

Waarom XToMe wel werkt en andere challenge response systemen niet.

Op het internet staan reacties waarom men zeker geen challenge response systemen (het anti spam mechanisme waarmee ook XToMe werkt) moet gebruiken. Echter de opmerkingen zijn van toepassing voor cr systemen in het algemeen en niet specifiek voor XToMe. Daarom geven wij hier aan of de opmerkingen van toepassing zijn voor XToMe.

Opmerking

Maar je kan toch de beveiliging met het captcha plaatje (de challenge, een plaatje met een nummer) omzeilen?

Door deze op een of andere vage website te zetten en dan een nietsvermoedende gebruiker dat nummer te laten valideren. Die input gebruik je dan weer om de e-mail terug te sturen. Het grote voordeel van e-mail is zelfs nog, dat er geen tijdslimiet aanhangt, zoals bij sommige captcha's, dus kun je ze op je gemak harvesten en rustig op allerlei vage sites laten valideren.

XToMe

Slim bedacht, maar het zal de spammer niet echt verder helpen bij XToMe.

Er zijn een aantal technieken in XToMe, die de spammer tegenwerken.

1. Binnen een gestelde periode moet er op een challenge worden gereageerd. Anders wordt de mail verwijderd.
2. Alle XToMe's (elke XToMe gebruiker heeft een XToMe op zijn PC geïnstalleerd) in de wereld werken samen (unieke eigenschap geen enkel cr systeem kan het). Met zijn alle kijken de XToMe's naar bepaalde kenmerken van een e-mail en bepalen of mail spamachtige trekjes vertoont. (hier houden wij het vaag, want de vijand luistert mee). Nee wij filteren niet en de privacy is ook niet in het gedrang. Op die spamachtige mail sturen alle XToMe servers per dag een beperkt aantal challenges. Pas als daar op gereageerd wordt, zal de volgende dag een volgende staffel challenges worden verstuurd. Dus een spammer stuurt 50.000 spam mails en de spammer ontvangt de eerste dag bijvoorbeeld 10 challenges. Worden deze bevestigd dan ontvangt men de volgende dag wederom 10 challenges. Dit gaat zo'n 6 dagen door. Dus de spammer ontvangt 60 challenges en als deze alle bevestigd worden dan komen er maar 60 spam berichten door van de 50.000. Elke spammer zal daar snel mee ophouden want daar kan je geen geld mee verdienen.
3. Als de spammer de techniek uit 2 wil omzeilen, dan is dat een heel karwei. Maar goed de spammer wil zijn viagra mail afleveren. Dan zal de spammer dus 50.000 challenges moeten ontvangen, kost de spammer bandbreedte maar ook word duidelijk waar de spammer zich bevindt. Vervolgens moet het plaatje op het net worden gezet en binnen 6 dagen moet de oplossing teruggestuurd worden. Mocht dit gebeuren dan heeft de gebruiker de mogelijkheid om zijn e-mail adres te verbergen bij een challenge, zodat de spammer niet automatisch kan bepalen waarnaar de oplossing van de challenge gestuurd moet worden. Dus om 1 spam mail af te leveren heeft de spammer 2 mails gestuurd. De gebruiker ziet dat het spam is en zet het e-mailadres op de blokkeerlijst. Kan de spammer weer van voren af aan beginnen. Theoretisch allemaal mogelijk, economisch killing voor de spammer

Opmerking

Uit wetenschappelijk onderzoek (www.ceas.cc/papers-2005/160.pdf) blijkt dat computers steeds beter in staat zijn om plaatjes met een cijfer- en lettercombinatie te interpreteren. Het lijkt dus een kwestie van tijd eer de spammer in staat is om automatisch een challenge te beantwoorden.

XToMe

Zie hierboven 1,2 en 3.

Opmerking

Maar als je dus een spamrun met een bestand adres maakt, dan sturen 50.000 XToMe's een plaatje terug naar die ene persoon. Die krijg dus een enorm achterlijke hoeveelheid plaatjes spam van iedereen, of als die persoon XToMe gebruikt, kent die de e-mail adressen niet en stuurt doodleuk weer 50.000 nieuwe plaatjes terug.

XToMe

Per adres limiteren alle XToMe's het aantal challenges, pas als die bevestigd zijn dan worden er nieuwe challenges gestuurd. Dus krijgt men een challenge van een mail die men niet verstuurt heeft dan reageert men (de ontvanger) daar niet op, krijgt men ook de andere challenges niet. Wel is het duidelijk geworden, voor de gebruiker, dat zijn e-mail adres wordt misbruikt. Gebruikt deze gebruiker XToMe dan zal deze mail (challenges) direct worden verwijderd en daar worden geen nieuwe challenges op verstuurd.

Feit is wel dat de spammer geen stap dichterbij zijn doel is gekomen, de spam mail zal niet worden afgeleverd.

Maar wat doet een spamfilter?

De bezitter van het e-mail adres krijgt mail, dat de spam mail niet was af te leveren (bounces) of reacties van boze gebruikers die de spammail hebben ontvangen. Al deze mails komen dan in zijn postvak aangezien een spamfilter ze niet tegenhoudt. Hier heeft XToMe een streepje voor. Dus wordt je e-mailadres misbruikt, laat het dan beschermen door XToMe.

Opmerking

En mail lists (nieuwsbrieven) of een mail van een automatisch winkel krijg je dus nooit meer?

XToMe

Nee niet correct. XToMe bezit een nieuwsbrief functionaliteit.

Oplossing 1.

Veronderstel je bestelt bij www.winkel.com en je verwacht van verkoop@winkel.com een bericht terug, dan zet je het domein (winkel.com) met de optie Nieuwsbrief op de doorlaatlijst. (control center (rechtsonder kruisje) rechtermuis aanklikken)

Tijdens een bepaalde periode worden alle ontvangen e-mail adressen van het domein winkel.com op de doorlaatlijst geplaatst. Na de periode blijven de e-mailadressen op de doorlaatlijst en het domein wordt van de doorlaatlijst verwijderd.

Oplossing 2.

Krijg je een bericht terug van verkoop@winkel_domein2.nl (wat meestal niet waarschijnlijk is) dan kijk bij het system/userpanel in de lijst informatie en laat daar de betreffende e-mail door (of zet het domein/e-mail adres op de doorlaatlijst).

In beide gevallen komt de mail door, je moet er wel iets voor doen.

Bestel je de volgende keer weer iets bij de winkel dan hoef je niks te doen.

Opmerking

De spamberichten blijven in je mailbox staan (bij de provider), dus die loopt langzaam vol.

XToMe

Als binnen een bepaalde periode niet gereageerd wordt op de mail dan wordt deze verwijderd.

Mocht de grote van de mailbox dan toch te klein zijn dan zijn er 2 mechanisme die je helpen;

1. Je kan de grote van de mailbox aan XToMe doorgeven mocht je de limiet van de mailbox naderen dan krijg je via de mail een bericht dat je mailbox bijna vol is. Via het system/userpanel kan je dan de mailbox opschoonen.

2. Zoals eerder aangegeven, kijken alle XToMe's of mail spamachtige trekjes vertoont. Men kan je eigen XToMe opdracht geven om te zorgen dat deze spam mails niet na 6 dagen worden verwijderd, naar na bijv. 3 dagen.
-

Opmerking

Ik heb mijn mailreader zo ingesteld dat ik alleen ASCII zie, dus zie ik helemaal geen plaatje.

XToMe

Het plaatje staat dan in de bijlage. Hetzelfde is van toepassing als de challenge op een mobiele telefoon wordt ontvangen

Opmerking

Het grote probleem is dat het probleem wordt verlegd naar afzender. Veel mensen nemen de moeite niet om te verifiëren als jij de moeite niet neemt om ze vooraf al in de doorlaatlijst te stoppen. Waarom is jouw tijd belangrijker dan de mijne, waarom zou ik de moeite doen om zoiets over te typen?

XToMe

Ja de verzender wordt om zijn medewerking gevraagd. Het vooraf in een doorlaatlijst plaatsen (ook bij een spamfilter) vergt veel meer tijd aan het doorworstelen van alle spam, dan dat een enkele verzender 1 keer een nummer moet bevestigen!

Waarom zou de zender moeite doen om zoiets over te typen?

Omdat je als afzender wil dat de ontvanger jouw mail ontvangt. Is dan 1 keer een nummer bevestigen te veel gevraagd, om in het vervolg ongestoord met elkaar te kunnen mailen en dat je weet dat jouw mail altijd bij de ontvanger aankomt. Of heb je liever dat je telkens maar moet afwachten of je mail niet in een spamfilter blijft hangen ivm een vage rede.

Opmerking

Moet je er zelf aan denken om zoveel mogelijk partijen alvast op de doorlaatlijst te zetten. Beginnend bij je hele adresboek en altijd als je je ergens aanmeld. Maar dat ga je vergeten.

XToMe

Je importeert bij het installeren (automatisch) je adresboek. Stuur je aan een nieuwe ontvanger een mail dan wordt automatisch zijn e-mail adres op de doorlaatlijst (doorlaatlijst) geplaatst. Alleen een onbekende afzender krijgt een challenge aangeboden. Trouwens, hoeveel onbekende mensen sturen jou op jaarbasis een mail 10. Hoeveel spam berichten komen er per dag toch door ... 2. Dat is op jaarbasis 700 berichten en het aantal zal elk jaar groeien. Dus helpen wij elkaar en jezelf of

Opmerking

Je moet het zelf actief bijhouden wie er op de doorlaatlijst moet komen te staan.

XToMe

Actief bijhouden is alleen van toepassing voor nieuwsbrieven verder merk je er niets van. Voor de rest neemt XToMe heel veel werk uithanden. Elke dag komt er geen spam binnen, nooit meer kijken of er een mail in de spambox zit, of deed je dat al niet meer. Met de argumentatie "als het belangrijk is dan laten zij mij het wel weten dat er iets in het spamfilter is blijven hangen".

Opmerking

XToMe werkt (momenteel) alleen in combinatie met Windows.

XToMe

Er komt een webbased versie.

Opmerking

Webbased versie? Nu vraag ik mij af... met de methode dat er eerst naar een bedrijf wordt gestuurd en daarna pas naar de e-mail client van de klant... is dat niet gevoelig voor man in the middle attacks? Of is deze zorg onterecht?

XToMe

De zorg is terecht, maar dat geldt ook voor een attack op een spamfilter dat gaat dan ook mis. Als er 10.000 computers tegen over 1 computer staan dan legt deze het altijd af.

Opmerking

De challenge heeft een grote van 35kb.

XToMe

Klopt dit vanwege 2 redenen.

1. Als je de challenge 2 talig instelt dan heeft de mail die grote, bij 1 taal 24kb
2. XToMe heeft voor challenge in een mail gekozen en niet middels een website. Dat heeft 2 voordelen;
 - a. De ontvanger van een challenge hoeft niet nog eens een webbrower te openen.
 - b. Als de challenge via een website wordt verstrekt, dan zit daar de zwakke schakel. Deze website dient dan altijd bereikbaar zijn. Het is heel makkelijk voor een spammer een website "plat" te leggen.

Maar zoals eerder aangegeven beperken wij het aantal challenges en de "last" van het versturen van challenges op spam wordt door alle XToMe's gedragen. (Alle XToMe's werken namelijk samen. Alle tegen enkele).

Opmerking

Zal dit verweer niet de start zijn voor spammers om gebruik te maken van veel geaccepteerde e-mail adressen voor Sender Address Forgery? Noem eens een leuke bekende in NL, de Rabobank?

XToMe

Ja helemaal waar.

Mocht bijvoorbeeld het email adres van de nieuwsbrief van Yahoo misbruikt worden en het adres staat op de doorlaatlijst (van je persoonlijke XToMe) dan komt de mail gewoon door.

Dit kunnen we op 2 manier verhelpen.

1. XToMe ondersteund het DomainKeys Identified Mail (DKIM) protocol, deze verifieert of de afzender van de mail daadwerkelijk de afzender is. Ondersteunen organisaties het DKIM protocol dan heeft de spammer geen kans.
 2. Bij het aanmelden van de bijv de Yahoo nieuwsbrief dient men altijd een captcha plaatje te ontcijferen. Als Yahoo nu deze tekenreeks telkens meestuurt in het onderwerp van de mail en men plaatst de tekenreeks op de woorden doorlaatlijst dan komt de mail netjes aan en spam blijft buiten. Daarmee is het probleem opgelost. Moet alleen Yahoo een kleine aanpassing maken.
-

Opmerking

Het perse moeten beantwoorden van een challenge door uw relatie voordat deze u kan mailen, is vervelend voor iemand die u kent en komt zelfs wantrouwend over. Sommige mensen zullen niet eens goed begrijpen wat er van hen verlangd wordt en de challenge niet beantwoorden of als iets 'SPAM-achtigs' wegdoen. De kans op dit laatste neemt toe als een Engelstalig cr-systeem de challenge heeft verstuurd.

XToMe

Helemaal waar, het is natuurlijk iets nieuws en mensen dienen daar aan te wennen. Net zoals veel mensen aan een e-mail programma hebben moeten wennen (wat eigenlijk toch complexer is dan het overtypen van een nummer).

Daarom heeft XToMe een aantal keuzes gemaakt;

1. Standaard challenge berichten, om de herkenbaarheid te verhogen (Oo Ik moet het nummer terugsturen).
2. De challenge berichten zijn twee talig.
3. De gewenste handeling wordt aangegeven met tekst en een plaatje.

Dat sommige mensen het als iets 'SPAM-achtigs' wegdoen, heeft te maken dat het gedrag van mensen zodanig is "aangetast" door het gebruik van spamfilters. Bij spamfilters moeten mensen altijd nog zelf even filteren, waarbij ze dan weer fouten kunnen maken. Een duidelijk teken dat spamfilters niet werken.

Opmerking

Het feit dat mailtjes pas binnenkomen als de afzender de juiste letter- en cijfercode heeft terug gestuurd, kan ertoe leiden dat belangrijke berichten vertraagd in uw mailbox komen. Dat kan in het zakelijke verkeer zelfs geld kosten.

XToMe

Als het echt een belangrijk bericht is dat snel moet worden afgeleverd dan besteed je er iets meer aandacht aan, zowel de zender als de ontvanger. Wie heeft ooit gezegd dat mailen een real time medium is? Bij een spamfilter weet je helemaal niks, het bericht staat namelijk in de spambox tussen alle spam. XToMe geeft altijd duidelijk aan hoe of wat. Alleen de mens kan dan nog een fout maken.

Opmerking

Heeft u een domein zoals @uwprovider.nl aan uw doorlaatlijst toegevoegd dan hangt een nieuw probleem in de lucht. Immers, spammers verzenden niet zelden e-mail waaraan zij als afzender volstrekt willekeurige namen en e-mailadressen koppelen. Zo kan het gebeuren dat ook spam verzonden wordt dat eindigt op @uwprovider.nl. U snapt het al, deze spam passeert ongestoord uw cr-systeem, omdat u @uwprovider.nl op de doorlaatlijst had gezet.

XToMe

Daarom is het niet verstandig om hele algemene (bekende) domeinnamen in de doorlaatlijst op te nemen. Maar anders is de kans natuurlijk heel klein, er zijn namelijk miljarden domein namen. Mocht het toch voorkomen dan kan men de domeinnaam van de doorlaatlijst halen. Alle individuele e-mailadressen van dit domein waren in de tussentijd op de doorlaatlijst geplaatst. Deze mensen kunnen nog ongestoord blijven mailen. Alleen nieuwe afzenders uit het domein krijgen een challenge aangeboden.

Opmerking

Afzenders kunnen een nieuw e-mailadres in gebruik nemen. U raadt het: uw cr-systeem kent het nieuwe e-mailadres niet en van het een op het andere moment krijgt u van uw relatie geen e-mail meer totdat deze opnieuw een challenge van uw cr-systeem heeft beantwoord.

XToMe

Klopt, zo zit het systeem nu eenmaal in elkaar.

Opmerking

Ook mensen die u een digitaal kaartje sturen via een website kunnen hun wens beter op een andere manier overbrengen. Immers, uw cr-systeem kent de afzender niet (vaak een e-mailadres dat eindigt op de domeinnaam van de betreffende kaartjeswebsite) en een bevestiging zit er ook niet in, omdat de betreffende website wel wat anders te doen heeft dan challenges beantwoorden.

XToMe

Jammer maar het is niet anders, dergelijk kaartjes zijn de grootste bron van virussen. Het werkt wel als de verzender van het digitale kaartje het e-mailadres gebruikt van degene die de kaart heeft aangevraagd, komt dat e-mailadres niet in de doorlaatlijst voor dan ontvangt deze een challenge. Daarom werk Hyves dus wel. Ook XToMe heeft zijn beperkingen.

Opmerking

Stel: Piet en Linda wisselen voor het eerst elkaars e-mailadressen uit. Piet stuurt Linda daarop een mailtje. Linda blijkt echter ook een cr-systeem te gebruiken dat vervolgens een challenge verstuurt naar Piet. Omdat Piets cr-systeem Linda ook nog niet kent, stuurt deze weer een challenge terug naar Linda enzovoorts. Goede cr-systemen vangen dit scenario op door iedereen aan wie in dit geval Piet een mailtje stuurt direct op de doorlaatlijst te zetten. Daar zit ook een nadeel aan: als Piet zonder dat hij dat weet een antwoordformulier op een malafide website invult en verstuurt, komt dat e-mailadres in de doorlaatlijst te staan en komt spam vanaf die malafide website voortaan direct binnen.

XToMe

XToMe heeft geen problemen met het 1^{ste} scenario. Het 2^{de} scenario "Piet zonder dat hij dat weet een antwoordformulier op een malafide website invult en verstuurt". Met invullen van een antwoordformulier verstuurt men geen mail via de XToMe server. Daardoor zal het adres van de website niet op de doorlaatlijst komen. Dus spam komt er niet door.

Opmerking

Mensen die blind of slechtziend zijn gebruiken software die mailtjes voorleest of omzet in braille. Een cr-systeem dat een challenge verzendt in de vorm van een plaatje is voor hen een probleem. Zij kunnen mogelijk niets met deze challenge met als gevolg dat hun e-mail niet aankomt bij de geadresseerde.

XToMe

Middels het XToMe persoonlijk standaard nummer (PSN) kan een visueel gehandicapten maar ook anderstalige die de challenge niet begrijpen, hun adres op de doorlaatlijst plaatsen. Gaat als volgt, je geeft niet alleen je e-mailadres door aan deze mensen maar ook het PSN. Als zij de PSN 1 keer in het onderwerp zetten dan wordt hun e-mailadres op de doorlaatlijst geplaatst, daardoor wordt alle mails van deze mensen in de toekomst doorgelaten.

Opmerking

Een cr-systeem handelt feitelijk tegenstrijdig aan het alom gehuldigde principe dat je spam nooit moet beantwoorden. Immers, een cr-systeem stuurt per definitie een challenge naar vreemde afzenders en doet dat dus ook bij spam. De spammer is u dankbaar: hij weet nu zeker dat uw mailadres bestaat!

XToMe

Eerst een fabeltje uit de wereld halen de spammer wist toch wel dat je adres bestaat. Er zijn heel eenvoudige manieren om te achterhalen of een e-mailadres bestaat. Maar nu het goede nieuws, mocht het een slimme spammer zijn dan stopt deze met het versturen van spam naar jouw e-mailadres om dat deze weet dat het toch geen zin heeft. Is het een domme spammer dan pleeg je hiermee een aanslag op zijn capaciteit. Dat voorkomt dan dat andere mensen lastig worden gevallen met zijn spam. Sterker nog onze business versie houdt de spammer aan het lijntje zodat zijn gehele capaciteit sterk afneemt.

Opmerking

Naast een lokaal cr-systeem dat op uw eigen computer zijn werk doet, bestaan ook cr-systemen op afstand, bijvoorbeeld ergens op een webserver. Afzenders die nog niet op uw doorlaatlijst staan moeten een webpagina bezoeken waar ze hun naam, e-mailadres én de reden waarom ze u willen mailen moeten invullen. Deze methode is ronduit onvriendelijk.

XToMe

Daarom maakt XToMe daar ook geen gebruik van. XToMe verstuurt zijn challenge via de mail.

Opmerking

Programma is niet te gebruiken met SSL (GMail etc.).

XToMe

Het is mogelijk voor zowel de XToMe versies die op je eigen PC/server draaien als voor de toekomstige Webbased versie. Kijk daarvoor op de website bij ondersteuning, veel gestelde vragen.

Opmerking

Ik ben paranoïde, ik klik op test (op de website van XToMe), outlook express wordt geopend met een mail naar q5000.com. Vervolgens kijk ik op www.q5000.com en dat staat me helemaal niet aan. De whois gegevens van XToMe zijn wel hetzelfde als die van de site, maar goed, ik zou er (nog) niet aan beginnen.

XToMe

Nee niet paranoïde. Aangezien XToMe diverse edities kent. Hebben wij diverse domein namen waar achter een bepaalde editie "schuil" gaat. In dit geval mail je naar de business editie met een autoresponder als je het nummer terugstuurt.

Opmerking

Dus mail van bedrijven de bulk reclame versturen komt dus ook niet aan. Ook als deze gewenst is.

XToMe

Is mogelijk, maar aangezien bulk reclame heel veel lijkt op spam hebben wij daar een mechanisme voor bedacht die geen inspanning vergt van de ontvanger. Het Opt-in systeem is een algemeen aanvaard systeem voor het op grote schaal verzenden van e-mail (vaak periodieke bijv. nieuwsbrieven, aanbiedingen). Iedere ontvanger heeft vooraf toestemming geven voor het toezenden van de e-mail. Hij of zij doet dit meestal door het eigen e-mail adres in te typen op het aanmeldingsformulier van een website, of door een 'subscribe'-mail te zenden naar het aanmeldadres.

XToMe heeft de mogelijkheid ingebouwd om het Opt-in systeem te ondersteunen. E-mail marketing bedrijven ontvangen dan van ons software om mail bij uw af te leveren.

Ontvangt u echter e-mail van deze E-mail marketing bedrijven en u hebt geen toestemming gegeven, stuur ons dan een klacht via contact (op de website van XToMe)). Na meerdere incidenten zal XToMe de verzender hierop aanspreken en zijn eventuele sancties niet uitgesloten.

Wij hebben er voor gezorgd dat spammers via deze methode geen spam kunnen sturen als zij het adres van de verzender gebruiken. In de (Small) Business Edition en Enterprise Edition kan de systeembeheerder deze lijst wijzigen.

Slotopmerking

Godskelere wat een klote filmpje is dat zeg..... (Animatie op de XToMe website)

XToMe

Dat we met deze animatie niet voor een Oscar nominatie in aanmerking komen begrijpen wij ook. Maar het is een communicatie middel om heel in het kort aan te geven hoe XToMe werkt. Wij zijn al sinds 2005 bezig met het ontwikkelen van XToMe wij investeren liever in het perfectioneren van XToMe dan in een perfecte animatie.
