

microsoft.public.vc.mfc: Re: Need strong crypto for sending my password via sockets.

Re: Need strong crypto for sending my password via sockets.

Source: <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2004-11/0194.html>

From: Daniel James (*wastebasket_at_nospam.aaisp.org*)

Date: 11/02/04

Date: Tue, 02 Nov 2004 18:40:22 GMT

In article news:<c882495.0410252337.b7f8837@posting.google.com>, Sergey Kochkarev wrote:

> *Try to use something simple yet effective – md5 or blowfish. They are free.*

MD5 and Blowfish are indeed free, but MD5 is not an encryption algorithm it is a digest (hash) algorithm. Furthermore the security of MD5 has been called into question recently as a number of attacks have shown that it is not as collision-proof as was thought.

3DES and AES are also free.

> *The procedure will look like the following: client asks for password, crypts it and sends to server. Server crypts it's own copy of password and compares crypted passwords ...*

A technique like that can work with a hash – the server would ask for the password and supply a random salt value, the client would hash the salt and the password together and send the result, the server would hash the salt and its copy of the password and compare. The salt is needed to prevent replay attacks. Note that this requires that the unencrypted password is stored at the server, which is not ideal.

It doesn't work well with an encryption algorithm like Blowfish because it requires that there is an encryption key known to both the client and the server but to nobody else.

SSL gets around this by creating a mechanism whereby a temporary encryption key can be generated by the client and sent to the server encrypted under the server's public key.

> *– that's how linux makes it.*

Linux hashes passwords using MD5 for checking locally – that's secure enough. Sending an MD5 hash of a password over the wire does not protect against replay attacks, so it should only be done on a secure/trusted

Re: Need strong crypto for sending my password via sockets.

microsoft.public.vc.mfc: Re: Need strong crypto for sending my password via sockets.

network.

Cheers,
Daniel.