Live Mesh and security related

Introducing security issues in 'cloud computing' in general, Live Mesh in particular and the mechanisms Microsoft created to protect your 'meshed' devices and your data.

Deb Shinder

Network administrator - *Microsoft recently released a preview of its new service technology Live Mesh. This is a 'cloud computing' service that we've been waiting for since Ray Ozzie hinted about it in a speech at Microsoft's conference in late March. It allows file sharing and synchronization between PC devices (even Mac and Windows Mobile). However with all that sharing, what is the security attached? This article will cover issues related to the security of 'cloud computing' in general and Live Mesh in particular, besides the mechanisms that Microsoft has built to protect devices. has been 'mesh' and your data.*

How to protect the 'Cloud'

Before going into Live Mesh, we need to clarify some questions about the security of 'cloud computing' in general. In some reports, experts have emphasized the fact that risks can be improved better by choosing the right service provider and taking steps in a timely manner with threats.

However, the characteristics that make 'cloud computing' have advantages can also make it a weakness. Cloud-based calculations make your data and in many cases your applications, accessible from anywhere in the world - but that also means, unless you There are strong measures to secure them, otherwise this is a 'detrimental benefit' because someone can have this access besides you. In fact, as some documents have shown, you may not even know where your data is stored in the world. For most security experts it is indeed a problem.

'Cloud computing' may also have some security advantages. Since your data is not 'live' on a local computer, it is not affected by syndromes such as losing a laptop because the data is stored locally. Although laptops can be encrypted, encrypted hard drives, equipped with multiple security software or remote data removal software - but whether your company employees can always tell Proper security for their computers? Therefore, storing data in a certain location in the 'cloud' can avoid such problems.

However, this centralized storage sometimes has its own risk. If a hacker has access to your data on your provider's server, this hacker will get it all. But if deployed properly, this type of storage will make it easier to protect all data in one location instead of protecting the files stored on different computers. And the cost of security may be reduced because the provider will spend money on their security mechanisms on a series of clients.

In short, when it comes to security, the 'cloud' has both its advantages and disadvantages. More or less depends on how it is implemented.

How does Live Mesh work?

Before we dive into the technological aspects, it should be noted that in its current incarnation, Microsoft is marketing Live Mesh as a customer service, not a targeted service. business. However, the company has released many of its products and services for its first customers, and many experts believe it can and will be extended to the business sector as well. up famous.

So what are the basic differences between 'cloud' and 'mesh'? The biggest difference here is: the mesh is a personal mesh (as opposed to the 'cloud' that you share with people who have never been known). Mesh includes other devices that you want to access data and programs: for example, your home workstation, workstation located in the office,; laptops and mobile devices (currently a preview of technology of Live Mesh only supports Windows computers, but Microsoft is planning to support Windows mobile devices and Mac OS X in the future).

Your information is automatically synchronized on the devices you join your mesh by installing the Mesh Operating Environment (MOE) software. You can also use the Live Mesh Remote Desktop feature to access desktop computers - including computers running XP Home and Vista Home that don't support incoming Remote Desktop connections. In addition, mesh also includes a 'cloud' component, Web-based Live Desktop so you can save files (up to 5GB) on Microsoft servers.

What does Microsoft do to protect the mesh?

This is a big question: What is the security here? Live Mesh authentication is based on Windows Live ID (previously known as Microsoft Passport). Passport is conceived as a single sign-on service for e-commerce. In 2007, a vulnerability was discovered in Live ID, this vulnerability allows users to register an error or an email address that does not exist with the service as it was fixed after it was discovered.

Live ID accounts can be verified in a variety of ways, including:

- Username and password
- Combination of Password / PIN
- WindowsRADIUS Cardspace Smart Card (for mobile and Xbox appraisal)
- Federation assessment (WS-Trust)

Since most Live ID users depend on the first method (the least secure), the security of the account depends on choosing a strong password. Live ID supports lengthy passwords (up to 16 characters) including symbols as well as alphanumeric characters. When you create your credentials, the Live ID interface will review and report on your password length.

Live ID must undergo periodic security audits by independent verifiers. Kim Cameron, a Passport expert, joined Microsoft as an Identity and Access architect and has had a lot of work in developing Live ID.

After the user or device is authenticated, Security Assertion Markup Language (SAML) tags are used for accessing mesh-based resources, SAML is an XML-based standard.

Tags are distinguished by a private key and have an expiration date after a certain time. The Live Mesh service checks the tags, if these cards are valid, then it will allow access. In general, access is allowed between two devices if the card shows that both devices belong to the same user or in the case of shared folders, if the card shows that both devices have the same The Live Mesh folder has been mapped.

Traffic between server and client is encrypted using HTTPS. Encrypt this to avoid some attacks. The devices you join to mesh must have their own keys. Only the client knows this private key, so traffic cannot be blocked and read in 'the cloud'. When you connect one device to another device via mesh, then asymmetric encryption is used to exchange keys and data and files are transmitted using AES 128 bits. The integrity of the data verified through the message authentication code (HMAC - Hash Message Authentication Code) has a code key, which uses a hash function with a security key.

Files stored on Microsoft servers in 'cloud' (5GB for Live Desktop storage for each user) are protected by access controls but not encrypted.

Another problem related to this is the Remote Desktop feature. The service that allows Remote Desktop, wlcrasvc.exe, is configured to launch completely automatically. If you end a process, another process will begin. If you want to disable this service to increase security, open a command prompt with administrator access and type **net stop wlcrasvc** . You can also disable the service in the Startup Type column in the Services console.

Finally: for the purpose of today - allowing customers to easily integrate their multiple devices and provide easy access, security can now be good enough. However, to become a viable option for the corporate world, where the consequence of data compromise is closely related to financial issues, we need to consider an 'security' option. high'.