

Re: Password Security

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.networks/2004-09/0178.html>

From: Callum Winter (*callum_at_REMOVE_THISwinter9999.fsnet.co.uk*)

Date: 09/08/04

Date: Wed, 8 Sep 2004 13:39:39 +0100

Hi Alun,

First thankyou for your reply.

Basically, Im working on an internet game, so good security isnt required much past the login process, the rest is general protocol packet tampering detection or prevention code, so really doesnt need encryption.

Yes the server will keep a database of users who have signed up to play, and obviously paying customers wont want their password cracked after some hacker has used a packet sniffer to get hold of a login packet. The database also will need to be encrypted just in case any hacker manages to get through our data server defences. Hopefully they wont as they wont know of this server, only the game hosting servers(which are middle men in the link), but safe is better than sorry.

We could of course prompt users to change their password on a regular basis, but the point is to make it difficult for hackers to crack passwords in the first place.

I understand IE has security built in (i think). Is it possible to use the algorithms in IE, somehow hook TCP to IE's security features maybe. (without having to learn java, or code to work within a web browser).

I will of course look round for some books. Are there any in particular (ISBN code if you know it) of a book that will cover my problem. Like you say it would be overkill to go much past securing login packets (which wont include much more than username and password), and the database of users on our data server, So the book must at least cover these topics and how to plug these features into C++ TCP/UDP code, including any interfaces required and where to get them.

One final question. If one can get hold of a secure transport interface then i assume a hacker could do the same and reverse engineer the algorithms and still manage to decode the login packets, so what Im asking is how secure is all this secure transport stuff in the first place. How long would it take to decode the encryption in a packet if they did manage to write a decryptor. Im quite new to all this so just want to get things clearer in my

head.

Hope you can provide that little bit more info for me.
Many thanks in advance.

Callum.

"Alun Jones [MSFT]" <alunj@online.microsoft.com> wrote in message
news:eCQBtmTIEHA.1656@TK2MSFTNGP09.phx.gbl...
> "*Callum Winter*" <callum@REMOVE_THISwinter9999.fsnet.co.uk> wrote in
message
> news:eGr#NOPIEHA.2868@TK2MSFTNGP11.phx.gbl...
> > *How*