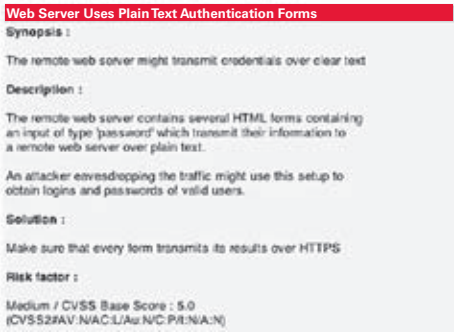
Frank Brokken / f.b.brokken@rug.nl

Twee soorten mensen

Als security manager heeft CIT-medewerker Frank Brokken de taak het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column doet Frank verslag van de stand van zaken met betrekking tot zijn missie.

Je zou kunnen stellen dat er twee soorten mensen zijn. Zij die zich afvragen wat er gebeurt en zij die dat helemaal niet interesseert. Tot de tweede groep personen reken ik bijvoorbeeld de mensen die van hun auto of computer zeggen 'hij moet het doen' zonder zich ook maar enigszins af te vragen wat er (al dan niet letterlijk) onder de motorkap gebeurt. Geldt dat ook voor u? Stop dan nu met het lezen van deze column, want die is dan niet aan u besteed.


Web Server Uses Plain Text Authentication Forms

Synopsis :

The remote web server might transmit credentials over clear text

Description :

The remote web server contains several HTML forms containing an input of type 'password' which transmit their information to a remote web server over plain text.

An attacker eavesdropping the traffic might use this setup to obtain logins and passwords of valid users.

Solution :

Make sure that every form transmits its results over HTTPS

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Hij-doet-het-niet

Zo, nu zijn we tenminste onder ons. En natuurlijk kun je het 'weten wat er onder de motorkap gebeurt' zo breed trekken als je maar wilt. Maar vraag het een willekeurige medewerker van de Servicedesk en hij of zij zal beamen dat gebeld worden met een 'hij-doet-het-niet'-probleem niet echt een duidelijke indicatie biedt van het probleem waarvoor de helpdesk eigenlijk gebeld werd. Een reactie als 'zit de stekker wel in het stopcontact?' (wat naar verluidt toch redelijk vaak de oorzaak van het probleem blijkt te zijn) ligt dan voor de hand.

Maar goed, dat zal ons niet snel overkomen, want wij zijn toch op z'n minst redelijk geïnteresseerd in wat zich zoal onder die motorkap afspeelt. Laten we daarom eens wat dichter bij huis blijven: beveiliging en het internet, om uiteindelijk terecht te komen bij een oud stokpaardje, e-mailbeveiliging, waarvoor nu eens niet geldt 'oude wijn in nieuwe zakken'. Of toch wel?

Clear text

Toen ik in 2000 de functie van security manager aanvaardde, was het eigenlijk al good practice in beveiligingsland om wenkbrauwfronsend te reageren op zogenaamde 'clear text'-protocollen. Het risico van het gebruik van 'clear text' is inmiddels weliswaar bekend bij de meeste systeembeheerders, maar helaas nog niet bij veel gebruikers.

Wie een website aanbiedt waarin middels een formulier persoonlijke informatie wordt gevraagd, zou zich moeten realiseren dat daarmee de vertrouwelijkheid van die gegevens wordt geschonden. De informatie komt in principe beschikbaar voor iedereen die zich 'op de route' tussen zender en ontvanger bevindt. Dat is zo algemeen bekend dat een programma als 'Nessus', dat kan worden gebruikt om zwakke plekken in de beveiliging van computers te detecteren, er expliciet voor waarschuwt.

Laat me een voorbeeld geven. Nog niet zo lang geleden werden 'oudere werknemers' van de RUG gevraagd om een vragenlijst in te vullen over hun functioneren, waarbij ook zaken als arbeidssatisfactie en andere aan de privésfeer grenzende informatie werd gevraagd. In een toelichtende brief werd de obligate opmerking gemaakt dat de gegevens 'vertrouwelijk' zouden

worden behandeld, en dat de vragenlijst elektronisch zou worden afgenomen.

Uiteraard werd de URL van de vragenlijst vermeld. De vragenlijst werd aangeboden op een Duits webadres. OK. Als ik meedoe aan het onderzoek dan zijn nu de onderzoekers en de medewerkers van het Duitse instituut dat de vragenlijst aanbiedt al op de hoogte van mijn privégegevens. Daarover werd in de brief niet gerept. Het is natuurlijk een kniesoor die daar op let, maar het boeiende komt nog: de verbinding was http, en dus clear text. Er zijn dus nog veel meer mensen of instanties die in principe toegang hebben tot de vragenlijstgegevens.

In het geval van de bewuste vragenlijst bleek die route langs ongeveer twintig tussenstations te lopen. Is dat niet wat veel voor de verbinding tussen Groningen en Düsseldorf? Jazeker, maar bij nader inzien misschien toch niet? De verbinding Groningen-Düsseldorf liep via Langley, Virginia. Opmerkelijk? Ik bied de eerste die mij vertelt wat ik bedoel een CD met prachtige Ierse folk-muziek aan....

Schengen

Http is clear text. Maar ook e-mail, dat misschien nog wel meer wordt gebruikt, is een clear text-protocol. Over e-mail is al zoveel geschreven dat ik zo langzaamaan aanneem dat u zich realiseert dat het versturen van e-mail vergelijkbaar is met het versturen van een ansicht- of briefkaart. Iedereen kan meegenieten en iedereen kan de afzender (suggereren te) zijn. Ik hoef op vakantie maar een briefkaart naar het CIT te sturen met daarop (aannemend dat Cees ook op vakantie is) de tekst 'groeten van Cees' om op z'n minst bij het secretariaat de indruk te wekken dat niet

ik, maar hij de briefkaart heeft gestuurd. 'Goh, Cees, was je in Eagleville? Ik dacht dat je naar Zuid-Frankrijk op vakantie was...'

Tja, e-mailbeveiliging. PGP of GPG? Ook daarover heb ik bij herhaling in deze column geschreven. Een prachtig systeem maar met een tamelijk steile 'leercurve', onder meer doordat het authenticeren van e-mail geen automatisch proces is. Hoe ging dat ook alweer met websites? Om gegarandeerd (en veilig) met een website te communiceren, maken we geen gebruik van een http- maar van een https-verbinding, die authenticatie en versleuteling biedt op basis van een certificaat dat door een certificaatautoriteit is uitgegeven. Dat klinkt bekend. Wanneer ik bij het passeren van een grens met een niet-Schengen land aan de douane mijn pas laat zien, dan accepteert men mijn identiteit op grond van het certificaat (paspoort) uitgegeven door de certificaatautoriteit de Nederlandse Overheid.

Voor webservers kunnen we dergelijke certificaten al enige jaren beschikbaar maken. Voor elke RUG https-webserver kan een gratis certificaat worden aangevraagd via de website (zie de link onderaan dit artikel).

Comodo

Oorspronkelijk werden de certificaten uitgegeven op basis van een overeenkomst tussen GlobalSign, Terena en SURFnet. Het contract met GlobalSign werd niet verlengd, maar vervangen door een contract met Comodo. Comodo biedt naast server-certificaten ook persoonlijke (Secure Multipurpose Internet Mail Extensions (S/MIME)) certificaten. Deze S/MIME-certificaten kunnen (binnenkort, waarschijnlijk al op dit moment) worden aangevraagd door alle RUG-medewerkers en -studenten.

Your Comodo FREE
Personal Email Certificate
is now ready for collection!

Net zoals dat bij GPG/PGP het geval is, kan e-mail dan worden geauthenticeerd en/of versleuteld. Het 'web of trust' dat het gebruik van PGP/GPG bemoeilijkt, speelt bij het gebruik van certificaten echter geen rol omdat die taak door de certificaatautoriteit is overgenomen. Ook wordt het gebruik van S/MIME-certificatenstandaard door meer mailprogramma's ondersteund dan GPG/PGP. Zodra de S/MIME-certificaten kunnen worden aangevraagd, zal dat uiteraard bekend worden gemaakt, onder meer op de security-website.

Groeten uit Eagleville,
Frank B. Brokken

- Programma waarmee zwakke plekken in de beveiliging van computers kan worden gedetecteerd: **www.nessus.org**
- Het aanvragen van een gratis certificaat voor een RUG https-webserver kan via **https://security.rc.rug.nl/apply/certreq.php**
- Security-website: **www.rug.nl/cit/security**