8. Anonymity, Digital Mixes, and Remailers

8.1. copyright

8.2. SUMMARY: Anonymity, Digital Mixes, and Remailers

8.2.1. Main Points

- Remailers are essential for anonymous and pseudonymous systems, because they defeat traffic analysis
- Cypherpunks remailers have been one of the major successes, appearing at about the time of the Kleinpaste/Julf remailer(s), but now expanding to many sites
- To see a list of sites: finger remailer- list@kiwi.cs.berkeley.edu (or http://www.cs.berkeley.edu/~raph/remailer-list.html)
  - Anonymity in general is a core idea

8.2.2. Connections to Other Sections

- Remailers make the other technologies possible

8.2.3. Where to Find Additional Information

- Very little has been written (formally, in books and journals) about remailers
  - David Chaum's papers are a start

8.2.4. Miscellaneous Comments

- This remains one of the most jumbled and confusing sections, in my opinion. It needs a lot more reworking and reorganizing.
  - Partly this is because of several factors
- a huge number of people have worked on remailers, contributing ideas, problems, code, and whatnot
- there are many versions, many sites, and the sites change from day to day
  - lots of ideas for new features
  - in a state of flux
- This is an area where actual experimentation with remailers is both very easy and very instructive...the "theory" of remailers is straighforward (compared to, say, digital cash) and the learning experience is better than theory anyway.
- There are a truly vast number of features, ideas, proposals, discussion points, and other such stuff. No FAQ could begin to cover the ground covered in the literally thousands of posts on remailers.

8.3. Anonymity and Digital Pseudonyms

8.3.1. Why is anonymity so important?

- It allows escape from past, an often-essential element of straighening out (an important function of the Western frontier, the French Foreign Legion, etc., and something we are losing as the dossiers travel with us wherever we go)
  - It allows new and diverse types of opinions, as noted below
- More basically, anonymity is important because identity is not as important as has been made out in our dossier society. To wit, if Alice wishes to remain anonymous or pseudonymous to Bob, Bob cannot "demand" that she provide here "real" name. It's a matter of negotiation between them. (Identity is not free...it is a credential like any other

and cannot be demanded, only negotiated.)
- Voting, reading habits, personal behavior...all are examples where privacy (= anonymity, effectively) are critical. The next section gives a long list of reasons for anonymity.

8.3.2. What's the difference between anonymity and pseudonymity? + Not much, at one level...we often use the term "digital pseudonym" in a strong sense, in which the actual identity cannot be deduced easily

- this is "anonymity" in a certain sense

- But at another level, a pseudonym carries reputations, credentials, etc., and is *not* "anonymous"
- people use pseudonyms sometimes for whimsical reasons (e.g., "From spaceman.spiff@calvin.hobbes.org Sep 6, 94 06:10:30"), sometimes to keep different mailing lists separate (different personnas for different groups), etc.

8.3.3. Downsides of anonymity

- libel and other similar dangers to reputations

- hit-and-runs actions (mostly on the Net)
- on the other hand, such rantings can be ignored (KILL file) - positive reputations

- accountability based on physical threats and tracking is lost

- Practical issue. On the Cypherpunks list, I often take "anonymous" messages less seriously.

- They're often more bizarre and inflammatory than ordinary posts, perhaps for good reason, and they're certainly harder to take seriously and respond to. This is to be expected. (I should note that some pseudonyms, such as Black Unicorn and Pr0duct Cypher, have established reputable digital personnas and are well worth replying to.)
  - repudiation of debts and obligations
  - infantile flames and run-amok postings

    - racism, sexism, etc.
    - like "Rumormonger" at Apple?
- but these are reasons for pseudonym to be used, where the reputation of a pseudonym is important

- Crimes...murders, bribery, etc.

- These are dealt with in more detail in the section on crypto anarchy, as this is a major concern (anonymous markets for such services)

8.3.4. "How will privacy and anonymity be attacked?"

- the downsides just listed are often cited as a reason we can't have "anonymity"
- like so many other "computer hacker" items, as a tool for the "Four Horsemen": drug-dealers, money-launderers, terrorists, and pedophiles.
- as a haven for illegal practices, e.g., espionage, weapons trading, illegal markets, etc.

- tax evasion ("We can't tax it if we can't see it.")

- same system that makes the IRS a "silent partner" in business transactions and that gives the IRS access to-- and requires--business records

- "discrimination"
    - that it enables discrimination (this *used* to be OK)
    - exclusionary communities, old boy networks

8.3.5. "How will random accusations and wild rumors be controlled in anonymous forums?"

- First off, random accusations and hearsay statements are the norm in modern life; gossip, tabloids, rumors, etc. We don't worry obsessively about what to do to stop all such hearsay and even false comments. (A disturbing trend has been the tendency to sue, or threaten suits. And increasingly the attitude is that one can express *opinions*, but not make statements "unless they can be proved." That's not what free speech is all about!)
- Second, reputations matter. We base our trust in statements on a variety of things, including: past history, what others say about veracity, external facts in our possession, and motives.

8.3.6. "What are the legal views on anonymity?"

- Reports that Supreme Court struck down a Southern law requiring pamphlet distributors to identify themselves. 9I don't have a cite on this.)

- However, Greg Broiles provided this quote, from *Talley v. State of California*, 362 U.S. 60, 64-65, 80 S.Ct. 536, 538-539 (1960) : "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." Greg adds: "It later says "Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes." [Greg Broiles, 1994-04-12]

- And certainly many writers, journalists, and others use pseudonyms, and have faced no legal action.

- Provided they don't use it to evade taxes, evade legal judgments, commit fraud, etc.
- I have heard (no cites) that "going masked for the purpose of going masked" is illegal in many jurisdictions. Hard to believe, as many other disguises are just as effective and are presumably not outlawed (wigs, mustaches, makeup, etc.). I assume the law has to do with people wearning ski masks and such in "inappropriate" places. Bad law, if real.

8.3.7. Some Other Uses for Anonymous Systems:

- Groupware and Anonymous Brainstorming and Voting

- systems based on Lotus Notes and designed to encourage wild ideas, comments from the shy or overly polite, etc.
- these systems could initially start in meeting and then be extended to remote sites, and eventually to nationwide and international forums
  - the NSA may have a heart attack over these trends...

- "Democracy Wall" for encrypted messages

- possibly using time-delayed keys (where even the public key, for reading the plaintext, is not distributed for some time)
- under the cover of an electronic newspaper, with all of the constitutional protections that entails: letters to the editor can be anonymous, ads need not be screened for validity,

advertising claims are not the responsibility of the paper, etc.

- Anonymous reviews and hypertext (for new types of journals) + the advantages - honesty - increased "temperature" of discourse
  - disadvantages
    - increased flames
    - intentional misinformation
- Store-and-forward nodes

- used to facillitate the anonymous voting and anonymous inquiry (or reading) systems
  - Chaum's "mix"

- telephone forwarding systems, using digital money to pay for the service - and TRMs?
- Fiber optics
- hard to trace as millions of miles are laid, including virtually untraceable lines inside private buildings

- suppose government suspects encrypted packets are going in to the buildings of Apple...absent any direct knowledge of crimes being aided and abetted, can the government demand a mapping of messages from input to output?
- That is, will the government demand full disclosure of all routings?
  - high bandwidth means many degrees of freedom for such systems to be deployed

- Within systems, i.e., user logs on to a secure system and is given access to his own processor

- in a 288-processor system like the NCR/ATT 3600 (or even larger)
- under his cryptonym he can access certain files, generate others, and deposit message untraceably in other mail locations that other agents or users can later retrieve and forward...
- in a sense, he can use this access to launch his own agent processes (anonymity is essential for many agentbased systems, as is digital money)

- Economic incentives for others to carry mail to other sites...
  - further diffusion and hiding of the true functions
- Binary systems (two or more pieces needed to complete the message)

- possibly using viruses and worms to handle the complexities of distributing these messages
- agents may handle the transfers, with isolation between the agents, so routing cannot be traced (think of scene in "Double-Crossed" where bales of marijuana are passed from plane to boat to chopper to trucks to cars)
  - this protects against conspiracies
  - Satellites

- physical security, in that the satellites would have to be shot down to halt the broadcasting

- scenario: WARC (or whomever) grants broadcast rights in 1996 to some country or consortium, which then accepts any and all paying customers

- cold cash
- the BCCI of satellite operators
  - VSATs, L-Band, Satellites, Low-Earth Orbit
    - Very Small Aperture Terminals
    - L-Band...what frequency?

- LEO, as with Motorola's Iridium, offers several advantages

- lower-power receivers and smaller antennas
- low cost to launch, due to small size and lower need for 10-year reliability
- avoidance of the "orbital slot" licensing morass (though I presume some licensing is still involved) - can combine with impulse or nonsinusoidal transmissions

8.3.8. "True Names"

8.3.9. Many ways to get pseudonyms:

- Telnet to "port 25" or use SLIP connections to alter domain name; not very secure
  - Remailers

8.3.10. "How is Pseudonymity Compromised?"

- slip-ups in style, headers, sig blocks, etc.
- inadvertent revealing, via the remailers
- traffic analysis of remailers (not very likely, at least not for non-NSA adversaries)
- correlations, violations of the "indistinguishability principle"

8.3.11. Miscellaneous Issues

- Even digital pseudonyms can get confusing...someone recently mistook "Tommy the Tourist" for being such an actual digital pseudonym (when of course that is just attached to all posts going througha particular remailer).

8.4. Reasons for Anonymity and Digital Pseudonyms (and Untraceable EMail)

8.4.1. (Thre are so many reasons, and this is asked so often, that I've collected these various reasons here. More can be added, of course.)

8.4.2. Privacy in general

8.4.3. Physical Threats

- "corporate terrrorism" is not a myth: drug dealers and other "marginal" businessmen face this every day
  - extortion, threats, kidnappings
  - and many businesses of the future may well be less "gentlemanly" than the conventional view has it

- witness the bad blood between Intel and AMD, and then imagine it getting ten times worse
- and national rivalries, even in ostensibly legal businesses (think of arms dealers), may cause more use of violence

- Mafia and other organized crime groups may try to extort payments or concessions from market participants, causing them to seek the relative protection of anonymous systems - with reputations
- Note that calls for the threatened to turn to the police for protection has several problems

- the activities may be illegal or marginally illegal (this is the reason the Mafia can often get involved and why it may even sometimes have a positive effect, acting as the cop for illegal activities)

- the police are often too busy to get involved, what with so much physical crime clogging the courts
- extortion and kidnappings can be done using these very techniques of cryptoanarchy, thus causing a kind of arms race

- battered and abused women and families may need the equivalent of a "witness protection program"
- because of the ease of tracing credit card purchases, with the right bribes and/or court orders (or even hacking), battered wives may seek credit cards under pseudonyms

- and some card companies may oblige, as a kind of politically correct social gesture

- or groups like NOW and Women Against Rape may even offer their own cards

- perhaps backed up by some kind of escrow fund
- could be debit cards

- people who participate in cyberspace businesses may fear retaliation or extortion in the real world
  - threats by their governments (for all of the usual reasons, plus kickbacks, threats to close them down, etcl)
  - ripoffs by those who covet their success...

8.4.4. Voting

- We take it for granted in Western societies that voting should be "anonymous"--untraceable, unlinkable
- we don't ask people "What have you got to hide?" or tell them "If you're doing something anonymously, it must be illegal."
- Same lesson ought to apply to a lot of things for which the government is increasingly demanding proof of identity for
  - Anonymous Voting in Clubs, Organizations, Churches, etc.

- a major avenue for spreading CA methods: "electronic blackballing," weighted voting (as with number of shares) + e.g., a corporation issues "voting tokens," which can be used to vote anonymously

- or even sold to others (like selling shares, except selling only the voting right for a specific election is cheaper, and many people don't much care about elections)

- a way to protect against deep pockets lawsuits in, say, race discrimination cases

- wherein a director is sued for some action the company takes-anonymity will give him some legal protection, some "plausible deniability"

- is possible to set up systems (cf. Salomaa) in which some "supervotes" have blackball power, but the use of these vetos is indistinguishable from a standard majority rules vote

- i.e., nobody, except the blackballer(s), will know whether the blackball was used!

- will the government seek to limit this kind of protocol?

- claiming discrimination potential or abuse of voting rights?

- will Justice Department (or SEC) seek to overturn anonymous voting?

- as part of the potential move to a "full disclosure" society?
- related to antidiscrimination laws, accountability, etc.

- Anonymous Voting in Reputation-Based Systems (Journals, Markets)
- customers can vote on products, on quality of service, on the various deals they've been involved in

- not clear how the voting rights would get distributed
- the idea is to avoid lawsuits, sanctions by vendors, etc. (as with the Bose suit) + Journals
- a canonical example, and one which I must include, as it combines anonymous refereeing (already standard, in primitive forms), hypertext (links to reviews), and basic freedom of speech issues
- this will likely be an early area of use
- this whole area of consumer reviews may be a way to get CA bandwidth up and running (lots of PK-encrypted traffic sloshing around the various nets)

8.4.5. Maintenance of free speech

- protection of speech

- avoiding retaliation for controversial speech

- this speech may be controversial, insulting, horrific, politically incorrect, racist, sexist, speciesist, and other horrible...but remailers and anonymity make it all impossible to stop
  - whistleblowing
  - political speech
- KKK, Aryan Resistance League, Black National Front, whatever
- cf. the "debate" between "Locke" and "Demosthenes" in Orson Scott Card's novel, "Ender's Game."
- (Many of these reasons are also why 'data havens' will eventually be set up...indeed, they already exist...homolka trial, etc.)

8.4.6. Adopt different personnas, pseudonyms

8.4.7. Choice of reading material, viewing habits, etc.

- to prevent dossiers on this being formed, anonymous purchases are needed (cash works for small items, not for video rentals, etc.)
  - video rentals
- (Note: There are "laws" making such releases illegal, but...)
  - cable t.v. viewing habits
  - mail-order purchases
- yes, they need your address to ship to, but there may be cutouts that delink (e.g., FedEx might feature such a service, someday

8.4.8. Anonymity in Requesting Information, Services, Goods

- a la the controversy over Caller ID and 900 numbers: people don't want their telephone numbers (and hence identities) fed into huge consumer-preference data banks

- of the things they buy, the videos they rent, the books they read. etc. (various laws protect some of these areas, like library books, video rentals)
- subscription lists are already a booming resale market...this will get faster and more finely "tuned" with electronic subscriptions: hence the desire to subscribe anonymously

- some examples of "sensitive" services that anonymity may be desired in (especially related to computers, modems, BBSes)
- reading unusual or sensitive groups: alt.sex.bondage, etc.

- or posting to these groups!
- recent controversy over NAMBLA may make such protections more desirable to some (and parallel calls for restrictions!)
- posting to such groups, especially given that records are perpetual and that government agencies read and file postings (an utterly trivial thing to do)
- requesting help on personal issues (equivalent to the "Name Witheld" seen so often)

- discussing controversial political issues (and who knows what will be controversial 20 years later when the poster is seeking a political office, for example?)

- given that some groups have already (1991) posted the past postings of people they are trying to smear!

- Note: the difference between posting to a BBS group or chat line and writing a letter to an editor is significant

- partly technological: it is vastly easier to compile records of postings than it is to cut clippings of letters to editors (though this will change rapidly as scanners make this easy)
- partly sociological: people who write letters know the letters will be with the back issues in perpetuity, that bound issues will preserve their words for many decades to come (and could conceivably come back to haunt them), but people who post to BBSes probably think their words are temporary + and there are some other factors
- no editing
- no time delays (and no chance to call an editor and retract a letter written in haste or anger)

- and letters can, and often are, written with the "Name Witheld" signature-this is currently next to impossible to do on networks

- though some "forwarding" services have informally sprung up

- Businesses may wish to protect themselves from lawsuits over comments by their employees
- the usual "The opinions expressed here are not those of my employer" may not be enough to protect an employer from lawsuits

- imagine racist or sexist comments leading to lawsuits (or at least being brought up as evidence of the type of "attitude" fostered by the company, e.g., "I've worked for Intel for 12 years and can tell you that blacks make very poor engineers.")

- employees may make comments that damage the reputations of their companies

- Note: this differs from the current situation, where free speech takes priority over company concerns, because the postings to a BBS are carried widely, may be searched electronically (e.g., AMD lawyers search the UseNet postings of 1988-91 for any postings by Intel employees besmirching the quality or whatever of AMD chips),
- and so employees of corporations may protect themselves, and their employers, by adopting pseudonyms

- Businesses may seek information without wanting to alert their competitors

- this is currently done with agents, "executive search firms," and lawyers
- but how will it evolve to handle electronic searches? + there are some analogies with filings of "Freedom of Information Act" requests, and of patents, etc.

- these "fishing expeditions" will increase with time, as it becomes profitable for companies to search though mountains of electronically-filed materials

- environmental impact studies, health and safety disclosures, etc. - could be something that some companies specialize in + Anonymous Consultation Services, Anonymous Stringers or Reporters

- imagine an information broker, perhaps on an AMIX-like service, with a network of stringers
- think of the arms deal newsletter writer in Hallahan's The Trade, with his network of stringers feeding him tips and inside information

- instead of meeting in secretive locations, a very expensive proposition (in time and travel), a secure network can be used
- with reputations, digital pseudonyms, etc.
  - they may not wish their actual identities known
- threats from employers, former employers, government agencies

- harassment via the various criminal practices that will become more common (e.g., the ease with which assailants and even assassins can be contracted for)

- part of the overall move toward anonymity - fears of lawsuits, licensing requirements, etc.
  - Candidates for Such Anonymous Consultation Services
    - An arms deals newsletter
- an excellent reputation for accuracy and timely information

- sort of like an electronic form of Jane's

- with scandals and government concern
- but nobody knows where it comes from

- a site that distributes it to subscribers gets it with another larger batch of forwarded material
  - NSA, FBI, Fincen, etc. try to track it down + "Technology Insider" reports on all kinds of new technologies

- patterned after Hoffler's Microelectronics News, the Valley's leading tip sheet for two decades
- the editor pays for tips, with payments made in two parts: immediate, and time-dependent, so that the accuracy of a tip, and its ultimate importance (in the judgment of the editor) can be proportionately rewarded

- PK systems, with contributors able to encrypt and then publicly post (using their own means of diffusion)

- with their messages containing further material, such as authentications, where to send the payments, etc. + Lundberg's Oil Industry Survey (or similar)

- i.e., a fairly conventional newsletter with publicly known authors
- in this case, the author is known, but the identities of contributors is well-protected + A Conspiracy Newsletter
- reporting on all of the latest theories of misbehavior (as in the "Conspiracies" section of this outline)

- a wrinkle: a vast hypertext web, with contributors able to add links and nodes
- naturally, their real name-if they don't care about real-world repercussions-or one of their digital pseudonyms (may as well use cryptonyms) is attached + various algorithms for reputations

- sum total of everything ever written, somehow measured by other comments made, by "voting," etc.
- a kind of moving average, allowing for the fact that learning will occur, just as a researcher probably gets better with time, and that as reputation-based systems become better understood, people come to appreciate the importance of writing carefully

- and one of the most controversial of all: Yardley's Intelligence Daily

- though it may come out more than daily!

- an ex-agent set this up in the mid-90s, soliciting contributions via an anonymous packet-switching sysem

- refined over the next couple of years
- combination of methods
- government has been trying hard to identify the editor, "Yardley"
- he offers a payback based on value of the information, and even has a "Requests" section, and a Classifed Ad section
- a hypertext web, similar to the Conspiracy Newsletter above

- Will Government Try to Discredit the Newsletter With False Information?

- of course, the standard ploy in reputation-based systems

- but Yardley has developed several kinds of filters for this

- digital pseudonyms which gradually build up reputations
- cross-checking of his own sort
    - he even uses language filters to analyze the text + and so what?
- the world is filled with disinformation, rumors, lies, half-truths, and somehow things go on... + Other AMIX-like Anonymous Services

- Drug Prices and Tips

- tips on the quality of various drugs (e.g., "Several reliable sources have told us that the latest Maui Wowie is very intense, numbers below...")

- synthesis of drugs (possibly a separate subscription)

- designer drugs
- home labs
- avoiding detection

- The Hackers Daily

- tips on hacking and cracking
- anonymous systems themselves (more tips)
- Product evaluations (anonymity needed to allow honest comments with more protection against lawsuits)

- Newspapers Are Becoming Cocerned with the Trend Toward Paying for News Tips - by the independent consultation services - but what can they do?
- lawsuits are tried, to prevent anonymous tips when payments are involved

- their lawyers cite the tax evasion and national security aspects
    - Private Data Bases

- any organization offering access to data bases must be concerned that somebody-a disgruntled customer, a whistleblower, the government, whoever-will call for an opening of the files - under various "Data Privacy" laws - or just in general (tort law, lawsuits, "discovery")
- thus, steps will be taken to isolate the actual data from actual users, perhaps via cutouts
- e.g., a data service sells access, but subcontracts out the searches to other services via paths that are untraceable
- this probably can't be outlawed in general-though any specific transaction might later be declared illegal, etc., at which time the link is cut and a new one is established-as this would outlaw all subcontracting arrangements!

- i.e., if Joe's Data Service charges $1000 for a search on widgets and then uses another possibly transitory (meaning a cutout) data service, the most a lawsuit can do is to force Joe to stop using this untraceble service
- levels of indirection (and firewalls that stop the propagation of investigations)

- Medical Polls (a la AIDS surveys, sexual practices surveys, etc.)
- recall the method in which a participant tosses a coin to answer a question...the analyst can still recover the important ensemble information, but the "phase" is lost

- i.e., an individual answering "Yes" to the question "Have you ever had xyz sex?" may have really answered "No" but had his answer flipped by a coin toss

- researchers may even adopt sophisticated methods in which explicit diaries are kept, but which are then transmitted under an anonymous mailing system to the researchers - obvious dangers of authentication, validity, etc.
    - Medical testing: many reasons for people to seek anonymity

    - AIDS testing is the preeminent example

- but also testing for conditions that might affect insurablity or employment (e.g., people may go to medical havens in Mexico or wherever for tests that might lead to uninsurability should insurance companies learn of the "precondition")

- except in AIDS and STDs, it is probably both illegal and against medical ethics to offer anonymous consultations - perhaps people will travel to other countries

8.4.9. Anonymity in Belonging to Certain Clubs, Churches, or Organizations

- people fear retaliation or embarassment should their membership be discovered, now or later

- e.g., a church member who belongs to controversial groups or clubs
- mainly, or wholly, those in which physical contact or other personal contact is not needed (a limited set)
    - similar to the cell-based systems described elsewhere
    - Candidates for anonymous clubs or organizations
        - Earth First!, Act Up, Animal Liberation Front, etc.
        - NAMBLA and similar controversial groups
- all of these kinds of groups have very vocal, very visible members, visible even to the point of seeking out television coverage
- but there are probably many more who would join these groups if there identities could be shielded from public group, for the sake of their careers, their families, etc.

- ironically, the corporate crackdown on outside activities considered hostile to the corporation (or exposing them to secondary lawsuits, claims, etc.) may cause greater use of anonymous systems
    - cell-based membership in groups

- the growth of anonymous membership in groups (using pseudonyms) has a benefit in increasing membership by people otherwise afraid to join, for example, a radical environmental group

8.4.10. Anonymity in Giving Advice or Pointers to Information

- suppose someone says who is selling some illegal or contraband product...is this also illegal?

    - hypertext systems will make this inevitable

8.4.11. Reviews, Criticisms, Feedback

- "I am teaching sections for a class this term, and tomorrow I am going to: 1) tell my students how to use a remailer, and 2) solicit anonymous feedback on my teaching. "I figure it will make them less apprehensive about making honest suggestions and comments (assuming any of them bother, of course)." [Patrick J. LoPresti patl@lcs.mit.edu, alt.privacy.anon-server, 1994-09-08]

8.4.12. Protection against lawsuits, "deep pockets" laws

- by not allowing the wealth of an entity to be associated with actions

- this also works by hiding assets, but the IRS frowns on that, so unlinking the posting or mailing name with actual entity is usually easier
    - "deep pockets"
- it will be in the interest of some to hide their identities so as to head off these kinds of lawsuits (filed for whatever reasons, rightly or wrongly)
- postings and comments may expose the authors to lawsuits for libel, misrepresentation, unfair competition, and so on (so much for free speech in these beknighted states)

- employers may also be exposed to the same suits, regardless of where their employees posted from

- on the tenuous grounds that an employee was acting on his employer's behalf, e.g., in defending an Intel product on Usenet
- this, BTW, is another reason for people to seek ways to hide some of their assets-to prevent confiscation in deep pockets lawsuits (or family illnesses, in which various agencies try to seize assets of anybody they can)
- and the same computers that allow these transactions will also allow more rapid determination of who has the deepest pockets!

- by insulating the entity from repercussions of "sexist" or "racist" comments that might provoke lawsuits, etc.

- (Don't laugh--many companies are getting worried that what their employees write on Usenet may trigger lawsuits against the companies.)

- many transactions may be deemed illegal in some jursidictions
- even in some that the service or goods provider has no control over

- example: gun makers being held liable for firearms deaths in the District of Columbia (though this was recently cancelled)
- the maze of laws may cause some to seek anonymity to protect themselves against this maze
  - Scenario: Anonymous organ donor banks

- e.g., a way to "market" rare blood types, or whatever, without exposing one's self to forced donation or other sanctions

- "forced donation" involves the lawsuits filed by the potential recipient
- at the time of offer, at least...what happens when the deal is consummated is another domain
- and a way to avoid the growing number of government stings

8.4.13. Journalism and Writing

- writers have had a long tradtion of adopting pseudonyms, for a variety of reasons

- because they couldn't get published under their True Names, because they didn't *want* their true names published, for the fun of it, etc.
  - George Elliot, Lewis Carroll, Saki, Mark Twain, etc.
  - reporters
  - radio disc jockeys
- a Cypherpunk who works for a technology company uses the "on air personna" of "Arthur Dent" ("Hitchhiker's Guide") for his part-time radio broadcasting job...a common situation, he tells me
  - whistleblowers
    - this was an early use
  - politically sensitive persons

- I subsequently got myself an account on anon.penet.fi as the "Lt.

- Starbuck" entity, and all later FAQ updates were from that account.
- For reasons that seemed important at the time, I took it upon myself to - become the moderator/editor of the FAQ." - <an54835@anon.penet.fi, 4-3-94, alt.fan.karla-homolka>

- Example: Remailers were used to skirt the publishing ban on the Karla Homolka case
  - various pseudonymous authors issued regular updates
  - much consternation in Canada!
- avoidance of prosecution or damage claims for writing, editing, distributing, or selling "damaging" materials is yet another reason for anonymous systems to emerge: those involved in the process will seek to immunize themselves from the various tort claims that are clogging the courts

- producers, distributors, directors, writers, and even actors of x-rated or otherwise "unacceptable" material may have to have the protection of anonymous systems
- imagine fiber optics and the proliferation of videos and talk shows...bluenoses and prosecutors will use "forum shopping" to block access, to prosecute the producers, etc.

8.4.14. Academic, Scientific, or Professional

- protect other reputations (professional, authorial, personal, etc.)
- wider range of actions and behaviors (authors can take chances)
  - floating ideas out under pseudonyms
- later linking of these pseudonyms to one's own identity, if needed (a case of credential transfer)
  - floating unusual points of view
- Peter Wayner writes: "I would think that many people who hang out on technical newsgroups would be very familiar with the anonymous review procedures practiced by academic journals. There is some value when a reviewer can speak their mind about a paper without worry of revenge. Of course everyone assures me that the system is never really anonymous because there are alwys only three or four people qualified to review each paper. :-) ...Perhaps we should go out of our way to make anonymous, technical comments about papers and ideas in the newsgroups to fascilitate the development of an anonymous commenting culture in cypberspace." [Peter Wayner, 1993-02-09]

8.4.15. Medical Testing and Treatment

- anonymous medical tests, a la AIDS testing

8.4.16. Abuse, Recovery

- personal problem discussions
  - incest, rape, emotional, Dear Abby, etc.

8.4.17. Bypassing of export laws

- Anonymous remailers have been useful for bypassing the ITARs...this is how PGP 2.6 spread rapidly, and (we hope!) untraceably from MIT and U.S. sites to offshore locations.

8.4.18. Sex groups, discussions of controversial topics

- the various alt.sex groups
- People may feel embarrassed, may fear repercussions from their employers, may not wish their family and friends to see their posts, or may simply be aware that Usenet is archived in many, many places, and is even available on CD- ROM and will be trivially searchable in the coming decades

- the 100% traceability of public postings to UseNet and other bulletin boards is very stifling to free expression and becomes one of the main justifications for the use of anonymous (or pseudononymous) boards and nets

- there may be calls for laws against such compilation, as with the British data laws, but basically there is little that can be done when postings go to tens of thousands of machines and are archived in perpetuity by many of these nodes and by thousands of readers
- readers who may incorporate the material into their own postings, etc. (hence the absurdity of the British law)

8.4.19. Avoiding political espionage

- TLAs in many countries monitor nearly all international communications (and a lot of domestic communications, too)

- companies and individuals may wish to avoid reprisals, sanctions, etc.
- PGP is reported to be in use by several dissident groups, and several Cypherpunks are involved in assisting them.
- "...one legitimate application is to allow international political groups or companies to exchange authenticated messages without being subjected to the risk of espionage/compromise by a three letter US agency, foreign intelligence agency, or third party." [Sean M. Dougherty, alt.privacy.anon-server, 1994-09-07]

8.4.20. Controversial political discussion, or membership in political groups, mailing lists, etc.

- Recall House UnAmerican Activities Committee

- and it's modern variant: "Are you now, or have you ever been, a Cypherpunk?"

8.4.21. Preventing Stalking and Harassment

- avoid physical tracing (harassment, "wannafucks," stalkers, etc.)
- women and others are often sent "wannafuck?" messages from the males that outnumber them 20-to-1 in many newsgroups-- pseudonyms help.
- given the ease with which net I.D.s can be converted to physical location information, many women may be worried.

- males can be concerned as well, given the death threats issued by, for example, S. Boxx/Detweiler.

- as it happens, S. Boxx threatened me, and I make my home phone number and location readily known...but then I'm armed and ready.

8.4.22. pressure relief valve: knowing one can flee or head for the frontier and not be burdened with a past

- perhaps high rate of recidivism is correlated with this inability to escape...once a con, marked for life (certainly denied access to high-paying jobs)

8.4.23. preclude lawsuits, subpoenas, entanglement in the legal machinery

8.4.24. Business Reasons

- Corporations can order supplies, information, without tipping their hand

- the Disney purchase of land, via anonymous cutouts (to avoid driving the price way up)
  - secret ingredients (apocryphally, Coca Cola)
  - avoiding the "deep pockets" syndrome mentioned above
- to beat zoning and licensing requirements (e.g., a certain type of business may not be "permitted" in a home office, so the homeowner will have to use cutouts to hide from

enforcers)
    - protection from (and to) employers

- employees of corporations may have to do more than just claim their view are not those of their employer

- e.g., a racist post could expose IBM to sanctions, charges

- thus, many employees may have to further insulate their identities

- blanc@microsoft.com is now blanc@pylon.com...coincidence?

- moonlighting employees (the original concern over Black Net and AMIX)

- employers may have all kinds of concerns, hence the need for employees to hide their identities
- note that this interects with the licensing and zoning aspects
    - publishers, service-prividers
    - Needed for Certain Kinds of Reputation-Based Systems

- a respected scientist may wish to float a speculative idea - and be able to later prove it was in fact his idea

8.4.25. Protection against retaliation

- whistleblowing

- organizing boycotts

- (in an era of laws regulating free speech, and "SLAPP" lawsuits)

- the visa folks (Cantwell and Siegel) threatening those who comment with suits
    - the law firm that posted to 5,000 groups...also raises the issue again of why the Net should be subsidized
    - participating in public forums
    - as one person threatened with a lawsuit over his Usenet comments put it:

- "And now they are threatening me. Merely because I openly expressed my views on their extremely irresponsible behaviour. Anyways, I have already cancelled the article from my site and I publicly appologize for posting it in the first place. I am scared :) I take all my words back. Will use the anonymous service next time :)"

8.4.26. Preventing Tracking, Surveillance, Dossier Society

- avoiding dossiers in general
- too many dossiers being kept; anonymity allows people to at least hold back the tide a bit
- headhunting, job searching, where revealing one's identity is not always a good idea
  - some headhunters are working for one's current employer!
  - dossiers

8.4.27. Some Examples from the Cypherpunks List

- S, Boxx, aka Sue D. Nym, Pablo Escobar, The Executioner, and an12070
  - but Lawrence Detweiler by any other name
  - he let slip his pseudonym-true name links in several ways
    - stylistic cues
- mention of things only the "other" was likely to have heard + sysops acknowledged certain linkings
- *not* Julf, though Julf presumably knew the identity of "an12070"
  - Pr0duct Cypher
- Jason Burrell points out: "Take Pr0duct Cypher, for example. Many believe that what (s)he's doing(*) is a Good Thing, and I've seen him/her using the Cypherpunk remailers to conceal his/her identity...* If you don't know, (s)he's the person who wrote PGPTOOLS, and a hack for PGP 2.3a to decrypt messages written with 2.6. I assume (s)he's doing it anonymously due to ITAR regulations." [J.B., 1994-09-05]
  - Black Unicorn
- Is the pseudonym of a Washington, D.C. lawyer (I think), who has business ties to conservative bankers and businessmen in Europe, especially Liechtenstein and Switzerland. His involvement with the Cypherpunks group caused him to adopt this pseudonym.
- Ironically, he got into a battle with S. Boxx/Detweiler and threated legal action. This cause a rather instructive debate to occur.

8.5. Untraceable E-Mail

8.5.1. The Basic Idea of Remailers

- Messages are encrypted, envelopes within envelopes, thus making tracing based on external appearance impossible. If the remailer nodes keep the mapping between inputs and outputs secret, the "trail" is lost.

8.5.2. Why is untraceable mail so important?

- Bear in mind that "untraceable mail" is the default situation for ordinary mail, where one seals an envelope, applies a stamp, and drops it anonymously in a letterbox. No records are kept, no return address is required (or confirmed), etc.

- regional postmark shows general area, but not source mailbox

- Many of us believe that the current system of anonymous mail would not be "allowed" if introduced today for the first time

- Postal Service would demand personalized stamps, verifiable return addresses, etc. (not foolproof, or secure, but...)
  - Reasons:
- to prevent dossiers of who is contacting whom from being compiled
  - to make contacts a personal matter
- many actual uses: maintaining pseudonyms, anonymous contracts, protecting business dealings, etc.

8.5.3. How do Cypherpunks remailers work?

8.5.4. How, in simple terms, can I send anonymous mail?

8.5.5. Chaum's Digital Mixes

- How do digital mixes work?

8.5.6. "Are today's remailers secure against traffic analysis?" - Mostly not. Many key digital mix features are missing, and the gaps can be exploited.

- Depends on features used:
  - Reordering (e.g., 10 messages in, 10 messages out)

- Quantization to fixed sizes (else different sizes give clues)
  - Encryption at all stages (up to the customer, of course)
- But probably not, given that current remailers often lack necessary features to deter traffic analysis. Padding is iffy, batching is often not done at all (people cherish speed, and often downcheck remailers that are "too slow")
- Best to view today's remailers as experiments, as prototypes.

8.6. Remailers and Digital Mixes (A Large Section!)

8.6.1. What are remailers?

8.6.2. Cypherpunks remailers compared to Julf's

- Apparently long delays are mounting at the penet remailer. Complaints about week-long delays, answered by:

- "Well, nobody is stopping you from using the excellent series of cypherpunk remailers, starting with one at remail@vox.hacktic.nl. These remailers beat the hell out of anon.penet.fi. Either same day or at worst next day service, PGP encryption allowed, chaining, and gateways to USENET." [Mark Terka, The normal delay for anon.penet.fi?, alt.privacy.anon-server, 1994-08-19]
  - "How large is the load on Julf's remailer?"

- "I spoke to Julf recently and what he really needs is $750/month and one off $5000 to upgrade his feed/machine. I em looking at the possibility of sponsorship (but don't let that stop other people trying)...Julf has buuilt up a loyal, trusting following of over 100,000 people and 6000 messages/day. Upgrading him seems a good idea...Yes, there are other remailers. Let's use them if we can and lessen the load on Julf." [Steve Harris, alt.privacy.anon-server, 1994-08-22]
- (Now if the deman on Julf's remailer is this high, seems like a great chance to deploy some sort of fee-based system, to pay for further expansion. No doubt many of the users would drop off, but such is the nature of business.)

8.6.3. "How do remailers work?"

- (The MFAQ also has some answers.)
- Simply, they work by taking an incoming text block and looking for instructions on where to send the remaining text block, and what to do with it (decryption, delays, postage, etc.)

- Some remailers can process the Unix mail program(s) outputs directly, operating on the mail headers
  - names of programs...
- I think the "::" format Eric Hughes came up with in his first few days of looking at this turned out to be a real win (perhaps comparable to John McCarthy's decision to use parenthesized s-expressions in Lisp?).

- it allows arbitary chaining, and all mail messages that have text in standard ASCII--which is all mailers, I believe--can then use the Cypherpunks remailers

8.6.4. "What are some uses of remailers?"

- Thi is mostly answered in other sections, outlining the uses of anonymity and digital pseudonyms: remailers are of course the enabling technology for anonymity.
  - using remailers to foil traffic analysis
- An interesting comment from someone not part of our group, in a discussion of proposal to disconnect U.K. computers from Usenet (because of British laws about libel, about pornography, and such): "PGP hides the target. The remailers discard the source info. THe more paranoid remailers introduce a random delay on resending to foil traffic analysis. You'd be suprised what can be done :-)...If you use a chain then the first remailer knows who you are but the destination is encrypted. The last remailer knows the destination but cannot know the source. Intermediate ones know neither." [Malcolm McMahon, JANET (UK) to ban USENET?, comp.org.eff.talk, 1994-08-30]
- So, word is spreading. Note the emphasis on Cyphepunks- type remailers, as opposed to Julf-style anonymous services.
  - options for distributing anonymous messages
    - via remailers

        - the conventional approach
        - upsides: recipient need not do anything special
- downsides: that's it--recipient may not welcome the message
    - to a newsgroup
        - a kind of message pool
        - upsides: worldwide dist
    - to an ftp site, or Web-reachable site
    - a mailing list

8.6.5. "Why are remailers needed?"

- Hal Finney summarized the reasons nicely in an answer back in early 1993.

- "There are several different advantages provided by anonymous remailers. One of the simplest and least controversial would be to defeat traffic analysis on ordinary email...Two people who wish to communicate privately can use PGP or some other encryption system to hide the content of their messages. But the fact that they are communicating with each other is still visible to many people: sysops at their sites and possibly at intervening sites, as well as various net snoopers. It would be natural for them to desire an additional amount of privacy which would disguise who they were communicating with as well as what they were saying. "Anonymous remailers make this possible. By forwarding mail between themselves through remailers, while still identifying themselves in the (encrypted) message contents, they have even more communications privacy than with simple encryption. "(The Cypherpunk vision includes a world in which literally hundreds or thousands of such remailers operate. Mail could be bounced through dozens of these services, mixing in with tens of thousands of other messages, re-encrypted at each step of the way. This should make traffic analysis virtually impossible. By sending periodic dummy messages which just get swallowed up at some step, people can even disguise *when* they are communicating.)" [Hal Finney, 1993-02-23] "The more controversial vision associated with anonymous remailers is expressed in such science fiction stories as "True Names", by Vernor Vinge, or "Ender's Game", by Orson Scott Card. These depict worlds in which computer networks are in widespread use, but in which many people choose to participate through pseudonyms. In this way they can make unpopular arguments or participate in frowned-upon transactions without their activities being linked to their true identities. It also allows people to develop reputations based on the quality of their ideas, rather than their job, wealth, age, or status." [Hal Finney, 1993-02-23]
- "Other advantages of this approach include its extension to electronic on-line transactions. Already today many records are kept of our financial dealings - each time we purchase an item over the phone using a credit card, this is recorded by the credit card company. In time, even more of this kind of information may be collected and possibly sold. One Cypherpunk vision includes the ability to engage in transactions anonymously, using "digital cash", which would not be traceable to the participants. Particularly for buying "soft" products, like music, video, and software (which all may be deliverable over the net eventually), it should be possible to engage in such transactions anonymously. So

this is another area where anonymous mail is important." [Hal Finney, 1993-02-23]

8.6.6. "How do I actually use a remailer?"

- (Note: Remailer instructions are posted *frequently*. There is no way I can keep up to date with them here. Consult the various mailing lists and finger sites, or use the Web docs, to find the most current instructions, keys, uptimes, etc._
  - Raph Levien's finger site is very impressive:
- Raph Levien has an impressive utility which pings the remailers and reports uptime:

- finger remailer-list@kiwi.cs.berkeley.edu
- or use the Web at http://www.cs.berkeley.edu/~raph/remailer-list.html
- Raph Levien also has a remailer chaining script at ftp://kiwi.cs.berkeley.edu/pub/raph/premail- 0.20.tar.gz
  - Keys for remailers
    - remailer-list@chaos.bsu.edu (Matthew Ghio maintains)

- "Why do remailers only operate on headers and not the body of a message? Why aren't signatures stripped off by remailers?"

- "The reason to build mailers that faithfully pass on the entire body of the message, without any kind of alteration, is that it permits you to send ANY body through that mailer and rely on its faithful arrival at the destination." [John Gilmore, 93-01-01]
  - The "::" special form is an exception
- Signature blocks at the end of message bodies specifically should *not* be stripped, even though this can cause security breaches if they are accidentally left in when not intended. Attempting to strip sigs, which come in many flavors, would be a nightmare and could strip other stuff, too. Besides, some people may want a sig attached, even to an encrypted message.
- As usual, anyone is of course free to have a remailer which munges message bodies as it sees fit, but I expect such remailers will lose customers.
- Another possibility is another special form, such as "::End", that could be used to delimit the block to be remailed. But it'll be hard getting such a "frill" accepted.
  - "How do remailers handle subject lines?"
- In various ways. Some ignore it, some preserve it, some even can accept instructions to create a new subject line (perhaps in the last remailer).
- There are reasons not to have a subject line propagated through a chain of remailers: it tags the message and hence makes traffic analysis trivial. But there are also reasons to have a subject line--makes it easier on the recipient--and so these schemes to add a subject line exist.

- "Can nicknames or aliases be used with the Cypherpunks remailers?"

- Certainly digitally signed IDs are used (Pr0duct Cypher, for example), but not nicknames preserved in fields in the remailing and mail-to-Usenet gateways.

- This could perhaps be added to the remailers, as an extra field. (I've heard the mail fields are more tolerant of added stuff than the Netnews fields are, making mail-to- News gateways lose the extra fields.)
  - Some remailer sites support them
- "If you want an alias assigned at vox.hacktic.nl, one - only- needs to send some empty mail to ping@vox.hacktic.nl and the adress the mail was send from will be inculded in the data-base...Since vox.hacktic.nl is on a UUCP node the reply can take some time, usually something like 8 to 12 hours."[Alex de Joode, usura@vox.hacktic.nl, 1994-08-29]

- "What do remailers do with the various portions of messages? Do they send stuff included after an encrypted block? Should they? What about headers?"
  - There are clearly lots of approaches that may be taken:

- Send everything as is, leaving it up to the sender to ensure that nothing incriminating is left - Make certain choices
- I favor sending everything, unless specifically told not to, as this makes fewer assumptions about the intended form of the message and thus allows more flexibility in designing new functions.

- For example, this is what Matthew Ghio had to to say about his remailer:

- "Everything after the encrypted message gets passed along in the clear. If you don't want this, you can remove it using the cutmarks feature with my remailer. (Also, remail@extropia.wimsey.com doesn't append the text after the encrypted message.) The reason for this is that it allows anonymous replies. I can create a pgp message for a remailer which will be delivered to myself. I send you the PGP message, you append some text to it, and send it to the remailer. The remailer decrypts it and remails it to me, and I get your message. [M.G., alt.privacy.anon-server, 1994-07-03]

8.6.7. Remailer Sites

- There is no central administrator of sites, of course, so a variety of tools are the best ways to develop one's own list of sites. (Many of us, I suspect, simply settle on a dozen or so of our favorites. This will change as hundreds of remailers appear; of course, various scripting programs will be used to generate the trajectories, handled the nested encryption, etc.)
- The newsgroups alt.privacy.anon-server, alt.security.pgp, etc. often report on the latest sites, tools, etc.

- Software for Remailers
  - Software to run a remailer site can be found at:
    - soda.csua.berkeley.edu in /pub/cypherpunks/remailer/
    - chaos.bsu.edu in /pub/cypherpunks/remailer/
- Instructions for Using Remailers and Keyservers

    - on how to use keyservers

- "If you have access to the World Wide Web, see this URL: http://draco.centerline.com:8080/~franl/pgp/pgp- keyservers.html" [Fran Litterio, alt.security.pgp, 199409-02]

- Identifying Remailer Sites
    - finger remailer-list@chaos.bsu.edu
        - returns a list of active remailers

- for more complete information, keys, and instructions, finger remailer.help.all@chaos.bsu.edu - gopher://chaos.bsu.edu/

- Raph Levien has an impressive utility which pings the remailers and reports uptime: - finger remailer-list@kiwi.cs.berkeley.edu

- or use the Web at http://www.cs.berkeley.edu/~raph/remailer-list.html
- Raph Levien also has a remailer chaining script at ftp://kiwi.cs.berkeley.edu/pub/raph/premail-0.20.tar.gz

- Remailer pinging

- "I have written and installed a remailer pinging script which collects detailed information about remailer features and reliability. To use it, just finger remailer-list@kiwi.cs.berkeley.edu There is also a Web version of the same information, at: http://www.cs.berkeley.edu/~raph/remailer-list.html" [Raph Levien, 1994-08-29]

- Sites which are down??
    - tamsun.tamu.edu and tamaix.tamu.edu

8.6.8. "How do I set up a remailer at my site?"

- This is not something for the casual user, but is certainly possible.
- "Would someone be able to help me install the remailer scripts from the archives? I have no Unix experience and have *no* idea where to begin. I don't even know if root access is needed for these. Any help would be appreciated." [Robert Luscombe, 93-04-28]
- Sameer Parekh, Matthew Ghio, Raph Levien have all written instructions...

8.6.9. "How are most Cypherpunks remailers written, and with what tools?"

- as scripts which manipulate the mail files, replacing headers, etc.
  - Perl, C, TCL
- "The cypherpunks remailers have been written in Perl, which facilitates experimenting and testing of new interfaces. The idea might be to migrate them to C eventually for efficiency, but during this experimental phase we may want to try out new ideas, and it's easier to modify a Perl script than a C program." [Hal Finney, 93-01-09]
- "I do appreciate the cypherpunks stuff, but perl is still not a very widely used standard tool, and not everyone of us want to learn the ins and outs of yet another language.....So I do applaud the C version..." [Johan Helsingius, "Julf," 93-01-09]

8.6.10. Dealing with Remailer Abuse

- The Hot Potato

- a remailer who is being used very heavily, or suspects abuse, may choose to distribute his load to other remailers. Generally, he can instead of remailing to the next site, add sites of his own choosing. Thus, he can both reduce the spotlight on him and also increase cover traffic by scattering some percentage of his traffic to other sites (it never reduces his traffic, just lessens the focus on him).
  - Flooding attacks
    - denial of service attacks
- like blowing whistles at sports events, to confuse the action
- DC-Nets, disruption (disruptionf of DC-Nets by flooding is a very similar problem to disruption of remailers by mail bombs)
  - "How can remailers deal with abuse?"
- Several remailer operators have shut down their remailers, either because they got tired of dealing with the problems, or because others ordered them to.
  - Source level blocking
- Paid messages: at least this makes the abusers *pay* and stops certain kinds of spamming/bombing attacks.
- Disrupters are dealt with in anonymous ways in Chaum's DC- Net schemes; there may be a way to use this here.
  - Karl Kleinpaste was a pioneer (circa 1991-2) of remailers. He has become disenchanted:
- "There are 3 sites out there which have my software: anon.penet.fi, tygra, and uiuc.edu. I have philosophical disagreement with the "universal reach" policy of anon.penet.fi (whose code is now a long-detached strain from the original software I gave Julf -- indeed, by now it may be a complete rewrite, I simply don't know); ...Very bluntly, having tried to run anon servers twice, and having had both go down due to actual legal difficulties, I don't trust people with them any more." [Karl_Kleinpaste@cs.cmu.edu, alt.privacy.anon-server, 1994-08-29]
  - see discussions in alt.privacy.anon-server for more on his legal problems with remailers, and why he shut his down

8.6.11. Generations of Remailers

- First Generation Remailer Characteristics--Now (since 1992)
  - Perl scripts, simple processing of headers, crypto
- Second Generation Remailer Characteristics--Maybe 1994

- digital postage of some form (perhaps simple coupons or "stamps")
  - more flexible handling of exceptions
- mail objects can tell remailer what settings to use (delays, latency, etc.(
  - Third Generation Remailer Characteristics--1995-7?
    - protocol negotiation
    - Chaum-like "mix" characteristics
- tamper-resistant modules (remailer software runs in a sealed environment, not visible to operator)
  - Fourth Generation Remailer Characteristics--1996-9?
    - Who knows?
    - Agent-based (Telescript?)
    - DC-Net-based

8.6.12. Remailer identity escrow

- could have some uses...
  - what incentives would anyone have?

- recipients could source-block any remailer that did not have some means of coping with serious abuse...a perfect free market solution
  - could also be mandated

8.6.13. Remailer Features

- There are dozens of proposed variations, tricks, and methods which may or may not add to overall remailer security (entropy, confusion). These are often discussed on the list, one at a time. Some of them are:
- Using one's self as a remailer node. Route traffic back through one's own system. - even if all other systems are compromised...

- Random delays, over and above what is needed to meet reordering requirements
  - MIRVing, sending a packet out in multiple pieces
  - Encryption is of course a primary feature.
  - Digital postage.
- Not so much a feature as an incentive/inducement to get more remailers and support them better.
  - "What are features of a remailer network?"

- A vast number of features have been considered; some are derivative of other, more basic features (e.g., "random delays" is not a basic feature, but is one proposed way of achieving "reordering," which is what is really needed. And "reordering" is just the way to achieve "decorrelation" of incoming and outgoing messages).

- The "Ideal Mix" is worth considering, just as the "ideal op amp" is studied by engineers, regardless of whether one can ever be built.

- a black box that decorrelates incoming and outgoing packets to some level of diffusion
- tamper-proof, in that outside world cannot see the internal process of decorrelation (Chaum envisioned tamper-resistant or tamper-responding circuits doing the decorrelation)
    - Features of Real-World Mixes:

- Decorrelation of incoming and outgoing messages. This is the most basic feature of any mix or remailer: obscuring the relationship between any message entering the mix and any message leaving the mix. How this is achieve is what most of the features here are all about.

- "Diffusion" is achieved by batching or delaying (danger: low-volume traffic defeats simple, fixed delays)
- For example, in some time period, 20 messages enter a node. Then 20 or so (could be less, could be more...there is no reason not to add messages, or throw away some) messages leave.

- Encryption should be supported, else the decorrelation is easily defeated by simple inspection of packets.

- public key encryption, clearly, is preferred (else the keys are available outside)
- forward encryption, using D-H approaches, is a useful idea to explore, with keys discarded after transmission...thus making subpoenas problematic (this has been used with secure phones, for example).

- Quanitzed packet sizes. Obviously the size of a packet (e.g., 3137 bytes) is a strong cue as to message identity. Quantizing to a fixed size destroys this cue.
- But since some messages may be small, and some large, a practical compromise is perhaps to quantize to one of several standards:

- small messages, e.g., 5K
- medium messages, e.g., 20K
- large messages...handled somehow (perhaps split up, etc.) - More analysis is needed.
    - Reputation and Service
        - How long in business?
        - Logging policy? Are messages logged?
        - the expectation of operating as stated

- The Basic Goals of Remailer Use

    - decorrelation of ingoing and outgoing messages
        - indistinguishability
- "remailed messages have no hair" (apologies to the black hole fans out there)

- no distinguishing charateristics that can be used to make correlations - no "memory" of previous appearance

- this means message size padding to quantized sizes, typically

- how many distinct sizes depends on a lot fo things, like traffic, the sizes of other messages, etc.

- Encryption, of course
    - PGP
    - otherwise, messages are trivially distinguishable
- Quantization or Padding: Messages

- padded to standard sizes, or dithered in size to obscure oringinal size. For example, 2K for typical short messages, 5K for typical Usenet articles, and 20K for long articles. (Messages much longer are hard to hide in a sea of much shorter messages, but other possibilities exist: delaying the long messages until N other long messages have been accumulated, splitting the messages into smaller chunks, etc.)

- "What are the quanta for remailers? That is, what are the preferred packet sizes for remailed messages?"

- In the short term, now, the remailed packet sizes are pretty much what they started out to be, e.g, 3-6KB or so. Some remailers can pad to quantized levels, e.g., to 5K or 10K or more. The levels have not been settled on.
- In the long term, I suspect much smaller packets will be selected. Perhaps at the granularity of ATM packets. "ATM Remailers" are likely to be coming. (This changes the nature of traffic analyis a bit, as the *number* of remailed packets increases.
- A dissenting argument: ATM networks don't give sender the control over packets...
- Whatever, I think packets will get smaller, not larger. Interesting issues.
- "Based on Hal's numbers, I would suggest a reasonable quantization for message sizes be a short set of geometrically increasing values, namely, 1K, 4K, 16K, 64K. In retrospect, this seems like the obvious quantization, and not arithmetic progressions." [Eric Hughes, 1994-08-29]
- (Eudora chokes at 32K, and so splits messages at about 25K, to leave room for comments without further splitting. Such practical considerations may be important to consider.)

- Return Mail
    - A complicated issue. May have no simple solution.
    - Approaches:

- Post encrypted message to a pool. Sender (who provided the key to use) is able to retrieve anonymously by the nature of pools and/or public posting.

- Return envelopes, using some kind of procedure to ensure anonymity. Since software is by nature never secure (can always be taken apart), the issues are complicated. The security may be gotten by arranging with the remailers in the return path to do certain things to certain messages.

- sender sends instructions to remailers on how to treat messages of certain types
- the recipient who is replying cannot deduce the identity, because he has no access to the instructions the remailers have.
- Think of this as Alice sending to Bob sending to Charles...sending to Zeke. Zeke sends a reply back to Yancy, who has instructions to send this back to Xavier, and so on back up the chain. Only if Bob, Charles, ..., Yancy collude, can the mapping in the reverse direction be deduced.
- Are these schemes complicated? Yes. But so are lot of other protocols, such as getting fonts from a screen to a laser printer
    - Reordering of Messages is Crucial
        - latency or fanout in remailers
            - much more important than "delay"
- do some calculations!

- the canard about "latency" or delay keeps coming up

- a "delay" of X is neither necessary nor sufficient to achieve reordering (think about it)
- essential for removing time correlation information, for removing a "distinguishing mark" ("ideal remailed messages have no hair")
    - The importance of pay as you go, digital postage
        - standard market issues
            - markets are how scarece resources are allocated
        - reduces spamming, overloading, bombing
        - congestion pricing
        - incentives for improvement
        - feedback mechanisms
            - in the same way the restaurants see impacts quickly
        - applies to other crypto uses besides remailers
    - Miscellaneous
- by having one's own nodes, further ensures security (true, the conspiring of all other nodes can cause traceability, but such a conspiracy is costly and would be revealed)

- the "public posting" idea is very attractive: at no point does the last node know who the next node will be...all he knows is a public key for that node
- so how does the next node in line get the message, short of reading all messages?

- first, security is not much compromised by sorting the public postings by some kind of order set by the header (e.g., "Fred" is shorthand for some long P-K, and hence the recipient knows to look in the Fs...obviously he reads more than just the Fs)

- outgoing messages can be "broadcast" (sent to many nodes, either by a literal broadcast or public posting, or by randomly picking many nodes)

- this "blackboard" system means no point to point communication is needed
  - Timed-release strategies
    - encrypt and then release the key later
- "innocuously" (how?)
- through a remailing service
- DC-Net
- via an escrow service or a lawyer (but can the lawyer get into hot water for releasing the key to controversial data?)
- with a series of such releases, the key can be "diffused"
- some companies may specialize in timed-release, such as by offering a P-K with the private key to be released some time later
- in an ecology of cryptoid entities, this will increase the degrees of freedom

- this reduces the legal liability of retransmitters...they can accurately claim that they were only passing data, that there was no way they could know the content of the packets

- of course they can already claim this, due to the encrypted nature
  - One-Shot Remailers
- "You can get an anonymous address from mg5n+getid@andrew.cmu.edu. Each time you request an anon address, you get a different one. You can get as many as you like. The addresses don't expire, however, so maybe it's not the ideal 'one-shot' system, but it allows replies without connecting you to your 'real name/address' or to any of your other posts/nyms." [Matthew Ghio, 1994-04-07]

8.6.14. Things Needed in Remailers

- return receipts

- Rick Busdiecker notes that "The idea of a Return-Receipt- To: field has been around for a while, but the semantics have never been pinned down. Some mailer daemons generate replies meaning that the bits were delivered." [R.B., 1994-08-08]
  - special handling instructions
    - agents, daemons
    - negotiated procedures
  - digital postage
    - of paramount importance!
    - solves many problems, and incentivizes remailers
  - padding
    - padding to fixed sizes
- padding to fixed powers of 2 would increase the average message size by about a third
  - lots of remailers
  - multiple jursidictions

    - robustness and consistency
    - running in secure hardware
        - no logs
        - no monitoring by operator
        - wipe of all temp files
    - instantiated quickly, fluidly
    - better randomization of remailers

8.6.15. Miscellaneous Aspects of Remailers

- "How many remailer nodes are actually needed?"

- We strive to get as many as possible, to distribute the process to many jurisdictions and with many opeators.
- Curiously, as much theoretical diffusivity can occur with a single remailer (taking in a hundred messages and sending out a hundred, for example) as with many remailers. Our intuition is, I think, that many remailers offer better diffusivity and better hiding. Why this is so (if it is) needs more careful thinking than I've seen done so far.
- At a meta-level, we think multiple remailers lessens the chance of them being compromised (this, however, is not directly related to the diffusivity of a remailer network-important, but not directly related).
- (By the way, a kind of sneaky idea is to try to always declare one's self to be a remailer. If messages were somehow traced back to one's own machine, one could claim: 'Yes, I'm a remailer." In principle, one could be the only remailer in the universe and still have high enough diffusion and confusion. In practice, being the only remailer would be pretty dangerous.)
    - Diffusion and confusion in remailer networks

- Consider a single node, with a message entering, and two messages leaving; this is essentially the smallest "remailer op"

- From a proof point of view, either outgoing message could be the one
- and yet neither one can be proved to be
- Now imagine those two messages being sent through 10 remailers...no additional confusion is added...why?
- So, with 10 messages gong into a chain of 10 remailers, if 10 leave...
- The practical effect of N remailers is to ensure that compromise of some fraction of them doesn't destroy overall security

- "What do remailers do with misaddressed mail?"

- Depends on the site. Some operators send notes back (which itself causes concern), some just discard defective mail. This is a fluid area. At least one remailer (wimsey) can post

error messages to a message pool--this idea can be generalized to provide "delivery receipts" and other feedback.
- Ideal mixes, a la Chaum, would presumably discard improperly-formed mail, although agents might exist to prescreen mail (not mandatory agents, of course, but voluntarily-selected agents)
- As in so many areas, legislation is not needed, just announcement of policies, choice by customers, and the reputation of the remailer.
- A good reason to have robust generation of mail on one's own machine, so as to minimize such problems.

- "Can the NSA monitor remailers? Have they?"
- Certainly they *can* in various ways, either by directly monitoring Net traffic or indirectly. Whether they *do* is unknown.

- There have been several rumors or forgeries claiming that NSA is routinely linking anonymous IDs to real IDs at the penet remailer.

- Cypherpunks remailers are, if used properly, more secure in key ways: - many of them - not used for persistent, assigned IDs

- support for encryption: incoming and outgoing messages look completely unlike - batching, padding, etc. supported
- And properly run remailers will obscure/diffuse the connection between incoming and outgoing messages--the main point of a remailer!

- The use of message pools to report remailer errors

- A good example of how message pools can be used to anonymously report things.
- "The wimsey remailer has an ingenious method of returning error messages anonymously. Specify a subject in the message sent to wimsey that will be meaningful to you, but won't identify you (like a set of random letters). This subject does not appear in the remailed message. Then subscribe to the mailing list errors-request@extropia.wimsey.com by sending a message with Subject: subscribe. You will receive a msg for ALL errors detected in incoming messages and ALL bounced messages." [anonymous, 93-08-23]
- This is of course like reading a classified ad with some cryptic message meaningful to you alone. And more importantly, untraceable to you.

- there may be role for different types of remailers
  - those that support encryption, those that don't
  - as many in non-U.S. countries as possible
    - especially for the *last* hop, to avoid subpoena issues
  - first-class remailers which remail to *any* address
  - remailers which only remail to *other remailers*

- useful for the timid, for those with limited support, etc.

- "Should mail faking be used as part of the remailer strategy?"

- "1. If you fake mail by talking SMTP directly, the IP address or domain name of the site making the outgoing connection will appear in a Received field in the header somewhere." "2. Fake mail by devious means is generally frowned upon. There's no need to take a back-door approach here--it's bad politically, as in Internet politics." [Eric Hughes, 94-01-31]
- And if mail can really be consistently and robustly faked, there would be less need for remailers, right? (Actually, still a need, as traffic analysis would likely break any "Port 25" faking scheme.)
- Furthermore, such a strategy would not likely to be robust over time, as it relies on exploiting transitory flaws and vendor specifics. A bad idea all around.

- Difficulties in getting anonymous remailer networks widely deployed

- "The tricky part is finding a way to preserve anonymity where the majority of sites on the Internet continue to log traffic carefully, refuse to install new software (especially anon-positive software), and are administrated by people with simplistic and outdated ideas about identity and punishment. " [Greg Broiles, 1994-08-08]

- Remailer challenge: insulating the last leg on a chain from prosecution
- Strategy 1: Get them declared to be common carriers, like the phone company or a mail delivery service
- e.g., we don't prosecute an actual package deliveryperson, or even the company they work for, for delivery of an illegal package

- contents assumed to be unknown to the carrier
- (I've heard claims that only carriers who make other agreements to cooperate with law enforcement can be treated as common carriers.)
    - Strategy 2: Message pools
        - ftp sites
- with plans for users to "subscribe to" all new messages (thus, monitoring agencies cannot know which, if any, messages are being sought)
- this gets around the complaint about too much volume on the Usenet (text messages are a tiny fraction of other traffic, especially images, so the complaint is only one of potentiality)
    - Strategy 3: Offshore remailers as last leg
- probably set by sender, who presumably knows the destination
- A large number of "secondary remailers" who agree to remail a limited number...
    - "Are we just playing around with remailers and such?"
- It pains me to say this, but, yes, we are just basically playing around here!
- Remailer traffic is so low, padding is so haphazard, that making correlations between inputs and outputs is not cryptographically hard to do. (It might *seem* hard, with paper and pencil sorts of calculations, but it'll be child's play for the Crays at the Fort.)
- Even if this is not so for any particular message, maintaining a persistent ID--such as Pr0duct Cypher does, with digital sigs--without eventually providing enough clues will be almost impossible. At this time.

- Things will get better. Better and more detailed "cryptanalysis of remailer chains" is sorely needed. Until then, we are indeed just playing. (Play can be useful, though.)
  - The "don't give em any hints" principle (for remailers)
    - avoid giving any information
- dont't say which nodes are sources and which are sinks; let attackers assume everyone is a remailer, a source
  - don't say how long a password is
  - don't say how many rounds are in a tit-for-tat tournament

8.7. Anonymous Posting to Usenet

8.7.1. Julf's penet system has historically been the main way to post anonymously to Usenet (used by no less a luminary than L. Detweiler, in his "an12070/S. Boxx" personna). This has particulary been the case with postings to "support" groups, or emotional distress groups. For example, alt.sexual.abuse.recovery.

8.7.2. Cryptographically secure remailes are now being used increasingly (and scaling laws and multiple jurisdictions suggest even more will be used in the future).

8.7.3. finger remailer.help.all@chaos.bsu.edu gives these results [as of 1994-09-07--get a current result before using!]

- "Anonymous postings to usenet can be made by sending anonymous mail to one of the following mail-to-usenet gateways: group.name@demon.co.uk group.name@news.demon.co.uk group.name@bull.com group.name@cass.ma02.bull.com group.name@undergrad.math.uwaterloo.ca group.name@charm.magnus.acs.ohio-state.edu group.name@comlab.ox.ac.uk group.name@nic.funet.fi group.name@cs.dal.ca group.name@ug.cs.dal.ca group.name@paris.ics.uci.edu (removes headers) group.name.usenet@decwrl.dec.com (Preserves all headers)"

8.8. Anonymous Message Pools, Newsgroups, etc.

8.8.1. "Why do some people use message pools?"

- Provides untracable communication
- messages
- secrets
- transactions

- Pr0duct Cypher is a good example of someone who communicates primarily via anonymous pools (for messages to him). Someone recently asked about this, with this comment:
  - "Pr0duct Cypher chooses to not link his or her "real life" identity with the 'nym used to sign the software he or she wrote (PGP Tools, Magic Money, ?). This is quite an understandable sentiment, given that bad apples in the NSA are willing to go far beyond legal hassling, and make death threats against folks with high public visibility (see the threads about an NSA agent threatening to run Jim Bidzos of RSA over in his parking lot)." [Richard Johnson, alt.security.pgp, 1994-07-02]

8.8.2. alt.anonymous.messages is one such pool group

- though it's mainly used for test messages, discussions of anonymity (though there are better groups), etc.

8.8.3. "Could there be truly anonymous newsgroups?"

- One idea: newgroup a moderated group in which only messages sans headers and other identifiers would be accepted. The "moderator"--which could be a program--would only post messages after this was ensured. (Might be an interesting experiment.)
- alt.anonymous.messages was newgrouped by Rick Busdiecker, 1994-08.
- Early uses were, predictably, by people who stumbled across the group and imputed to it whatever they wished.

8.9. Legal Issues with Remailers

8.9.1. What's the legal status of remailers?

- There are no laws against it at this time.
- No laws saying people have to put return addresses on messages, on phone calls (pay phones are still legal), etc.
- And the laws pertaining to not having to produce identity (the "flier" case, where leaflet distributors did not have to produce ID) would seem to apply to this form of communication.
  - However, remailers may come under fire:
    - Sysops, MIT case
- potentially serious for remailers if the case is decided such that the sysop's creation of group that was conducive to criminal pirating was itself a crime...that could make all involved in remailers culpable

8.9.2. "Can remailer logs be subpoenaed?"

- Count on it happening, perhaps very soon. The FBI has been subpoenaing e-mail archives for a Netcom customer (Lewis De Payne), probably because they think the e-mail will lead them to the location of uber-hacker Kevin Mitnick. Had the parties used remailers, I'm fairly sure we'd be seeing similar subpoenas for the remailer logs.
  - There's no exemption for remailers that I know of!
  - The solutions are obvious, though:
- use many remailers, to make subpoenaing back through the chain very laborious, very expensive, and likely to fail (if even one party won't cooperate, or is outside the court's jurisdiction, etc.)
- offshore, multi-jurisdictional remailers (seleted by the user)
- no remailer logs kept...destroy them (no law currently says anybody has to keep e-mail records! This may change...)
  - "forward secrecy," a la Diffie-Hellman forward secrecy

8.9.3. How will remailers be harassed, attacked, and challenged?

8.9.4. "Can pressure be put on remailer operators to reveal traffic logs and thereby allow tracing of messages?"

- For human-operated systems which have logs, sure. This is why we want several things in remailers:
  - no logs of messages
  - many remailers

- multiple legal jurisdictions, e.g., offshore remailers (the more the better)
- hardware implementations which execute instructions flawlessly (Chaum's digital mix)

8.9.5. Calls for limits on anonymity

- Kids and the net will cause many to call for limits on nets, on anonymity, etc.

- "But there's a dark side to this exciting phenomenon, one that's too rarely understood by computer novices. Because they offer instant access to others, and considerable

anonymity to participants, the services make it possible for people - especially computer-literate kids - to find themselves in unpleasant, sexually explicit social situations... And I've gradually come to adopt the view, which will be controversial among many online users, that the use of nicknames and other forms of anonymity must be eliminated or severly curbed to force people online into at least as much accountability for their words and actions as exists in real social encounters." [Walter S. Mossberg, Wall Street Journal, 6/30/94, provided by Brad Dolan]

- Eli Brandt came up with a good response to this: "The sound-bite response to this: do you want your child's name, home address, and phone number available to all those lurking pedophiles worldwide? Responsible parents encourage their children to use remailers."
- Supreme Court said that identity of handbill distributors need not be disclosed, and pseudonyms in general has a long and noble tradition
- BBS operators have First Amendment protections (e.g.. registration requirements would be tossed out, exactly as if registration of newspapers were to be attempted)

8.9.6. Remailers and Choice of Jurisdictions

- The intended target of a remailed message, and the subject material, may well influence the set of remailers used, especially for the very important "last remailer' (Note: it should never be necessary to tell remailers if they are first, last, or others, but the last remailer may in fact be able to tell he's the last...if the message is in plaintext to the recipient, with no additional remailer commands embedded, for example.)
- A message involving child pornography might have a remailer site located in a state like Denmark, where child porn laws are less restrictive. And a message critical of Islam might not be best sent through a final remailer in Teheran. Eric Hughes has dubbed this "regulatory arbitrage," and to various extents it is already common practice.
- Of course, the sender picks the remailer chain, so these common sense notions may not be followed. Nothing is perfect, and customs will evolve. I can imagine schemes developing for choosing customers--a remailer might not accept as a customer certain abusers, based on digital pseudonyms < hairy).

8.9.7. Possible legal steps to limit the use of remailers and anonymous systems

- hold the remailer liable for content, i.e., no common carrier status
- insert provisions into the various "anti-hacking" laws to criminalize anonymous posts

8.9.8. Crypto and remailers can be used to protect groups from "deep pockets" lawsuits

- products (esp. software) can be sold "as is," or with contracts backed up by escrow services (code kept in an escrow repository, or money kept there to back up committments)

- jurisdictions, legal and tax, cannot do "reach backs" which expose the groups to more than they agreed to

- as is so often the case with corporations in the real world, which are taxed and fined for various purposes (asbestos, etc.)
- (For those who panic at the thought of this, the remedy for the cautious will be to arrange contracts with the right entities...probably paying more for less product.)

8.9.9. Could anonymous remailers be used to entrap people, or to gather information for investigations?

- First, there are so few current remailers that this is unlikely. Julf seems a non-narc type, and he is located in Finland. The Cypherpunks remailers are mostly run by folks like us, for now.
- However, such stings and set-ups have been used in the past by narcs and "red squads." Expect the worse from Mr. Policeman. Now that evil hackers are identified as hazards, expect moves in this direction. "Cryps" are obviously "crack" dealers.
- But use of encryption, which CP remailers support (Julf's does not), makes this essentially moot.

8.10. Cryptanalysis of Remailer Networks

8.10.1. The Need for More Detailed Analysis of Mixes and Remailers

- "Have remailer systems been adequately cryptanalyzed?"

- Not in my opinion, no. Few calculations have been done, just mostly some estimates about how much "confusion" has been created by the remailer nodes.
- But thinking that a lot of complication and messiness makes a strong crypto system is a basic mistake...sort of like thinking an Enigma rotor machine makes a good cipher system, by today's standards, just because millions of combinations of pathways through the rotor system are possible. Not so.
  - Deducing Patterns in Traffic and Deducing Nyms
    - The main lesson of mathematical cryptology has been that seemingly random things can actually be shown to have structure. This is what cryptanalysis is all about.
- The same situation applies to "seemingly random" message traffic, in digital mixes, telephone networks, etc. "Cryptanalysis of remailers" is of course possible, depending on the underlying model. (Actually, it's always possible, it just may not yield anything, as with cryptanalysis of ciphers.)

- on the time correlation in remailer cryptanalysis

- imagine Alice and Bob communicating through remailers...an observer, unable to follow specific messages through the remailers, could still notice pairwise correlations between messages sent and received by these two

- like time correlations between events, even if the intervening path or events are jumbled

- e.g., if within a few hours of every submarine's departure from Holy Loch a call is placed to Moscow, one may make draw certain conclusions about who is a Russian spy, regardless of not knowing the intermediate paths
- or, closer to home, correlating withdrawals from one bank to deposits in another, even if the intervening transfers are jumbled + just because it seems "random" does not mean it is
- Scott Collins speculates that a "dynamic Markov compressor" could discern or uncover the nonrandomness in remailer uses
- Cryptanalysis of remailers has been woefully lacking. A huge fraction of posts about remailer improvements make hand-waving arguments about the need for more traffic, longer delays, etc. (I'm not pointing fingers, as I make the same informal, qualitative comments, too. What is needed is a rigorous analysis of remailer security.)
- We really don't have any good estimates of overall security as a function of number of messages circulating, the latency (number of stored messages before resending), the number of remailer hops, etc. This is not cryptographically "exciting" work, but it's still needed. There has not been much focus in the academic community on digital mixes or

remailers, probably because David Chaum's 1981 paper on "Untraceable E-Mail" covered most of the theoretically interesting material. That, and the lack of commercial products or wide usage.

- Time correlations may reveal patterns that individual messages lack. That is, repeated communicatin between Alice and Bob, even if done through remailers and even if time delays/dwell times are built-in, may reveal nonrandom correlations in sent/received messages.

- Scott Collins speculates that a dynamic Markov compressor applied to the traffic would have reveal such correlations. (The application of such tests to digital cash and other such systems would be useful to look at.)
  - Another often overlooked weakness is that many people send test messages to themselves, a point noted by Phil Karn: "Another way that people often let themselves be caught is that they inevitably send a test message to themselves right before the forged message in question. This shows up clearly in the sending system's sendmail logs. It's a point to consider with remailer chains too, if you don't trust the last machine on the chain." [P.K., 1994-09-06]
  - What's needed:
- aggreement on some terminology (this doesn't require consensus, just a clearly written paper to de facto establish the terminology)
- a formula relating degree of untraceability to the major factors that go into remailers: packet size and quantization, latency (# of messages), remailer policies, timing, etc.
- Also, analysis of how deliberate probes or attacks might be mounted to deduce remailer patterns (e.g., Fred always remails to Josh and Suzy and rarely to Zeke).
- I think this combinatorial analysis would be a nice little monograph for someone to write.

8.10.2. A much-needed thing. Hal Finney has posted some calculations (circa 1994-08-08), but more work is sorely needed.

8.10.3. In particular, we should be skeptical of hand-waving analyses of the "it sure looks complicated to follow the traffic" sort. People think that by adding

"messy" tricks, such as MIRVing messages, that security is increased. Maybe it is, maybe it isn't. But it needs formal analysis before claims can be confidantly believed.

8.10.4. Remailers and entropy

- What's the measure of "mixing" that goes on in a mix, or remailer?
- Hand=waving about entropy and reordering may not be too useful.

- Going back to Shannon's concept of entropy as measuring the degree of uncertainty...
  - trying to "guess" or "predict' where a message leaving one node will exit the system

- not having clear entrance and exit points adds to the difficulty, somewhat analogously to having a password of unknown length (an attacker can't just try all 10- character passwords, as he has no idea of the length)
- the advantages of every node being a remailer, of having no clearly identified sources and sinks

- This predictability may depend on a *series* of messages sent between Alice and Bob...how?

- it seems there may be links to Persi Diaconis' work on "perfect shuffles" (a problem which seemed easy, but which eluded solving until recently...should give us comfort that our inability to tackle the real meat of this issue is not too surprising

8.10.5. Scott Collins believes that remailer networks can be cryptanalyzed roughly the same way as pseudorandom number generators are analyzed, e.g., with

dynamic Markov compressors (DNCs). (I'm more skeptical: if each remailer is using an information-theoretically secure RNG to reorder the messages, and if all messages are the same size and (of course) are encypted with information-theoretically secure (OTP) ciphers, then it seems to me that the remailing would itself be information-theoretically secure.)

8.11. Dining Cryptographers

8.11.1. This is effectively the "ideal digital mix," updated from Chaum's original hardware mix form to a purely software-based form.

8.11.2. David Chaum's 1988 paper in Journal of Crypology (Vol 1, No

1. outlines a way for completely untraceable communication using only software (no tamper-resistant modules needed)
   - participants in a ring (hence "dining cryptographers")

- Chaum imagines that 3 cryptographers are having dinner and are informed by their waiter that their dinner has already been paid for, perhaps by the NSA, or perhaps by one of themselves...they wish to determine which of these is true, without revealing which of them paid!
- everyone flips a coin (H or T) and shows it to his neighbor on the left

- everyone reports whether he sees "same" or "different"

- note that with 2 participants, they both already know the other's coin (both are to the left!)
- however, someone wishing to send a message, such as Chaum's example of "I paid for dinner," instead says the opposite of what he sees

- some analysis of this (analyze it from the point of view of one of the cryptographers) shows that the 3 cryptographers will know that one of them paid (if this protocol is executed faithfully), but that the identity can't be "localized"
  - a diagram is needed...
  - this can be generalized...
    - longer messages
      - use multiple rounds of the protocol
    - faster than coin-flipping

- each participant and his left partner share a list of "pre-flipped" coins, such as truly random bits (radioactive decay, noise, etc.) stored on a CD-ROM or whatever
- they can thus "flip coins" as fast as they can read the disk
  - simultaneous messages (collision)
    - use back-off and retry protocols (like Ethernet uses)
  - collusion of participants
- an interesting issue...remember that participants are not restricted to the simple ring topology
- various subgraphs can be formed
- a participant who fears collusion can pick a subgraph that includes those he doubts will collude (a tricky issue)
  - anonymity of receiver
- can use P-K to encrypt message to some P-K and then "broadcast" it and force every participant to try to decrypt it (only the anonymous recipient will actually succeed)
- Chaum's complete 1988 "Journal of Cryptology" article is available at the Cypherpunks archive site, ftp.soda.csua.edu, in /pub/cypherpunks

8.11.3. What "DC-Net" Means

- a system (graph, subgraphs, etc.) of communicating participants, who need not be known to each other, can communicate information such that neither the sender nor the recipient is known
  - unconditional sender untraceability

- the anonymity of the broadcaster can be information- theoretically secure, i.e., truly impossible to break and requiring no assumptions about public key systems, the difficulty of factoring, etc.

- receiver untraceability depends on public-key protocols, so traceability is computationally-dependent
  - but this is believed to be secure, of course
  - bandwidth can be increased by several means
    - shared keys
    - block transmission by accumulating messages
    - hiearchies of messages, subgraphs, etc.

8.12. Future Remailers

8.12.1. "What are the needed features for the Next Generation Remailer?"

- Some goals

- generally, closer to the goals outlined in Chaum's 1981 paper on "Untraceable E-Mail"
  - Anonymity
  - Digital Postage, pay as you go, ,market pricing
  - Traffic Analysis foiled
  - Bulletproof Sites:
- Having offshore (out of the U.S.) sites is nice, but having sites resistant to pressures from universities and corporate site administrators is of even greater practical consequence. The commercial providers, like Netcom, Portal, and Panix, cannot be counted on to stand and fight should pressures mount (this is just my guess, not an aspersion against their backbones, whether organic or Internet).
- Locating remailers in many non-U.S. countries is a Good Idea. As with money-laundering, lots of countries means lots of jurisdictions, and the near impossibility of control by one country.
  - Digital Postage, or Pay-as-you-Go Services:
- Some fee for the service. Just like phone service, modem time, real postage, etc. (But unlike highway driving, whose usage is largely subsidized.)
- This will reduce spamming, will incentivize remailer services to better maintain their systems, and will
  - Rates would be set by market process, in the usual way. "What the traffic will bear." Discounts, favored customers, rebates, coupons, etc. Those that don't wish to charge, don't have to (they'll have to deal with the problems).
  - Generations

    - 1st Gen--Today's Remailer:
    - 2nd Gen--Near Future (c. 1995)
    - 3rd Gen
    - 4th Gen-

8.12.2. Remailing as a side effect of mail filtering

- Dean Tribble has proposed...
- "It sounds like the plan is to provide a convenient mail filtering tool which provides remailer capability as a SIDE EFFECT! What a great way to spread remailers!" [Hal Finney, 93-01-03]

8.12.3. "Are there any remailers which provide you with an anonymous account to which other people may send messages, which are then forwarded to you in a PGP-encrypted form?" Mikola Habryn, 94-04

- "Yes, but it's not running for real yet. Give me a few months until I get the computer + netlink for it. (It's running for testing though, so if you want to test it, mail me, but it's not running for real, so don't *use* it.)" [Sameer Parekh, 94-04-03]

8.12.4. "Remailer Alliances"

- "Remailer's Guild"

- to make there be a cost to flakiness (expulsion) and a benefit to robustness, quality, reliability, etc. (increased business)
    - pings, tests, cooperative remailing
    - spreading the traffic to reduce effectiveness of attacks
    - which execute protocols
- e.g., to share the traffic at the last hop, to reduce attacks on any single remailer

8.13. Loose Ends

8.13.1. Digital espionage

- spy networks can be run safely, untraceably, undetectably
  - anonymous contacts, pseudonyms
- digital dead drops, all done electronically...no chance of being picked up, revealed as an "illegal" (a spy with no diplomatic cover to save him) and shot
- so many degrees of freedom in communications that controlling all of them is essentially impossible
- Teledesic/Iridium/etc. satellites will increase this capability further
- unless crypto is blocked--and relatively quickly and ruthlessly--the situation described here is unstoppable
- what some call "espionage" others would just call free communication
- (Some important lessons for keeping corporate or business secrets...basically, you can't.)

8.13.2. Remailers needs some "fuzziness," probably

- for example, if a remailer has a strict policy of accumulating N messages, then reordering and remailing them, an attacker can send N - 1 messages in and know which of the N messages leaving is the message they want to follow; some uncertainly helps here
- the mathematics of how this small amount of uncertainty, or scatter, could help is something that needs a detailed analysis
- it may be that leaving some uncertainty, as with the keylength issue, can help

8.13.3. Trying to confuse the eavesdroppers, by adding keywords they will probably pick up on

- the "remailer@csua.berkeley.edu" remailer now adds actual paragraphs, such as this recent example:

- "I fixed the SKS. It came with a scope and a Russian night scope. It's killer. My friend knows about a really good gunsmith who has a machineshop and knows how to convert stuff to automatic."
  - How effective this ploy is is debatable

8.13.4. Restrictions on anonymous systems

- Anonymous AIDS testing. under FDA review for 5 delayed release on the badly and perhaps kill test result...they want the existing system to prevail. mention this to show that anonymous systems are somtimes opposed for ideological reasons.)

Revision #3
Created 23 June 2022 03:47:30 by c0mmando
Updated 23 June 2022 03:51:15 by c0mmando