Conférence RSA: sécurité des accès, où s'arrêtera-t-on?

Amsterdam – Un dîner reste le lieu idéal pour glaner quelques indiscrétions sur quelques développements futurs. Le cocktail de presse de RSA Security n'a pas sacrifié à cette honorable tradition. Ainsi, Burt Kaliski, directeur des labos 'Recherche' de RSA s'est lâché sur les cartes d'identification. Pourquoi, s'exclame-t-il, ne pas généraliser leur usage dans les produits grand public? Ceci permettrait d'en assurer le suivi depuis la palette d'expédition jusqu'au client final… Il explique: la technologie existe -et depuis longtemps. Il s'agit tout simplement d'une étiquette radio intégrée dans une carte. La simple proximité d'un lecteur de fréquences radio permet ?d'exciter? l'étiquette (une boucle métallique qui est ainsi alimentée par la fréquence radio et signale sa présence au lecteur). Employée depuis près de vingt ans pour identifier le bétail, cette technologie d'une simplicité déconcertante avait sombré dans l'oubli. RSA la remet au goût du jour en proposant pour bientôt des cartes d'identification grand public qui devraient « cartonner »… A suivre? **Sécurité + interopérabilité = SAML** Une chose est sûre, en matière de sécurité -et surtout de budgets sécurité- les utilisateurs boudent. L'effet 11 septembre et guerre du Golfe est retombé. A force de faire plus avec moins (pression sur l'action en bourse, etc.), les entreprises n'ont vraiment pas envie d'investir massivement dans des technologies propriétaires à 99,99%, lesquelles, par définition, ne coopèrent pas entre elles. Mais, tout comme dans le stockage, l'interopérabilité vient au goût du jour dans la sécurité (et tout particulièrement dans les services Web). Le nouvel outil magique pour y parvenir s'appelle **SAML** (*Security assertions markup language*): c'est un sur-ensemble de XML qui doit notamment d'échanger les informations entre partenaires commerciaux via Internet. SAML est en pleine standardisation via le comité OASIS (Organization for the Advancement of Structured Information Standards) -ce qui constitue un bon point. Mais ses vrais avantages tiennent au fait qu'il offre un bon niveau d'interopérabilité, puisque, grâce à lui, les places de marché électroniques, les fournisseurs de services et les utilisateurs finaux (quelle que soit leur taille), peuvent échanger des informations sécurisées, ou bien des services Web, voire des autorisations d'accès ou d'usage sans qu'il soit nécessaire pour le moindre partenaire concourant à ce processus de changer un iota de sa solution de sécurité. Mazette! Bref, SAML devient l'esperanto des échanges d'informations propres à la sécurisation d'une transaction. Il ouvre toute grande la porte à une gestion fédérative de l'identité d'un utilisateur, autrement dit à l'emploi d'une authentification unique pour dialoguer avec un ensemble de sites business. En effet, grâce à SAML, tout utilisateur fonctionne dans un mode Single-Sign-on valable pour une multitude de sites (tout au moins, ceux qui utilisent ce format dans le contexte d'une communauté de services). L'intérêt d'une telle approche est évident. Cela permet notamment à un utilisateur nomade (par exemple, un audit d'entreprise) de se promener de filiale en filiale en retrouvant à chaque fois ses accréditations sur le site de l'entreprise auditée, sans avoir besoin, à chaque fois, de redemander des droits d'accès. Enfin, SAML s'avère une solution largement ouverte puisqu'il a été conçu pour fonctionner avec un bon nombre de protocoles de transport de données, dont HTTP, SMTP, FTP, tout comme avec des gabarits d'échange de données sous XML, dont SOAP, Biztall et ebXML. On l'aura compris: RSA y croit! Outre un rôle important (aux côtés de Netigrity, disons-le) dans la définition de son standard, il en a fait son cheval de bataille pour rassembler les grands du secteur -dont Sun, IBM, HP et BEA Systems. Et quoi qu'il en soit, c'est un moyen de contrer Microsoft et ses

spécifications W-S Security.