek per gebruiker. De gebruiker hoeft zijn eigen salt niet te weten, maar de salt is wel publiekelijk toegankelijk. Dus als de aanvaller maar één persoon specifiek target help een salt niet heel erg veel.(Weir, 2011)

```
/**
 * Salts a password based on a supplied salt.
 *
 * @param string $password The md5()'ed password.
 * @param string $salt The salt.
 * @return string The password hash.
 * @deprecated deprecated since version 1.8.9 Please use other alternatives.
 */
function salt_password($password, $salt)
{
    return md5(md5($salt).$password);
}

/**
 * Generates a random salt
 *
 * @return string The salt.
 */
function generate_salt()
{
    return random_str(8);
}
```

(MyBB group, 2017)

Binnen in MyBB wordt er per user een string van acht characters gegenereerd, als salt. Het wachtwoord gaat eerst door één ronde van MD5, daarna gaat de salt door een ronde van MD5. Dan word de ge-MD5'd salt en wachtwoord aan elkaar gezet, en dan gaat dat nog door één extra ronde van MD5. In het geval van MyBB met wat we eerder hebben gezien hangt wachtwoord veiligheid grotendeels op de schouders van de salt tegenwoordig. Verder zijn de MD5 rondes niet erg goed in het veiligstellen van de wachtwoorden van de gebruikers.

Dit heeft Matt Weir in 2011 laten zien tijdens zijn Defcon talk, aangetoond met de publieke MySpace hacked lijst uit 2009. Deze lijst kwam uit als de al gekraakte wachtwoorden. Vervolgens hebben ze de wachtwoorden eenmaal door MD5 heen gehaald om een database te simuleren. In twee minuten en dertig seconden heeft hij ongeveer dertig procent van de lijst ge-cracked.(Weir, 2011)

2.1.1 Brute force attacks

Bij een brute force attack blijf je steeds een nieuw wachtwoord proberen totdat je een wachtwoord vind wat na de encryptie/hashing stappen hetzelfde resultaat geeft.

Brute force attacks kunnen natuurlijk iets efficiënter door frequentie modellen te introduceren, deze modellen hebben als doel om karakters/combinaties die zeldzaam zijn later uit-te-testen, met als gevolg dat de password cracker sneller meer wachtwoorden heeft ge-cracked.(Apostol, 2012)

2.1.2 Brute force preventieve stappen

Om niet een slachtoffer te worden van een brute force attack is vrijwel onmogelijk. Als de aanvaller genoeg tijd en/of processing kracht heeft dan komt hij/zij er altijd doorheen. Maar je kan wel de tijd die het kost om je wachtwoord te laten kraken extreem verhogen door de zoekruimte te vergroten, de volgende maatregelen helpen hierbij.

- Een langer wachtwoord kost meer tijd. Probeer je wachtwoorden minimaal met acht karakters te maken.
- Voeg een hoofdletter, een kleine letter, een getal en een speciaal karakter toe aan je wachtwoord.
- Gebruik combinaties die niet veel voorkomen. Bijvoorbeeld: De letter q is vrij zeldzaam, maar in meeste woorden wordt de q gevolgd met een u, vermijdt dus de q-u combinatie.

(Weir, 2011)

2.1.3 Dictionary attacks

Een dictionary attack is meer gefocust. Bij een dictionary attack geef je de cracking software minstens twee sets, één set met woorden en één set met mutatieregels. Vervolgens zal de cracking software het woord proberen met één of meerdere mutatieregel(s). Vaak wordt dit gebruikt in combinatie met frequentie modellen om sneller een grotere hoeveelheid van wachtwoorden te kraken.(Weir et al, 2010)

2.1.4 Dictionary attacks preventieve stappen

Uitgebreide dictionary attacks kunnen veel gaan lijken op een brute force attack, als er te veel regels worden toegepast. De beste manier om een dictionary attack zoveel mogelijk tijd te laten kosten is door woorden en standaard mutatie regels te voorkomen. Slechte voorbeelden zijn:

- Password123
Het woord "password" wordt extreem snel gechecked, en de mutatieregels, 123 na het woord plaatsen en de eerste letter als hoofdletter, zijn ook erg populair.
- 3xpl0r3r
Het vervangen van letters met nummers volgens de "l3375p34k"(leetspeak) conventies ziet er veilig uit, maar wordt snel opgepakt door een mutatieregel.

Dus probeer op willekeurige plekken letters, nummers of symbolen in te voegen.(Weir, 2011)

2.2 Password managers

Password managers zijn applicaties die voor de gebruiker wachtwoorden genereert die compleet willekeurig zijn, een erg groote lengte hebben, ze voor de gebruiker lokaal encrypt en opslaat voor later gebruik. Dit process zorgt ervoor dat de gebruiker de wachtwoorden zelf niet hoeft te onthouden. Deze wachtwoorden worden beveiligd achter één "master password" deze moet de gebruiker zelf onthouden, er zijn ook alternatieven op dit master password zoals Yubikey. Yubikey is een usbtje wat als je inplugged op de computer met de password manager, de password manager die usb gebruikt om de user in de password manager in te loggen.

Bij password managers kan de gebruiker kiezen voor een offline password manager of een online password manager. Een offline password manager is vaak een veiliger idee, de enige manier om bij de database van wachtwoorden te komen is immers moet je op het device zijn waar de password manager op staat. Maar een online password manager is vele malen makkelijker te gebruiken, bijvoorbeeld op momenten dat de gebruiker in wilt loggen op een computer van een ander.

Bij een password manager is er één groot probleem en dat is dat je garandeert dat er een single point of failure in je security systeem zit. Als je password managers wachtwoord wordt gecompriemd dan zijn all je huidige wachtwoorden gecompriemd. Maar het grote voordeel is dat je wachtwoord op elke website extreem lastig te kraken zijn en als het toch gebeurt dan is maar één account gecompriemd.

(McCarney, 2012)

3. Extra security stappen

Tegenwoordig zijn er veel websites met extra stappen om te verifiëren dat de correcte gebruiker aan het inloggen is. Over het algemeen heet dit “Two factor authentication”. Ook zijn er veel sites die een e-mail zullen sturen naar de gebruiker als er wordt ingelogd op het account vanaf een nieuw IP address, deze noemen we vaak “activity alerts”.

3.1 Two factor authentication

Two factor authentication is een vrij simpele tweede manier om te verifiëren dat we de correcte gebruiker hebben. De eerste factor is dat de gebruiker het juiste wachtwoord heeft ingevuld. Dus zodra er een tweede manier is om te verifiëren dat de correcte gebruiker inlogt op een account is dit al “two factor authentication”. In de praktijk zien we dat meeste two factor authentication methoden een kleine hoeveelheid nummers gebruiken die in een korte tijdperiode blijven veranderen.(de Borde, Duncan, 2012)

3.1.1 Sim kaart two factor authentication

Bij sim kaart two factor authentication wordt een tekstbericht naar de gebruikers telefoon gestuurd over sms. De code die de gebruiker ontvangt is dan bruikbaar voor een relatief lange periode van tijd zodat de gebruiker de tijd heeft om het bericht te ontvangen en in te loggen.

Voordelen van sim kaart two factor authentication

- Geen extra tokens zijn nodig omdat de gebruiker (meestal) toch al zijn/haar telefoon bij zich heeft.
- Afhankelijk van de implementatie worden de passcodes automatisch vervangen op het moment van aanvragen, hierdoor is de code die wordt ontvangen door de gebruiker altijd valide(tot de code is gebruikt, of ververst).
- Het is gebruikersvriendelijk.

Nadelen van sim kaart two factor authentication

- De mobiele telefoon moet altijd door de gebruiker worden meegenomen, opgeladen zijn en connectie hebben met het telefonisch netwerk. Als de telefoon berichten niet meer kan tonen zoals als wanneer het scherm kapot gaat of restart door een update is het onmogelijk voor de gebruiker om in te loggen.
- De gebruiker moet zijn telefoon nummer delen met de two factor authentication service provider, hierdoor is er minder persoonlijke privacy en het stelt de gebruiker open tot potentiële spam.
- Text berichten met mobiele telefoons over SMS zijn **niet** encrypted en kunnen dus makkelijk worden gestolen door een derde partij.(Toorani et al, 2010)
- Text berichten worden vaak niet instant ontvangen, hierdoor kost het authenticatie process extra tijd.
- Meestal negeert account herstel sim kaart authenticatie.(Rosenblatt et al, 2015)
- Sim cloning kan een aanvaller toegang geven tot mobiele telefoon connecties.

Naast deze nadelen is het ook nog mogelijk voor de aanvaller om de mobiele provider te bellen en zichzelf voor te doen als een klant die zijn sim kaart kwijt is geraakt. Als deze

social engineering aanval werkt dan kan de aanvaller een sim kaart met de contactgegevens van zijn doelwit ontvangen en op deze manier langs de two factor authentication heen komen.

3.1.2 Google authenticator

Google Authenticator is een applicatie waar een two factor authentication code op wordt gegenereerd. Dit doet google door middel van een Time-based One-time Password algorithm(TOTP) en HMAC-based One Time Password Algorithm(HOTP).(Google, 2016)

Het typisch gebruik van de Google authenticator is dat de gebruiker de app installeert op een device dat compatibel is met het programma. Vervolgens stuurt een server een secret key over een beveiligde connectie, hierdoor kan de applicatie zelfs zonder internetconnectie een code genereren die synchroon is met de huidige actieve code op de server.

3.2 Activity alerts

Veel websites hebben tegenwoordig activity alerts, als er een log in poging op een gebruikersaccount wordt gemaakt vanaf een nieuw IP adres is het hoogstwaarschijnlijk dat websites dit soort informatie naar het e-mailadres van de gebruiker zullen sturen.

Naast een nieuw IP adres zijn er ook veel sites die de locatie opzoeken van het IP adres dat werd gebruikt, als deze te veel afwijkt van de gewoonlijke sets van IP adressen word er een e-mail verstuurt.

Als een website dit soort service aanbiedt is het hoogst aangeraden om hier gebruik van te maken. Als een website dit niet heeft kan de gebruiker nog steeds vaak zien wat er met het account gebeurt is via activity history. Bij websites waar dit de enige optie is wordt het aangeraden om hier regelmatig naar te kijken.(Hampapur, 2003)

4. Bedreigingen

Naast het proberen te kraken van een gebruikersaccount en wachtwoord zijn er andere bedreigingen waar gebruikers actief voor moeten zoeken om het risico te minimaliseren.

4.1 Phishing

Bij een phishing aanval wordt er een e-mail verstuurd door de aanvaller die lijkt op een legitieme e-mail van een bedrijf zoals de e-mail in de afbeelding (zie afbeelding 1) Phishing krijgt zijn naam door “fishing” en “password” samen te voegen, want deze e-mails zijn aan het vissen voor wachtwoorden.

Als de link wordt gevolgd van de phishing e-mail komt de gebruiker op een website die lijkt op de inlog website van het bijbehorende bedrijf, maar het is daadwerkelijk een website waarbij inloggen niet werkt. Wat gebeurt er als op deze website op de inlogbutton wordt gedrukt? In plaats van dat de gegevens naar de bedrijfs server worden gestuurd worden ze naar de aanvaller gestuurd, hierdoor heeft de gebruiker zijn gegevens aan de aanvaller gegeven.

Ondanks dat phishing e-mails vaak niet door junk/spam filters heen komen zijn de aanvallen nog steeds erg succesvol (Egelman, et al, 2008).

Hoe detecteren we een phishing poging als gebruiker?

Bekijk het adres waar de e-mail vandaan kwam. Vergelijk het met het e-mailadres van eerdere legitieme e-mails.

Let op de site waar de e-mail u naartoe stuurt. In de meeste gevallen zullen officiële websites over https communiceren.


 Cooperatieve Rabobank U.A. [NL] | <https://www.rabobank.nl/particulieren/>

Figure 2 Rabobank, rabobank.nl

De officiële url van de rabobank ziet er zo uit. Het linker onderdeel toont aan dat de website waar uw computer mee communiceert, communiceert door middel van https. Let op! Een aanvaller kan ook een https certificaat halen voor zijn neppe website.

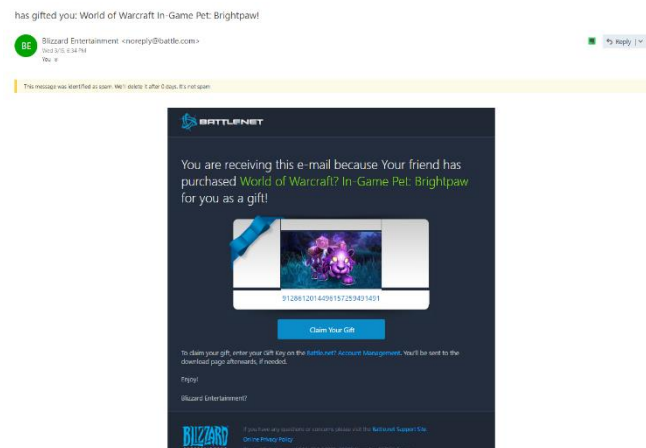


Figure 1 E-mail, persoonlijk ontvangen

4.2 Keyloggers

Keyloggers zijn één van de meest serieuze vorm van malware, een keylogger houdt in een log alle activiteit van het keyboard bij en in de meeste gevallen verstuurd het deze data naar een derde partij.(Holz et al, 2009). Er zijn twee groote branches van keyloggers, software based keyloggers en hardware based keyloggers.(pctools, 2017) Hardware keyloggers zijn relatief makkelijk om te vinden(zie figuur 3) maar de software varianten zijn een stuk lastiger om te detecteren. Al helemaal als we kijken naar hoeveel verschillende varianten er zijn.



Figure 3Wikipedia, Keylogger-hardware-PS2-example-connected.jpg

- **Hypervisor-based:** De keylogger kan in theorie in een malware hypervisor zitten en vervolgens draaien onder het operating system, wat dus met rust wordt gelaten door het operating systeem, het wordt haast een virtual machine.
- **Kernel-based:** Een programma op het device krijgt root toegang, verstopt zichzelf in het operating systeem en ontvangt keyboard invoer dat door de kernel heen gaat. Deze zijn erg lastig om te maken en te detecteren omdat ze op het operating systeem niveau draaien en hierdoor dus volledig toegang hebben tot de hardware.
- **API-based:** Deze keyloggers maken gebruik van API hooks in bestaande programma's zodat zij bij de keyboard events kunnen, alsof het een standaard applicatie was in plaats van malware.
 - Windows APIs zoals GetAsyncKeyState(), GetForegroundWindow(), etc. Worden gebruikt om het keyboard te pollen.(Canavan, 2005) Een nog recentier voorbeeld polled de BIOS voor pre-boot authenticatie PINs die nog niet uit memory zijn gedelete.(Brossard, 2008)
- **Form grabbing based:** Form grabbing-based keyloggers loggen websites forms(zoals een inlog form) door het form op te slaan tijdens het submit event. Dit gebeurt als de gebruiker een form verstuurt, gewoonlijk door op een knop op de site te drukken of door op enter te drukken. Dit soort keylogger slaat de data op voordat het wordt verstuurt over het internet.
- **Javascript-based:** Een kwaadaardig script tag is geïnjecteerd in de webpagina, dit script zal dan luisteren voor key events zoals onKeyUp(). Scripts kunnen worden geïnjecteerd via een groote range van methodes zoals cross-site scripting, man-in-the-browser, man-in-the-middle of als de website's broncode is aangepast.(Threatpost, 2016)
- **Memory injection based:** Memory Injection (Man in the Browser)-based keyloggers Executeren hun logging door de geheugen tafels van de browser en andere systemen functies aan te passen. Door het aanpassen van de geheugen tafels of het direct injecteren van het geheugen kan de malware auteur langs de Windows User Account Control komen.(Krebs on Security, 2011)
- **Packet analyzers:** Deze keyloggers proberen netwerkverkeer geassocieerd met een HTTP POST event te ontvangen om non-encrypted wachtwoorden te loggen. Dit is moeilijker gemaakt door met HTTPS te communiceren, wat ook één reden was dat HTTPS is gecreëerd.

- **Remote access software keyloggers:** Dit is een lokaal stuk software dat toetsen logged met de mogelijkheid om de logs te versturen naar een ander device. Methodes om dit te doen:
 - Data word geupload naar een website, database of een FTP server.
 - Data is regelmatig naar een e-mail adres verstuurt.
 - De software stelt de aanvaller mogelijk om in te loggen op het lokale device via het internet of het lokale netwerk zodat de aanvaller de logs kan ophalen uit de target device.

Software keyloggers kunnen op meerdere manieren worden geïnstalleerd. In veel gevallen wordt een stuk software illegaal gedownload en tijdens de installatie van de software wordt de keylogger ook wordt geïnstalleerd. Wat ook een optie is is om een installatie usb te maken, deze voor een korte periode van tijd in de device van een target pluggen, lang genoeg dat de software zichzelf kan installeren in de achtergrond. Dit werkt vergelijkbaar met hoe een CD automatisch een bepaald programma opstart als de CD in een computer wordt gedaan.

4.3 Man in the middle attacks

Een man in the middle attack is wanneer iemand alle data over een netwerk ontvangt en doorstuurt naar de persoon die het had moeten ontvangen.

In meeste gevallen kan de aanvaller niet heel veel met de data omdat de data encrypted is, bijvoorbeeld als je over https met een server communiceert. Maar als de aanvaller de "handshake" meemaakt heeft hij de keys van de encrypted communicatie. (Kaufman, et al, 2002) Deze handshake komt voor in public key cryptography, waarvan er tegenwoordig veel voorbeelden zijn, immers in 1996 is het concept al bedacht. (Golob, Solomon. 1996)

Ter illustratie. Alice en Bob gaan een gesprek met elkaar aan, maar Mallory is een man in de middle attack aan het uitvoeren.

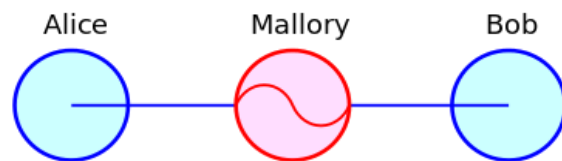


Figure 4(Wikipedia, Man in the middle attack)

- Alice stuurt een bericht naar Bob, deze word ontvangen door Mallory
 Alice "Hoi Bob, het is Alice. Geef mij jou key." → Mallory Bob
- Mallory verstuurt een kopie van het bericht naar Bob, Bob kan niet zien dat het bericht niet echt verstuurt is door Alice, het lijkt alsof het bericht van Alice komt.
 Alice Mallory "Hoi Bob, het is Alice. Geef mij jou key." → Bob
- Bob verstuurt zijn key
 Alice Mallory "[Bob's key]" ← Bob
- Mallory vangt Bob's key met haar eigen key en verstuurt deze naar Alice alsof het de key van Bob is.
 Alice ← [Mallory's key] Mallory Bob
- Alice encrypt haar bericht met wat zij denk dat de key van bob is zodat alleen bob het bericht kan openen
 Alice "Zie je zo bij de bus halte"[Encrypted met Mallory's key] → Mallory Bob
- Vervolgens kan Mallory het bericht lezen, en aanpassen zover zij wil en het doorsturen naar bob.
 Alice Mallory "Zie je zo bij de rivier"[Encrypted met Bob's key] → Bob

- Bob denk dat het bericht veilig vanaf Alice af is gekomen.
- Bob gaat naar de rivier en wordt beroofd door Mallory.
(Wikipedia, Man in the middle attack)

Dit voorbeeld toont dat in principe het moment van de handshake moet worden vertrouwd, in het geval dat dit niet wordt vertrouwd is het altijd mogelijk dat er een man in the middle attack plaatsvindt.

Tegenwoordig vinden de meeste man in the middle attacks zich plaats op netwerken van publiek bereikbare wifi punten zoals die van een restaurant. Als een aanvaller fysiek contact kan maken met de router is het mogelijk dat hij een extra computer tussen het netwerk van het restaurant zet en het internet.

Het advies hier is dan dus ook, als gebruiker, probeer nooit in te loggen op belangrijke accounts zoals een PayPal account over een publiek netwerk.

Conclusie

Account veiligheid voor gebruikers zoals in dit paper is behandeld, is niet volledig in de hand van de gebruiker, maar er zijn zeker stappen om het beter te maken. Zoals gezien in dit paper is een laptop al sterk genoeg om ongeveer dertig procent van de wachtwoorden van de MySpace lijst te kraken in een paar minuten. Om hier beter tegen te verdedigen is het aangeraden om een wachtwoord strategie te bedenken. Dit soort wachtwoord strategieën moeten niet op een naïeve manier worden geconstrueerd, vertrouw niet op leetspeak als een goede manier om getallen en speciale karakters in het wachtwoord te mixen. Maar om het nog beter te maken is het aangeraden om de computer de wachtwoorden te laten bedenken door middel van een password manager. Hier door zijn de wachtwoorden vrijwel willekeurig waardoor dictionary attacks niet zo goed zullen werken en door de lengte van de wachtwoorden zullen brute force attacks ook erg traagzaam gaan. Zelfs deze methoden zijn niet onfeilbaar, hierdoor is het aangeraden om ook two factor authentication te gebruiken waar mogelijk.

Gebruikers moeten zichzelf ook beter beschermen tegen bedreigingen. In meeste gevallen betekent het dat de gebruiker onbetrouwbare applicaties en USB's geen toegang moet geven tot hun device. Maar zelfs als al deze maatregelen worden genomen dat het niet onfeilbaar is, aanvallers blijven nieuwe kleine foutjes vinden, die in sommige gevallen al jaren in een programma bestaan.

Bronnenlijst

Apostel, K, (2012) Brute-force Attack, ISBN:613627454X 9786136274546

de Borde, Duncan. "Two-factor authentication" (PDF).gearchiveerd van het origineel (PDF) op January 12, 2012.

Brossard, J (03, 08, 2008). "Bypassing pre-boot authentication passwords by instrumenting the BIOS keyboard buffer (practical low level attacks against x86 pre-boot authentication software)" (PDF). Iviz Technosolutions. Geraadpleegd op (13, 3, 2017) <https://www.defcon.org/images/defcon-16/dc16-presentations/brossard/defcon-16-brossard-wp.pdf>

Canavan, J "The Evolution of Malicious IRC Bots" (PDF). Symantec. (26, 11, 2005): 23–24. Geraadpleegd op 25 03 2017 <https://www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf>

Cloudflare. (1 maart 2017). Quantifying the Impact of "Cloudbleed", geraadpleegd op (29 3, 2017) van <https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed/>

Egelman, S & Faith Cranor, L & Hong J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings doi:10.1145/1357054.1357219

Golob, Solomon W. (1996). "ON FACTORING JEVONS' NUMBER". Cryptologia. 20 (3): 243. doi:10.1080/0161-119691884933

Google,(2016) These implementations support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC, <https://github.com/google/google-authenticator>

Hampapur, A & Brown, L & Connell, J & Pankanti, S & Senior, A & Tian, Y (2012) Smart surveillance: applications, technologies and implications doi: 10.1109/ICICS.2003.1292637

Holz, T. & Engelberth, M & Freiling, F. Learning more about the underground economy: a case-study of keyloggers and dropzones. In Proceedings of the 14th European conference on Research in computer security, ESORICS'09, 2009, ISBN:3-642-04443-3 978-3-642-04443-4

Kaufman, C & Perlman, R & Speciner, M. Network Security: Private Communication in a Public World, Second Edition. Prentice Hall PTR. p. 169. ISBN 978-0-13-046019-6

Krebs on Security "SpyEye Targets Opera, Google Chrome Users". Geraadpleegd op (26, 3, 2017) <https://krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/>

MyBB group, (10, 1, 2017) MyBB forum software (Version 1.8.10). Geraadpleegd op (20, 3, 2017) <https://mybb.com/download/>

McCarney, D & Barrera, D & Clark, J & Chiasson, S & Oorschot, P.(2012) Tapas: design, implementation, and usability evaluation of a password manager. Doi: 10.1145/2420950.2420964

Pctools, what is a keylogger, Geraadpleegd op (29, 03, 2017) <http://www.pctools.com/security-news/what-is-a-keylogger/>

Rabobank.nl, Geraadpleegd op (25, 3, 2017) <https://www.rabobank.nl/particulieren/>

Rosenblatt, S & Cipriani, J (15 June, 2015). "Two-factor authentication: What you need to know (FAQ)". CNET. geraadpleegd op (17, 3, 2017) <https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>

Threatpost | The first stop for security news. "Web-Based Keylogger Used to Steal Credit Card Data from Popular Sites". (06 10 2016). Geraadpleegd op (24, 03, 2017) <https://threatpost.com/web-based-keylogger-used-to-steal-credit-card-data-from-popular-sites/121141/>

Toorani, M & Beheshti A. A. (2010) SSMS - A Secure SMS Messaging Protocol for the M-payment Systems. doi: 10.1109/ISCC.2008.4625610

Weir, M. (2011, 1, 11), DEFCON 17: Cracking 400,000 Passwords, or How to Explain to Your Roommate why Power Bill is a High, geraadpleegd op, (17, 3, 2017), <https://www.youtube.com/watch?v=0WPny7wk960>

Weir, M & Aggarwal, S & Collins, M & Stern, H. (2010) Testing metrics for password creation policies by attacking large sets of revealed passwords. Doi: 10.1145/1866307.1866327

Wikipedia, Man in the middle attack Geraadpleegd op (29, 03, 2017) https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Wikipedia, File:Keylogger-hardware-PS2-example-connected.jpg geraadpleegd op (29, 3, 2017) <https://en.wikipedia.org/wiki/File:Keylogger-hardware-PS2-example-connected.jpg>

Peer reviews

Ritchie Pieters:

Beoordelingsformulier Onderzoeksrapport research skills / stage

Student: Sjors Datum: 31-3 Nagekeken door: R. L. H. de

Aan ingangsvoorwaarden¹ (alle onderdelen zijn aanwezig en de tekst is leesbaar en zakelijk) voldaan ☒ ja / ☐ nee Cijfer: 8

Onderdeel	Onvoldoende (markeer hieronder wat er onvoldoende is)	Voldoende (markeer de tekst bij voldoende als het voldoende is)
1. Samenvatting	Een of meerdere onvolkomenheden spelen een rol: De samenvatting... - geeft niet de kern van het rapport weer; - is niet te begrijpen zonder het rapport te lezen; - is niet een lopend geheel; - bevat eigen mening en/of nieuwe mededelingen.	De samenvatting geeft de kern van het onderzoeksrapport weer. De samenvatting is een lopend verhaal dat te begrijpen is zonder het rapport te hoeven lezen. Het bevat geen eigen mening of nieuwe mededelingen.
2. Inleiding	Een of meerdere onvolkomenheden spelen een rol: - De inleiding bevat niet alle voorgeschreven onderdelen, te weten: de opdracht, hoe je het aangepakt hebt en de structuur van het rapport; - De inleiding geeft de hoofdvraag niet helder weer.	De inleiding bevat de voorgeschreven onderdelen (de opdracht, hoe je het aangepakt hebt en de structuur van het rapport) en geeft de hoofdvraag helder weer. N.B. De aanpak mag eventueel ook in een apart (methode)hoofdstuk staan.
3. Structuur	Een of meerdere onvolkomenheden spelen een rol: - Er is geen genummerde hoofdstuk- en paragraafindeling; - Namen van hoofdstukken en paragrafen zijn niet informatief.	Het rapport heeft een informatieve genummerde hoofdstuk- en paragraafindeling.
4. Bronnen	De tekst wordt niet onderbouwd met relevante en betrouwbare bronnen en/of er wordt niet correct naar verwezen.	De tekst wordt onderbouwd met relevante en betrouwbare bronnen; naar deze bronnen wordt correct verwezen (APA).
5. Uiterlijk	Het rapport ziet er slordig uit.	Het hele rapport heeft een verzorgd uiterlijk.
Opmerkingen	mis nog hulpjes + paginaverandering	

¹ Als niet aan de ingangsvoorwaarden wordt voldaan, wordt het rapport niet verder nagekeken. De verplichte onderdelen zijn: Titelpagina, inhoudsopgave (inclusief paginanummering), samenvatting, inleiding met methode (of dit in twee aparte hoofdstukken), resultaten, conclusie en/of aanbevelingen, bronnenlijst. Optioneel zijn voorwoord, voetnoten, bijlagen, lijst van symbolen, verklarende woordenlijst. Het rapport is in begrijpelijk Nederlands geschreven en het taalgebruik past bij een onderzoeksrapport.

Onderdeel	Onvoldoende (markeer hieronder wat er onvoldoende is)	Voldoende (markeer de tekst bij voldoende)	Goed (markeer de tekst bij goed)
6. Inhoud: Hoofdstukken en paragrafen	Hoofdstukken en paragrafen in de kerntekst bevatten geen inleidende passage en zijn niet logisch opgebouwd.	Hoofdstukken en paragrafen in de kerntekst bevatten geen inleidende passage of zijn niet logisch opgebouwd.	Hoofdstukken en paragrafen in de kerntekst bevatten een inleidende passage en zijn logisch opgebouwd ✓
7. Inhoud: Deelvragen	Niet alle deelvragen worden beantwoord en/of de antwoorden zijn niet gebaseerd op de analyse van de gegevens.	Alle deelvragen worden beantwoord, maar niet allemaal op basis van analyse van de gegevens.	Alle deelvragen worden beantwoord op basis van analyse van de gegevens. ✓
8. Inhoud: Conclusie	Een of meerdere onvolkomenheden spelen een rol: - De conclusie geeft geen antwoord op de hoofdvraag; - De conclusie bevat nieuwe informatie.	De conclusie geeft antwoord op de hoofdvraag en bevat geen nieuwe informatie. ✓	De conclusie geeft een goed beargumenteerd antwoord op de hoofdvraag en bevat geen nieuwe informatie.
Opmerkingen			

Onvoldoende (1-5)	Voldoende (6)	Ruim voldoende (7)	Goed (8)	Zeer goed (9)	Excellent (10)
Er is niet aan de ingangsvoorwaarden voldaan. Of: Een of meerdere onderdelen van onderdeel 2-8 zijn onvoldoende. De mate van onvoldoende kan hier worden uitgedrukt in het cijfer 1-5.	De onderdelen 2-8 zijn allemaal voldoende.	De onderdelen 2-8 zijn minimaal voldoende en 1 onderdeel van 6-8 is goed.	De onderdelen 1-8 zijn minimaal voldoende, twee onderdelen van 6-8 zijn goed. ✓	De onderdelen 1-5 zijn voldoende en 6-8 goed.	Een perfect verslag.

Beoordelingsformulier Onderzoeksrapport research skills / stage

Student: Sjors Gielen Datum: 31-3-2017 Nagekeken door: Thomas Haagsma

Aan ingangsvoorwaarden¹ (alle onderdelen zijn aanwezig en de tekst is leesbaar en zakelijk) voldaan ja / nee Cijfer: 2

Onderdeel	Onvoldoende (markeer hieronder wat er onvoldoende is)	Voldoende (markeer de tekst bij voldoende als het voldoende is)
1. Samenvatting	Een of meerdere onvolkomenheden spelen een rol: De samenvatting... - geeft niet de kern van het rapport weer; - is niet te begrijpen zonder het rapport te lezen; - is niet een lopend geheel; - bevat eigen mening en/of nieuwe mededelingen.	De samenvatting geeft de kern van het onderzoeksrapport weer. De samenvatting is een lopend verhaal dat te begrijpen is zonder het rapport te hoeven lezen. Het bevat geen eigen mening of nieuwe mededelingen. X
2. Inleiding	Een of meerdere onvolkomenheden spelen een rol: - De inleiding bevat niet alle voorgeschreven onderdelen, te weten: de opdracht, hoe je het aangepakt hebt en de structuur van het rapport; - De inleiding geeft de hoofdvraag niet helder weer.	De inleiding bevat de voorgeschreven onderdelen (de opdracht, hoe je het aangepakt hebt en de structuur van het rapport) en geeft de hoofdvraag helder weer. N.B. De aanpak mag eventueel ook in een apart (methode)hoofdstuk staan. X
3. Structuur	Een of meerdere onvolkomenheden spelen een rol: - Er is geen genummerde hoofdstuk- en paragraafindeling; - Namen van hoofdstukken en paragrafen zijn niet informatief.	Het rapport heeft een informatieve genummerde hoofdstuk- en paragraafindeling. X
4. Bronnen	De tekst wordt niet onderbouwd met relevante en betrouwbare bronnen en/of er wordt niet correct naar verwezen.	De tekst wordt onderbouwd met relevante en betrouwbare bronnen; naar deze bronnen wordt correct verwezen (APA). X
5. Uiterlijk	Het rapport ziet er slordig uit.	Het hele rapport heeft een verzorgd uiterlijk. X
Opmerkingen	<u>nog geen tabel pagina maar word later gedaan</u>	

¹ Als niet aan de ingangsvoorwaarden wordt voldaan, wordt het rapport niet verder nagekeken. De verplichte onderdelen zijn: Titelpagina, inhoudsopgave (inclusief paginanummering), samenvatting, inleiding met methode (of dit in twee aparte hoofdstukken), resultaten, conclusie en/of aanbevelingen, bronnenlijst. Optioneel zijn voorwoord, voetnoten, bijlagen, lijst van symbolen, verklarende woordenlijst.
Het rapport is in begrijpelijk Nederlands geschreven en het taalgebruik past bij een onderzoeksrapport.

Onderdeel	Onvoldoende (markeer hieronder wat er onvoldoende is)	Voldoende (markeer de tekst bij voldoende)	Goed (markeer de tekst bij goed)
6. Inhoud: Hoofdstukken en paragrafen	Hoofdstukken en paragrafen in de kerntekst bevatten geen inleidende passage en zijn niet logisch opgebouwd.	Hoofdstukken en paragrafen in de kerntekst bevatten geen inleidende passage of zijn niet logisch opgebouwd.	Hoofdstukken en paragrafen in de kerntekst bevatten een inleidende passage en zijn logisch opgebouwd. X
7. Inhoud: Deelvragen	Niet alle deelvragen worden beantwoord en/of de antwoorden zijn niet gebaseerd op de analyse van de gegevens.	Alle deelvragen worden beantwoord, maar niet allemaal op basis van analyse van de gegevens.	Alle deelvragen worden beantwoord op basis van analyse van de gegevens. X
8. Inhoud: Conclusie	Een of meerdere onvolkomenheden spelen een rol: - De conclusie geeft geen antwoord op de hoofdvraag; - De conclusie bevat nieuwe informatie.	De conclusie geeft antwoord op de hoofdvraag en bevat geen nieuwe informatie. X	De conclusie geeft een goed beargumenteerd antwoord op de hoofdvraag en bevat geen nieuwe informatie.
Opmerkingen			

Onvoldoende (1-5)	Voldoende (6)	Ruim voldoende (7)	Goed (8)	Zeer goed (9)	Excellent (10)
Er is niet aan de ingangsvoorwaarden voldaan. Of: Eén of meerdere onderdelen van onderdeel 2-8 zijn onvoldoende. De mate van onvoldoende kan hier worden uitgedrukt in het cijfer 1-5.	De onderdelen 2-8 zijn allemaal voldoende.	De onderdelen 2-8 zijn minimaal voldoende én 1 onderdeel van 6-8 is goed.	De onderdelen 1-8 zijn minimaal voldoende, twee onderdelen van 6-8 zijn goed. X	De onderdelen 1-5 zijn voldoende en 6-8 goed.	Een perfect verslag.