Ryzom - Bug # 621

Status:	New	**Priority:**	Normal
Author:	kaetemi	**Category:**	
Created:	06/17/2009	**Assignee:**	
Updated:	09/29/2010	**Due date:**	
Subject:	Login service casts pointer to uint32 and sends it over network.		

Description

At line 163 in connection_client.cpp, the login service hacks a *NLNET::TSockId* into a login cookie. *NLNET::TSockId* is a typedef for *NLNET::CBufSock ** (a pointer to the socket with buffer). A similar setup occurs in connection_web.cpp at line 173.

```
    CLoginCookie c;
    c.set((uint32)(uintptr_t)from, rand(), uid);
```

When the user chooses a shard, it sends this cookie to the welcome service of a shard, which passes it back to the login service when it responds.

At line 408 or 412 it directly casts the *uint32* from the cookie back into a *NLNET::TSockId*, and passes it to the ClientsServer->send function, which uses it as a pointer.

```
    ClientsServer->send (msgout, (TSockId)cookie.getUserAddr ()); ...
    ... void CCallbackServer::send (const CMessage &buffer, TSockId hostid, bool /* log */) ...
    ... CBufServer::send (buffer, hostid); ...
    ... pushBufferToHost( buffer, hostid ); ...
    ... if ( hostid->pushBuffer( buffer ) ) // <- hostid is the TSockId that was cast from a uint32 received from the network
```

Might be problematic on 64bit systems, and may result in security issues when accepting third party shards on a login service.

History

#1 - 09/29/2010 09:43 pm - kervala

- Project changed from NeL to Ryzom

- Category deleted (Net)