

Instaurer la confiance de bout en bout – Où en est-on ?

Lorsque nous avons exposé notre vision « End to End Trust » (Confiance de bout en bout) lors de la conférence RSA en avril 2008, nous nous sommes engagés à réaliser un certain nombre d'actions. Pour commencer, nous avons cherché à déterminer des scénarios qui nous permettraient de donner forme à notre vision. Nous avons entamé des discussions à ce sujet et sur sa réalisation avec les pouvoirs publics, des partenaires industriels, des clients, des analystes et des groupes d'intérêt public. Nous avons également invité cette communauté à nous faire part de leurs commentaires sur le livre blanc de présentation de notre vision et sur le [site Web dédié](#). Ce communiqué a pour objectif de vous rapporter certains des commentaires que nous avons reçus, de partager nos vues sur ces commentaires et de vous tenir informés sur l'avancement d'un scénario auquel nous travaillons. Nous vous exposerons dans des communiqués ultérieurs d'autres scénarios que nous avons à l'étude ainsi que nos stratégies visant à démontrer nos concepts et à matérialiser notre vision d'un Internet plus digne de confiance.

Commentaires d'ordre général

Les commentaires que nous avons reçus sur notre projet portaient en général sur des questions d'identité, de responsabilité et de confidentialité, avec un intérêt plus marqué pour la couche « utilisateurs » de la pile sécurisée (par opposition au matériel, aux logiciels et aux données). Ces commentaires ont été globalement positifs. Les utilisateurs reconnaissent qu'il faut mettre en place des décisions plus efficaces pour renforcer la sécurité, basées sur des attributs d'identité (l'âge, par exemple), et créer des mécanismes obligeant davantage à rendre compte pour les activités en ligne. De là, plusieurs questions clés se sont fait jour.

Anonymat et contrôle utilisateur

Tout d'abord, certains s'inquiètent de savoir comment nous protégeons l'anonymat (et les principes qu'il sous-tend, comme la liberté de parole), dans un Internet où les mesures d'authentification sont plus strictes. Pour cette question, beaucoup ont indiqué qu'il était important de laisser l'utilisateur décider des informations qu'il divulgue et de l'instant où il le fait, c'est un principe de confidentialité très important (à savoir, le contrôle exercé par l'utilisateur). Comme l'explique l'un de ces commentateurs : « J'imagine que ça ne sera pas éternellement parfait, mais je ne souhaite en aucun cas que ces changements induisent une perte de libertés individuelles et une perte de contrôle. Le contrôle doit en définitive rester entre les mains de l'utilisateur ». De même, un autre commentateur a insisté sur le fait que les individus ont un droit « de propriété et de contrôle de leur identité » et « d'être anonymes et de contrôler leur identité en même temps. » Comme je l'ai indiqué dans le livre blanc, nous sommes convaincus que pour instaurer une confiance de bout en bout, il faut permettre aux utilisateurs et à leurs agents de prendre des décisions appropriées sur l'information qu'ils veulent partager et sur les individus qui méritent leur confiance. Tout en admettant que l'utilisateur doit rester maître de ses informations, plusieurs personnes ont

également indiqué que ce contrôle était par nature nécessairement lié à la qualité de l'expérience utilisateur qui lui est proposée. Pour être plus précis, beaucoup ont déclaré que pour faire un choix éclairé, l'utilisateur doit recevoir les bonnes informations au bon moment. En même temps, le fait de donner à l'utilisateur trop d'informations et trop d'options peut nuire à l'expérience utilisateur. La difficulté consiste à donc à trouver l'équilibre parfait.

Accès

Les opinions étaient plus divergentes dans un domaine particulier que beaucoup désignaient sous le terme « accès ». Une petite minorité d'usagers, qui assimilent l'Internet au réseau routier public, a proposé que l'Internet soit équipé de barrières et que les utilisateurs soient obligés de s'enregistrer pour y accéder. Les données correspondantes seraient accessibles par des autorités chargées de faire appliquer les lois et de prendre les mesures appropriées. D'autres ont prévenu de façon implicite des risques de cette approche en indiquant que « l'utilisateur n'acceptera pas un Internet réglementé et contrôlé et qui limite la liberté d'expression individuelle. » Naturellement, dans de nombreux pays, il est possible de passer des appels anonymes (à l'aide d'un téléphone public ou d'un téléphone portable jetable, par exemple), d'envoyer des courriers électroniques anonymes (sans indiquer d'adresse pour la réponse, par exemple), et l'anonymat est protégé dans les textes juridiques, même s'il existe un risque de préjudice. Tout ceci laisse à penser que les sociétés en sont venues à la conclusion que les avantages sociaux et économiques de l'expression anonyme étaient plus importants que les risques que présente l'anonymat.

Instaurer une confiance de bout en bout dans la pratique

Plusieurs personnes se sont penchées avec beaucoup d'application sur les aspects pratiques liés à la mise en pratique concrète de notre vision. Certaines ont avancé qu'il fallait définir des « authenticateurs certifiés » chargés de valider des identités. D'autres ont indiqué le rôle prépondérant que pouvaient jouer les fournisseurs d'accès à Internet (FAI), en faisant appliquer certaines règles (le filtrage de courriers électroniques non signés, par exemple) et en obligeant à une plus grande responsabilité (un fournisseur pourrait suivre des échanges de données au cas où une autorité civile en ferait la demande par voie légale). D'autres ont soulevé des questions ou des inquiétudes quant au pouvoir accordé à ces organisations pour surveiller le trafic du réseau et établir des profils comportementaux. Certains ont également donné leurs avis sur la réalisation pratique d'une telle vision et se sont concentrés sur deux thèmes. D'abord, beaucoup ont salué l'analyse exposée dans le livre blanc et la clarté de la « décomposition » de la question de la sécurité qui en est faite ; cette analyse laisse entrevoir des progrès possibles dans certains domaines, même si des progrès dans tous les domaines ne sont pas réalisés. Par exemple, la signature des applications peut être améliorée même si d'autres composantes de la structure de confiance ne suivront pas. Ensuite, il a été mis en avant l'énormité de la tâche à la lumière de l'inertie qui règne en général à l'heure du changement. Il faudra une synergie et un consensus entre de nombreuses organisations pour que notre vision d'une confiance de bout en bout se concrétise plus globalement (et non pas seulement en partie). Bien que beaucoup aient indiqué que la priorité à l'intégration de la technologie, de la société, de la politique et de l'économie était justifiée, il est clair que l'intégration et l'alignement de ces quatre disciplines au niveau des instances internationales reste une tâche audacieuse. Naturellement, tous espèrent des actions concrètes, tout en jugeant le dialogue très utile. À cet effet, nous allons examiner ci-dessous l'un des scénarios présentés dans le livre blanc.

Scénario de contrôle d'identité

Dans le livre blanc que nous avons publié en avril, nous avons abordé le concept de contrôle d'identité (in-person proofing) pour l'authentification d'attributs d'identité sur Internet. Nous avons exposé brièvement un cas d'application de ce concept. Il s'agirait pour les établissements scolaires d'identifier leurs élèves et leur fournir des données d'identification numériques pour qu'ils puissent se rendre dans des cours électroniques où tous les autres membres sont des enfants d'âge similaire. Pour mieux protéger les enfants sur Internet, des solutions de vérification d'âge sont envisagées par les pouvoirs publics, les associations de défense des enfants, les instances éducatives et les fournisseurs en informatique pour conserver une séparation entre les interactions des enfants en ligne et celles des adultes.

Au cours des derniers mois, nous avons approfondi cette idée et développé une approche conceptuelle pour ce scénario (visitez <http://www.microsoft.com/endtoendtrust> pour plus de détails). Cette approche utilise une technologie de cartes d'informations numériques (Windows CardSpace en est un exemple, le projet open source Higgins en est un autre) comme infrastructure pour créer des cartes d'identité numériques. Les enfants peuvent utiliser leur carte d'identité numérique pour prouver leur âge avant d'accéder à un site Internet qui leur en fait la demande, ou pour des événements hors ligne où ils doivent prouver leur identité à l'école ou dans d'autres institutions. Nous avons soumis ce concept à l'ISTTF (Internet Safety Technical Task Force), dirigé par le Berkman Center for Internet and Society de l'Université de Harvard. Nous avons soumis cette proposition à la Commission européenne qui a lancé une consultation publique sur la vérification de l'âge des internautes. Les deux groupes évalueront les solutions proposées et fourniront leur rapport dans les prochains mois. Nous félicitons le Centre Berkman de Harvard et la Commission européenne d'avoir pris l'initiative d'examiner ces solutions de vérification d'âge.

Le cadre que nous avons défini est une solution qui envisage la vérification de l'âge d'un point de vue essentiellement technique. Nous pensons toutefois que les aspects non techniques du problème seront aussi difficiles à résoudre que les aspects techniques, sinon plus. Pour que cette vision devienne réalité, les experts en développement de l'enfant, les pouvoirs publics et les entreprises doivent coopérer ensemble pour répondre à d'autres questions et d'autres difficultés.

Au-delà de la vérification de l'âge à proprement parler, si le contrôle d'identité doit devenir la base de l'authentification des attributs d'identité sur Internet, il reste à trouver des réponses à de nombreuses questions qui nous ont été rapportées à la suite de la publication du livre blanc. En voici quelques-unes :

- Pouvons-nous réutiliser les systèmes et les fonctionnalités de contrôle d'identité actuels (vérification des documents d'identité dans les bureaux de poste, vérification de la présence des élèves d'un établissement scolaire, vérification d'identité avant la délivrance du permis de conduire ou d'un document d'identité, vérification de l'identité des clients d'une banque) ?
- Quels types d'organisations pourraient et devraient engager une telle démarche et prouver qu'elles ont mis en œuvre ce concept ?
- Quelles organisations devraient être logiquement les premières à « consommer » des attributs d'identité basés sur le contrôle d'identité ? Est-ce dans le secteur privé où des sites de réseau sociaux pourraient chercher des solutions efficaces pour protéger les enfants ?

Est-ce dans le secteur public où une identité robuste est et doit être exigée pour toute interaction avec un organisme public ou administratif (par exemple, pour déposer une demande d'allocation auprès d'une administration) ? Ou les deux ? Comment les risques réglementaires et économiques influent-ils sur la volonté des organisations de se positionner sur le marché du contrôle et de l'authentification de l'identité ? Faut-il créer un contexte réglementaire plus favorable et fournir d'autres garanties (p. ex., la limitation à 50 \$ des pertes pour fraude à la consommation a permis de promouvoir la sécurité des cartes de crédit) ?

- Comment traiter les échecs, si l'on attribue ou perd par erreur des informations d'identification ?

Nous espérons que des initiatives telles que celles du Centre Berkman et de la Commission européenne permettront d'alimenter ces débats importants.

Ce qui reste à faire pour instaurer la confiance de bout en bout

Les défis que pose la mise en adéquation des solutions informatiques avec les exigences sociales, économiques et politiques sont décisifs et réels, comme je l'ai souligné dans mon livre blanc. Nous restons persuadés qu'il est possible de les relever collectivement. À la lumière de ce livre blanc et des commentaires qu'il a suscités, nous réfléchissons davantage (1) aux voies dans lesquelles nous voulons impliquer tous ces groupes d'intérêts, (2) à la façon d'identifier plus clairement les problèmes qui doivent être résolus et dans quelles sphères, et (3) à la façon de catalyser les bonnes actions par les bonnes personnes et au bon moment. Nous tiendrons également compte de ces commentaires à mesure que nous créerons d'autres scénarios pour concrétiser notre vision.

Pour résumer, les concepts exposés par le livre blanc sur la Confiance de bout en bout ont à la fois été bien accueillis et ont soulevé des inquiétudes. C'est la marque d'un débat sain sur l'avenir d'Internet. Nous vous remercions pour tous vos commentaires et pour l'intérêt que vous avez porté à ces questions. Pour ceux d'entre vous qui n'ont pas encore lu le livre blanc, ou qui n'ont pas encore participé à nos discussions sur nos forums ou ailleurs, je vous encourage à le faire en vous rendant sur le site <http://www.microsoft.com/endoendtrust>. Nous vous tiendrons informés au cours des prochains mois des résultats de ces débats et des prochaines étapes.

Les informations contenues dans ce document représentent l'opinion actuelle de Microsoft Corporation sur les points cités à la date de publication. Microsoft s'adapte aux conditions fluctuantes du marché et cette opinion ne doit pas être interprétée comme un engagement de la part de Microsoft ; de plus, Microsoft ne peut pas garantir la véracité de toute information présentée après la date de publication.

Ce document est uniquement fourni à titre indicatif et MICROSOFT N'APPORTE AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, À CE DOCUMENT.

L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans la permission expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur tout ou partie des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2008 Microsoft Corp. Tous droits réservés.

Microsoft, Windows et Windows CardSpace sont soit des marques déposées, soit des marques de fabrique de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Les autres noms de sociétés et de produits mentionnés dans ce document sont des marques de leurs propriétaires respectifs.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • États-Unis.