Certificaat van echtheid

Frank Brokken
f.b.brokken@rug.nl

ICT-security

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

In 1962 verscheen de film The Longest Day in de bioscopen, de verfilming van de landing in Normandië op 6 juni 1944. Ik kan me herinneren dat ik als 12-jarig jongetje gefascineerd was door de aanplakborden bij de bioscoop en ik geloof dat ik die film inmiddels minstens zeven keer heb gezien.

Uit de film 'The Longest Day'

Soldaten van de Amerikaanse luchtlandingsdivisie

In de vroege ochtend van de 6e juni 1944 landden de 82e en 101e Amerikaanse Airborne Divisies in de velden achter de landingszone, waar zij de opdracht hadden om de nazi-infrastructuur te vernietigen en bruggen te bezetten.
Verschillende eenheden van deze luchtlandingsdivisies landden op ruime afstand van hun doelen, waarna het zaak was om te voet het doel te bereiken, en zo nodig aansluiting te zoeken bij andere eenheden.

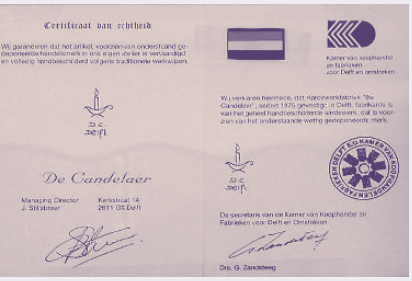
Speelgoed

Met name eenheden van de 82e luchtlandingsdivisie raakten geïsoleerd, en vaak zochten kleine groepjes para's contact met eenheden van de 101e divisie. Bij de voorbereiding van de hele operatie was dit voorzien en om die reden was elke soldaat uitgerust met een 'krekel', een klik-klak-geluid makend stukje speelgoed.
Het protocol schreef vervolgens voor dat je, wanneer je geïsoleerd zou raken van je kameraden, veilig achter een boom of bosje moest wachten totdat andere soldaten op gehoorsafstand waren. Op dat moment diende de krekel te worden gebruikt, die dan het bekende klik-klak-geluid gaf. Wanneer de klik-klak werd beantwoord door een klik-klak van de andere partij, dan had die partij zich voldoende geïdentificeerd en kon je je veilig bij hen aansluiten. Simpel en toch eenvoudig, nietwaar? Omdat de *bad guys* zo vreselijk veel op je vriendjes lijken, kan zo'n protocol erg nuttig zijn om niet in de handen van de vijand terecht te komen.

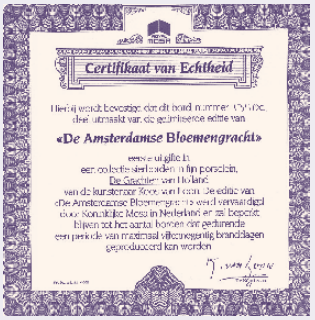
Toch kan het op een aantal manieren mis gaan. Bijvoorbeeld doordat je denkt dat je je aan het protocol houdt, maar dat in feite niet doet. Beroemd is het fragment van de geïsoleerd geraakte paratroeper die een groepje soldaten ziet naderen, zich verstopt achter een boom, zijn krekel gebruikt, opgelucht te voorschijn komt zodra hij het krekelgeluid als antwoord krijgt, om vervolgens tot zijn stomme en laatste verbazing te worden neergeschoten door de groep nazi-soldaten. In zijn haast om aansluiting te vinden bij zijn vriendjes was hij zo gespitst op het horen van het klik-klak-geluid dat hij het geluid van het doorladen van een geweer verwarde met het geluid van de krekel. Een droeve en fatale vergissing....
Deze situatie brengt me dan vanzelf bij de moderne tijd, waarin we ons gewapend met webbrowsers op het gevaarlijke internetpad begeven. Ja, toch?

Modern jasje

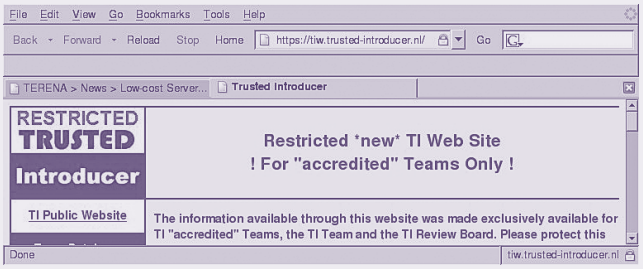
Laten we bovenstaande passage nog eens herhalen, maar dan voorzien van een modern jasje:
"Toch kan het op een aantal manieren mis gaan. Bijvoorbeeld, doordat je denkt dat je je aan het protocol houdt, maar dat in feite niet doet. Beroemd is het fragment van *de browsende internetgebruiker* (geïsoleerd geraakte paratroeper) die *een website probeert te benaderen* (groepje soldaten ziet naderen), *het door de website getoonde certificaat zonder meer accepteert* (zijn krekel gebruikt, en te voorschijn komt zodra hij het krekelgeluid als antwoord krijgt) om vervolgens tot zijn stomme verbazing te merken dat *zijn bankrekening wordt geplunderd* (hij wordt neergeschoten). In zijn haast om *contact te vinden met de gewenste website* (aansluiting te vinden bij zijn vriendjes) was hij zo gespitst op het zien van die website (horen van het klik-klak-geluid) dat



Certificaat van echtheid van de Aardewerkfabriek De Candelaer



Certificaat van Echtheid van de Koninklijke Mosa



Https-verbinding met het slotje rechts onderin

hij *het vertoonde certificaat zonder meer accepteerde* (het geluid van het doorladen van een geweer verwarde met het geluid van de krekel). Een droeve en fatale vergissing...."

Certificaten zijn er niet voor niets, en ze bestaan al lange tijd in allerlei vormen en maten. De mosategel garandeert de echtheid van de fijn-porceleinen sierborden, de Candelaer geeft een certificaat af waarmee wordt gegarandeerd dat de aardewerkfabriek de Candelaer handgeschilderd aardewerk heeft geleverd.

Hoed u voor namaak

Kloppen dergelijke certificaten nou ook? Dat hangt er maar vanaf. Ik kan natuurlijk ook zo'n certificaat maken, en met een beetje klei en wat verf prullaria bakken (handenarbeid was nooit mijn sterke kant) om vervolgens mijn prul tegen grof geld voorzien van 'certificaat van echtheid' te verkopen. Hoe voorkom je als goedwillende klant of gebruiker dat je in deze val trapt?

'Hoed u voor namaak' heet het dan. En dat doe je doordat de certificaathouder een wettig gedeponeerd handelsmerk gebruikt, dat bijvoorbeeld notarieel is vastgelegd. Op het internet gebeurt dat doordat er equivalente constructies bestaan, zogenaamde 'Certificaat Autoriteiten'.

Deze Certificaat Autoriteiten verifiëren en garanderen dat een website ook feitelijk de website van de organisatie is die de website aanbiedt. Webbrowsers accepteren dergelijke gecertificeerde websites zonder dat de gebruiker het door de website aan de browser getoonde certificaat nog hoeft te zien. Zo'n verbinding is een https-verbinding, die op z'n minst wordt gekenmerkt door een slotje in het 'go-to'-venstertje en rechts onderin.

Dergelijke certificaten zijn niet alleen handig om *phishing* (het uitvissen van persoonskritische informatie via fake-e-mails of fakewebsites) te helpen voorkomen, maar kunnen ook gebruikt worden om bijvoorbeeld te certificeren dat software afkomstig is van de organisatie die de software verspreidt.

De RUG schaft jaarlijks een aantal van dergelijke certificaten aan. Dergelijke certificaten moeten worden gekocht en zijn dan een jaar geldig. De RUG heeft echter, onder andere doordat de RUG een 'Terena Level II accredited computer security team' herbergt, nauwe banden met de Terena-organisatie. Terena heeft inmiddels een contract gesloten met GlobalSign om universiteiten en bepaalde onderzoeksinstituten tegen zeer lage kosten van deze certificaten te voorzien.

Nieuwe certificaatstructuur

Ter voorbereiding van het gebruik van deze GlobalSign gebaseerde certificering is inmiddels de werkgroep 'certificaten' opgericht. Deze werkgroep, bestaande uit RC-medewerkers Anke Breeuwsma, Frank Brokken, Hopko Meijering en Frans Velthuis, zal de komende maanden de overgang naar de standaard GlobalSign-certificaten voorbereiden. Als alles meezit, is de nieuwe structuur rond april van dit jaar operationeel.

De werkgroep zal de komende tijd naast het voorbereiden van de overgang naar de nieuwe certificaatstructuur ook inventariseren waar binnen de RUG welke certificaten worden gebruikt en zal tevens een voorlichtingscampagne starten die sterk op het 'dagelijks gebruik' van certificaten zal zijn gericht. Wie nu al meer informatie wil hebben, kan uiteraard contact opnemen met de leden van de werkgroep.

Tenslotte nog een afrondend organisatorisch puntje. De werkgroep zal zich voor wat betreft certificaten richten op de RUG als organisatie. Persoonlijke certificaten zijn formeel gezien echter ook mogelijk. Persoonlijke certificaten zouden dan kunnen worden gebruikt om de RUG-gecertificeerde authenticiteit van RUG-medewerkers vast te stellen. De werkgroep acht het gebruik van dergelijke individugebonden certificaten minder wenselijk, onder andere omdat GPG (*Gnu's Privacy Guard, Pretty Good Privacy*) daarvoor een betere infrastructuur biedt.

Individugebonden GPG-public keys kunnen overigens evengoed als certificaten door de RUG worden gesigneerd. Details hierover kunnen eveneens door de werkgroepleden worden verstrekt. In de te starten voorlichtingscampagne zal ook aan GPG aandacht worden geschonken.

Frank B. Brokken
(RUG-gecertificeerd Security Manager)

Links

- Meer informatie over *phishing*: **www.webopedia.com/TERM/p/phishing.html**
- Terena: **www.terena.nl**
- Global Sign: **www.globalsign.net**
- Meer informatie over GPG: **www.pgpi.org, en www.gnupg.org**