

Re: Requesting additional authentication from remote user

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.ras_routing/2004-10/0063.html

From: Vin McLellan (vin_at_theworld.com)

Date: 10/07/04

Date: 6 Oct 2004 23:35:53 -0700

Mark <Mark@discussions.microsoft.com> asked:

> > [...]Is there an additional
> > authentication mechanism that you can configure on the Windows2000
> > Domain controller to request an additional piece of information from
> > the user (for example like a pin number) just to verify the user is
> > who they are?

Along with a lot of useful IAS information, the reply from Microsoft's "James McIllece" <jamesmci@online.microsoft.com> noted:

> *Offhand I don't know of an authentication method that requires both
> password-based credentials and a smart card. You might look into RSA
> SecurID (which works with IAS), as that is an interesting alternative. The
> whitepaper on how to deploy RSA SecurID with IAS is located at
> <http://www.microsoft.com/windowsserver2003/technologies/ias/default.aspx>
> and is called "Enterprise Deployment of Wireless & Remote Access with RSA
> SecureID and Microsoft Internet Authentication Service."*

The latest version of RSA SecurID for Windows, developed in close collaboration with Microsoft, installs an RSA Authentication Agent — which demands two factor authentication (a memorized PIN and a SecurID 60-second token-code), and reports to a central audit log — to restrict access to a Windows network domain.

Corporate insiders, who otherwise roam the enterprise network freely, will still have to present their credentials for access to the DC.

What RSA calls SecurID for Windows (SID4Win) actually pushes strong, auditable, two-factor authentication out in both directions from the network perimeter that has been its traditional focus.

SID4Win replaces the Windows logon screen with a SecurID logon screen, doing away with the irritating two-layer authentication process. Rather ingeniously, it does this while leaving the Windows security

microsoft.public.win2000.ras_routing: Re: Requesting additional authentication from remote user

model intact and unchanged. The Windows password, as long and complex as necessary, is now submitted to the OS by the RSA Authentication Manager after the SecurID authentication is validated. (The user is even prompted to change his Windows password, if that is required by the corporate security policy. Draconian password policies become painless.)

RSA, for which I have been a consultant for many years, now provides RSA Authentication Agents for corporate XP desktops on the enterprise network, and for mobile XP laptops as well. Even when these PCs are temporarily off the Net, their users will still be required to present a valid username, a memorized PIN, and their SecurID token-code to logon to these machines.

See RSA's data sheet, white paper, and webcast on SID4Win at:
<<http://www.rsasecurity.com/node.asp?id=1173>>.

(OT -- but how, you ask? The RSA Authentication Manager now loads these protected PCs with a secure cache of future SecurID token-codes -- for some variable number of days, pre-set for groups or an individual by the network admin -- so the user can use his SecurID to access his company laptop at 35,000 feet, on a cross-country Red Eye, or whenever his PC is temporarily disconnected from the Net.

(When the user next connects to the Net, the RSA Authentication Agent uploads an audit record of what has happened in the interim, and downloads a new secure cache of SecurID token-codes for future offline use.)

Market demand for strong authentication, and a secure audit trail, to protect access to network domains -- and PC-based repositories of proprietary and confidential corporate data, as well -- seems to reflect, at least in the US, the additional security required for compliance with the various new external regulatory regimes: Basel II, Sarbanes-Oxley, HIPAA, GLBA, etc.

Mark is not alone among the savvy administrators (and auditors) who have wanted these additional controls for a long time, but I suspect that it is only the external pressures that made these joint product enhancements feasible, even inevitable.

(RSA, btw, is now providing this SID4Win functionality without charge to its existing customers that are running the most recent version of the RSA ACE/Server. That's probably most of their 15,000+ enterprise customers.)

Suerte,
_Vin

Re: Requesting additional authentication from remote user