Mocking your customer is not a way to sell more... or it is? (http://www.sandon.it/node/99)

Posted on: Fri, 07/03/2015 - 22:11 **By:** ldsandon

Resident Embarcadero wizard of Oz, David Intersimone, has been so bold to write about Delphi "security" (http://community.embarcadero.com/index.php/blogs/entry/the-rad-studio-xe8-summer-northern-hemisphere-and-winter-southern-hemisphere-of-security). You know I already wrote about the utterly lack of security in Datasnap (but relying on web server security using https), but there are some true pearls in that article.

For example (in the comments) "*only challenge we have (being a US company) is in shipping any encryption technology without an export license. For DataSnap encryption filter we have examples for PC1 and RSA which are not under export restrictions*." Well, if you are a company unable to comply with export legislation, it's better you stop to sell abroad. If you're too lazy or mean to get an export license - something every competitor of you did - well, why should I buy your products?

Shipping an unknown algorithm you got for free from somewhere on the Internet, it is not a professional behaviour.. although groupie like Nick Hodges will tell it's impossible to obtain a license, although everybody else did. Sure, you need some paperwork, yet nothing beyond what a company with the aim of selling worlwide should be able to do, especially at the price Delphi is sold. Also, if Interbase **supports AES** and other algorithms **which actually do need an export license**, why Delphi can't??

It is also not true that "RSA" is not under export restrictions. Only version with keys of 1024 bits or less are exempt (and also using weak symmetric keys and algorithms), and of course those key length and algorithms are no longer considered secure, some browsers start even to refuse certificate with weak encryption altogether. It's clear Intersimone really doesn't know what he's talking about.

Lockbox 2 cannot be considered a good library any longer because it still uses old, outdated algorithms and weak keys. I hoped the recent news about SSL3 being fatally flawed, for example, would have taught why relying on too old implementations can be very risky, but nope. Still say that old library is good, because it's free and there's not much else for Delphi.

"*DataSnap provides a way for the Client to safely communicate with the Server, using a secured transfer of JSON (JavaScript Object Notation) data content over TCP/IP, HTTP and HTTPS. The ability to define filters at both ends of the communication channel, for encryption and compression purposes, improves the securit*y."

HTTP is of course not secure at all, HTTPS is as much secure as your web server configuration is (hint: self-signed certificates are not secure at all...). When you properly protect a channel, you can transfer data in any format you like, JSON or not. But an acronym is always good to make it "really technical". While Embarcadero still pretends filters can be used to protect the connection, it's just

plainly false and deceveing, as I already wrote about (http://www.sandon.it/?q=node/57). App Thetering suffers from the same lazy and bad design.

Windows CryptoAPI links are really outdated ones, especially since today you should use the newer CNG API (http://msdn.microsoft.com/it-it/library/windows/desktop/aa376210(v=vs.85).aspx), since Windows 2003 too will be end of life in a few days. Time to update your bookmarks, Mr. Intersimone, and maybe avoiding to use Google's "I'm feeling lucky" button.

And you still wonder why after all these years Delphi never wrapped Windows CryptoAPI in a library, instead of relying on unknown algorithm (you don't need an export license to wrap the Microsoft provided one, Microsoft is still a US company but does its homework), or OpenSSL like Indy, with the need to update it yourself - and these kind of libraries must be updated, you can't rely on old version with known vulnerabilities.

I really wonder how a company could post officially such crap. Especially a company whose products should be aimed at professional developers. It's really mocking your customers. Embarcadero is saying "we're sure you're so an unskilled developer we can write this crap, and still sell you products. You're a moron, and we take advantage of it".

Oh well, the latest article on delphifeeds today is another "migrating from BDE to..." one.

Maybe Embarcadero is right.

- Log in (http://www.sandon.it/user/login?destination=/comment/reply/node/99/comment_node_blog%23comment-form) to post comments