



Sterke authenticatie

Het is bekend dat alleen het gebruik van wachtwoorden als authenticatiemiddel in veel gevallen niet veilig genoeg is. Hierover zijn de meningen vrij unaniem. Desondanks gebruiken de meeste organisaties nog steeds (alleen) het wachtwoord als authenticatiemiddel. De reden is dat het grootschalig invoeren van sterke authenticatie duur is.

Bij het gebruik van een token (something you have) moet er worden geïnvesteerd in authenticatiemiddelen en in het beheer (uitgifte, registratie, intrekken) van deze middelen.

Om deze redenen is er gezocht naar unieke biometrische kenmerken als authenticatiemiddel. In dit artikel wordt "typeprint" als authenticatiemiddel besproken.

Typeprint authenticatie kijkt naar de (unieke) eigenschappen waarmee een gebruiker toetsaanslagen maakt. Hierbij spelen de snelheid waarmee een toets wordt ingedrukt en de tijd tussen twee toetsen een rol. Dit patroon zou voor elke individu uniek zijn.

Het idee van het gebruik van toetsaanslagen als herkenningsmiddel voor personen is al veel ouder.

Al in het tijdperk van de telegrafie, waarbij morsecode werd gebruikt konden telegrafisten aan de wijze waarop de seinsleutel werd bediend herkennen wie er aan de andere kant zat.

In de jaren 80 van de vorige eeuw werd dit concept verder uitgewerkt. Uit deze tijd stamt ook een onderzoek van het National Bureau of Standards (NBS), het tegenwoordige National Institute of Standards, naar de betrouwbaarheid van biometrische authenticatiemiddelen.

<i>Biometrics</i>	<i>FAR*</i>	<i>FRR**</i>
Fingerprint	~0%	~1%
Voiceprint	~1.6%	~8.1%
Typeprint	~0.01%	~3.0%

*FAR: False acceptance rate: ten onrechte geaccepteerd door het systeem.

**FRR: False rejection rate: ten onrechte geweigerd door het systeem.

Typeprint als authenticatiemiddel zou sinds die tijd verbeterd zijn, zo wordt door de leveranciers van producten aangegeven. Verder is het mogelijk om bij afwijzen van een gebruiker, aanvullende vragen te stellen, zodat een gebruiker die zijn (biometrische) dag niet heeft toch kan inloggen.

Grootschalige ervaring met deze manier van authenticatie is er echter helaas niet.

De voordelen van typeprint ten opzichte van andere vormen van authenticatie zijn groot. Uitgifte van authenticatiemiddelen is niet noodzakelijk. Het toetsenbord is het authenticatiemiddel. Op deze manier kan tegen geringe kosten en een lage acceptatiedrempel van gebruikers, sterke authenticatie worden ingevoerd.

Veel security specialisten zijn (nog) erg terughoudend over deze techniek. De vraag is wat er gebeurt als gebruikers vanuit meerdere locaties (bijvoorbeeld thuis), gebruik makend van een ander toetsenbord, inloggen.

Toepassing van deze vorm van authenticatie lijkt geschikt als toegang tot internet diensten. Het is bekend dat veel internetdiensten, last hebben van fraude ten gevolge van identity theft.

Deze vorm van authenticatie zou dan als aanvullende authenticatie moeten worden gebruikt.

Bronnen:

ID Control met het product KeystrokeID:

http://www.idcontrol.net/index.php?option=com_docman&task=doc_download&gid=25&Itemid=88&mode=view

BioPassword: <http://www.biopassword.com/password-authentication-software.php>

TimesOnline: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article1667057.ece

Nieuws op assutools.com

Ons assortiment van kennisobjecten is de laatste twee maanden uitgebreid met een compliance object voor de systeemanalyse (SA2L). Hiermee kan op basis van de uitkomsten van de systeemanalyse worden nagegaan in hoeverre de organisatie voldoet aan gestelde security richtlijnen op grond van de systeemanalyse.

Zie voor meer informatie: <http://www.assutools.com/products/compliance.htm>

Actueel

Het RDS systeem gevoelig voor manipulatie

Tegenwoordig maken veel autoradio's gebruik van RDS (Radio Data System). RDS is een datasignaal dat door een radiozender wordt meegestuurd en additionele informatie over de zender, flietsmeldingen of andere informatie kan meegeven. Navigatiesystemen gebruiken vaak RDS-TMC (Traffic Message Channel) voor informatie over files.

Twee Italiaanse onderzoekers hebben vorige maand aangetoond dat dit populaire RDS systeem erg kwetsbaar is voor misbruik.

Het RDS-TMC kanaal is onbeveiligd.

Op de CanSecWest conferentie in Canada demonstreerden zij een PC met software en een broadcaster en lieten zien hoe eenvoudig boodschappen geïnjecteerd kunnen worden. Overigens is het wel zo dat er alleen gebruik kan worden gemaakt van bestaande message codes. Er kunnen geen free format berichten worden verstuurd.

Daar tegenover staat dat er veel codes zijn, waardoor veel verschillende soorten berichten kunnen worden verstuurd. Als u een dezer dagen op uw radiodisplay in de auto leest dat er een terroristische aanval heeft plaatsgevonden op de A2, dan heeft u mogelijk te maken met zo'n vorm van injectie.

Voer voor paniekzaaiers of een serieuze bedreiging? Misschien moeten we er aan wennen niet alles te geloven wat op ons display verschijnt.

Bron:

<http://www.zdnet.nl/news.cfm?id=67613>