13. Activism and Projects

13.1. copyright

13.2. SUMMARY: Activism and Projects

13.2.1. Main Points

13.2.2. Connections to Other Sections

13.2.3. Where to Find Additional Information

13.2.4. Miscellaneous Comments

13.3. Activism is a Tough Job

13.3.1. "herding cats"

..trying to change the world through exhortation seems a particulary ineffective notion

13.3.2. There's always been a lot of wasted time and rhetoric

on the Cypherpunks list as various people tried to get others to follow their lead, to adopt their vision. (Nothing wrong with this, if done properly. If someone leads by example, or has a particularly compelling vision or plan, this may naturally happen. Too often, though, the situation was that someone's vague plans for a product were declared by them to be the standards that others should follow. Various schemes for digital money, in many forms and modes, has always been the prime example of this.)

13.3.3. This is related also to what Kevin Kelley calls "the fax effect."

When few people own fax machines, they're not of much use. Trying to get others to use the same tools one has is like trying to convince people to buy fax machines so that you can communicate by fax with them...it may happen, but probably for other reasons. (Happily, the interoperability of PGP provided a common communications medium that had been lacking with previous platform-specific cipher programs.)

13.3.4. Utopian schemes are also a tough sell.

Schemes about using digital money to make inflation impossible, schemes to collect taxes with anonymous systems, etc.

13.3.5. Harry Browne's "How I Found Freedom in an Unfree World" is well worth reading;

he advises against getting upset and frustrated that the world is not moving in the direction one would like.

13.4. Cypherpunks Projects

13.4.1. "What are Cypherpunks projects?"

- Always a key part--perhaps *the* key part--of Cypherpunks activity. "Cypherpunks write code." From work on PGP to remailers to crypto toolkits to FOIA requests, and a bunch of other things, Cypherpunks hack the system in various ways.
- Matt Blaze's LEAF blower, Phil Karn's "swIPe" system, Peter Wayner's articles...all are examples. (Many Cypherpunks projects are also done, or primarily done, for other reasons, so we cannot in all cases claim credit for this work.)

13.4.2. Extensions to PGP

13.4.3. Spread of PGP and crypto in general.

- education
- diskettes containing essays, programs
- ftp sites
- raves, conventions, gatherings

13.4.4. Remailers

- ideal Chaumian mix has certain properties
  - latency to foil traffic analysis
  - encryption
  - no records kept (hardware tamper-resistance, etc.)

- Cyperpunks remailers
- julf remailers

- abuses

- flooding, because mail transmission costs are not borne by sender
  - anonymity produces potential for abuses
    - death threats, extortion
- Progress continues, with new features added. See the discussion in the remailers section.

13.4.5. Steganography

- hiding the existence of a message, for at least some amount of time
  - security through obscurity
  - invisible ink, microdots
  - Uses
- in case crypto is outawed, may be useful to avoid authorities
- if enough people do it, increases the difficulty of enforcing anti-crypto laws (all
  - Stego
- JSTEG: soda.berkeley.edu:/pub/cypherpunks/applications/jsteg
  - Stego: sumex-aim.stanford.edu

13.4.6. Anonymous Transaction Systems

13.4.7. Voice Encryption, Voice PGP

- Clipper, getting genie out of bottle
- CELP, compression, DSPs
- SoundBlaster approach...may not have enough processing power
  - hardware vs. pure software
- newer Macs, including av Macs and System 7 Pro, have interesting capabilities

- Zimmermann's plans have been widely publicized, that he is looking for donations, that he is seeking programming help, etc.

- which does not bode well for seeing such a product from him
  - frankly, I expect it will come from someone else
  - Eric Blossom is pursuing own hardware board, based on 2105
  - "Is anyone building encrypted telephones?"

- Yes, several such projects are underway. Eric Blossom even showed a

- PCB of one at a Cypherpunks meeting, using an inexpensive DSP chip.

- Software-only versions, with some compromises in speech quality

- probably, are also underway. Phil Zimmermann described his progress at

- the last Cypherpunks meeting.

- ("Software-only" can mean using off-the-shelf, widely- available DSP

- boards like SoundBlasters.)

- And I know of at least two more such projects. Whether any will
- materialize is anyone's guess.
- And various hacks have already been done. NeXT users have had
- voicemail for years, and certain Macs now offer something similar.
- Adding encryption is not a huge obstacle.
- A year ago, several Cypherpunks meeting sites around the U.S. were
- linked over the Internet using DES encryption. The sound quality was
- poor, for various reasons, and we turned off the DES in a matter of
- minutes. Still, an encrypted audio conference call.

13.4.8. DC-Nets

- What it is, how it works
- Chaum's complete 1988 "Journal of Cryptology" article is available at the Cypherpunks archive site, ftp.soda.csua.edu, in /pub/cypherpunks
  - Dining Cryptographers Protocols, aka "DC Nets"
- "What is the Dining Cryptographers Problem, and why is it so important?" + This is dealt with in the main section, but here's David Chaum's Abstract, from his 1988 paper"
- Abstract: "Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys. respectively. It can be adapted to address efficiently a wide variety of practical considerations." ["The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.]
- DC-nets have yet to be implemented, so far as I know, but they represent a "purer" version of the physical remailers we are all so familiar with now. Someday they'll have have a major impact. (I'm a bigger fan of this work than many seem to be, as there is little discussion in sci.crypt and the like.)
- "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.
- available courtesy of the Information Liberation Front at the soda.csua.berkeley.edu site
- Abstract: "Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys. respectively. It can be adapted to address efficiently a wide variety of practical considerations." ["The Dining Cryptographers Problem:

Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.]

- Note that the initials "D.C." have several related meanings: Dining Cryptographers, Digital Cash/DigiCash, and David Chaum. Coincidence?
  - Informal Explanation
- Note: I've posted this explanation, and variants, several times since I first wrote it in mid-1992. In fact, I first posted it on the "Extropians" mailing list, as "Cypherpunks" did not then exist.
- Three Cypherpunks are having dinner, perhaps in Palo Alto. Their waiter tells them that their bill has already been paid, either by the NSA or by one of them. The waiter won't say more. The Cypherpunks wish to know whether one of them paid, or the NSA paid. But they don't want to be impolite and force the Cypherpunk payer to 'fess up, so they carry out this protocol (or procedure): Each Cypherpunk flips a fair coin behind a menu placed upright between himself and the Cypherpunk on his right. The coin is visible to himself AND to the Cypherpunk on his left. Each Cypherpunk can see his own coin and the coin to his right. (STOP RIGHT HERE! Please take the time to make a sketch of the situation I've described. If you lost it here, all that follows will be a blur. It's too bad the state of the Net today cannot support figures and diagrams easily.) Each Cypherpunk then states out loud whether the two coins he can see are the SAME or are DIFFERENT, e.g., "Heads-Tails" means DIFFERENT, and so forth. For now, assume the Cypherpunks are truthful. A little bit of thinking shows that the total number of "DIFFERENCES" must be either 0 (the coins all came up the same), or

2. Odd parity is impossible. Now the Cypherpunks agree that if one of them paid, he or she will SAY THE OPPOSITE of what they actually see. Remember, they don't announce what their coin turned up as, only whether it was the same or different as their neighbor. Suppose none of them paid, i.e., the NSA paid. Then they all report the truth and the parity is even (either 0 or 2 differences). They then know the NSA paid. Suppose one of them paid the bill. He reports the opposite of what he actually sees, and the parity is suddenly odd. That is, there is 1 difference reported. The Cypherpunks now know that one of them paid. But can they determine which one? Suppose you are one of the Cypherpunks and you know you didn't pay. One of the other two did. You either reported SAME or DIFFERENT, based on what your neighbor to the right (whose coin you can see) had. But you can't tell which of the other two is lying! (You can see you right-hand neighbor's coin, but you can't see the coin he sees to his right!) This all generalizes to any number of people. If none of them paid, the parity is even. If one of them paid, the parity is odd. But which one of them paid cannot be deduced. And it should be clear that each round can transmit a bit, e.g., "I paid" is a "1". The message "Attack at dawn" could thus be "sent" untraceably with multiple rounds of the protocol.

- The "Crypto Ouija Board": I explain this to people as a kind of ouija board. A message, like "I paid" or a more interesting "Transfer funds from...," just "emerges" out of the group, with no means of knowing where it came from. Truly astounding.
  - Problems and Pitfalls
- In Chaum's paper, the explanation above is given quickly, in a few pages. The *rest* of the paper is then devoted to dealing with the many "gotchas" and attacks that come up and

that must be dealt with before the DC protocol is even remotely possible. I think all those interested in protocol design should read this paper, and the follow-on papers by Bos, Pfitzmann, etc., as object lessons for dealing with complex crypto protocols. + The Problems:

- 1. Collusion. Obviously the Cypherpunks can collude to deduce the payer. This is best dealt with by creating multiple subcircuits (groups doing the protocol amongst themselves). Lots more stuff here. Chaum devotes most of the paper to these kind of issues and their solutions.

2. With each round of this protocol, a single bit is transmitted. Sending a long message means many coin flips. Instead of coins and menus, the neighbors would exchange lists of random numbers (with the right partners, as per the protocol above, of course. Details are easy to figure out.)
3. Since the lists are essentially one-time pads, the protocol is unconditionally secure, i.e., no assumptions are made about the difficulty of factoring large numbers or any other crypto assumptions.
4. Participants in such a "DC-Net" (and here we are coming to the heart of the "crypto anarchy" idea) could exchange CD-ROMs or DATs, giving them enough "coin flips" for zillions of messages, all untraceable! The logistics are not simple, but one can imagine personal devices, like smart card or Apple "Newtons," that can handle these protocols (early applications may be for untraceable brainstorming comments, secure voting in corportate settings, etc.)
5. The lists of random numbers (coin flips) can be generated with standard cryptographic methods, requiring only a key to be exchanged between the appropriate participants. This eliminates the need for the one-time pad, but means the method is now only cryptographically secure, which is often sufficient. (Don't think "only cryptographically secure" means insecure...the messages may remain encrypted for the next billion years)
6. Collisions occur when multiple messages are sent at the same time. Various schemes can be devised to handle this, like backing off when you detect another sender (when even parity is seen instead of odd parity). In large systems this is likely to be a problem. Deliberate disruption, or spamming, is a major problem--a disruptor can shut down the DC-net by sending bits out. As with remailes, anonymity means freedom from detection. (Anonymous payments to send a message may help, but the details are murky to me.)
    - Uses

- ◦ Untraceable mail. Useful for avoiding censorship, for avoiding lawsuits, and for all kinds of crypto anarchy things.
- ◦ Fully anonymous bulletin boards, with no traceability of postings or responses. Illegal materials can be offered for sale (my 1987 canonical example, which freaked out a few people: "Stealth bomber blueprints for sale. Post highest offer and include public key."). Think for a few minutes about this and you'll see the profound implications.
- ◦ Decentralized nexus of activity. Since messages "emerge" (a la the ouija board metaphor), there is no central posting area. Nothing for the government to shut down, complete deniability by the participants. - * Only you know who your a partners are...in any given circuit. And you can be in as many circuits as you wish. (Payments can be made to others, to create a profit motive. I won't deal with this

issue, or with the issue of how reputations are handled, here.)
- It should be clear that DC-nets offer some amazing opportunities. They have not been implemented at all, and have received almost no attention compared to ordinary Cypherpunks remailers. Why is this? The programming complexity (and the underlying cryptographic primitives that are needed) seems to be the key. Several groups have announced plans to imlement some form of DC-net, but nothing has appeared.
  - software vs. hardware,
  - Yanek Martinson, Strick, Austin group, Rishab
- IMO, this is an ideal project for testing the efficacy of software toolkits. The primitives needed, including bit commitment, synchronization, and collusion handling, are severe tests of crypto systems. On the downside, I doubt that even the Pfaltzmans or Bos has pulled off a running simulation...

13.4.9. D-H sockets, UNIX, swIPe

- swIPe

- Matt Blaze, John I. (did coding), Phil Karn, Perry Metzger, etc. are the main folks involved
  - evolved from "mobile IP," with radio links, routing
  - virtual networks
  - putting encryption in at the IP level, transparently
  - bypassing national borders
  - Karn
  - at soda site
  - swIPe system, for routing packets
    - end to end, gateways, links, Mach, SunOS

13.4.10. Digital Money, Banks, Credit Unions

- Magic Money
- Digital Bank
- "Open Encrypted Books"
- not easy to do...laws, regulations, expertise in banking
- technical flaws, issues in digital money

- several approaches
  - clearing
  - tokens, stamps, coupons
  - anonymity-protected transactions

13.4.11. Data Havens

- financial info, credit reports
  - bypassing local jurisdictions, time limits, arcane rules

- reputations
- insider trading
- medical
- technical, scientific, patents
- crypto information (recursively enough)
- need not be any known location...distributed in cyberspace
- One of the most commercially interesting applications.

13.4.12. Related Technologies

- Agorics
- Evolutionary Systems
- Virtual Reality and Cyberspace
- Agents

- Computer Security
  - Kerberos, Gnu, passwords
    - recent controversy
    - demon installed to watch packets
    - Cygnus will release it for free
  - GuardWire
- Van Eck, HERF, EMP

- Once Cypherpunk project proposed early on was the duplication of certain NSA capabilities to monitor electronic communications. This involves "van Eck" radiation (RF) emitted by the CRTs and other electronics of computers.

- Probably for several reasons, this has not been pursued, at least not publically. - legality - costs - difficulty in finding targets of opportunity - not a very CPish project!

13.4.13. Matt Blaze, AT&T, various projects

- a different model of trust...multiple universes
  - not heierarchical interfaces, but mistrust of interfaces
  - heterogeneous

    - where to put encryption, where to mistrust, etc.
- wants crypto at lowest level that is possible
    - almost everything should be mistrusted

- every mistrusted interface shoud be cryptographically protected...authentication, encryption
    - "black pages"---support for cryptographic communication
        - "pages of color"
- a collection of network services that identiy and deliver security information as needed...keys, who he trusts, protocols, etc.
    - front end: high-level API for security requirements
        - like DNS? caching models?
    - trusted local agent...

- "people not even born yet" (backup tapes of Internet communications)

- tapes stored in mountains, access by much more powerful computers
    - "Crytptographic File System" (CFS)
        - file encryption
- no single DES mode appears to be adequate...a mix of modes
    - swIPe system, for routing packets
        - end to end, gateways, links, Mach, SunOS

13.4.14. Software Toolkits

- Henry Strickland's TCL-based toolkit for crypto

- other Cypherpunks, including Hal Finney and Marianne Mueller, have expressed good opinions of TCL and TCL-TK (toolkit)
    - Pr0duct Cypher's toolkit
    - C++ Class Libraries
    - VMX, Visual Basic, Visual C++
    - Smalltalk

13.5. Responses to Our Projects (Attacks, Challenges)

13.5.1. "What are the likely attitudes toward mainstream Cypherpunks projects, such as remailers, encryption, etc.?"

- Reaction has already been largely favorable. Journalists such as Steven Levy, Kevin Kelly, John Markoff, and Julian Dibbell have written favorably. Reaction of people I have talked to has also been mostly favorable.

13.5.2. "What are the likely attitudes toward the more outre projects, such as digital money, crypto anarchy, data havens, and the like?"

- Consternation is often met. People are frightened.
- The journalists who have written about these things (those mentioned above) have gotten beyond the initial reaction and seem genuinely intrigued by the changes that are coming.

13.5.3. "What kinds of *attacks* can we expect?"

- Depends on the projects, but some general sorts of attacks are likely. Some have already occurred. Examples:

- flooding of remailers, denial of service attacks--to swamp systems and force remailers to reconsider operations

- this is fixed (mostly) with "digital postage" (if postage covers costs, and generates a profit, then the more the better)

- deliberately illegal or malicicious messages, such as death threats

- designed to put legal and sysop pressures on the remailer operator
- several remailers have been attacked this way, or at least have had these messages

- source-blocking sometimes works, though not of course if another remailer is first used (many issues here)
  - prosecution for content of posts
    - copyright violations
- e.g., forwarding ClariNet articles through Hal Finney's remailer got Brad Templeton to write warning letters to Hal - pornography - ITAR violations, Trading with the Enemy Act - espionage, sedition, treason - corporate secrets,
- These attacks will test the commitment and courage of remailer or anonymizing service operators

13.6. Deploying Crypto

13.6.1. "How can Cypherpunks publicize crypto and PGP?"

- articles, editorials, radio shows, talking with friends
- The Net itself is probably the best place to publicize the problems with Clipper and key escrow. The Net played a major role--perhaps the dominant role--in generating scorn for Clipper. In many way the themes debated here on the Net have tremendous influence on media reaction, on editorials, on organizational reactions, and of course on the opinion of technical folks. News spreads quickly, zillions of theories are aired and debated, and consensus tends to emerge quickly.
  - raves, Draper
  - Libertarian Party, anarchists...
  - conferences and trade shows
    - Arsen Ray Arachelian passed out diskettes at PC Expo

13.6.2. "What are the Stumbling Blocks to Greater Use of Encryption (Cultural, Legal, Ethical)?"

- "It's too hard to use"

- multiple protocols (just consider how hard it is to actually send encrypted messages between people today)
  - the need to remember a password or passphrase
  - "It's too much trouble"

- the argument being that people will not bother to use passwords
- partly because they don't think anything will happen to them
  - "What have you got to hide?"
    - e.g.,, imagine some comments I'd have gotten at Intel had I encrypted everything
- and governments tend to view encryption as ipso facto proof that illegalities are being committed: drugs, money laundering, tax evasion
- recall the "forfeiture" controversy
- BTW, anonymous systems are essentially the ultimate merit system (in the obvious sense) and so fly in the face of the "hiring by the numbers" de facto quota systems now creeeping in to so many areas of life...there may be rules requiring all business dealings to keep track of the sex, race, and "ability group" (I'm kidding, I hope) of their employees and their consultants

- Courts Are Falling Behind, Are Overcrowded, and Can't Deal Adequately with New Issues-Such as Encryption and Cryonics
  - which raises the issue of the "Science Court" again
  - and migration to private adjudication

- scenario: any trials that are being decided in 1998-9 will have to have been started in 1996 and based on technology and decisions of around 1994

- Government is taking various steps to limit the use of encryption and secure communication

- some attempts have failed (S.266), some have been shelved, and almost none have yet been tested in the courts
  - see the other sections...

13.6.3. Practical Issues

- Education
- Proliferation
- Bypassing Laws

13.6.4. "How should projects and progress best be achieved?"

- This is a tough one, one we've been grappling with for a couple of years now. Lots of approaches.
  - Writing code
  - Organizational

    - Lobbying
- I have to say that there's one syndrome we can probably do w,the Frustrated Cyperpunks Syndrome. Manifested by someone flaming the list for not jumping in to join them on their (usually) half-baked scheme to build a digital bank, or write a book, or whatever. "You guys just don't care!" is the usual cry. Often these flamers end up leaving the list.
- Geography may play a role, as folks in otherwise-isolated areas seem to get more attached to their ideas and then get angry when the list as a whole does not adopt them (this is my impression, at least).

13.6.5. Crypto faces the complexity barrier that all technologies face

- Life has gotten more complicated in some ways, simpler in other ways (we don't have to think about cooking, about shoeing the horses, about the weather, etc.). Crypto is currently fairly complicated, especially if multiple paradigms are used (encryption, signing, money, etc.).
- As a personal note, I'm practically drowning in a.c. adaptors and power cords for computers, laser printers, VCRs, camcorders, portable stereos, laptop computers, guitars, etc. Everything with a rechargeable battery has to be charged, but not overcharged, and not allowed to run- down...I forgot to plug in my old Powerbook 100 for a couple of months, and the lead-acid batteries went out on

  me. Personally, I'm drowning in this crap.

- I mention this only because I sense a backlash coming...people will say "screw it" to new technology that actually complicates their lives more than it simplifies their lives. "creating a client" continue to do (A nation that hardly embrace things change,

13.6.6. "How can we general and encryption in particular?

- Fact is, most people never think about real security. Safe manufacturers have said that improvements in safes were driven by insurance rates. A direct incentive to spend more money to improve security (cost of better safe < cost of higher insurance rate). Right now there is almost no economic incentive for people to worry about PIN security, about protecting their files, etc. (Banks eat the costs and pass them on...any bank which tried to save a few bucks in losses by requiring 10-digit PINs--which people would *write down* anyway!--would lose customers. Holograms and pictures on bank cards are happening because the costs have dropped enough.) Personally, my main interests is in ensuring the Feds don't tell me I can't have as much security as I want to buy. I don't share the concern

quoted above that we have to find ways to give other people security.
- Others disagree with my nonchalance, pointing out that getting lots of other people to use crypto makes it easier for those who already protect themselves. I agree, I just don't focus on missionary work.
- For those so inclined, point out to people how vulnerable their files are, how the NSA can monitor the Net, and so on. All the usual scare stories.

13.7. Political Action and Opposition

13.7.1. Strong political action is emerging on the Net

- right-wing conspiracy theorists, like Linda Thompson

- Net has rapid response to news events (Waco, Tienenmen, Russia)

- with stories often used by media (lots of reporters on Net, easy to cull for references, Net has recently become tres trendy)
  - Aryan Nation in Cyberspace
- (These developments bother many people I mention them to. Nothing can be done about who uses strong crypto. And most fasicst/racist situations are made worse by state sponsorship--apartheid laws, Hitler's Germany, Pol Pot's killing fields, all were examples of the state enforcing racist or genocidal laws. The unbreakable crypto that the Aryan Nation gets is more than offset by the gains elsewhere, and the undermining of central authority.)
- shows the need for strong crypto...else governments will infiltrate and monitor these political groups

13.7.2. Cypherpunks and Lobbying Efforts

- "Why don't Cypherpunks have a lobbying effort?"
- we're not "centered" near Washington, D.C., which seems to be an essential thing (as with EFF, ACLU, EPIC, CPSR, etc.)

- D.C. Cypherpunks once volunteered (April, 1993) to make this their special focus, but not much has been heard since. (To be fair to them, political lobbying is pretty far-removed from most Cypherpunks interests.)

    - no budget, no staff, no office

- "herding cats" + no financial stakes = why we don't do more
- it's very hard to coordinate dozens of free-thinking, opinionated, smart people, especially when there's no whip hand, no financial incentive, no way to force them into line

- I'm obviously not advocating such force, just noting a truism of systems

- "Should Cypherpunks advocate breaking laws to achieve goals?"

- "My game is to get cryptography available to all, without violating the law. This mean fighting Clipper, fighting idiotic export restraints, getting the government to change it's stance on cryptography, through arguements and letter pointing out the problems ... This means writing or promoting strong cryptography...By violating the law, you give them the chance to brand you "criminal," and ignore/encourage others to ignore what you have to say." [Bob Snyder, 4-28-94]

13.7.3. "How can nonlibertarians (liberals, for example) be convinced of the need for strong crypto?"

- "For liberals, I would examine some pet cause and examine the consequences of that cause becoming "illegal." For instance, if your friends are "pro choice," you might ask them what they would do if the right to lifers outlawed abortion. Would they think it was wrong for a rape victim to get an abortion just because it was illegal? How would they feel about an abortion "underground railroad" organized via a network of "stations" coordinated via the Internet using "illegal encryption"? Or would they trust Clipper in such a situation? "Everyone in America is passionate about something. Such passion usually dispenses with mere legalism, when it comes to what the believer feels is a question of fundamental right and wrong. Hit them with an argument that addresses their passion. Craft a pro-crypto argument that helps preserve the object of that passion." [Sandy Sandfort, 199406-30]

13.7.4. Tension Between Governments and Citizens

- governments want more monitoring...big antennas to snoop on telecommunications, "
- people who protect themselves are sometimes viewed with suspicion
    - Americans have generally been of two minds about privacy:

- None of your damn business, a man's home is his castle..rugged individualism, self-sufficiency, Calvinism
  - What have you got to hide? Snooping on neighbors

- These conflicting views are held simultaneously, almost like a tensor that is not resolvable to some resultant vector - this dichotomy cuts through legal decisions as well

13.7.5. "How does the Cypherpunks group differ from lobbying groups like the EFF, CPSR, and EPIC?"

- We're more disorganized (anarchic), with no central office, no staff, no formal charter, etc.
- And the political agenda of the aforementioned groups is often at odds with personal liberty. (support by them for public access programs, subsidies, restrictions on businesses, etc.)
- We're also a more radical group in nearly every way, with various flavors of political extremism strongly represented. Mostly anarcho-capitalists and strong libertarians, and many "no compromises" privacy advocates. (As usual, my apologies to any Maoists or the like who don't feel comfortable being lumped in with the libertarians...if you're out there, you're not speaking up.) In any case, the house of Cypherpunks has many rooms.
- We were called "Crypto Rebels" in Steven Levy's "Wired" article (issue 1.2, early 1993). We can represent a *radical alternative* to the Beltway lawyers that dominate EFF, EPIC, etc. No need to compromise on things like Clipper, Software Key Escrow, Digital Telephony, and the NII. But, of course, no input to the legislative process.
- But there's often an advantage to having a much more radical, purist body out in the wings, making the "rejectionist" case and holding the inner circle folks to a tougher standard of behavior.
- And of course there's the omnipresent difference that we tend to favor direct action through technology over politicking.

13.7.6. Why is government control of crypto so dangerous?

- dangers of government monopoly on crypto and sigs
  - can "revoke your existence"

- no place to escape to (historically an important social relief valve)

13.7.7. NSA's view of crypto advocates

- "I said to somebody once, this is the revenge of people who couldn't go to Woodstock because they had too much trig homework. It's a kind of romanticism about privacy and the kind of, you know, "you won't get my crypto key until you pry it from my dead cold fingers" kind of stuff. I have to say, you know, I kind of find it endearing." [Stuart Baker, counsel, NSA, CFP '94]

13.7.8. EFF

- eff@eff.org

- How to Join
  - $40, get form from many places, EFFector Online,
  - membership@eff.org
- EFFector Online
  - ftp.eff.org, pub/EFF/Newsletters/EFFector
- Open Platform
  - ftp://ftp.eff.org/pub/EFF/Policy/Open_Platform

- National Information Infrastructure

13.7.9. "How can the use of cryptography be hidden?"

- Steganography
  - microdots, invisible ink

- where even the existence of a coded message gets one shot + Methods for Hiding the Mere Existence of Encrypted Data

- in contrast to the oft-cited point (made by crypto purists) that one must assume the opponent has full access to the cryptotext, some fragments of decrypted plaintext, and to the algorithm itself, i.e., assume the worst

- a condition I think is practically absurd and unrealistic
- assumes infinite intercept power (same assumption of infinite computer power would make all systems besides one-time pads breakable)
- in reality, hiding the existence and form of an encrypted message is important

- this will be all the more so as legal challenges to crypto are mounted...the proposed ban on encrypted telecom (with $10K per day fine), various governmental regulations, etc.

- RICO and other broad brush ploys may make people very careful about revealing that they are even using encryption (regardless of how secure the keys are)

- steganography, the science of hiding the existence of encrypted information - secret inks - microdots - thwarting traffic analysis - LSB method
  - Packing data into audio tapes (LSB of DAT)
- LSB of DAT: a 2GB audio DAT will allow more than 100 megabytes in the LSBs

- less if algorithms are used to shape the spectrum to make it look even more like noise
- but can also use the higher bits, too (since a real- world recording will have noise reaching up to perhaps the 3rd or 4th bit)

- will manufacturers investigate "dithering" circuits? (a la fat zero?)

- but the race will still be on

- Digital video will offer even more storage space (larger tapes) - DVI, etc. - HDTV by late 1990s
- Messages can be put into GIFF, TIFF image files (or even noisy faxes)

- using the LSB method, with a 1024 x 1024 grey scale image holding 64KB in the LSB plane alone
- with error correction, noise shaping, etc., still at least 50KB
- scenario: already being used to transmit message through international fax and image transmissions
  - The Old "Two Plaintexts" Ploy
- one decoding produces "Having a nice time. Wish you were here."
- other decoding, of the same raw bits, produces "The last submarine left this morning."
- any legal order to produce the key generates the first message

- authorities can never prove-save for torture or an informant-that another message exists

- unless there are somehow signs that the encrypted message is somehow "inefficiently encrypted, suggesting the use of a dual plaintext pair method" (or somesuch spookspeak)
- again, certain purist argue that such issues (which are related to the old "How do you know when to stop?" question) are misleading, that one must assume the opponent has nearly complete access to everything except the actual key, that any scheme to combine multiple systems is no better than what is gotten as a result of the combination itself
  - and just the overall bandwidth of data...

13.7.10. next Computers, Freedom and Privacy Conference will be March 1995,

San Francisco

13.7.11. Places to send messages to

- cantwell@eff.org, Subject: I support HR 3627
- leahy@eff.org, Subject: I support hearings on Clipper

13.7.12. Thesis: Crypto can become unstoppable if critical mass is reached

- analogy: the Net...too scattered, too many countries, too many degrees of freedom
- so scattered that attempts to outlaw strong crypto will be futile...no bottlenecks, no "mountain passes" (in a race to the pass, beyond which the expansion cannot be halted except by extremely repressive means)

13.7.13. Keeping the crypto genie from being put in the bottle

- (though some claim the genie was never *in* the bottle, historically)
- ensuring that enough people are using it, and that the Net is using it
  - a *threshold*, a point of no return

13.7.14. Activism practicalities

- "Why don't we buy advertising time like Perot did?"
- This and similar points come up in nearly all political discussions (I'm seeing in also in talk.politics.guns). The main reasons it doesn't happen are: - ads cost a lot of money

- casual folks rarely have this kind of money to spend
- "herding cats" comes to mind, i.e., it's nearly impossible to coordinate the interests of people to gather money, set up ad campaigns, etc.
- In my view, a waste of efforts. The changes I want won't come through a series of ads that are just fingers in the dike. (More cynically, Americans are getting the government they've been squealing for. My interest is in bypassing their avarice and repression, not in changing their minds.)

- Others feel differently, from posts made to the list. Practically speaking, though, organized political activity is difficult to achieve with the anarchic nonstructure of the Cypherpunks group. Good luck!

13.8. The Battle Lines are Being Drawn

13.8.1. Clipper met with disdain and scorn, so now new strategies are being tried...

13.8.2. Strategies are shifting, Plan B is being hauled out

- fear, uncertainty, and doubt
- fears about terrorists, pornographers, pedophiles, money launderers

13.8.3. corporate leaders like Grove are being enlisted to make the Clipper case

13.8.4. Donn Parker is spreading panic about "anarchy" (similar to my own CA)

13.8.5. "What can be done in the face of moves to require national ID cards, use

official public key registries, adhere to key escrow laws, etc?"

- This is the most important question we face.
- Short of leaving the country (but for where?) or living a subsistence-level lifestyle below the radar screens of the surveillance state, what can be done?
  - Some possibilities, not necessarily good ones:
    - civil disobedience
      - mutilation of cards, "accidental erasure," etc.
- forgeries of cards...probably not feasible (we understand about digital sigs)
- creation of large black markets...still doesn't cover everything, such as water, electricity, driver's licenses, etc...just too many things for a black market to handle
- lobby against these moves...but it appears the momentum is too strong in the other direction

13.9. "What Could Make Crypto Use more Common?"

13.9.1. transparent use, like the fax machine, is the key

13.9.2. easier token-based key and/or physical metrics for security

- thumbprint readers
- tokens attached to employee badges
- rings, watches, etc. that carry most of key (with several bits remembered, and a strict "three strikes and you're out" system)

13.9.3. major security scares, or fears over "back doors" by the government,

may accelerate the conversion

- all it may take are a couple of very large scandals

13.9.4. insurance companies may demand encryption, for several reasons

- to protect against theft, loss, etc.
- to provide better control against viruses and other modifications which expose the companies they ensure to liability suits
- same argument cited by safe makers: when insurance companies demanded better safes, that's when customers bought them (and not before)

13.9.5. Networks will get more complex and will make conventional security systems unacceptable

- "Fortress" product of Los Altos Technologies
- too many ways for others to see passwords being given to a remote host, e.g., with wireless LANs (which will necessitate ZKIPS)
- ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)
  - the whole explosion in bandwidth

13.9.6. The revelations of surveillance and monitoring of citizens and corporations will serve to increase the use of encryption, at first by people with something to hide, and then by others. Cypherpunks are already helping by

spreading the word of these situations.

- a snowballing effect
- and various government agencies will themselves use encryption to protect their files and their privacy

13.9.7. for those in sensitive positions, the availability of new bugging methods will accelerate the conversion to secure systems based on encrypted telecommunications and the avoidance of voice-based systems

13.9.8. ordinary citizens are being threatened because of what they say on networks, causing them to adopt pseudonyms

- lawsuits, ordinary threats, concerns about how their employers will react (many employers may adopt rules limiting the speech of their employees, largely because of concerns they'll get sued)

- and some database providers are providing cross-indexed lists of who has posted to what boards-this is freely available information, but it is not expected by people that their postings will live forever
  - some may see this as extortion
  - but any proposed laws are unlikely to succeed

- so, as usual, the solution is for people to protect themselves via technological means

13.9.9. "agents" that are able to retransmit material will make certain kinds of anonymous systems much easier to use

13.10. Deals, the EFF, and Digital Telephony Bill

13.10.1. The backroom deals in Washington are flying...

apparently the Administration got burned by the Clipper fiasco (which they could partly write-off as being a leftover from the Bush era) and is now trying to "work the issues" behind the scenes before unveiling new and wide-reaching programs. (Though at this writing, the Health Bill is looking mighty amateurish and seems ulikely to pass.)

13.10.2. We are not hearing about these "deals" in a timely way.

I first heard that a brand new, and "in the bag," deal was cooking when I was talking to a noted journalist. He told me that a new deal, cut between Congress, the telecom industry, and the EFF-type lobbying groups, was already a done deal and would be unveiled so. Sure enough, the New and Improved Digital Telephony II Bill appears a few weeks later and is said by EFF representatives to be unstoppable. [comments by S. McLandisht and others, comp.org.eff.talk, 1994-08]

13.10.3. Well, excuse me for reminding everyone that this country is allegedly still

a democracy.

I know politics is done behinde closed doors, as I'm no naif, but deal-cutting like this deserves to be exposed and derided.

13.10.4. I've announced that I won't be renewing my EFF membership.

I don't expect them to fight all battles, to win all wars, but I sure as hell won't help *pay* for their backrooms deals with the telcos.

13.10.5. This may me in trouble with my remaining friends at the EFF,

but it's as if a lobbying groups in Germany saw the handwriting on the wall about the Final Solution, deemed it essentially unstoppable, and so sent their leaders to Berchtesgaden/Camp David to make sure that the death of the Jews was made as painless as possible. A kind of joint Administration/Telco/SS/IG Farben "compromise." While I don't equate Mitch, Jerry, Mike, Stanton, and others with Hitler's minions, I certainly do think the inside-the-Beltway dealmaking is truly disgusting.

13.10.6. Our freedoms are being sold out.

13.11. Loose ends

13.11.1. Deals, deals, deals!

- pressures by Administration...software key escrow, digital telephony, cable regulation
- and suppliers need government support on legislation, benefits, spectrum allocation, etc
- reports that Microsoft is lobbying intensively to gain control of big chunks of spectrum...could fit with cable set-top box negotiations, Teledesic, SKE, etc.

- EFF even participates in some of these deals. Being "inside the Beltway" has this kind of effect, where one is either a "player" or a "non-player." (This is my interpretation of how power corrupts all groups that enter the Beltway.) Shmoozing and a desire to help.

13.11.2. using crypto to bypass laws on contacts and trade with other countries

- one day it's illegal to have contact with China, the next day it's encouraged

- one day it's legal to have contact with Haiti, the next day there's an embargo (and in the case of Haiti, the economic effects fall on on the poor--the tens of thousands fleeing are not fleeing the rulers, but the poverty made worse by the boycott

- (The military rulers are just the usual thugs, but they're not "our" thugs, for reasons of history. Aristide would almost certainly be as bad, being a Marxist priest. Thus, I consider the breakin of the embargo to be a morally good thing to do.
- who's to say why Haiti is suddenly to be shunned? By force of law, no less!

13.11.3. Sun Tzu's "Art of War" has useful tips (more useful than "The Prince")

- work with lowliest
- sabotage good name of enemy
- spread money around
- I think the events of the past year, including...

13.11.4. The flakiness of current systems...

- The current crypto infrastructure is fairly flaky, though the distributed web-of-trust model is better than some centralized system, of coure. What I mean is that many aspects are slow, creaky, and conducive to errors.
- In the area of digital cash, what we have now is not even as advanced as was seen with real money in Sumerian times! (And I wouldn't trust the e-mail "message in a bottle" approach for any nontrivial financial transactions.)
- Something's got to change. The NII/Superhighway/Infobahn people have plans, but their plans are not likely to mesh well with ours. A challenge for us to consider.

13.11.5. "Are there dangers in being too paranoid?"

- As Eric Hughes put it, "paranoia is cryptography's occupational hazard."

- "The effect of paranoia is self-delusion of the following form--that one's possible explanations are skewed toward malicious attacks, by individuals, that one has the technical knowledge to anticipate. This skewing creates an inefficient allocation of mental energy, it tends toward the personal, downplaying the possibility of technical error, and it begins to close off examination of technicalities not fully understood. "Those who resist paranoia will become better at cryptography than those who do not, all other things being equal. Cryptography is about epistemology, that is, assurances of truth, and only secondarily about ontology, that is, what actually is true. The goal of cryptography is to create an accurate confidence that a system is private and secure. In order to create that confidence, the system must actually be secure, but security is not sufficient. There must be confidence thatthe way by which this security becomes to be believed is robust and immune to delusion. "Paranoia creates delusion. As a direct and fundamental result, it makes one worse at cryptography. At the outside best, it makes one slower, as the misallocation of attention leads one down false trails. Who has the excess brainpower for that waste? Certainly not I. At the worst, paranoia makes one completely ineffective, not only in technical means but even more so in the social context in which cryptography is necessarily relevant." [Eric Hughes, 1994-05-14]
  - King Alfred Plan, blacks
    - plans to round up 20 million blacks
    - RFK, links to LAPD, Western Goals, Birch, KKK
    - RFA #9, 23, 38

- organized crime situation, perhaps intelligence community - damaging to blacks, psychological

13.11.6. The immorality of U.S. boycotts and sanctions

- as with Haiti, where a standard and comparatively benign and harmless military dictatorship is being opposed, we are using force to interfere with trade, food shipments, financial dealings, etc.
- invasion of countries that have not attacked other countries...a major new escalation of U.S. militarism
  - crypto will facillitate means of underming imperialism

13.11.7. The "reasonableness" trap

- making a reasonable thing into a mandatory thing
- this applies to what Cypherpunks should ever be prepared to support

- An example: A restaurant offers to replace dropped items (dropped on the floor, literally) for free...a reasonable thing to offer customers (something I see frequently). So why not make it the law? Because then the reasonable discretion of the restaurant owner would be lost, and some customers could "game against" (exploit the letter of the law) the system. Even threaten lawsuits.

- (And libertarians know that "my house, my rules" applies to restaurants and other businesses, absent a contract spelling exceptions out.)
- A more serious example is when restaurants (again) find it "reasonable" to hire various sorts of qualified people. What may be "reasonable" is one thing, but too often the government decides to *formalize* this and takes away the right to choose. (In my opinion, no person or group has any "right" to a job unless the employer freely offers it. Yes, this could included discrimination against various groups. Yes, we may dislike this. But the freedom to choose is a much more basic right than achieving some ideal of equality is.)
- And when "reasonableness" is enforced by law, the gameplaying increases. In effect, some discretion is needed to reject claims that are based on gaming. Markets naturally work this way, as no "basic rights" or contracts are being violated.
- Fortunately, strong crypto makes this nonsense impossible. Perforce, people will engage in contracts only voluntarily.

13.11.8. "How do we get agreement on protocols?"

- Give this idea up immediately! Agreement to behave in certain ways is almost never possible.
  - Is this an indictment of anarchy?
- No, because the way agreement is sort of reached is through standards or examplars that people can get behind. Thus, we don't get "consensus" in advance on the taste of Coca Cola...somebody offers Coke for sale and then the rest is history.
- PGP is a more relevant example. The examplar is on a "take it or leave it" basis, with minor improvements made by others, but within the basic format.

Revision #1
Created 23 June 2022 03:56:07 by c0mmando
Updated 23 June 2022 03:57:57 by c0mmando