



Theft Of Service Attacks

**Subscription Service &
Website Vulnerabilities**



Theft Of Service Attacks

Presented at Defcon 11 by:

Robert Sheehy

rjs@zendtech.com

Zendtech Services

www.zendtech.com

Presentation updates are available at:

<http://www.zendtech.com/defcon11/tos>



What Are Theft Of Service Attacks?

- Application Level Attack
- Attacker Gains Increased Access To Restricted or Limited Resources
- Opportunistic Attack
- Typically does not result in system administration access.



Example Targets for TOS Attack

- Software Registrations & Downloads
- Adult Web Sites
- Web Hosting Accounts
- Proxy/Anonymity Services
- Dial-up Internet Service
- Email/Usenet Service
- Shell Accounts
- Financial News Services
- Domain Name Registrations



What Is Stolen?

- **Increase access to a service providers systems (Shell Accounts)**
- **Avoidance Of DNS Registration Fees**
- **Usenet Access**
- **Dial-up Internet Access**
- **Web hosting (for data piracy & pornography storage, e-mail spamming, ect...)**
- **Increased Access to restricted content**
- **Software**



Security Holes Commonly Used for ToS attacks

- **Instant Account Creation Vulnerabilities**
- **Subscription Data In HTML Forms**
- **Authentication data stored in user cookies**
- **Paypal Subscription Payments**
- **Application, Server & or Operation System specific vulnerability exploits.**



Obscuring The Attack

- Putting in the order during a holiday weekend
 - Backlog of orders from a long holiday weekend may result in less attention to order details
 - Even if there is human review, the attack might be overlooked during high sales volume



Who Is The Attacker?

- A Technically Savvy Customer.
- A Competitor.
- An e-mail spammer or other criminal.
- Someone looking for a deal.
- A legitimate customer's friend.



Theft of Service Attack Types

- Software Copy Protection Circumvention
- Abuse Of A Legitimate Account
- Bypassing the Billing System
- User defined changes to the subscription terms or price.

Copy Protection Circumvention

■ Cracks & Serial Number Websites

- www.astalavista.box.sk

- www.cracks.am

- www.cerials.net

- www.cracks.wz

■ Piracy Newsgroups on Usenet

- alt.binaries.cracks

- alt.binaries.warez.0-day

- alt.binaries.cd.image

Abuse of a Legitimate Account

- Choosing “**login**”/”**password**” as your username/passwd pair.
 - Makes remembering passwords much easier.
 - Allows for anonymous account sharing.
 - Makes the admin feel dumb when they find it.



Abuse of a Legitimate Account

- Multiple Users of a single user account
 - Easy to detect, if the effort is made.
 - Normally results in account termination for Terms Of Service violation if detected.
- Account sharing is less likely to occur if the account exposes customer's data, such as home address or credit card number.

Bypassing The Billing System

■ Cookie Poisoning

- Alter cookie data to assume identity of a subscribing user

- Cookie Editor v1.5

 - Available from

 - <http://www.proxoft.com/CookieEditor.asp>

- WinHex

 - Ability to edit non-persistent cookies in memory.

 - Available from <http://www.sf-soft.de/>

Bypassing The Billing System

■ Free Trial Accounts

- Open to repeated use and abuse
- User is disqualified if they have previously used the same credit card or mail address for a previous free subscription
 - Open to repeated credit card fraud (especially if nothing is actually charged).
 - New credit cards with new numbers are also easy to obtain.
 - New Email addresses are easy to obtain.



Bypassing The Billing System

- Application Specific Attacks

- Bugs in the account signup process

- “Account Verification” pages that can be used to reactivate cancelled accounts.

- Subscription & Account Maintenance

- Account Upgrade/Downgrade may be open to attack, while the initial subscription process is secure.



Subscription Specific Attacks

- Alter subscription terms
 - Premium Account at Basic Account Price
 - Yearly Account at monthly account price
- Attacking the re-subscription process
- Attacking user verification pages
 - Subscribe to a yearly account
 - 24 hours later, cancel the account
 - Use verify page to reactivate account

HTM Form Alteration Attacks

- For “GET” forms, change URL parameters
- For “POST” forms, view the HTML source, and change the value of the Hidden input types.
 - type=“hidden” OR type=hidden (“ char is optional)

HTM Form Alteration Attacks

- For “GET” forms, change URL parameters
 - `http://website.com/script.cgi?var1=value1&var2=value2`
 - For “POST” forms
 - view the HTML source in text editor
 - change the value of the “hidden” input types.
- <input type=“hidden” name=“price” value=“19.95”>**

HTTP_REFERER

- Used to validate that form was loaded from proper domain
- EASY TO DEFEAT!
- HTTP_REFERER variable used to flag suspicious orders for further human review.
- Just because HTTP_REFERER is wrong does not mean the order is fraudulent.

HTTP_REFERER faking method #1

- Place edited HTML form source onto web server.
- Change hosts file to map expected domain name to the new server.
- Load the Page using the proper URL.
- Remove hosts file entry.
- Wait for DNS cache to expire, or flush the cache, then submit altered form to the target site.

HTTP_REFERER faking method #2

- Method utilizes browser proxy Support
- Edit hosts file as in method #1
- Load altered page from your web server
- Enter proxy server information
- Submit Form
- Proxy will not use hosts information, and will send altered form data with a faked HTTP_REFERER.

Automatic Form Submission

Using the lynx and echo commands.

```
echo `email=first.last@somewhere.com&\`  
username=username&\`  
password=tmp-passwd&&\`  
passconfirm=tmp-passwd&\`  
Submit=Submit\n---\n" \  
| lynx -post_data http://somesite.com/form.cgi
```

- ❑ Quotes Are Important (because of & Characters)
- ❑ Pipe echo command output to lynx



Combination Of Attacks

- Change subscription period from monthly to a yearly subscription.
- Change the subscription options to buy a “premium” account at the “basic” price.
- Transaction will look normal on casual inspection of the billing records.



O'Reilly's Safari Bookshelf Security

- System tries to enforce a “No Offline Archiving” policy, detailed in their Terms Of Service Agreement.
- Three strikes your out if the system detects massive downloading
- Session Limit (One login allowed – Cookie Based session tracking)
- Restriction On Library Access - Can only select X number of titles for access (X varies with subscription type)



Beating Safari's Security

Books must be kept on bookshelf for 30 days

- Does not matter if you cancel the account every month.
- Just create a brand new account every month
- If reusing a credit card, you will not have any waiting time for bookshelf slots to open.
- If using a new card, you get a new 14-day trial.



Beating Safari's Security

- **Free Trial Account Abuse – Bypass Billing**
 - **Get a new e-mail address**
 - **Sign Up for 14-day trial with a new CC.**
 - **Pick the books to fill your 10 bookshelf slots.**
 - **Use Offline Explorer to make an offline copy.**
 - **Cancel the account before the trial expires.**
 - **Cancel CC – Get a replacement from your bank with new numbers.**
 - **Repeat when new card arrives.**

Beating Safari's Security

- Offline Explorer – metaproducts.com
 - Used 2.8.1220 Service Release 1 during testing.
 - Demo version is usable
 - Wget not successfully tested – Gave up
- Only One Open HTTP Connection Used
- 30 Second Delay between file retrieval
- Used the ISBN number as URL filter
 - `sortOrder=asc&view=&xmlid=0-7357`
 - `sortOrder=asc&view=&xmlid=0-596`
- Started at the bookshelf, went 5 levels deep

Beating Safari's Security

- Only One Open HTTP Connection Used
- 30 Second Delay between file retrieval
- Use the ISBN number for URL filter
 - “sortOrder=asc&view=&xmlid=0-7357”
 - “sortOrder=asc&view=&xmlid=0-596”
 - xmlid is the ISBN number of the book.
- Start at the bookshelf, go 5 levels deep



Beating Safari's Security

- The idea of Digital Rights Management is unenforceable without causing major inconveniences to legitimate users.
- DRM objectives conflicts with easy of use designs..



ITKnowledge.com

- Offered 14 Day Trial – Once per credit card #
 - Similar to O'Reilly.
- Unsuccessful Attempt to stop offline archiving via login cookies.
 - Easily defeated.
- Subscribers received complete access to entire library.

ITKnowledge.com

- Created Their Own Security Hole
 - Sent e-mail to previous subscribers who cancelled during the 14-day evaluation period offering another 14-day free trial
 - No Credit Card Required For Signup
 - The 2nd 14-day free trial never expired
 - The signup for the 14-day trial never ended.
 - ITKnowledge went out of business
 - User's have full access to entire library for free, normally costing \$295 a year.



Important Notice to Our Customers

The ITKnowledge sites were shut down permanently on February 28, 2001. The content from the sites has been taken off-line and will not be made available on any other EarthWeb site.

If you are interested in similar services, you may want to look at:

<http://www.books24x7.com>

<http://www.informit.com>

<http://www.netlibrary.com>

At this time, we are processing refunds for outstanding subscriptions. If you have any questions, please email us at: custservice@dice.com.

Thank you for your patronage.

The ITKnowledge Team



eBay Seller Fee Avoidance

- Use of the non-bidding bidder form negates the eBay listing fees.
 - Refund system seems to be automated.
 - Buyer could be given a discount to not report fraud.
 - No incentive for buyer to report seller fraud when they are compensated by the buyer.



Software Theft With Paypal

- Depending upon implementation, users are paying a fee to learn the value of the “return” HTML form variable.
- Automated Key Return & Paypal is often exploitable by changing the price.
- A legitimate, but small, payment is made for an order. The system acknowledges payment, but does not verify the correct amount was paid.

Software Theft With Paypal

- View Page Source, look for paypal URL:

https://www.paypal.com/cart/add=1&business=paypal%40finite-tech.com&item_name=IPSec+Client+Software&item_number=ASL-IPSEC-CLIENT-WIN&amount=90.00&shipping=12.00&return=http%3A//www.chillywall.com/success.html&cancel_return=http%3A//www.chillywall.com/cancel.html

- [return=http://www.chillywall.com/success.html](http://www.chillywall.com/success.html)

Purchase Success

Thank you for your purchase of ChillyWall and/or our other security products.

If you purchased a ChillyWall this unit will ship to the address that was indicated on your order typically within 2 working days.

If you purchased Astaro Security Linux Software you can download the software [here](#). Your license will be e-mailed to you within 2 working days. You can proceed with your Astaro installation since the download is a 30 evaluation which can be activated for all features purchased when you enter your license.

If you purchased [VPN Client software](#) then the following links will provide you with the software and documentation.

[Software](#)

[User Manual](#)

[Release Notes](#)



Paypal Subscription Payments

- Purchase of the paypal guarantee
 - May expose bugs in payment processing
 - Valid only for physical items, effects of purchase may not be tested in subscription system.
- A legitimate, but small, payment is made. The system acknowledges payment, but does not verify the correct amount was paid – Just assumes it was.

```
<form action="https://www.paypal.com/cgi-bin/webscr" method="post">
<input type="hidden" name="cmd" value="_xclick-subscriptions">
<input type="hidden" name="business" value="paypal@zendtech.com">
<input type="hidden" name="item_name" value="Web Hosting">
<input type="hidden" name="item_number" value="WebHost11">
<input type="image" src="pics/x-click-but20.gif" border="0"
  name="submit"> $295.00
<input type="hidden" name="a1" value="0.00"> Setup Fee
<input type="hidden" name="p1" value="2"> Valid for 2
<input type="hidden" name="t1" value="M"> Months
<input type="hidden" name="a3" value="295.00"> Re-occurring Fee
<input type="hidden" name="p3" value="1"> Billed Once
<input type="hidden" name="t3" value="Y"> a year
<input type="hidden" name="src" value="1">
<input type="hidden" name="sra" value="1">
</form>
```



Finding Vulnerable Systems

- Internet Search Engines
 - New sites directory listing
 - Searching for vulnerable site criteria (example: Instant or Immediate Activation / Paypal Use / Subscriptions)
- Selfseek Web Search Spider (illumix.com)
- Systems you use (or want to use) everyday.



Preventing Form Alteration

Method #1 Variable Change Detection

- CRC checksum of form variables
 - Open to reverse engineering attacks.
 - Does not guarantee security, just makes a possible attack more complex.
- Checking the HTTP Referrer URL
 - Can be easily faked



Preventing Form Alteration

Method #2 Not Using Form Variables

- It's the “right” way.
 - Extra programming and complexity is required for the server to track user sessions.
 - Security is not guaranteed, systems could still be vulnerable to other forms of attack.



Credit Card Payment Attack

- Possible Attacks
 - Credit Card Fraud
 - Price Alteration
 - Avoiding Payment
 - Subscription Term Extension
- Especially vulnerable when using hidden form inputs for payment parameters.



How To Spot ToS Attacks

- Audit existing orders/subscriptions to verify subscription parameters have not been altered.
- Do not trust what your custom application tells you, it may be lie.
- Look for sudden increases in system utilization.
- Make sure whomever processes orders knows to verify the amount paid is the amount owed.



Detecting Credit Fraud

- Have all order verified by human eyes
- Follow all security procedures from credit merchant



How To Protect Against ToS

- **Verify All Orders Manually**
- Regularly Audit Account Activity
- Do not trust the security of your system automation.
- Do not overlook accounting inconsistencies, they may be indicators of fraud.



Attack Response Options

- Depends Upon nature of the attack
 - How abusive was the attack?
 - “Login”/”Password” is not really fraud
 - Account Cancellation may be only option
 - Fixing security whole, may be only option.
 - Can the user be tracked down?
 - Will law enforcement care?
 - Will the publicity of the hack be worse then the hack itself.



Attack Response Options

- Ignore The Attack
 - Let all users continue discounted subscription
- Account Cancellation
- Account Modification
- Back Billing



Recovering Losses

- Back Billing Customer
- Involve Law Enforcement
- Write off the loss
 - Most often there is no way to recover losses.
 - Considered to be the victims fault for being a victim.



DirecTV Theft Of Service

- Thousands Of DirecTV Customers Sued
 - Threatening Letter Intimidation Tactic
 - Millions Have Been Paid Already To Settle
 - No proof, other than purchase records, no proof of actual use



DirecTV Theft Of Service

- Can They Do This?
- Will They Get Away With It?



DirecTV Lawsuit Information

- www.legal-rights.org
- http://www.legal-rights.org/PAYPAL_AFFIDAVIT.html



Final Points

- Very simple attacks
- Security Oversights in newer sites
- Hit and miss attack, more an annoyance than a real problem to most retailers.
- Victim system admin gets little sympathy from law enforcement or colleagues.

Final Points

- Sites vulnerable to ToS attacks are usually vulnerable to other simple attacks.
- Most likely effective on newer websites that use a custom application or misconfigured 3rd party product.



Final Points

- Easy to perform
- Depending upon attack, legal fraud is not always committed (It's generally considered the victims fault for not taking basic security precautions.)
- A company could be put out of business with the time it takes them to notice a vulnerability has been discovered.