9. november 2010

Til Udvalget for Videnskab og Teknologi

Jeg har været i korrespondance med IT- og Telestyrelsen, hvor jeg har prøvet at få dem til at forklare mig hvordan jeg kan sikre mig at et NemID-interface på en web-side sender mine login-data til NemID, og ikke til hjemmesiden eller en tredje-part.

Efter mere end en måned med har jeg fået følgende svar:

> Peter Lind Damkjær fra DanID har svaret følgende på dine spørgsmål:
> "Det er korrekt, at man i princippet kan lave en ikke-signeret applet, så den ser ud som om, den er DanID's applet. Brugere med særlig indsigt vil kunne skelne dette ved at kigge på HTML-koden, downloade og verificere Java-appletten uden om browser-interfacet.

Hvilket jo er en ekstremt svær opgave, da Javascript kan ændre på koden, så man ville være nødt til at læse alle dele og frames på siden som kan indeholde JavaScript, inklusiv CSS.

Det er ikke mit indtryk at IT- og Telestyrelsen tager problemet seriøst.

Det ville være nemt at lave et sikkert login, hvis man bare sørgede for at alle logins foregik på en https-beskyttet side ejet af NemID, og man så derefter blev sendt videre til den side man ønskede at logge ind på. Det ville også gøre det muligt at vide, om et NemID-login på en side man ellers ikke kendte var til at stole på. Jeg er uforstående over for hvorfor denne løsning ikke er valgt, eller i det mindste er i gang med at blive implementeret.

Indtil en løsning er lavet, hvor man kan verificere modtageren, så bør NemID som et absolut minimum lave en liste over sider som har ret til at bruge NemID, som man manuelt kan checke. Ellers har jeg jo ingen mulighed for at vide om den side som jeg indtaster mine oplysninger på bare er en fishing-side som prøver at stjæle mine oplysninger.

Det er måske relevant at nævne her, at hvis man modtager stjålne login-oplysninger "live", så kan man spørge brugeren om koden fra pap-arket, og på den måde have nok til for eksempel at overføre penge fra brugerens netbank. Så mens 2-faktor koden hjælper, så kan man stadig gøre stor skade.

Desuden har jeg lige (8 november 2010) fået et brev fra NemID med nye brugsbetingelser gennem min netbank. I de nye betingelser står der blandt andet:

> Du skal sikre at andre ikke får mulighed for at aflure din adgangskode, når du indtaster den

Det kan jeg ikke se hvordan jeg har mulighed for at forhindre, så længe at jeg ikke har rimelig mulighed for at vide om det der vises i min browser faktisk er en NemID-applet. Det ville derfor være rimeligt at dette krav fjernes, indtil NemID har lavet en løsning hvor det er teknisk muligt at verificere at NemID er modtageren, og ikke en tredjepart som prøver at aflure min adgangskode.

Jeg vil lige nævne to andre urelaterede problemer med NemID

1. NemID kræver uden nogen god grund adgang til at læse og skrive vilkårlige filer på min PC. Som beskrevet på http://www.version2.dk/artikel/15865-danid-java-applet-skal-beskytte-mod-man-in-the-middle-angreb er der gjort forsøg på at argumentere for valget, men det lyder for mig som tynde efterrationaliseringer. Det er meget dårlig sikkerheds-praksis at kræve ubegrænset adgang til en brugers PC uden nogen grund!
2. NemID er min eneste grund til at have Java installeret. Men det at have Java installeret åbner mange muligheder for sikkerheds-huller i Java, som ellers ikke ville have påvirket mig. Da der

ikke er nogen god grund til at NemID ikke bare bruger almindelig HTML/JavaScript/HTTPS, er det meget uheldigt fra et sikkerheds-synspunkt at kræve en Java-plugin installeret.

Med venlig hilsen,

Thue Janus Kristensen
Rymarksvej 35, 3. 1.
2900 Hellerup