How to increase your anonymity on the internet.

Internet Anonymity

By

Aaron Grothe

August 6, 2002

CERT Conference 2002

Overview

- Anonymity
  - Why?
  - Is it possible?
- Proxies/Services/Products
  - Proxies
  - Services
  - Products

Overview (2)

- Other Means
- Do it yourself
- Weird, Wild Stuff
- Future
- Contact Info
- Resources
- Conclusion

Why?

- Because you can!
- Classic Examples
  - Whistle blowers
  - People doing research on medical issues
  - Privacy Nuts (Tinfoil Hat wearing segment)
- Classic counter-examples
  - Crime
  - Terrorism

Is it Possible?

- Within reason. Yes.
  - If you are already on your government's radar they have a variety of easier ways to track you.
    - Keystroke loggers
    - Video surveillance
  - Seeking anonymity itself may raise flags with some groups
    - Downloading programs such as peek-a-booty or hacktivismo.

Proxies/Services/Products

- Proxies
  - Proxies attempt to make it harder to trace your location on the web.
    - They can do this by stripping information out of the data stream (advertisements, javascript, vbscript)
    - They may also route the request through a series of proxies to make it harder to trace the origin of the request
    - They may also encrypt the information to make inspection more difficult

Common Proxies

- Crowds
- Java Anonymous Proxy (JAP)
- Peek-a-booty
- Hacktivismo
- Zero Knowledge Systems (ZKS) Freedom
- Others

Crowds

- Developed by Lucent Labs
- Basic idea is to fade into a crowd of similar requests
  - User submits query to the crowd proxy. Proxy forwards it to another machine in the crowd which may either forward it again or process the request and route the results back through the chain to the originator
  - Encrypts transmission between proxies

Crowds (2)

- Last node sends request in the clear.
  - Introduces the concept of plausible deniability, "I did not make that request. Someone else using my proxy must have."
- Relatives
  - Jondo – clean room implementation of Crowds protocol based upon published specs, not compatible with Crowds
  - Jcrowds – java implementation of crowds

Crowds (3)

- Problems
  - Finding a crowd
  - Export restrictions
  - May be susceptible to traffic analysis
  - Lucent knows who is running crowd proxies has a t-shirt giveaway contest
  - Have to register to get code
  - Compromising a node is possible risk

Java Anonymous Proxy (JAP)

- No real trust is assumed with regards to the node structure (a node may be compromised)
- Sends request to intermediate servers called Mixes.
- Request batching to reduce traffic analysis

Java Anonymous Proxy (JAP) -2

- Problems
  - Uptime, uses a series of research/edu machines
  - Batching of requests can slow results
  - Relatively small number of proxies

Peek-a-booty

- Started by members of the Cult of the Dead Cow (cDc)
- May be used in several modes
  - Simple SSL front end, no software installation/configuration needed on client machine
  - Full Proxy installation

Peek-a-booty (2)

- Peek-a-Booty has received a LOT of press
  - Made Wired magazine's Vaporware 2001 list
  - The cDc group has quite a reputation
  - Baltimore technologies announced they already had a way to detect/defeat Peek-a-Booty before it even came out
- Works on a P2P system so system should scale as nodes are added.

Peek-a-booty (3)

- Problems
  - Still early in development cycle
  - Competing for mindshare/developers with Hacktivismo
  - Finding nodes can be difficult
  - With the browser version how to trust first node?

Hacktivismo

- Developed by another part of the cDc group
- Uses a protocol called six/four named after the Tinanmen massacre
- Has not released the source code as of August 4, 2002
- Apparently may be a split off the peek-a-booty code base.

Zero Knowledge Systems (ZKS) Freedom

- Built around the concept of nyms (pseudonyms)
  - A user would buy a set of nyms from ZKS then they would select a nym for that session
  - All traffic would be routed to ZKS servers which would then reroute and encrypt traffic between multiple nodes
  - ZKS supposedly did not have sufficient knowledge to be able to identify a nym

Zero Knowledge Systems (ZKS) Freedom (2)

- Problems
  - ZKS canceled service (was not profitable)
  - Required installing software by clients which was difficult for some users to do.
- The End?
  - ZKS has released the Freedom source code under an RSARef style license.

Misc. Programs

- CGI-Proxy
  - Allows a person to create their own proxy node, relatively easily
- Triangle Boy
  - P2P proxy system. Creation of Safeweb.

Services

- Services require very little skill configuration on the users part. It may be as simple as pointing the browser to another address
  - Anonymizer
    - User connects to http://www.anonymizer.com and then surfs the web.
    - Anonymizer strips potentially dangerous information from the data stream and returns "safe" code
    - Anonymizer has had issues trying to balance a rich web experience with security

Products

- Personal Proxies
  - Adsubtract, Webwasher, JunkBuster all work along similar lines. They attempt to remove ads/cookies from data requested from the Internet
- Ghostsurf
  - Ghostsurf is a program that attempts to find random proxies on the web and route traffic through them to make it harder to detect your identity

Other Means

- Libraries – most libraries have free internet access. Some request you have a valid photo ID or library card
- Cybercafe – most cybercafes have no ID requirement. Be wary of cameras however
- Prepaid ISPs – work on a principle similar to prepaid calling cards. Can be bought with cash at some computer stores.

Other Means (2)

- Free ISPs – The strongest link between you and your ISP is your billing information. Free ISPs remove this component. Also, some such as Netzero allow you to block caller-id.
- Pre-paid data-capable cellular phones – buy with cash and use it with a free ISP and you are relatively hard to trace. May change with E911 requirements.

Other Means (3)

- Wifi 802.11 – bring up your computer near any company and piggyback off their Net. Note: may be of dubious legality

Do It Yourself

- How I achieve relative anonymity on the internet
  - Use a Netzero account registered with a few "accidental" misspellings "Baron Grubba" instead of Aaron Grothe.
    - Block caller-id
  - Go to proxys4all.com and find a proxy
    - Enter the proxy into the Internet Explorer proxy window

Do It Yourself (2)

- Use combination of Netzero/Proxy to browse web.
- Use hushmail or hotmail for e-mail, again a few unfortunate misspellings in the registration process.
- Complete online activity
- Periodically wipe drive of system to remove residual information.

Do It Yourself (3)

- Improvements to current situation I'm considering
  - Using a proxy hunter to automatically find a new proxy and make switching proxies during a session easy
  - Use either Vmware or a Sun Box with a SUNPci card to make it easier to reformat the drive of the system to return it to a clean state

Weird Wild Stuff

¢ Cloning

¢ Swapping also known as Bob & Carol & Ted & Alice

¢ Freenik

Cloning

- www.tracenoizer.org has created the idea of creating near duplicates of a person and putting them on the web
- Aaron Grothe might become
  - Aron Groth, Aaron Growthy or even
  - Baron Grubba
- The goal is to reduce the amount of personal information available about you

Swapping: B&C&T&A

- Basic identity information is swapped within a group. May be permutations of identities like Cloning.
- Similar to the concept of people swapping Buyer loyalty cards (E.g. Baker's cards)
  - A family of four suddenly starts buying nothing both Ramen noodles and cheap beer, might through off a few statistics in the database

Freenik

- Offshot of Sputnik http://www.sputnik.com
- Sputnik is a product that allows people to easily setup Wireless 802.11 lans, and share some of their bandwidth.
  - You have to register to use Sputnik
- Freenik is a free offshoot that allows people to setup anonymous wireless access points for people to use.

Future

- Peek-a-booty and Hacktivismo should both revitalize this segment. Resulting in exciting new developments in the next 6-18 months
- As long as Governments allow some access to the internet, people will find a way around whatever obstacles are thrown in their way.

Contacting Me

- E-mail
  - grothe@earthlink.net
  - ajgrothe@hushmail.com

Resources

- Know the Rules, Use the Tools Privacy in the Digital Age: A resource for Internet users
  - Published by Senate Judiciary Committee
    - Apparently withdrawn after September 11th. Still can be found at various mirrors by doing a google search

Resources

- Do-it-yourself Internet Anonymity by Thomas C. Greene: *The Register*
  - *http://www.theregister.co.uk/content/archive/22831.html*
- Internet anonymity for Windows power users by Thomas C. Greene: *The Register*
  - *http://www.theregister.co.uk/content/archive/23208.html*

Conclusion

- Q & A

How to increase your anonymity on the internet.
Addendum

During the talk some questions were raised and I mentioned some additional sources. These slides are a random capture of most of that information.

August 6, 2002

GNUnet

- GNUnet http://www.gnu.org/software/GNUnet/ is a distributed p2p based content delivery system.
- Works by allowing for retrieval of information via encrypted channels
- A bit more work than a lot of the proxy systems, but also probably more secure

E-mail gateways

- There still exist some e-mail gateways to the web.
- They allow you to send an e-mail message in a format and they will return the information to you via e-mail.
- Combined with stenography, they might be an effective anti-censorship tool

Anonymizer 2.0

¢ Anonymizer has announced a major upgrade to their software.

¢ Should be faster/more complete and deliver a better web experience while improving security.

Other Services

- A small discussion of a few other services such as freenet, publius, and infranet came up.
- All are interesting projects, infranet's use of stenography is very cool
- They tend to require more skill on the end-users part
- Don't necessarily map to the users current web experience

Other Resources

- Wardriving.com has a lot of information about how to do anonymous access via 802.11
  - Discusses information such as
    - How to change MAC addresses dynamically
    - Which cards work best
  - Where good wireless zones are in some metro areas

Testing your Privacy

- Privacy.net has a section that will allow you to analyze how much information you are leaking via your web browser
  - http://www.privacy.net/analyze

Other Good Resources

- Protect Yourself Online by Matthew Danda
  - http://www.amazon.com/exec/obidos/ASIN/0735611882/qid=1028703949/sr=8-1/ref=sr_8_1/103-2191464-4695858
- Smart Computer Learning Series published a book on "Computer Privacy & Security" which has a lot of good information
  - Talks about some of the changes in privacy since September 11

Organizations

- Electronic Frontier Foundation (EFF) http://www.eff.org is an organization that deals with a lot of these issues
- Electronic Privacy Information Center (EPIC) http://www.epic.org is another good organization

Final Thoughts

- Just because you're paranoid doesn't mean that they aren't out to get you – Anonmous