USER-MANAGED ACCESS: VEILIG ONLINE DATA DELEN

Cordny Nederkoorn is een software tester werkzaam bij Immune-IT, een softwaretestconsultancy-bedrijf met klanten in Nederland en België. Hij is per email bereikbaar via cclnederkoorn@hotmail.com

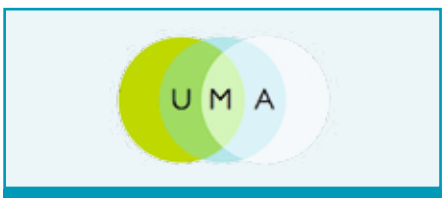
Cordny kwam met de UMAWG in aanraking bij de Cloud Identity Summit 2010 in Colorado, Verenigde Staten, waar hij een van de grondleggers van UMA, Eve Maler, ontmoette en gefascineerd werd door haar verhaal. Eve wilde graag een kwaliteitsslag maken met haar protocol en vroeg om hulp. Nu, anderhalf jaar later, heeft Cordny onder andere meegeholpen aan een interoperabiliteit testplan voor de implementaties van UMA bij verschillende organisaties en bedrijven.

Steeds meer mensen delen hun gegevens online. Met als gevolg dat de gedeelde data verspreid wordt over diverse sites. Hierdoor wordt het voor de data-eigenaar moeilijk te achterhalen wie waar toegang heeft tot zijn data. Data privacy en beveiliging zijn hierdoor in het geding. Hiervoor is nu een oplossing ontwikkeld: het *User-Managed Access* (UMA) protocol. UMA luidt een nieuw tijdperk in van User-centric Access control voor web-based applicaties zoals social networks, content-sharing portals en personal clouds. Dit artikel geeft een introductie tot UMA en haar online mogelijkheden.

UMA

De tijd die mensen online besteden is, zowel zakelijk als privé, toegenomen. Hierbij delen zij hun gegevens met derden, waarvan vaak niet duidelijk is wie er toegang tot hun gegevens heeft. Het User-Managed Access (UMA) protocol geeft de eindgebruiker de controle over haar online data.

Kantara Initiative
Een internationaal, open samenwerkingsverband van individuen uit de identity community, werkzaam in verschillende branches, die samenwerken aan oplossingen voor identity issues: interoperability & compliance testing (bv. SAML); identity assurance; beleid en wetgeving; eigenaarschap & aansprakelijkheid; privacy; UX & usability; cross community coordination; educatie; marketing; use cases en tools



Afb.1. UMA

UMA is ontworpen door een werkgroep van Kantara Initiative, de User-Managed Access Working Group (UMAWG). Kantara Initiative is een professionele organisatie, toegewijd aan het verbinden en harmoniseren van de identity-gemeenschap door middel van acties die meehelpen aan het veiligstellen van identity-based online interacties. Hierbij wordt misbruik van persoonlijke informatie voorkomen, zodat netwerken privacy-beschermend en betrouwbaar worden.

De UMAWG is ontstaan in 2009 nadat verschillende personen uit de identity community het mogelijk wilde maken dat een individu zelf de autorisatie kan beheren van de data die hij/zij wil delen tussen de online services. Daarnaast wilden zij een facilitatiecentrum vormen voor interoperabele implementaties van de te ontwerpen specificaties. De leden van de UMAWG, de UMAnitarians, ontwerpen de specificaties voor het UMA-protocol met de bedoeling de draft specificaties over te dragen als standaard aan de Internet Engineering Task Force (IETF). Een autorisatieprotocol maken en implementeren is lastig, maar door aan het begin van de specificaties al bezig te zijn met de testbaarheid ervan heeft dit voordelen tijdens de implementatie omdat van tevoren al goed is nagedacht over wat de mogelijke risico's bij implementatie zijn. De testbaarheid van het UMA-protocol is onderzocht door de specificatie om te zetten in pseudocode om te kijken of bepaalde stappen onvolledig of onvermeld zijn. Daarnaast is gekeken hoe in de specificatie is omgegaan met de verplichte (de 'MUSTs') en de optionele (de 'MAYs') stappen en/of eigenschappen. De testbevindingen hiervan gaven vaak verhitte discussies tijdens de wekelijkse UMA-teleconferences. Op een gegeven moment gingen de ontwerpers zelf ook pseudocode toepassen om zo mogelijke bevindingen voor te zijn. Deze kwaliteitsslag werd dus gemaakt, en toont aan dat een tester wel degelijk nut heeft bij de ontwikkeling van een specificatie.

> Vaak niet duidelijk wie toegang tot gegevens heeft

Stappen UMA

Nu we wat meer weten van UMA kunnen we ons wat meer verdiepen in haar eigenschappen.
UMA is gebouwd op het OAuth 2.0, een protocol, ontworpen om perso-

nen webservices te autoriseren voor het toegang krijgen tot de protected resources van een andere webservice.

OAuth 2.0
OAuth is een open standaard voor autorisatie. Gebruikers kunnen zo een programma/website toegang geven tot hun gegevens, zonder vermelding van gebruikersnaam en wachtwoord. In plaats daarvan wordt met tokens gewerkt die een bepaalde geldigheidsduur hebben en toegang verlenen aan slechts 1 type gegeven.

In vergelijking met OAuth 1.0 is OAuth 2.0 compleet nieuw, met meer nadruk op o.a. usability en performance.

Het grote verschil met van UMA met OAuth 2.0 is dat UMA de autorisatie-server (zie onder) bij een derde partij legt, die functioneert ten behoeve van de data-eigenaar.
UMA heeft een aantal specifieke deelnemers, die ik met een typische UMA use case zal illusteren: het verzenden van een online aangekocht boek.
De deelnemers worden vermeld met daarachter genoemd de rol van de deelnemer in het UMA-protocol.

Alice (UMA: de *authorizing user*) koopt een boek bij Books.com (UMA: de *requester*). Het adres van de klant staat in een online adressenboek AdresBoek (UMA: een *host*), waarbij de host toegang verleent op basis van een access policy gemaakt door bijvoorbeeld een Social Network zoals het fictieve SocialMe (UMA: *authorization Manager* / AM).

Alice heeft deze *access policy* bij SocialMe ingesteld. Dit betekent dat Alice zelf kan bepalen via SocialMe wie waar toegang heeft tot haar adres (UMA: *protected resource*).
Om aan dit proces te voldoen wordt het UMA-protocol doorlopen. Dit bestaat uit de volgende drie stappen: 'Bescherm de resource', 'Krijg Autorisatie' en 'Access de resource'.

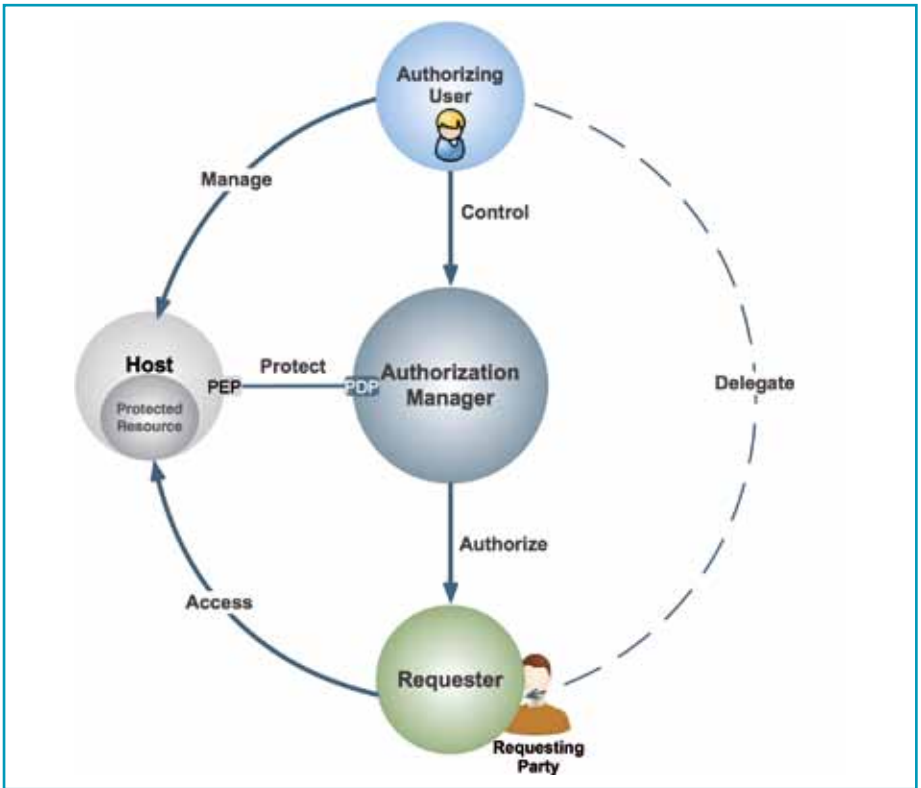
Een autorisatieprotocol maken en implementeren is lastig

Deze stappen zijn uitvoerig beschreven in het UMA Core Protocol, wat nog altijd aan verandering onderhevig is. Daarom worden nu de belangrijkste eigenschappen per stap besproken met behulp van het al besproken voorbeeld: het verzenden van een online gekocht boek.

>Bescherm de resource
Hierbij zijn de authorizing user Alice, de host AdresBoek en de Authorization Manager SocialMe betrokken.
Alice heeft AdresBoek gekozen voor het beheer van haar online resources. AdresBoek heeft Alice geïntroduceerd aan SocialMe, door middel van een OAuth-interactie.
Hierbij heeft AdresBoek een access token van SocialMe gekregen. Via de protection API van SocialMe vertelt AdresBoek aan SocialMe welke resources (lees: adressen) een *access policy* hebben.
Daarnaast geeft, buiten het UMA-protocol om, Alice opdracht aan SocialMe welk toegangsbeleid moet worden toegewezen aan de betreffende adressen.

>Krijg autorisatie
Hierbij zijn de requester Books.com, host AdresBoek en AM SocialMe betrokken.
Bij deze stap wordt AdresBoek benaderd door Books.com (met de access token van SocialMe) om toegang te krijgen voor het door AdresBoek beheerde adres van Alice.
AdresBoek valideert de status van de token bij SocialMe en bij succesvolle validatie krijgt Books.com autorisatie om toegang te krijgen tot het adres van Alice.

>Toegang tot de resource
Hierbij krijgt, indien aan stap 1 en 2 is voldaan, Books.com toegang tot het adres van Alice, beheerd door Adres-



Afb.2. UMA players

Boek. Nu kan Books.com het door Alice gekochte boek naar haar opsturen.
Zoals al gezegd, een meer gedetailleerde beschrijving van de UMA-stappen kunt u vinden in het UMA Core Protocol dat te vinden is op de UMAWG-website. Let wel, UMA is nog steeds in ontwikkeling en de documentatie is aan verandering onderhevig.

Status UMA

In juni 2011 vond de officiële lancering plaats van het UMA-protocol: de publicatie van een draft recommendation voor het UMA-protocol en toevoeging ervan aan de IETF-standaarden.
Dankzij deze lancering en ondanks mogelijke toekomstige veranderingen, zijn UMAnitarians begonnen met het implementeren van UMA in online applicaties. De bekendste (en de oudste) is die van Newcastle University met het SMART project.

UMA is nog steeds in ontwikkeling

SMART staat voor Student-Managed Access to Online Resources, oftewel een online data access management system voor studenten in het Hoger Onderwijs.
Andere voorbeelden zijn een mobile location scenario (Fraunhofer Institute) en het Health Data Exchange-project hData (MITRE). Implementaties, gebaseerd op UMA, met actuele toepassingen. Tot op heden is er helaas nog geen Nederlandse implementatie bij de UMAWG bekend. Meer implementaties zijn te vinden op de UMAWG-website.
Zoals ik al zei in de introductie, meer mensen delen hun gegevens online. UMA stelt hen in staat de toegang tot hun data zelf te beheren, wat de online privacy en veiligheid van deze personen waarborgt.
UMA is in ontwikkeling en de UMAWG verwelkomt graag nieuwe (Nederlandse) UMAnitarians die mee willen werken aan nieuwe use cases, relaties met claims, interoperabiliteit met OpenID-Connect en implementaties van UMA. Wie wil er nou niet meewerken aan een veilig en privacygericht internet?

Verwijzingen

website UMAWG: http://kantarainitiative.org/confluence/display/uma/Home

website OAuth 2.0: http://oauth.net/2/

BLACK HAT EUROPE 2012

AMSTERDAM REVISITED

Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is tevens voorzitter van de MSP-ISAC. Hij is bereikbaar via lex.dunn@capgemini.com.

Na twee jaar in Barcelona was het Black Hat Europe circus weer neergestreken in Amsterdam. Op 14, 15 en 16 maart was Krasnapolsky weer even het domein van de witte en zwarte hoeden. Hoe zit dat nu eigenlijk met "Black Hat" en "Black Hat Sessions"? Black Hat Europe is de Europese variant van de in Amerika al langer bekende Black Hat sessies (meestal in exotische plaatsen als Las Vegas ;-)). De Black Hat Sessions zijn een Nederlandse aangelegenheid en worden georganiseerd door Madison Ghurka, dit jaar op 4 april in de Reehorst in Ede (een verslag hiervan staat in het volgende nummer). In IB4 2010 en IB4 2011 vindt u verslagen van de eerdere Black Hat sessies in Barcelona.
Terug naar Krasnapolsky. De openingsspeech was voor Whitfield Diffie, bekend van de Diffie-Hellman key exchange, een van de grondslagen van de moderne cryptografie. Hij had het onder andere over "defense" versus "offense" en concludeerde dat je maar beter aan de "offense" kant kunt staan: als een aanval succesvol is ben je de held, doe je daarentegen "defense" dan wordt elke mislukking breed uitgemeten. Verder was de strekking van zijn betoog dat de huidige cryptografie voldoende beveiliging biedt, maar dat de vertrouwelijkheid steeds vaker door de "menselijke factor" wordt doorbroken (denk aan Bradley Manning, die WikiLeaks geheime US documenten toespeelde).
De drie dagen werden gevuld met zeer interessante en vaak ook erg technische sessies, in drie tracks. Een hoogtepunt (wat mij betreft):
U hebt een iPhone of Android toestel? En u heeft daar uw wachtwoorden/pincodes/credit card nummer in opgeslagen? Natuurlijk gebruik makend van zo'n handige "app", een "secure password manager" met "military-grade encryption"? Yeah, right! Niet dus. Onderzoek van een groot aantal vrij verkrijgbare, maar ook commerciële apps voor zowel iPhone als Android, door Andrey Belenko en Dmitry Sklyarov toonde tot hun verbijstering aan dat een aantal van deze apps niet eens de data te versleutelen, maar alleen het wachtwoord om de data in te zien! Bij de wel versleutelde data was het in veel gevallen erg makkelijk (lees: binnen enkele minuten) om middels "brute force" de data te ontsluiten.

Meer informatie is te vinden op de website van Black Hat: http://www.blackhat.com/html/bh-eu-12/bh-eu-12-home.html