Dr. Bob "discovers" Datasnap 2010 security is nonexistent (http://www.sandon.it/node/52)

Posted on: Sun, 01/24/2010 - 23:50 **By:** ldsandon

I've complained a lot about the security (or better, lack of) of Datasnap 2010. The usual answer was that I was wrong, and anyway filters could be used to implement it. Now Bob Swart - who wrote the Delphi 2010 Datasnap white paper - filed two QC entries (http://www.delphifeeds.com/go/s/64604) about Datasnap security. The first asking for HTTPS support, the other reporting a serious performance issue when using filters.

I agree that if you support HTTP there's no reason not supporting HTTPS (but remember the underlying transport is managed by Indy), but why don't add SSL support to TCP connections too? Remember that SSL is in no way tied to HTTP. It is a more generic specification - and TSL also allows to use the same port for both encrypted and unencrypted connections. I prefer by far plain TCP in LAN scenarios where HTTP overhead and limits are useless.

Should be SSL the only choice? Of course not, and SSL has the drawback of needing certificate creation, distribution and management. You need to setup a CA, make revocation lists accessible, issue and revoke certificates. It is true that in an Active Directory domain with an Enterprise CA most of this tasks are automatic, but Delphi lacks a library to access Windows CryptoAPI and certificate stores. Putting your .crt file in the application directory is not the smartest move. especially those with the private keys - insider threats are an issue as outsider ones are.

And when an application runs within an AD domain, there are better ways to protect the communication channel, identify endpoints, and allow for single sign-on without using certificates, for example exploiting AD iteself, and Kerberos. Using Windows Server 2003 Active Directory Application Mode (http://www.microsoft.com/windowsserver2003/adam/default.mspx)/Active Directory Lightweight Directory Services (http://msdn.microsoft.com/en-us/library/aa705886(VS.85).aspx) is even possible to take advantage of AD security on standalone servers or server with specific needs without touching the whole domain Active Directory schema.

Of course this is not an "xplat" approach, thereby I am sure BorCodeDero will not even think about it - and I am not sure they have ever heard of ADAM or AD LDS - for the matter, those designing Datasnap 200x look to have never heard about security at all.

- Log in (http://www.sandon.it/user/login?destination=/comment/reply/node/52/comment_node_blog%23comment-form) to post comments