april 2009 nummer 2

INFORMATIEBEVEILIGING

Claims Based Access Control goed alternatief voor RBAC?

Trust management als basis voor online vertrouwen

Behavioral information security: attitude, kennis en gedrag bepalend

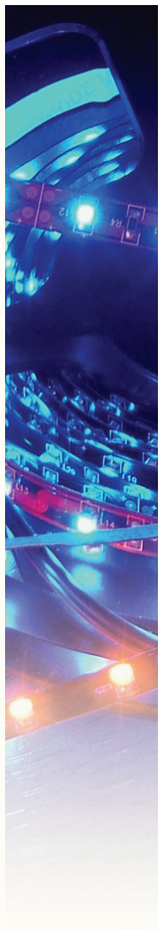
IBpedia is kennis maken én kennis delen

ib

PvIB
Platform voor InformatieBeveiliging

Trust management als methode voor authenticatie en autorisatie

Vertrouwen in beveiliging, is beveiligen met vertrouwen



Auteur: Andor Demarteau > drs. A. Demarteau is in augustus 2008 afgestudeerd bij Capgemini op het onderwerp trust management. De titel van de bijbehorende scriptie luidt: "Requirements for a Human-Centric Trust Management System in an Open De-Perimeterised Network Environment". Sinds oktober 2008 is Andor bij Capgemini werkzaam als consultant op het gebied van IT security en ethical hacking. Andor is te bereiken via e-mail: andor.demarteau@capgemini.com.

Vertrouw jij er ook altijd op dat de persoon die op een computer inlogt inderdaad diegene is aan wie je de credentials hebt verstrekt? Zo ja, weet je dat heel zeker? Vertrouw jij er ook altijd op dat de laptop die op jouw netwerk wordt aangesloten niet vol zit met malware en virussen? En dat deze door de werknemer goed wordt onderhouden? Is het bovendien wel de laptop die je hem of haar hebt gegeven? En hoe weet je dat zo zeker? Weet je zeker dat die E-bay verkoper met een verkoop feedback van honderd procent er uiteindelijk niet met jouw geld vandoor gaat? Oftewel, vertrouw jij het seller/buyer feedbacksysteem van E-bay of die betreffende verkoper voor de volle honderd procent?

In de online wereld van tegenwoordig is een begrip als vertrouwen een steeds groter en steeds vaker terugkerend buzzword. Want hoe weet je nu zeker dat je ook echt te maken hebt met een betrouwbare persoon of service, zonder dat je die persoon ook echt 'kent' of offline kunt ontmoeten?

In dit artikel geef ik je een blik in een toekomst waarin vertrouwen het belangrijkste middel wordt op basis waarvan beslissingen kunnen worden genomen in de steeds verder oprukkende online wereld van vandaag. Als je er even over nadenkt, doen we dit eigenlijk allemaal al, elke dag weer.

1. Wat is trust management?

De term 'trust management' werd voor het eerst gebruikt in 1996 door Matt Blaze in zijn design artikel voor het PolicyMaker systeem en drie jaar later voor de opvolger KeyNote. De meeste literatuur die te vinden is en zich bezig zegt te houden met dit onderwerp is feitelijk slechts bezig met het opstellen van een systeem van certificaten en de verificatie daarvan. Hoewel dit soort systemen al als een flinke stap voorwaarts kunnen worden gezien ten opzichte van statische access control lists, is deze vooruitgang slechts gebaseerd op het vertrouwen in het certificaat en de naïeve instelling dat het certificaat altijd in handen zal zijn, en blijven, van de rechtmatige eigenaar. Helaas weten wij als informatiebeveiligers wel beter. Zeker gezien de steeds groter wordende realiteit van identiteitsdiefstal en het bijbehorende misbruik. Hoewel het een aardige basis vormt, is een systeem van certificaten en de verificatie daarvan niet wat ik versta onder trust management. En een dergelijk systeem is zeker niet voldoende als systeem voor toegangs- en permissiecontrole.

Maar wat is trust management dan wel?

Trust management is het gebruik van onderlinge vertrouwensrelaties als basis voor beslissingen over authenticatie en autorisatie. Oftewel, alle acties en transacties die je onderneemt worden gebruikt om te bepalen of jij als toegangsverzoeker betrouwbaar genoeg bent om toegang te krijgen. Hierbij neemt het systeem in acht dat als jij voor een bepaalde organisatie werkt, je betrouwbaarder bent dan iemand die daar niet werkt. Vooropgesteld blijft een belangrijk basisbeginsel: ben jij wie je zegt dat je bent en zo ja, kan het systeem dat met een aan volledige zekerheid grenzende waarschijnlijkheid vaststellen? Maar daar blijft het niet bij. Als toegangsverzoeker kun je de vertrouwensvraag natuurlijk ook omdraaien: is de service waar je toegang toe wilt hebben ook daadwerkelijk de service die jij denkt dat het is en is die service en/of de beherende organisatie wel betrouwbaar genoeg om zaken mee te doen?

Een trust management systeem geeft je geen antwoord op deze vragen, het geeft je wel informatie over de betrouwbaarheid van de andere partij in het algemeen. De uiteindelijke beslissing is niet aan het systeem, maar aan de gebruikers daarvan. Het systeem vertelt je immers slechts wat het weet over een bepaalde identiteit, gegeven bepaalde parameters, jij beslist of het antwoord voldoende reden is door te gaan.

2. Waarom trust management?

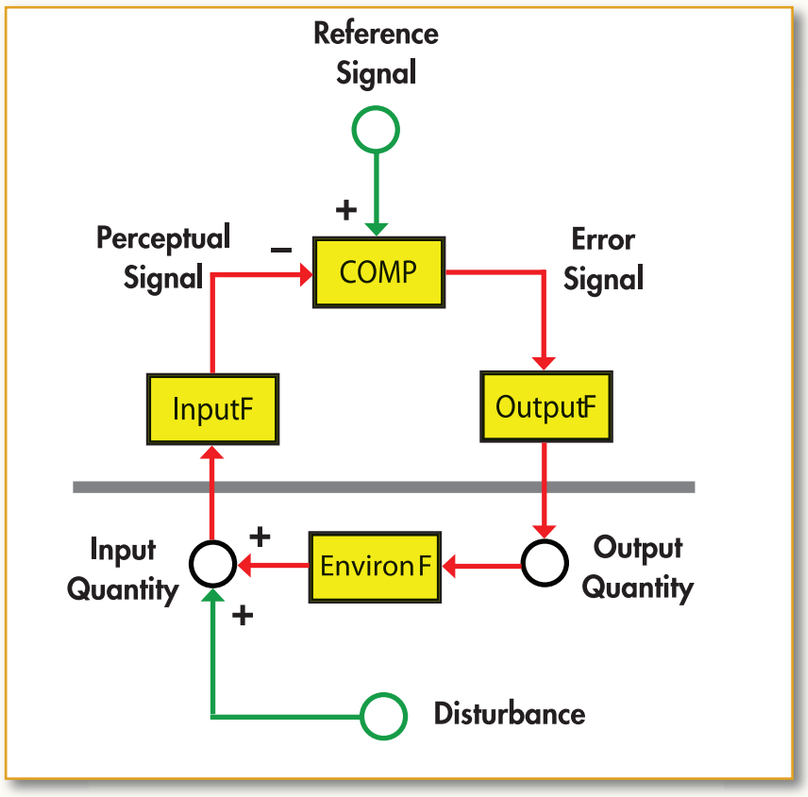
Zoals reeds gezegd handelen we elke dag al op basis van vertrouwen, dit geldt echter vaak alleen in de offline wereld. Waar we online denken op basis van vertrouwen te kunnen handelen, is het vaak het systeem of de organisatie achter een site waarop vertrouwd wordt en niet de persoon aan de andere kant van de verbinding.
Steeds vaker doen we online zaken met mensen die we offline niet kennen en

waarmee het ook onmogelijk of zeer onpraktisch is die offline connectie tot stand te brengen. Denk bijvoorbeeld aan een webshop in de Verenigde Staten of een softwarefirma in Australië, niet bepaald praktisch. Trust management biedt hier een oplossing voor, doordat het systeem op basis van eigen observaties en aanbevelingen van derden een overzicht kan geven van het gedrag van de andere partij. Op basis hiervan kun je dan zelf bepalen of iemand betrouwbaar genoeg is om de transactie door te laten gaan. Uiteindelijk is de vraag: is het risico dat ik met deze transactie loop aanvaardbaar genoeg, gegeven de mate van betrouwbaarheid van de andere partij? Als je weet of iemand betrouwbaar is of niet, geeft dit een belangrijk stuk informatie om het risico te bepalen dat je loopt.

3. Gedragswetenschappen: perceptie en referentie

Als je iets over menselijk gedrag wilt zeggen en daar zijn we nu wel mee bezig, heb je toch iets nodig dat een verklaring voor dat gedrag kan geven of het op zijn minst kan beschrijven. In de gedragswetenschappen zijn er vele richtingen die je kunt kiezen, ik heb ervoor gekozen een theorie te gebruiken die buiten de mainstream academische wereld valt. Reden hiervoor? Omdat deze theorie mij als bèta het meest aanspreekt en een realistisch en herkenbaar beeld schetst over hoe wij als mensen werken.

Perceptual Control Theory (kortweg PCT) is een theorie die gebaseerd is op gesloten causale verbanden. Elk verband bestaat uit vier elementen: perceptie, referentie, verstoring en foutsignalering. Het systeem werkt als volgt: initieel worden de interne waarde (referentie) en de opgedane waarnemingen (perceptie) met elkaar vergeleken. Als deze aan elkaar gelijk zijn, gebeurt er verder niets. Echter, als deze vergelijking verstoord raakt, ontstaat er een foutsignalering die moet worden opgelost. De resulterende actie die nu wordt gegenereerd om de ontstane fout op te lossen, dient ervoor om de referentie en perceptie weer in evenwicht te brengen. Oftewel: de gegenereerde actie is een tegenbeweging die probeert de verstoring ongedaan te maken.



Laat ik dit met enkele voorbeelden verduidelijken. Als je in een kamer zit en je krijgt het koud, dan is de perceptie van de temperatuur lager dan de referentie daarvan (de temperatuur die jij aangenaam vindt) en is er dus een foutsignaal (temperatuur te laag) wat zal leiden tot een actie: of je trekt een trui aan of je zet de verwarming hoger. Je ziet dus dat de gekozen actie probeert de verstoring (een verandering van de temperatuur) tegen te gaan.

Hetzelfde geldt voor een hongergevoel. In dit geval is het de vergelijking van de waarde van je bloedsuikerwaarde (perceptie) met de gewenste bloedsuikerwaarde (referentie). De actie die je moet ondernemen is iets eten om de waarde weer op peil te krijgen. Ook hier zie je dat de actie bedoeld is om de verstoring, de te lage bloedsuikerwaarde, op te heffen.

Eigenlijk merk je dus helemaal niets van je eigen referenties of percepties, slechts de ontstane verschillen worden opgemerkt en zo mogelijk geheel of gedeeltelijk opgelost door een tegenactie te ondernemen.

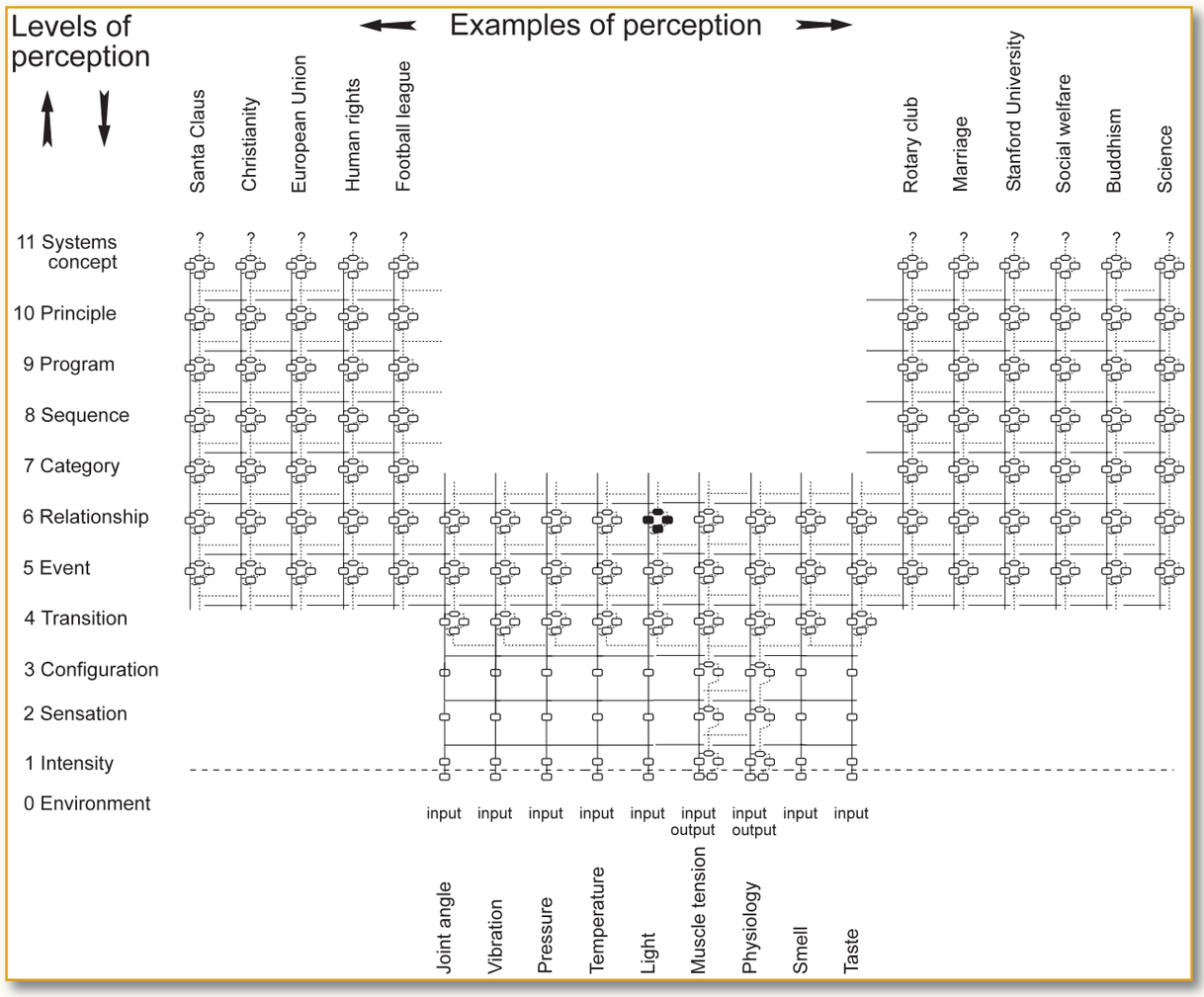
Uiteindelijk is ons menselijk lichaam opgebouwd uit een complete hiërarchie van deze 'control loops' waarbij de perceptie van hogere niveaus bestaat uit de gecombineerde percepties van lagere niveaus plus de ontstane foutsignalen. In het totaal zijn er twaalf niveaus te onderscheiden. Zie hiervoor het diagram op de volgende pagina.

Verderop in dit artikel komen we terug op de betekenis van PCT voor dit onderwerp.

4. Wat is vertrouwen?

In het kort komt het eigenlijk hier op neer: ik vertrouw iemand omdat ik daar in andere situaties positieve ervaringen mee heb of omdat iemand die ik vertrouw diegene aanraadt voor die specifieke transactie. Ik baseer mijn vertrouwen dus op eigen observaties en op aanbevelingen van anderen waarbij zowel positieve als negatieve ervaringen een rol spelen. Echter, voor iemand anders hoeft dat in geen geval zo te zijn. Sommige mensen vertrouwen iedereen van nature totdat het tegendeel bewezen is, anderen redeneren weer precies andersom.

Zou jij je leaseauto uitlenen aan een collega puur op basis van het feit dat hij een no-risk polis zou kunnen krijgen? Waarschijnlijk niet. Maar even je pen uitlenen omdat hij of zij een handtekening moet zetten is over het algemeen geen probleem. Mits dat natuurlijk niet jouw gegraveerde pen is die je van je broer voor je afstuderen hebt gekregen, tenzij... Of misschien ook wel.



Het mag duidelijk zijn dat er veel verschillende factoren ten grondslag liggen aan een beslissing of je iemand voldoende vertrouwt voor een gegeven actie of transactie, voordat je akkoord gaat of niet. Sommigen zullen hun leaseauto wel uitlenen, anderen doen dat niet. De basis waarop zij deze beslissing nemen, is vaak irrationeel en dus niet parameteriseerbaar. Het hangt er maar net vanaf hoe groot het risico voor jezelf is.

Met een theorie als PCT kun je wel een model van vertrouwen opstellen waarbij iemands interne waarden en beslissingen worden afgezet tegen zijn waarnemingen. Hoeveel weet jij over die andere persoon en kun je zijn gedrag matchen aan jouw interne referenties? Is het inderdaad een veilige rijder of alleen in zijn/haar eigen auto?

Probleem blijft dat we vertrouwen niet kunnen verklaren, we kunnen het slechts beschrijven en modelleren. Maar dan is er dus nu een conflict ten aanzien van de benaming trust management, toch?

5. Reputatie als basis van vertrouwen

Ja en nee. Ja, omdat we eigenlijk geen werkbare definitie hebben weten te vinden voor vertrouwen. Nee, omdat gebleken is dat er toch een mogelijkheid is namelijk: reputatie. En nee, niet om vertrouwen te definiëren, maar wel omdat het een van de pijlers is van vertrouwen.

In mijn omschrijving van vertrouwen heb ik het al min of meer cadeau gegeven, je neemt een beslissing op basis van je ervaringen met en/of aanbeveling over een bepaalde persoon. Letterlijk is dit een definitie van de reputatie van een persoon of organisatie. Maar wat maakt dit nu zo verschillend van vertrouwen?

Reputatie is eigenlijk niets meer of minder dan de beoordeling van het gedrag van een persoon of instelling en hoe meer gegevens bekend zijn, hoe nauwkeuriger de reputatie te bepalen valt. Vertrouwen daarentegen gaat net een stapje verder. Hoewel je dezelfde basisgegevens gebruikt, komt daar ook vaak een emotionele en/of specifiek voor die situatie toepasselijke extra referentie aan te pas. Reputatie is vaak een generieker gegeven en is minder afhankelijk van persoonlijke of emotionele invloeden.

Laten we terugkeren naar de voorbeelden van het uitlenen van de leaseauto en de pen van hierboven. Als iemand een no-risk polis zou kunnen krijgen, rijdt hij blijkbaar erg veilig en is dus zijn reputatie als automobilist goed. Of je hem daarnaast met jouw auto vertrouwt, is een extra stap waar vaak meer bij komt kijken en waarbij andere ervaringen een rol gaan spelen. Hetzelfde geldt ook voor het uitlenen van je pen. Als hij die altijd netjes terugbrengt en dat geldt ook voor andere spullen die hij eventjes leent, dan is zijn reputatie als iemand die zijn beloften nakomt duidelijk. Of je dan ook die voor jou emotioneel bijzondere pen met inscriptie uitleent, zegt dus niets over de reputatie van de ander, maar wel over het risico dat jij niet wilt lopen dat die pen toch zoekraakt, ook al geeft de reputatie daarvoor geen aanleiding.

Vertrouwen in beveiliging, is beveiligen met vertrouwen

In beide voorbeelden is duidelijk dat reputatie een grote rol speelt. Of je de persoon ook echt vertrouwt, is dus net even een stap verder en hangt, naast de reputatie van die persoon, nog van meer zaken af. En dat is nu precies waarom reputatie wel en vertrouwen niet bruikbaar is.

6. Reputatie, perceptie en referentie

Internet wordt meer en meer een integraal onderdeel van ons dagelijks leven. Ik verwacht dat dit dusdanige vormen gaat aannemen dat je op een gegeven moment zelfs niet eens meer door hoeft te hebben dat je iets online aan het doen bent. Je kledingkast geeft je bijvoorbeeld een kledingadvies gebaseerd op je agenda, reistijden, vervoermiddelen en de weersverwachting.
Komt die weersverwachting nu van internet of je persoonlijke weerstation? Is het comfort van een bepaald vervoermiddel (auto of trein) en de daarbij behorende kledingkeuze jouw voorkeur of een advies van de vervoerder? Of misschien wel een combinatie van beide? Hoe het systeem de verschillende bronnen verwerkt zal volledig transparant zijn voor de gebruiker.

Voor een goed reputatiegebaseerd systeem, dat op deze indringende manier het vertrouwen van de gebruikers op de proef stelt, is een systeem vereist dat gebaseerd is op gedragswetenschappen. Simpelweg omdat het moet doen 'wat jij als gebruiker verwacht dat het doet'. Iedereen kent het aloude voorbeeld wel 'mijn computer doet niet wat ik wil'.

Enerzijds voldoet PCT hieraan omdat heel duidelijk per 'control loop' en per niveau in de hiërarchie te bepalen valt wat de referentie is. Waaraan moet een bepaalde waarde voldoen en wat de perceptie is: wat neem ik waar en wat kan ik vergelijken met de gegeven referentiewaarde? En als een bepaald niveau er niet uitkomt, wordt de vraag hogerop in de hiërarchie gesteld. Of in de terminologie van PCT: we kunnen geen actie genereren om de waargenomen verstoring op te lossen, we sturen onze waarnemingen en foutsignalering naar een niveau hoger.

Anderzijds voldoet PCT simpelweg omdat het afkomstig is uit de hoek van onderzoek in cybernetica, waarin altijd maar weer geprobeerd wordt om menselijk gedrag na te bootsen in machines (robotica). En laat dat nu juist zijn wat we met een op gedrag gebaseerd trust management systeem proberen te bereiken?

7. Reputatie als middel voor authenticatie en autorisatie

En dan nu het antwoord op de gestelde vragen aan het begin van dit artikel. Mocht je dit als beveiliger zelf nog niet bedacht hebben, het antwoord op de eerste vragen is toch echt: 'nee', dat weet je niet en 'nee' met de huidige technieken is dat vaak niet of nauwelijks controleerbaar. Het is met de huidige systemen onmogelijk te bepalen of diegene die inlogt met een bepaalde gebruikersnaam ook echt diegene is die jij denkt, en hoopt, dat het is. En wat betreft die laptop, nee MAC-address filtering is geen optie. Natuurlijk kom je met biometrie en dergelijke een aardig eind, maar volledig sluitend is het niet.

Ook reputatiesystemen zonder degelijke identificatie zijn waardeloos wat dat betreft. Alleen als je de identiteit van de gebruiker kunt controleren en vaststellen, is het mogelijk om de aan die identiteit gekoppelde reputatie te gebruiken als maatstaf voor authenticatie en autorisatie. Welke waarde je er uiteindelijk aan hangt en welke waarde voldoende is voor toegang is een beslissing die per gebruiker of gebruikersgroep en per niveau van beveiliging zal verschillen.
Belangrijkste is echter dat je via een reputatiesysteem de gegevens krijgt om de juiste afweging te kunnen maken.
En ja, privacy zal een handelsmiddel worden. Bij dit soort systemen zal het belangrijkste zijn: hoeveel privacy ben jij als gebruiker bereid op te geven voor toegangsrechten. Dat is nu al zo, maar hopelijk heb je er dan ook zelf echt controle over.

8. En E-Bay dan?

Even voor de goede orde, ik heb het hier over het reputatiesysteem van E-Bay waarbij je als koper en verkoper een waarde van onbetrouwbaar, neutraal of betrouwbaar kan geven aan elke transactie die je hebt voltooid.

Dit lijkt waterdicht, toch? Helaas…
Het is heel simpel te omzeilen, eigenlijk. Neem honderd vrienden of collega's. Verhandel onder die personen items van maximaal twee euro, laat iedereen aan iedereen een volledig positieve feedback geven. Bied vervolgens iets te koop aan voor 100.000 euro en wacht af. Is het geld binnen, dan…

Hoe kan dit? E-Bay verzuimt het om een waarde te hechten aan de waarde van afgehandelde transacties en dus het risico ervan. Oftewel: je reputatie kan geweldig zijn met alles onder de twintig euro, maar alles er ruim boven? Aan het E-Bay reputatie system is dat niet af te lezen als gebruiker. Een echt reputatiesysteem neemt die weging wel mee.

E-bay is hiermee een klassiek voorbeeld van een reputatiesysteem dat valt in de categorie van PolicyMaker en KeyNote. Vertrouwen in het systeem en de organisatie en niet in de koper of verkoper.

9. Conclusies

Trust management, of liever reputation management, is iets waaraan vrijwel niet valt te ontkomen. Internet wordt steeds belangrijker en een steeds groter integraal onderdeel van ons dagelijks leven. Trust management is de enige manier waarop we in onze globale online wereld een houvast hebben ten aanzien van wat we dreigen te verliezen. Hoe in te schatten of die ander echt is wie hij beweerd te zijn en is diegene ook betrouwbaar genoeg? Als je iemand in real life tegenkomt, kun je dat als persoon goed inschatten, maar via slechts een scherm en een stuk tekst?

Helaas zien we in de offline wereld precies wat er gebeurt als het vertrouwen en de basis daarvan, de reputatie, ontbreekt of weggevallen is. Kijk maar naar de huidige financiële crisis en het wantrouwen ten aanzien van de financiële wereld. Het is niet ondenkbaar dat eenzelfde effect in de online wereld mogelijk is. Echter, dan zijn de gevolgen nog groter dan wie dan ook nu kan overzien. Probeer maar eens een voorstelling te maken van een wereld zonder online handel, lukt dat je nog?