Internet : Le PKI (Public Key Infrastructure), dÃ©mystifiÃ©
Internet
PostÃ© par : JulieM
PubliÃ©e le : 25/7/2011 15:00:00

Le PKI (Public Key Infrastructure) a Ã©tÃ© saluÃ© comme la solution la plus sÃ»re pour authentifier les utilisateurs, les terminaux et les documents aux tous dÃ©buts de lâ□□Internet. Il a suscitÃ© une excitation croissante et une foule dâ□□articles, incitant les dÃ©cideurs informatiques Ã se pencher sur la question.

Puis, trÃ¨s brutalement, le PKI a reÃ§u un formidable retour de bÃ¢ton de la part des mÃ©dias. Tout dâ□□un coup, il sâ□□est retrouvÃ© comparÃ© Ã Â« une vÃ©ritable usine Ã gaz, un marteau quâ□□on utiliserait pour tuer un moucheron Â». On lui a reprochÃ© sa complexitÃ© arbitraire, le fait quâ□□il exigeait des opÃ©rations dâ□□Ã©changes de clÃ©s avec dâ□□autres organismes, conduisant Ã de nombreuses interventions manuelles, pour par exemple envoyer des emails chiffrÃ©s ou signÃ©s numÃ©riquement.

Chris Harget prÃ´ne La DÃ©mystification des PKI

Beaucoup trop complexe pour les simples mortels que sont les informaticiens, il existait sÃ»rement des mÃ©thodes dâ□□authentification simplifiÃ©es telles quâ□□OTP Ã la disposition des entreprises. PKI sâ□□est presque transformÃ© en un croquemitaine informatique.

Un Ã©vÃ©nement surprenant sâ□□est alors produit, ou plutÃ´t, deux Ã©vÃ©nements. Tout dâ□□abord, les Etats ont adoptÃ© le PKI et de puissants logiciels de gestion des donnÃ©es dâ□□identification (credential management software - CMS) ont Ã©tÃ© crÃ©Ã©s en vue dâ□□automatiser une grande partie du processus dâ□□Ã©mission, de mise Ã jour et de rÃ©vocation de ces donnÃ©es.

Des Ã©diteurs gÃ©rant leur propre Ã©cosystÃ¨me tels que Microsoft, Juniper et Cisco ont intÃ©grÃ© le PKI Ã leurs offres. Les logiciels de CMS se sont finalement fait une place dans les applications. Ils ont Ã©tÃ© une solution idÃ©ale et beaucoup plus simple pour les PKI dits en boucle fermÃ©e, câ□□est-Ã -dire dans les cas oÃ¹ lâ□□Ã©metteur et lâ□□authentificateur font partie de la mÃªme organisation, dâ□□oÃ¹ une rÃ©duction trÃ¨s importante des Ã©lÃ©ments du systÃ¨me.

En second lieu, des aspects des OTP les plus courants se sont vus exposÃ©s Ã des attaques de sÃ©curitÃ© (on peut par exemple citer la violation de sÃ©curitÃ© subie par RSA, suivie de lâ□□attaque contre Lockheed Martin). En consÃ©quence, les entreprises ont commencÃ© Ã se demander quelles Ã©taient les meilleures mÃ©thodes dâ□□authentification disponibles.

Le PKI se voir aujourdâ□□hui offrir une seconde chance. Beaucoup de gens continuent dâ□□avoir une rÃ©action de rejet instinctive, suspectant que le PKI a Ã©tÃ© inventÃ© pour leur donner lâ□□impression dâ□□Ãªtre stupides, mais un systÃ¨me PKI moderne en boucle fermÃ©e et gÃ©rÃ© par une application est exactement lâ□□inverse. Les nouvelles appliances CMS sont conÃ§ues de maniÃ¨re Ã ce que les Ã©quipes informatiques sans mÃªme connaÃ®tre les PKI puissent dÃ©ployer une solution de carte intelligente aussi sÃ©curisÃ©e que pour le secteur militaire.

RÃ©trospectivement, un peu comme ces images ou informations virales qui se propagent parfois en masse sur Internet, le PKI a souffert dâ□□une surmÃ©diatisation avant que les outils permettant de le gÃ©rer nâ□□aient Ã©tÃ© mis en place. Les spÃ©cialistes de la sÃ©curitÃ© se sont trop enthousiasmÃ©s Ã son sujet et se sont attelÃ©s Ã dÃ©finir le nec plus ultra des solutions PKI, alors que peu dâ□□entreprises avaient rÃ©ellement besoin de ses fonctions les plus Ã©sotÃ©riques, complexes et exagÃ©rÃ©ment consommatrices de main-dâ□□Å□uvre. Lorsque les fournisseurs de solutions PKI se sont emballÃ©s en tentant de former les utilisateurs Ã tous les scÃ©narios dâ□□utilisation possibles, ils ont en fait dÃ©tournÃ© les usagers potentiels des scÃ©narios les plus Ã©conomiques et les plus porteurs de valeur. Si je vous disais que je peux vous proposer un appareil quâ□□il vous suffit de connecter Ã votre PC, fonctionnant comme un lecteur de cartes et vous permettant dâ□□accÃ©der en toute sÃ©curitÃ© aux PC, aux rÃ©seaux, aux applications en cloud et aux rÃ©seaux virtuels privÃ©s (VPN), il y a fort Ã parier que les rÃ©actions seront heureuses . Puisquâ□□en effet, le PKI prÃ©sentÃ© aujourdâ□□hui nâ□□a plus rien Ã voir avec sa toute premiÃ¨re mouture.