ونيو 2014

هل قمت بإختيار مقدم هوية مؤخرا؟

Wilton Robin

مدير التوعية التقنية
الهوية والخصوصية

Internet Society

الملخص
في هذه الورقة البحثية نلقي نظرة على التغييرات في عالم تقديم الهوية. حيث تشهد الهوية الرقمية تطورا من نموذج "رجعي" إلى آخر تنبؤي بصورة متزايدة إستنادًا على البيانات السلوكية و وسائل الاعتماد التقليدية على حد سواء. هنالك أيضًا توجه من الاعتمادات المنعزلة إلى تأكيدات هوية وسمات أكثر قابلية للتحول. من المحتمل أن تقدم هذه التغييرات مزيد من الخيارات والسلطة للفرد و لكن في شكل إحتمالات فقط. تحتوي نماذج الهوية الناشئة أيضًا على مشاكل خفية يحتاج المستخدمون إلى معرفتها إذا كان يتوقع أن يكون لهم تأثير على السوق من خلال الممارسة الفعلية للاختيار.

السياق
يواصل عالم الهوية الرقمية التطور بوتيرة واحدة، مفهوم الهوية الرقمية بحد ذاته يضم الآن عدة أشكال مختلفة، وبصورة رئيسية الأشكال الثلاثة التالية:

- الهويات التقليدية "الرجعية"، حيث تمر من خلال عملية تسجيل موثوقة لتتلقى من طرف ثالث، الاعتماد الذي يمكنك تقديمه في وقت لاحق لمصادقة نفسك؛
- الهويات "المؤكدة ذاتيا" ذات الثقة المتدنية، حيث يقوم الطرف الثالث بإصدار وثيقة إعتماد صحيحة من حيث تركيب المعرفات و سيقوم بتأكيد ذلك عند الطلب.
- الهويات "السلوكية"، حيث يجمع مقدمو الخدمات بيانات كافية عن الفرد لإثبات أن نفس الشخص يقوم بالزيارة عدة مرات.

ومن الجدير بالذكر أن النوع الثالث من تحديد الهوية (السلوكية) لا يحتاج في الغالب إلى أي إجراء محدد من جانب المستخدم. إذا قام موقع معين بوضع ملف تعريف ارتباط (cookie) للمتصفح، أو سجل عنوان الإنترنت (IP) الخاص بك، فهذا يكفي لتشكيل أساس للهوية السلوكية - رغم أنه هنالك طرق أكثر تطورا بكثير أيضا.

وقد تطور مقدمو الهوية (IDPs) أيضا، و واصلوا القيام بذلك. أول مقدمي الهوية الذين يتعرف عليهم المستخدمون هم على الارجح أحد ثلاثة أنواع:

- الحكومة (وخصوصا في حالة وثائق الاعتماد غير الرقمية مثل جوازات السفر ورخص القيادة وهلم جرا)؛
- المؤسسة التعليمية (إصدار هوية الطالب للوصول المباشر إلى موارد الطلاب والمكتبات والشبكات، وما إلى ذلك)؛
- صاحب العمل (إصدار تسجيلات الدخول للبريد الإلكتروني، وتطبيقات الأعمال إلى آخره).

لأغراض التعميم و التبسيط، يصدر جميع مقدمي الهوية المذكورين بيانات إعتماد منعزلة. قد لا يكون الاعتماد الصادر عن الحكومة مثلا صالحًا للاستعمال لتسجيل الدخول إلى أنظمة صاحب العمل الخاص بك (إلا إذا كانت الحكومة نفسها هي صاحب العمل ولكن هذه حالة خاصة). بيانات تعريف (ID) الطالب الذي استخدمته طيلة أيام الجامعة ربما لن يعمل في أنظمة صاحب العمل الخاص بك، أيضا. كما تقدم، فإن ذلك مجرد تبسيط ، مخططات الهوية التكاملية تسمح بسد الفجوات بين بيانات الإعتماد المنعزلة إلا أنه من الشائع في هذه المخططات أن يكون عملها محصورا في نطاق معين كالتعليم العالي أو الحكومة أو تسجيل وحيد لكل المنظمات التجارية [1].

الاختيار
ميزة أخرى بارزة تتعلق بجميع الأمثلة الثلاثة هي أنك، كمستخدم، لديك القليل أو لا خيار على

[1] هناك استثناءات ملحوظة، مثل نظام بيانات تعريف البنك (BankID) الاسكندنافي، الذي يسد الفجوة بين القطاع العام و التجاري، أوالمخططات التكاملية في صناعة الدفاع و الفضاء حيث هناك درجة عالية من التفاعل بين الجهات الحكومية والمتعاقدين معها.

الإطلاق في هذه المسألة. إذا قمت بالتسجيل في إحدى الجامعات أو عملت في وظيفة، ربما لن يكون لديك خيار سوى الاشتراك في خدمة المصادقة المقدمة لك، أو مواجهة إحتمال محاولة العمل دون الوصول إلى الموارد على شبكة الإنترنت (والذي يُعد في هذه الأيام، وفي كثير من الأحيان أمرًا مستحيلاً).

هنالك نوعان من الطرق التي يدخل بها الإختيار في المعادلة، أولا مع ظهور برامج مثل OpenID و OAuth اكتسب المستخدمون خيار تقييم مدى ملكيتهم لمورد معين (مثل عنوان البريد الإلكتروني أو حساب على الإنترنت) وبالتالي ضمنا هويتهم.

ثانيا برامج مثل stTru of Web" Thawte" (الآن توقف للأسف) أو معرف الهوية الموحد (UnitedID) الناشئ[2]، تسعى لتوفر للمستخدمين إعتماد مستمر مرتبط ببيانات تعريف مصادق عليها ذاتيا (مثل عنوان البريد الإلكتروني أو رمز المصادقة authentication token).
UnitedIDمثير للاهتمام بشكل خاص، حيث أنه يسعى إلى تقديم هوية جديرة بالثقة على الانترنت إلى عموم المستهلكين بالسوق دون اللجوء إلى الطراز التجاري الشائع لنموذج تقديم الخدمات عبر الإنترنت الذي تموله الإعلانات.

قد يكون أو لا يكون هذا الاعتماد جديرا بالثقة بطبيعته. في البداية يعتمد ذلك على مدى موثوقية عملية التسجيل. إذا كان من السهل جدا بالنسبة لي الحصول على اعتماد صحيح من حيث التركيب يؤكد أنني غريس كيلي، فإن ذلك سيضعف فائدة النظام. ومع ذلك، إذا كان الاعتماد مستمرا بما فيه الكفاية فإنه قد لا يهم أنه يؤكد إنني غريس كيلي ، حيث أنه مع مرور الوقت يستطيع الإعتماد أن يتحصل على الثقة بنفس الطريقة التي يفعلها أي إنسان و ذلك عن طريق بناء سجل من السلوك جدير بالثقة باستمرار.

ولكن انتظر: هل هناك فئة أخرى من مقدمي الهوية توفر للمستخدمين الاختيار وتسمح لهم بالمصادقة على العديد من مقدمي الخدمات المختلفة؟ بطريقة ما، نعم. إذا كنت قبلت من قبل العرض لتسجيل الدخول إلى خدمة غير معروفة (س) بإستخدام معرف جوجل الخاص بك، أو الفيسبوك أو تويتر (على سبيل المثال لا الحصر)، فأنت قد حصلت على مقدم للهوية بصورة افتراضية بدون
اختيار أي واحد بوعي منك. بطريقة ما، قد يكون أكثر دقة أن نقول أنك إخترت استخدام مقدم هوية تم اختياره مسبقا لك. في الوقت الحالي، سوف أشير إليه بإسم "مقدم الهوية الاجتماعي". و الذين لديهم تأثيرات على الخصوصية ينبغي إعتبارها بعناية.

التأثيرات
أحد الخيارات التي ذكرتها أعلاه كان خيار المصادقة الذاتية (OpenID، OAuth، UnitedID وغيرها)، حيث يكون مقدم الهوية كذلك تماما و مصادقة الهوية (مباشرة عن طريق وثائق الاعتماد، أو بشكل غير مباشر عن طريق الوصول الضمني) هي كل ما تفعله. برامج مثل هذه تعيش أو تموت عن طريق قدرتها على جذب عدد مقدر من الأطراف المعتمدة (RPs). إذا لم تتمكن من جذب ما يكفي، أو لم تتمكن من جذب الأطراف المعتمدة التي لا غنى عنها لحياة المستخدم على الانترنت، وبرامج المصادقة الذاتية لديها صعوبة في إضافة قيمة و يحتمل أن تضمر لعدم استخدامها. كملاحظة جانبية، حتى برامج الحكومة الملزم استخدامها عمليا (مثل نظام التوثيق في المملكة المتحدة للإقرارات الضريبية عبر الإنترنت) يمكن أن تعاني من هذه المشكلة؛ المعرف الذي يمكنك استخدامه فقط في مكان واحد، مرة واحدة في السنة، يضيف قيمة قليلة، ويصعب تذكره ويسهل تجاهله.

من هذا المنظور، فإن الميزة الكبيرة لمقدمي الهوية الاجتماعية هو أن لديهم ما يمكن وصفه على نحو فعال بالكتلة الحرجة التلقائية في كل من وتيرة التفاعل وعدد المشتركين. فمن الممكن جدا أن تتفاعل مع مقدم الهوية الاجتماعي بشكل أكثر تواترا من تفاعلك مع أي خدمة أخرى على الإنترنت كبريد

[2] الصفحة الرئيسية للمعرف المتحد: http:/unitedid.org/about/

العمل الإلكتروني الخاص بك. فخدمة مثل الفيسبوك (Facebook) التي يعتقد أن لديها حوالي 750 مليون مستخدم نشط يوميا[3]، تقدم الروابط المعتمدة RPS إمكانية الوصول إلى (وعن طريق) مجموعة ضخمة للمستخدم مع مصادقة بنقرة واحدة. بمعنى آخر أن هذه هي الغاية المنشودة لمقدمي الهوية. لن يقوم المستخدم بالدخول إلى هذه الخدمات من أجل المصادقة فقط و لكن يدخل للقيام بنشاطات أخرى و إذا كانت المصادقة ناتج جانبي لذلك فلا مانع. بلغة أخرى، إذا كان الدخول إلى مقدم الهوية الخاص بك يعني أنه يمكنك القيام بنشاطاتك الأخرى دون الحاجة إلى المصادقة من جديد فإن ذلك يجعل الأمر أكثر سهولة.

و الآن، ما هو الجانب السلبي لذلك؟ في كلمة واحدة، الشمولية. قدرة مقدم الهوية الخاص بك على تسجيل جميع الأماكن التي قمت بالمصادقة بها.

نستطيع القول بأن هذه ليست مشكلة جديدة، حيث كانت الشمولية هي الانتقاد الذي وجه إلى الموجة الأولى الناضجة لمقدمي الهوية التكاملية[4]. ولكن هناك اختلاف طفيف ففي موجة الإنشاء تلك كان مقدمي الهوية جزءا من دائرة الثقة من خلال وجود علاقات تعاقدية متفق عليها من قبل بين مقدمي الهوية (IDPs) و الأطراف المعتمدة (RPs) بالإضافة إلى شروط الخدمة مع المستخدمين.
كان السبب الأساسي لوجود مقدم الهوية هو علاقة الثقة بينه وبين المستخدم. إذا كنت تثق في مقدم الهوية الخاص بك للتحقق من هويتك، فمن المتوقع أن تثق بهم في عدم إساءة إستعمال بياناتك.

ولكن في نموذج مقدم الهوية الاجتماعي كما تقدم، فإن التوثيق في جوهره عبارة عن أثر جانبي.
نموذج الأعمال الرئيسي هو التحكم بالبيانات الشخصية (من خلال التجميع وإعادة البيع للمعلنين).
لذلك ففي مصلحة مقدم الهوية الاجتماعي جمع أكبر قدر ممكن من المعلومات عن الأنشطة الخاصة بك على الانترنت والحصول على مقابل مادي من تلك البيانات. بل إن من مصلحة مقدم الهوية الاجتماعي بناء أدق صورة شاملة لسلوكك الإجتماعي، و الذي يشمل المجموعات الفرعية من معارفك التي قد ترغب في فصلها
(على سبيل المثال، معارف العمل أوالأسرة و الأصدقاء).

و بأخذ ذلك في الإعتبار فإنه إذا كان لديك معرف بيانات (ID) في جوجل + Google تستخدمه للنشاط الشخصي على الانترنت فقط،
فإنه يمكن لجوجل أن يرى السلوك الإجتماعي الشخصي الخاص بك. و الآن إذا قرر صاحب العمل الخاص بك إستخدام جهة خارجية للتقويم و إختار تقويم جوجل (Google) لفعل ذلك و كان عليك المصادقة باستخدام معرف بياناتك الشخصي الخاص بك على + Google، يصبح بإمكان جوجل بصورة مفاجئة أن يتعرف إلى العلاقات بين سلوكك الإجتماعي و سلوكك في العمل. و المحصلة بالنسبة لجوجل هي صورة أكثر ثراء وشمولا وأكثر قدرة على جلب مقابل مادي لسلوكك الإجتماعي. أما النتيجة بالنسبة لك هي تلاشي الحدود بين بياناتك الشخصية و تلك الخاصة بالعمل على شبكة الإنترنت، وهذا سيء بالنسبة للخصوصية الشخصية وتحديد المصير على الانترنت.

تذكر أن هذا التلاشي بين الحدود ليس شيئا سجلت له بشكل واضح بل هو أحد الآثار الجانبية لاختيار أحد مقدمين الهوية الاجتماعية. في الواقع، هذا السلوك الإجتماعي و تلاشي الحدود هو عامل مهم للدرجة التي أفضل أن أشير إليه بمقدمي هوية السلوك الإجتماعي.
وهذا أيضا يعكس حقيقة أن السلوك الإجتماعي يصعب تزويره وهو أحد أكثر الأشكال إستقرارا لمعرفات السلوك وهذا يعيدنا إلى
ملاحظتنا السابقة أن الهوية الرقمية تشمل الآن الهويات السلوكية وكذلك الهويات التقليدية.

إستنتاجات

---

[3] http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebookstats/

[4] أبرز الأمثلة للاتحادات القائمة على SAML المصممة لتحالف الحرية / مواصفات OASIS

أولا، الإعتمادات المصدرة بواسطة طرف ثالث لن تذهب بعيدا. سوف تستمر الحكومات في إحتياجها إلى إصدار إعتمادات تحت سيطرتهم ولأغراض خاصة مثل ضبط الحدود و ترخيص المركبات وهلم جرا. قد تصدر بعض من تلك الاعتمادات في أشكال يمكن تقديمها للمصادقة في القطاع التجاري، ولكن الرغبة إليها لا تزال محدودة حتى بعد بضعة عقود من توفرها فنيا.

ثانيا، سيستمر المستخدمون في مواجهة القرار حول ما اذا كان عليهم قبول الراحة و السهولة التي يوفرها مقدم هوية السلوك الإجتماعي، حتى لو أصبحوا أكثر وعيا بمآخذ القيام بذلك من حيث الشمولية والخصوصية وتقرير المصير. تذكر فقط أن من مصلحة مقدم هوية السلوك الإجتماعي أن تركز فقط على السهولة و الراحة وليس الجانب السلبي المتعلق بالخصوصية، بهذه الطريقة يحصلون على المزيد من المعلومات و بالتالي مقابل مادي أكبر.

ثالثا، في النظام الإيكولوجي الخاص بالمصادقة المتكون من مقدمي الهوية (IDPs) و الأطراف المعتمدة (RPS) و المستخدمين، هناك مكان لفئة الإعتمادات المصدقة ذاتيا والمستمرة التي تسمح للفرد (1) بالتحكم بالهوية أو الشخصية التي يختار تأكيدها و (2) بناء سجل للسلوك الجدير بالثقة و ربطه بشكل موثوق بنفسه بدلا من أي شخص آخر. ولكن تلك الفئة ما تزال جديدة و هشة و تعتمد على مدى إدراك الأطراف المعتمدة (RPS) لقيمة هذه التأكيدات و تجميعها لمقدمي الهوية المعنيين.

كما يقدم هذا النموذج الثالث الإمكانات لخدمات مقدمي الهوية التي لا تعتم على الحصول على مقابل مادي للبيانات الشخصية - ولكن إذا لم يكن هذا هو النموذج التجاري الذي يحافظ عليه، فماذا سيكون؟

CC BY SA