Anonymity Services and the Law:
How to Safely Provide Anonymity Technology on the Internet

Len Sassaman
The Shmoo Group
rabbi@shmoo.com

Introduction to Anonymity Services

Network anonymity services

- Shield the identity of the user
- Conceal other identifying factors
- Dissociate users' actions with identity

- Do not conceal that those actions occur!
- Anonymity != privacy

Types of Anonymity Services

Covert anonymity

- User is not automatically flagged as a user of anonymity technology.
- User often has more credibility.
- Does not attract suspicion.
- Inconspicuous web proxies.
- Free web email accounts through proxies.
- Peek-a-Booty.

Overt anonymity

- User is known to be anonymous.
- Credibility is more often questioned.
- Known remailers
- Anonymizer.com addresses
- Other services are a mixture of covert and overt anonymity.

Who Operates Public Anonymity Services?

Commercial Organizations

- Often provide anonymity services for profit.
- Have an interest in protecting their customers identities.
- Usually do not offer strong anonymity – payment hurdles.
- Ex: Anonymizer.com
- Ex: Zero Knowledge Systems.

Universities and NGOs

- Offer services “For the good of the community”.
- Implement theoretical concepts.
- Possibly have a specific need.
- Are able to avoid the issue of anonymous payments.
- Ex: MIT’s nym.alias.net
- Ex: Voice of America

Individuals

- Much the same as NGOs
- Believe in the right to anonymity
- Desire personal use of the technology
- Wish to demonstrate technical ability
- Put theory into practice
- Ex: Mixmaster remailers
- Ex: Freenet

Governments/Militaries

- Operate anonymous “tip hotlines”
- Need anonymity for investigation or espionage
- Wish to undermine foreign government policies
- Ex: Safeweb and CIA

Differences: Commercial vs. Others

- Commercial anonymity services tend to be weaker
- Commercial anonymity services tend to be more popular
- Address passive concerns:
  - Protect financial data
  - Hide personal information
  - Thwart data mining
- Anonymous communication is secondary

Why Commercial Anonymity is Different

Hard to sell

- Payment collection (no anonymous cash!)
- Cost of operating service
- Need for a large anonymity set
- Uncertain demand
- Legal restrictions
- Abuse complications

Hard to buy

- Payment rendering (no anonymous cash!)
- Uncertainty of anonymity strength
- Availability of service
- Local network restrictions
- Ease of use

Differences between Strengths

Weak anonymity

- Protection from the casual attacker
- Spam avoidance
- Anonymous online forums
- “Trust the operator or the law”

Strong anonymity

- Protection from ISP snooping
- Protection from government monitoring
- Protection in the case of server compromise (hacker-proofing)
- “Trust the mathematics”

Examples

- Free web mail accounts
- SSL anonymous proxies
- Anonymous ISPs
- Anonymous mail relays
- Mix-net remailer systems

Need for free anonymity

- Strong anonymity has important uses
- Commercial solutions are lacking
- Publicly accessible non-profit anonymity services are the main source of strong anonymity
- Anonymous digital cash would change this

A Brief History of Remailers

Mix-nets

- Paper by David Chaum written in 1981
- Described a method of anonymous communication
- Strong anonymity – no universally trusted authority
- Return addresses
- Not implimented by Chaum

anon.penet.fi

- Pseudonym server
- Based on software created by Karl Kleinpaste
- Maintained by Julf Helsingius in Finland
- Operational in the early 1990's
- Fairly weak anonymity, but easy to use
- More than 500,000 registered users
- Fell victim to a "legal attack" by the Church of Scientology
- http://www.penet.fi/press-english.html

Cypherpunk remailers

- Borrowed ideas from Chaum
- Joint work by Eric Hughes, Hal Finney
- Written in 1992
- Improved by Raif Levien, Matt Ghio, and others (statistics generation, latency)
- Used PGP for encryption and nesting
- Traffic analysis still possible
- “Type I Remailers”
- Type I nymservers exist

Mixmaster remailers

- Implimentation of Chaum's Mix-net idea
- Work begun in 1993 by Lance Cottrell
- Addresses multiple shortcomings in the Type I system
- Software rewritten in 1998 by Ulf Möller
- Currently the most widely used remailer software
- Known as "Type II Remailers"

Zero Knowledge Freedom

- Email services on top of the ZKS Freedom network
- Strong anonymity, ease of use, and return addresses (persistant pseudonyms)
- Commercial enterprise that was too costly
- Possible future as open source?

The Mechanics of Strong Anonymity

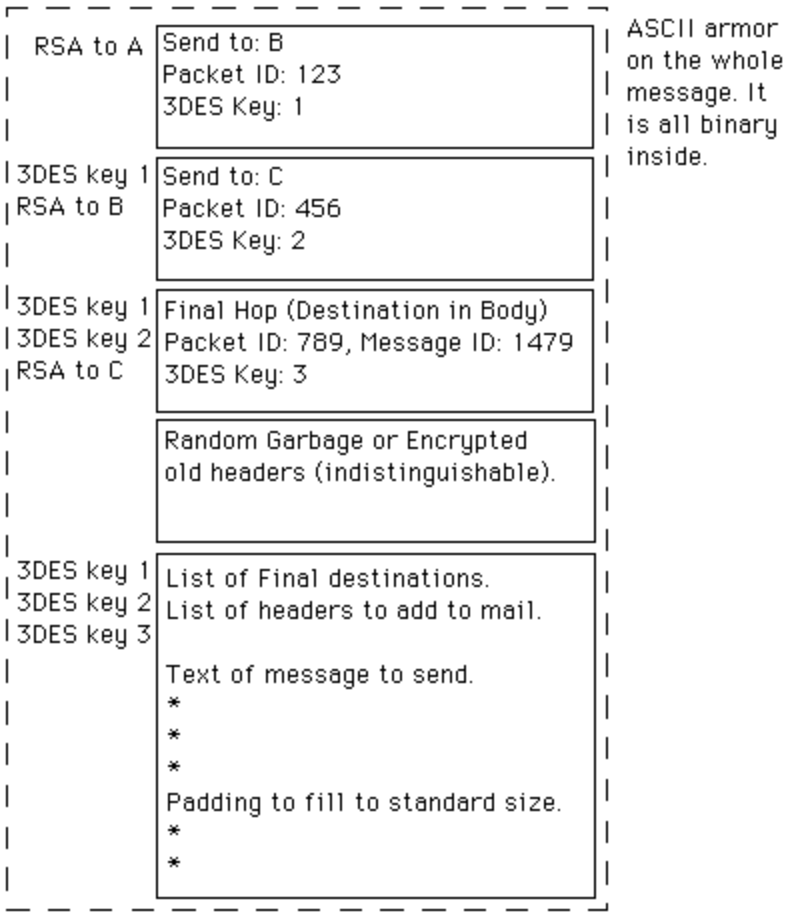
David Chaum’s mix-nets

- Multi-layered encyption chains
- Indistinguishable message packets
- Random reordering at each hops
- Return address reply blocks

Mixmaster

- A mix-net implimentation
- Clients available for Windows, Macintosh, Unix
- Servers available for Unix and Windows
- Low hardware resource requirements
- Reliable network connection
- Mail server capabilities

A Mixmaster Packet



Journey of a mixed message

- Chain selection
- Encryption
- Padding/splitting
- Transmission
- What the operator can see
- What an outside observer would know
- Importance of a large anonymity set
- Cover traffic

Flaws in Mixmaster

- Tagging attacks
- Flooding attacks
- Key compromise
- Need for forward secrecy
- Reliability failings
- Ease of use
- Lack of return address capability

Preventing and Handling Abuse

Types of Abuse

Spam

- Remailers are ill-suited for email spam
- High latency, easy detection
- Open-relays are much better
- Usenet spam is still a problem

Piracy

- Most remailers block binary transfers
- Anonymity is decreased by sending large, multi-packet messages
- Email is a poor medium for file transfer
- Throw-away shell/ftp accounts, irc, and p2p systems are more popular for warez

Targeted harassment

- Directed abusive messages at individuals
- Floods from one or more remailers
- Usenet flames

Prevention

Stopping abuse

- Individual remailer block-lists
- The Remailer Abuse Blacklist
  - http://www.paracrypt.com/remailerabuse/
- Local filtering
- Do not need to know the ID of abuser
- Avoid being a target of abuse
- Spam and flood detection tools for remops
- Middleman remailers

Why a remop can’t reveal abusers’ True Names

- Only the last hop is usually known
- No logs
- No chain information
- Decryption keys aren’t useful in last hop
- All chained hops are needed
- START-TLS forward secrecy

Why remops don’t keep logs

- Disk space / resource drain
- Local user privacy concerns
- Not useful for abuse investigations

Complications in Dealing with Abuse Complaints

- Responding to individuals
- Responding to organizations
- Responding to ISPs
- Responding to legal authorities
- The problem of mail-to-news gateways

Inside a Mixmaster Remailer

Walk-through of a live system

- Remailer program location
- Mail handling
- Remailer packet handling
- Logging
- Abuse processing

Interacting with Law Enforcement

When LEO's want answers

- Explain that you are operating a remailer
  - (The more overt the anonymity, the easier this is will be)
- Offer to help as much as you can
- Offer abuse counter-measures
- Remember: you do not need to talk to LEOs! Know your Miranda rights.
- If you are treated as a suspect, it is likely due to technical ignorance on the LEO's part
- Last resorts: turn to EFF, ACLU, EPIC

First impressions

- Corresponding website is the first thing an investigator will see
- Have information on remailers and their benefits available
- Be friendly with local law enforcement
- Don’t be a criminal!

Personal experiences

- How I became a remop
- What I expected
- My law enforcement inquiries
  - FBI
  - US Secret Service
- What I would do differently now

Legal status of remailers

- First Amendment issues
- Electronic Frontiers Georgia case
- UK’s RIP Bill
- Current US Administration
- Where remailers might be banned

Post “September 11th”

- Media reaction
- Number of remailers operating
- Political opinion of anonymity
- Remailers: Tools **against** terror
- What about public libraries?

What Can be Improved?

What programmers can do

- Next generation remailers
  - Security improvements
  - Mixminion (Type III)
- User interface enhancements!
- IETF standardization
- Mail client support
- Java web applets
  - Mixlet

What law makers can do

- Ensure legality of anonymity services
- Legal protections for remailer operators

What the revolutionaries can do

- Steps to take if remailers are banned in your country
- Ways of operating remailers anonymously
- Ways of maintaining anonymity without remailers
- What happens if the US bans remailers?

What the public can do

- We need more remops
- We need more stable remailers
- We need more remailer users
- User testimonials
- Use public opinion to our advantage
- Social benefit of remailers must be known

Comments

Len Sassaman
rabbi@shmoo.com