

Re: Anonymous Anonymity – Request For Comments

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-07/0292.html>

From: Craig Skelton (cskelton_at_gmail.com)

Date: 07/19/05

Date: Mon, 18 Jul 2005 19:00:49 -0700

To: bugtraq@securityfocus.com

Take a look at Tor.

<http://tor.eff.org/>

One of the biggest problems with Tor is bandwidth disparity.

On 7/17/05, Gandalf The White <gandalf@digital.net> wrote:

> *Greetings and Salutations:*

>

> *I realize that this is not specifically a Bugtraq issue, but I have posted*

> *this to Usenet to the Privacy forums and received little to no response. I*

> *also consider Bugtraq to be the haven of the most premier security analysts*

> *available on "The Internet". I would appreciate your comments on the below*

> *and request that you reply directly to my e-mail address.*

>

> *Thank you*

>

> *Ken*

>

> *Anonymous Anonymity – Request For Comments*

>

> *"I think paranoia can be instructive in the right doses. Paranoia is a*

> *skill." – John Shirley*

>

> *This document is available / updated at the following:*

> http://digital.net/~gandalf/Anonymous_Anonymity.htm

>

> *I would like to first ask the community to read this and comment on the*

> *"Issues" section. I am struggling with the how to fix the issues presented.*

> *If you can conceive a better way to fix the first issue I would appreciate*

> *that input. If there is a solution that is already well known, please tell*

> *me. Thanks.*

>

> *Table Of Contents:*

> *1) Abstract*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

> 2) *High Level Description*

> 3) *Description*

> 4) *Issues*

>

> *Abstract:*

> *The current state of anonymous proxies do not provide adequate protection for the entity wishing to preserve their anonymity. Anonymous remailers and their ISP's have had court orders to have their logs subpoenaed in court (i). There is also a "trust" that the anonymous proxy is truly anonymous.*

>

> *Given that Country "C" restricts access to certain sites on "The Internet" located in country "A". Also given that country "C" wishes to gain knowledge of which of its citizens are trying to access restricted sites, country "C" could set up anonymous proxies in country "N" to monitor its own citizens. In addition if country "C" wished to monitor already popular anonymous sites for traffic, they could install a employee in the offices of the ISP that serves the popular anonymous site and have that employee surreptitiously monitor the traffic going to / leaving that site.*

>

> *Proposed is a truly anonymous system wherein no one entity has a complete picture of the transaction. This system can be installed on a corporate LAN (Local Area Network) to allow anonymous access of "sensitive" data (Example Anonymous employee suggestions, Human Resources "sensitive" procedures / documentation (medical forms, complaint procedures)) or it can be installed on "The Internet".*

>

> *I have seen the statement "Information Wants to Be Free". I would revise that statement to "Information Will Be Free". The information does not care one way or the other. But humans, simply by their curiosity and need to explore ideas will make the information free.*

>

> *High Level Description:*

>

> *The software will facilitate the transfer of files (HTTP, FTP, etc.) between two computers using anonymous proxies. Every machine will have "the least" amount of knowledge to make the transfer possible. One computer (the end point) will have access to the data and will know the intermediary proxy but will not know what computer the file is ultimately destined for. Another computer (the intermediary server or the intermediary proxy) will know what two computers the file is being transferred between but will not know the contents of the file. The last computer (The destination / anonymous machine) will know what the file is and who the proxy is, but not where the file is coming from.*

>

> *When the software is launched, it decides how much bandwidth is available for the connection. If it is a low bandwidth then the machine will perform the services of an Intermediate Proxy or End Point. If high bandwidth then the machine can perform as a Intermediary Server and / or as a Intermediary Proxy. This information is only known by the machine that runs the software, it is not told to any other computer. This way nobody know if a computer is a server or just a transfer agent.*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

- >
- > *Connections are made to other computers, requests are sent out for*
- > *additional connections until "enough" (depending on bandwidth) connections*
- > *are made. Scalability is not an issue, as connections / servers are*
- > *overloaded traffic will simply be dropped or passed onto other servers that*
- > *are not as loaded.*
- >
- > *Searches are passed to all connected machines. If the operator makes a*
- > *selection then that data is transferred to the machine. Searches are*
- > *performed via full URI Scheme (ii) request, by words or phrases contained in*
- > *the file or by filename (or parts thereof). Files retrieved (either from*
- > *"The Internet" or from another machine) are saved in cache on each machine.*
- > *When the file cache is full, the files that haven't been accessed for the*
- > *longest time are deleted. This allows for a "shadow" Internet, sites that*
- > *are censored or deleted are still available via the Anonymous Anonymity*
- > *network.*
- >
- > *I have looked at The Freenet Project (iii), and they deserve the credit in*
- > *this project for the idea of a "shadow" Internet, but the Anonymous*
- > *Anonymity Network is fundamentally different. On The Freenet Project web*
- > *pages are published only on the The Freenet Project (and does not allow for*
- > *searching), the Anonymous Anonymity Network allows for searching of not only*
- > *files on the Anonymous Anonymity Network but also the anonymous transfer of*
- > *files into the Anonymous Anonymity Network from "The Internet", thus*
- > *connecting "The Internet" with the Anonymous Anonymity Network. Also, the*
- > *files do not have to be passed from node to node to get to the final*
- > *destination (as in The Freenet Project), they are fetched and sent (via one*
- > *hop) to the final requestor.*
- >
- > *Detailed Description:*
- > *There are up to five devices involved in each transaction.*
- > *1) Destination Machine – The machine that wishes to remain anonymous*
- > *2) Intermediary Server.*
- > *3) Intermediary Proxy.*
- > *4) End point – HTTP anonymous Proxy or file server*
- > *5) The (HTTP, FTP, NNTP, etc) server that the Anonymous Machine wishes to*
- > *reach.*
- >
- > *With this anonymous network, as with the original design of "The Internet",*
- > *there is no central server. The software is initiated on the users machine.*
- > *The bandwidth is detected:*
- > *1) "Low Bandwidth" – Less than 512 kilobits / second the machine establishes*
- > *itself mainly as a Intermediary Proxy / End Point.*
- > *2) "High Bandwidth" – Greater than 512 kilobits per second and TCP port 80*
- > *inbound allowed, the machine establishes itself mainly as a Intermediary*
- > *Server.*
- >
- > *All connections / communications will use the HTTPEncode encoding.*
- > *HTTPEncode uses the same idea as UUEncode with a slight difference. Whereas*
- > *UUEncode takes binary data and encodes it into "plain text", HTTPEncode*
- > *takes that binary data one step further. The binary data is not only*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

- > encoded to ASCII characters, the HTTPEncode will create HTTP wrappers that
- > add HTTP tags to the beginning and end of the data, and throw in random HTML
- > tags inside the data. The encoding will also redistribute the character
- > count so that the end product has approximately the same character
- > distribution as "normal" HTML pages. This is to avoid transport layer -->
- > application layer firewalls that look for tunneling over port 80.
- >
- > When the software is installed the user is asked if they have any filtering
- > software that blocks what sites they are able to go to / monitors what sites
- > they go to. If they do then their machine is not allowed to be an end point
- > that fetches "fresh" web pages. Any firewall devices will have to be set up
- > to allow inbound port 80 (or port "X", user defined (since some ISP's block
- > port 80)) connections. If this cannot be done then this machine is
- > primarily a outbound / Intermediary Proxy connect machine.
- >
- > The software then attempts connection to a Intermediary Server. The IP
- > address of an initial intermediary server can be entered manually or
- > downloaded from a web site. The IP addresses are checked against WhoIs or
- > ARIN to see if they are geographically diverse. IPv6 will make this process
- > easier because it addresses according to the location of the machine.
- > Servers that are "farthest away" will be chosen over servers that are
- > "close". Intermediary servers should have port 80 open as an inbound
- > connection so that they appear to be another web server. If the machine has
- > determined that it has the capabilities to be a Intermediary Server then it
- > should allow connections to itself as a Intermediary Server. The machine
- > should also search for other Intermediary Servers so that requests are
- > distributed between many servers. Note: If inbound port 80 cannot be
- > established then that machine can still act as a server by making the port
- > 80 outbound connection when asked to by another machine (see next paragraph
- > handing off to another server). Obviously when the port 80 outbound
- > connection is made two way communications can then ensue.
- >
- > If a server has too many nodes, it should pass any new connections off to
- > another server and notify the machine that is trying to connect of this
- > handoff so that it can establish a direct connection to the other server.
- > If an Intermediary Proxy is using more than 50% of its bandwidth proxying
- > connections, then additional connection requests should be denied.
- >
- > All connections / communications should be encrypted with the exception of
- > the request. Each connection creates a unique encryption public/private key
- > pair for use in communication (this is so that the user cannot be identified
- > by using the same public key over and over again).
- >
- > Routing – Since data is routed node to node, the routing will not allow
- > least cost (efficient) routing. Just individual direct connections will be
- > in the routing table (IP Address / Search Request). Data would be "routed"
- > by each node keeping a table of incoming IP Address / search request hashes
- > paired with outgoing IP Address / search request hashes. The route back
- > being (of course) the path of pairs of IP Address's and search request
- > hashes that are related. This gives each node the "least knowledge" of the
- > source and destination. An Intermediary Server should not know whether a

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

- > *node that is connected is another Intermediary Server or a Anonymous Machine*
- > *or an End Point.*
- >
- > *Searches can be of the form:*
- > *1) URI Scheme request (http, https, ftp, gopher, file, etc)*
- > *2) File Name (or parts of file name)*
- > *3) Data in file (words, phrases, ANDed words or ORed words)*
- >
- > *The search request is added to the public key and hashed, this is to make*
- > *each search unique. This is referred to as the search hash. The search*
- > *with a unique public key and search hash is passed from the Anonymous*
- > *Machine to all Intermediary Servers. When a search request is seen, a*
- > *lookup of the search hash is made on the server in the "already known*
- > *searches" search table and if the hash of the search matches a already*
- > *received search, the search is dropped (this search has already been through*
- > *this machine). If the search is not dropped, the search hash is stored in a*
- > *lookup table with the IP Address that the search was received from. The*
- > *Intermediary Server passes the entire search to all Intermediary Servers*
- > *Anonymous Machines and End Point machines it knows except for the machine*
- > *the search request came from (the server doesn't know what "kind" of machine*
- > *it is connected to). If an end point machine can satisfy the request / has*
- > *matches for the request then that data relating to the request is encrypted*
- > *using the public key and passed back to the Intermediary Server with the*
- > *search response hash number. The response data from the end point machine*
- > *is the URI, the URI hash, the size of the file and the date of the file*
- > *(when the file was created). When positive responses are received then*
- > *those responses are returned via the routing (above) to the IP Address that*
- > *initiated the request.*
- >
- > *The Anonymous Machine then (by operator choice or by random) chooses a one*
- > *of the hashes to act on the request. If no node has the URI available in*
- > *cache then a node that can connect to the URI is chosen. If any node*
- > *returns a hash indicating that they have the file, then a second search*
- > *request is sent out via another connection (i.e do not send the hash request*
- > *out via the server that the original search response came in from) using the*
- > *hash as the search request. Nodes that have that hash return the hash and*
- > *hash dictionary (see below). If the file is large, this search hash / hash*
- > *dictionary will allow the Anonymous Machine to transfer parts of the file*
- > *from many sources. The Anonymous Machine will also be able to offer*
- > *portions of the file out when as they are received if other machines are*
- > *looking for that same file. Note: To further obfuscate the "real" requests,*
- > *Anonymous Machines should take random incoming requests / pick random words*
- > *and send them out as fake requests to Intermediary Servers. Results from*
- > *these fake requests are, of course, ignored.*
- >
- > *When the search table fills, requests are dropped in a FIFO manner for a*
- > *specific IP Address. If someone tries to flood the network with requests to*
- > *empty the tables, only the IP Address they are connected to will suffer, not*
- > *other IP Address's.*
- >
- > *Note: The positive responses to the search may be a form of "I can act as*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

- > *your proxy for that URL, but I don't have the URL" or "I have the entire*
- > *URL, and this is the last date that I accessed that page plus here is the*
- > *hash of the data on that page". The operator can choose whether they want a*
- > *copy (possibly stale) or if they want to chose a proxy that can get the*
- > *current page. All links on that page are different files that are searched*
- > */ requested for. Additionally (in this manner) the Anonymous Anonymity*
- > *network could host its own WWW network where those pages were only*
- > *accessible to someone connected to the Anonymous Anonymity network, or via a*
- > *machine proxying for the Anonymous Anonymity network.*
- >
- > *When the Anonymous Requester receives a request that is acceptable, a*
- > *connection request is sent along the path that is in the response data using*
- > *the IP Address / search hash connection pair generated in the previous*
- > *paragraph. This connection request has a new public key associated with the*
- > *request. The Intermediary Proxy Server sends out a request on all*
- > *connections for a proxy and randomly chooses one of those responses and*
- > *requests that Intermediary Proxy IP address. The IP address of this*
- > *Intermediary Proxy is sent to the path of both the End Point machine and the*
- > *Anonymous Requester.*
- >
- > *The End Point machine and the Anonymous Requester set up connections with*
- > *the Intermediary Proxy on TCP Port 80. Again, data is encrypted and then*
- > *HTTPEncoded. The Intermediary Proxy knows the source and destination, but*
- > *not what data is being exchanged. When the data exchange is complete the*
- > *connection is terminated.*
- >
- > *The whole idea behind this network is for each node to know the minimum*
- > *information for the system to work. The less a node knows the less*
- > *information that can be pieced together to get the whole picture. In*
- > *training for Security Clearances the quote goes something like "Unclassified*
- > *information can easily be combined to reveal classified information."*
- >
- > *File name:*
- > *The file name is retuned with a SHA-2 hash and a SHA-2 hash dictionary. The*
- > *SHA-2 hash is just a SHA-2 hash of the file. The SHA-2 Hash Dictionary is a*
- > *SHA-2 hash of "X" bytes of the file (where "X" is size of file / 1023 and*
- > *where "X" is greater than 32 Kbytes). The Anonymous Machine would request*
- > *chunk "y" of the file from the End Point. These requests would continue*
- > *until the Anonymous Machine has all the chunks it needs or until the*
- > *connection is broken. In this manner the Anonymous Machine could be*
- > *requesting parts of a particular file while also sending out parts of a*
- > *particular file to other users. If the file is less than 32 MBytes then the*
- > *hash table would be 32 Kbytes chunks of the file with the number of hashes*
- > *indicated in the hash table. This hash allows (in the case, for example, of*
- > *large FTP URI Scheme requests) requests to be made of parts of the file*
- > *being requested if it is a large file. The file hash and the hash segment*
- > *of the file would be requested, therefore several machines could be sending*
- > *parts of the file to the anonymous requester at the same time.*
- >
- >
- > *Issues:*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

- > 1) *The issue with a party owning the server and the anonymous proxier and /*
 - > *or the intermediary machine. This is essentially the Man In The Middle*
 - > *attack. The attacker "owns" the server in the middle which directs the*
 - > *anonymous machine to proxies and end point devices that it also controls,*
 - > *therefore the server knows the anonymous machine and what they are*
 - > *requesting. Same thing if the attacker wants to find out what files are on*
 - > *the end point machine, they act like the anonymous requester and the*
 - > *intermediary servers / proxies and make requests. While this issue is not*
 - > *completely solved by the above scheme, it is mitigated by the Anonymous*
 - > *Machine searching on the hash after the initial responses are received.*
 - > *Even if the server is acting as a man in the middle, the server would need*
 - > *to maintain a table of URIs / hashes returned. As the network grows this*
 - > *table would become huge.*
- >
- > 2) *HTTPS connections. The HTTPS transfer would require several data*
 - > *requests that would require the end point to serve up multiple pages to the*
 - > *anonymous requester. the Man In The Middle attack would be mitigated by the*
 - > *fact that the anonymous requester would be able to verify the SSL*
 - > *certificate of the site that they are visiting.*
- >
- > 3) *Abuse of the anonymous system by someone who is stalking, etc. The IP*
 - > *address of the proxier is the address that shows up on the logs and stalking*
 - > */ spamming / etc. would be blamed on whoever owns the IP Proxier address.*
- >
- > 4) *Not being able to make HTTP requests that divulge the end stations IP*
 - > *address. (Example <http://www.whatismyip.com/>)*
- >
- > 5) *Creation of HHTPEncode algorithm that ensures even letter distribution /*
 - > *HTML format of data.*
- >
- > 6) *Spammers – Assuming that the this system is programmed in open source,*
 - > *you will (at some time) have some smart spammer figure out a way to redirect*
 - > *HTTP requests to them and they will serve out their own spamvertized pages.*
 - > *Same with data files, nodes could put out data files that have nothing to do*
 - > *with the request made. A local file should be kept where the user can*
 - > *ignore all responses from a specific connection or ignore a specific hash.*
 - > *The file would be only locally significant because if it became global then*
 - > *nefarious people could "poison" sites that are serving out good information*
 - > *and say that these are "bad" sites.*
- >
- > 7) *Thomas J. Boschloo wrote "The problem remains, how to download this*
 - > *software without drawing attention onto oneself!"*
- >
- > i) *Newman, Ron and Copeland, Frank "The Church of Scientology vs. Grady*
 - > *Ward" (Specifically "Scientology targets ISPs and anonymous remailers").*
 - > *URL: <http://www.xs4all.nl/~kspaink/cos/rnewman/grady/home.html> Wednesday,*
 - > *July 24, 1996 (Accessed July 4, 2005)*
- > ii) *IANA Registry of URI Schemes "Uniform Resource Identifier (URI*
 - > *SCHEMES". URL: <http://www.iana.org/assignments/uri-schemes> 03 June 2005*
 - > *(Accessed July 4, 2005)*
- > iii) *The Freenet Project "The Freenet Project – index – beginner". URL:*

SecurityFocus Bugtraq: Re: Anonymous Anonymity – Request For Comments

> <http://freenetproject.org>, 04 July 2005

>

>

> *I would appreciate any and all comments on the above Anonymous Anonymity
> network. Specifically any solutions to the presented problems or if someone
> has already covered this ground I would appreciate pointers to their work.*

>

> *Thank you for your comments.*

>

> *Ken Hollis*

>

> -----

> *Do not meddle in the affairs of wizards for they are subtle and
> quick to anger.*

> *Ken Hollis – Gandalf The White – gand...@digital.net – O- TINLC*

> *WWW Page – <http://digital.net/~gandalf/>*

> *Trace E-Mail forgery – <http://digital.net/~gandalf/spamfaq.html>*

> *Trolls crossposts – <http://digital.net/~gandalf/trollfaq.html>*

> *Woodworking For Geeks – <http://digital.net/~gandalf/woodmain.htm>*

>

>

--

Craig

cskelton@gmail.com