6. The Need For Strong Crypto

6.1. copyright

6.2. SUMMARY: The Need For Strong Crypto

6.2.1. Main Points

- Strong crypto reclaims the power to decide for one's self, to deny the "Censor" the power to choose what one reads, watches, or listens to.

6.2.2. Connections to Other Sections

6.2.3. Where to Find Additional Information

6.2.4. Miscellaneous Comments

- this section is short, but is less focussed than other sections; it is essentially a "transition" chapter.

6.3. General Uses of and Reasons for Crypto

6.3.1. (see also the extensive listing of "Reasons for Anonymity," which makes many points about the need and uses for strong crypto)

6.3.2. "Where is public key crypto really needed?"

- "It is the case that there is relatively little need for asymmetric key cryptography in small closed populations. For example, the banks get along quite well without. The advantage of public key is that it permits private communication in a large and open population and with a minimum of prearrangement." [WHMurray, sci.crypt, 1994-0825]
- That is, symmetric key systems (such as conventional ciphers, one time pads, etc.) work reasonably well by prearrangement between parties. And of course one time pads have the additional advantage of being information- theoretically secure. But asymmetric or public key methods are incredibly useful when: the parties have not met before, when key material has not been exchanged, and when concerns exist about storing the key material. The so- called "key management problem" when N people want to communicate pairwise with each other is well-founded.
- And of course public key crypto makes possible all the other useful stuff like digital money, DC-Nets, zero knowledge proofs, secret sharing, etc.

6.3.3. "What are the main reasons to use cryptography?"

- people encrypt for the same reason they close and lock their doors
  - Privacy in its most basic forms
    - text -- records, diaries, letters, e-mail
    - sound -- phone conversations
    - other --video

- phones, intercepts, cellular, wireless, car phones, scanners + making listening illegal is useless (and wrong-headed)

- and authorites are exempt from such laws
  - people need to protect, end to end

- "How should I protect my personal files, and my phone calls?"

- Personally, I don't worry too much. But many people do. Encryption tools are widely available.
- Cellular telephones are notoriously insecure, as are cordless phones (even less secure). There are laws about monitoring, small comfort as that may be. (And I'm largely opposed to such laws, for libertarian reasons and because it creates a false sense of security.)
- Laptops are probably less vulnerable to Van Eck types of RF monitoring than are CRTs. The trend to lower power, LCDs, etc., all works toward decreasing vulnerability. (However, computer power for extracting weak signals out of noise is increasing faster than RF are decreasing...tradeoffs are unclear.)
  - encrypting messages because mail delivery is so flaky
- that is, mail is misdelivered,via hosts incorrectly processing the addresses
- encryption obviously prevents misunderstandings (though it does little to get the mail delivered correctly)
  - Encryption to Protect Information
    - the standard reason
    - encryption of e-mail is increasing
- the various court cases about employers reading ostensibly private e-mail will sharpen this debate (and raise the issue of employers forbidding encryption; resonances with the mostly-settled issue of reasonable use of company phones for private calls-more efficient to let some personal calls be made than to lose the time of employees going to public phones)

- encryption of faxes will increase, too, especially as technology advances and as the dangers of interception become more apparent

- also, tighter links between sender and receive, as opposed to the current "dial the number and hope it's the right one" approach, will encourage the additional use of encryption
- "electronic vaulting" of large amounts of information, sent over T1 and T3 data networks, e.g., backup material for banks and large corporations

- the miles and miles of network wiring within a corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan, and so on-cannot all be checked for taps...who would even have the

records to know if some particular wire is going where it should? (so many undocumented hookups, lost records, ad hoc connections, etc.)

- the solution is to have point-to-point encryption, even withing corporations (for important items, at least)
  - wireless LANs

- corporations are becoming increasingly concerned about interception of important information-or even seemingly minor information-and about hackers and other intruders - calls for network security enhancement - they are hiring "tiger teams" to beef up security + cellular phones

- interceptions are common (and this is becoming publicized)
- modifications to commercial scanners are describe in newsletters
- something like Lotus Notes may be a main substrate for the effective introduction of crypto methods (ditto for hypertext)
- encryption provides "solidity" to cyberspace, in the sense of creating walls, doors, permanent structures
- there may even be legal requirements for better security over documents, patient files, employee records, etc.

- Encryption of Video Signals and Encryption to Control Piracy

- this is of course a whole technology and industry
- Videocypher II has been cracked by many video hackers
- a whole cottage industry in cracking such cyphers
- note that outlawing encryption would open up many industries to destruction by piracy, which is yet another reason a wholesale ban on encryption is doomed to failure
- Protecting home videos--several cases of home burglaries where private x-rated tapes of stars were taken, then sold (Leslile Visser, CBS Sports)
- these general reasons will make encryption more common, more socially and legally acceptable, and will hence make eventual attempts to limit the use of crypto anarchy methods moot
  - Digital Signatures and Authentication

- for electronic forms of contracts and digital timestamping

- not yet tested in the courts, though this should come soon (perhaps by 1996)

- could be very useful for proving that transactions happened at a certain time (Tom Clancy has a situation in "Debt of Honor" in which all Wall Street central records of stock trades are wiped out in a software scheme: only the records of traders are useful, and they are worried about these being fudged to turn profits...timestamping would help immensely)

- though certain spoofs, a la the brilliant penny scam, are still possible (register multiple trades, only reveal the profitable ones)
  - negotiations

    - AMIX, Xanadu, etc.

- is the real protection against viruses (since all other scanning methods will increasingly fail)

- software authors and distributors "sign" their work...no virus writer can possibly forge the digital signature
    - Proofs of identity, passwords, and operating system use
- ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)

- operating systems and databases will need more secure procedures for access, for agents and the like to pay for services, etc. - unforgeable tokens
    - Cyberspace will need better protection
        - to ensure spoofing and counterfeiting is reduced (recall Habitat's problems with people figuring out the loopholes)
- if OH is also working on "world- building" at Los Alamos, he may be using evolutionary systems and abstract math to help build better and more "coherent" worlds

- agents, demons, structures, persistent objects
- encryption to protect these structures

- the abstract math part of cyberspace: abstract measure spaces, topologies, distance metrics

- may figure in to the balance between user malleabilty and rigidity of the space
- Chaitin's AIT...he has obtained measures for these
    - Digital Contracts
        - e-mail too easily forged, faked (and lost, misplaced)
        - Anonymity
            - remailing
            - law avoidance
            - samizdats,
    - Smart cards, ATMs, etc.
    - Digital Money
    - Voting
    - Information Markets
        - data havens, espionage
    - Privacy of Purchases
        - for general principles, to prevent a surveillance society
        - specialized mailing lists
            - vendors pay to get names (Crest labels)
            - Smalltalk job offers
- in electronic age, will be much easier to "troll" for specialized names
- people will want to "selectively disclose" their interests (actually, some will, some won't)

6.3.4. "What may limit the use of crypto?"

- "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

- 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...

- 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 (regulatory arbitrage)
- 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

6.3.5. "What are some likely future uses of crypto?"

- Video conferencing: without crypto, or with government access, corporate meetings become public...as if a government agent was sitting in a meeting, taking notes. (There may be some who think this is a good idea, a check on corporate shenanigans. I don't. Much too high a price to pay for marginal or illusory improvements.)
  - presenting unpopular views

    - getting and giving medical treatments
        - with or without licenses from the medical union (AMA)
        - unapproved treatments
    - bootleg medical treatments
    - information markets
    - sanctuary movements, underground railroads
        - for battered wives
        - and for fathers taking back their children
        - (I'm not taking sides)
    - smuggling
    - tax evasion
    - data havens
    - bookies, betting, numbers games
    - remailers, anonymity
    - religious networks (digital confessionals)
    - digital cash, for privacy and for tax evasion
    - digital hits
- newsgroup participation -- archiving of Netnews is commonplace, and increases in storage density make it likely that in future years one will be able to purchase disks with "Usenet, 1985-1995" and so forth (or access, search, etc. online sites)

6.3.6. "Are there illegal uses of crypto?"

- Currently, there are no blanket laws in the U.S. about encryption.

- There are specific situations in which encryption cannot be freely used (or the use is spelled out)
    - over the amateur radio airwave...keys must be provided
- Carl Elllison has noted many times that cryptography has been in use for many centuries; the notion that it is a "military" technology that civilians have some how gotten ahold of is just plain false.

- and even public key crypto was developed in a university (Stanford, then MIT)

6.4. Protection of Corporate and Financial Privacy

6.4.1. corporations are becoming increasingly concerned about interception of important information-or even seemingly minor information-and about hackers and other intruders

- calls for network security enhancement
- they are hiring "tiger teams" to beef up security

- cellular phones

- interceptions are common (and this is becoming publicized)
- modifications to commercial scanners are describe in newsletters
- something like Lotus Notes may be a main substrate for the effective introduction of crypto methods (ditto for hypertext)

6.4.2. Corporate Espionage (or "Business Research")

- Xeroxing of documents
  - recall the way Murrray Woods inspected files of Fred Buch, suspecting he had removed the staples and Xeroxed the documents for Zilog (circa late 1977)
  - a precedent: shapes of staples
  - colors of the paper and ink...blues, for example
    - but these low-tech schemes are easy to circumvent
- Will corporations crack down on use of modems?
- after all, the specs of a chip or product could be mailed out of the company using the companies own networks!

- applies to outgoing letters as well (and I've never heard of any company inspecting to this detail, though it may happen at defense contractors)
  - and messages can still be hidden (covert channels)
- albeit at much lower bandwidths and with more effort required (it'll stop the casual leakage of information)
- the LSB method (though this still involves a digital storage means, e.g., a diskette, which might be restricted)
- various other schemes: buried in word processing format (at low bandwidth)

- subtleties such as covert channels are not even considered by corporations-too many leakage paths!

- it seems likely that government workers with security clearances will face restrictions on their access to AMIX- like systems, or even to "private" use of conventional databases

- at least when they use UseNet, the argument will go, they can be overseen to some extent
  - Offsite storage and access of stolen material

- instead of storing stolen blueprints and schematics on company premises, they may be stored at a remote location

- possiby unknown to the company, via cryptoanarchy techniques

- "Business research" is the euphemism for corporate espionage
  - often hiring ex-DIA and CIA agents
- American companies may step up their economic espionage once it is revealed just how extensive the spying by European and Japanese companies has been
  - Chobetsu reports to MITI
  - Mossad aids Israeli companies, e.g., Elscint. Elbit
- Bidzos calls this "a digital Pearl Harbor" (attacks on network security)

- would be ironic if weaknesses put into encryption gear came back to haunt us

- corporations will want an arms length relationship with corporate spies, to protect themselves against lawsuits, criminal charges, etc.
  - third party research agencies will be used

6.4.3. Encryption to Protect Information

- the standard reason

- encryption of e-mail is increasing

- the various court cases about employers reading ostensibly private e-mail will sharpen this debate (and raise the issue of employers forbidding encryption; resonances with the mostly-settled issue of reasonable use of company phones for private calls-more efficient to let some personal calls be made than to lose the time of employees going to public phones)

- encryption of faxes will increase, too, especially as technology advances and as the dangers of interception become more apparent

- also, tighter links between sender and receive, as opposed to the current "dial the number and hope it's the right one" approach, will encourage the additional use of encryption

- "electronic vaulting" of large amounts of information, sent over T1 and T3 data networks, e.g., backup material for banks and large corporations

- the miles and miles of network wiring within a corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan, and so on-cannot all be checked for taps...who would even have the records to know if some particular wire is going where it should? (so many undocumented hookups, lost records, ad hoc connections, etc.)

- the solution is to have point-to-point encryption, even withing corporations (for important items, at least)
    - wireless LANs
- encryption provides "solidity" to cyberspace, in the sense of creating walls, doors, permanent structures
- there may even be legal requirements for better security over documents, patient files, employee records, etc.

6.4.4. U.S. willing to seize assets as they pass through U.S. (Haiti, Iraq)

6.4.5. Privacy of research

- attacks on tobacco companies, demanding their private research documents be turned over to the FDA (because tobacco is 'fair game" for all such attacks, ...)

6.4.6. Using crypto-mediated business to bypass "deep pockets" liability suits, abuse of regulations, of the court system, etc.

- Abuses of Lawsuits: the trend of massive judgments...several million for a woman burned when she spilled hot coffee at a MacDonald's ($160K for damages, the rest for "punitive damages")
    - billions of dollars for various jury decisions

- "deep pockets" lawsuits are a new form of populism, of de Tocqueville's pocket-picking

- For example, a shareware author might collect digital cash without being traceable by those who feel wronged
- Is this "right"? Well , what does the contract say? If the customer bought or used the product knowing that the author/seller was untraceable, and that no additional warranties or guarantees were given, what fraud was committed?
- crypto can, with some costs, take interactions out of the reach of courts
- replacing the courts with PPL-style private-produced justice

6.4.7. on anonymous communication and corporations

- Most corporations will avoid anonymous communications, fearing the repercussions, the illegality (vis-a-vis antitrust law), and the "unwholesomeness" of it
- Some may use it to access competitor intelligence, offshore data havens, etc.
- Even here, probably through "arm's length" relationships with outside consultants, analogous to the cutouts used by the CIA and whatnot to insulate themselves from charges
- Boldest of all will be the "crypto-zaibatsu" that use strong crypto of the crypto anarchy flavor to arrange collusive deals, to remove competitors via force, and to generally pursue the "darker side of the force," to coin a phrase.

6.5. Digital Signatures

6.5.1. for electronic forms of contracts

- not yet tested in the courts, though this should come soon (perhaps by 1996)

6.5.2. negotiations

6.5.3. AMIX, Xanadu, etc.

6.5.4. is the real protection against viruses (since all other scanning methods will increasingly fail)

- software authors and distributors "sign" their work...no virus writer can possibly forge the digital signature

6.6. Political Uses of Crypto

6.6.1. Dissidents, Amnesty International

- Most governments want to know what their subjects are saying...
- Strong crypto (including steganography to hide the existence of the communications) is needed
  - Myanmar (Burma) dissidents are known to be using PGP

6.6.2. reports that rebels in Chiapas (Mexico, Zapatistas) are on the Net, presumably using PGP

- (if NSA can really crack PGP, this is probably a prime target for sharing with the Mexican government)

6.6.3. Free speech has declined in America--crypto provides an antidote

- people are sued for expressing opinions, books are banned ("Loompanics Press" facing investigations, because some children ordered some books)

- SLAPP suits (Strategic Lawsuiits Against Public Participation), designed to scare off differing opinions by threatening legal ruination in the courts

- some judges have found for the defendants and ordered the SLAPPers to pay damages themselves, but this is still a speech-chilling trend
- crypto untraceability is good immunity to this trend, and is thus *real* free speech

6.7. Beyond Good and Evil, or, Why Crypto is Needed

6.7.1. "Why is cryptography good? Why is anonymity good?"

- These moral questions pop up on the List once in a while, often asked by someone preparing to write a paper for a class on ethics or whatnot. Most of us on the list probably think the answers are clearly "yes," but many in the public may not think so. The old dichotomy between "None of your damned business" and "What have you got to hide?"
- "Is it good that people can write diaried unread by others?" "Is it good that people can talk to each other without law enforcement knowing what they're saying?" "Is it good that people can lock their doors and hide from outsiders?" These are all essentially equivalent to the questions above.
- Anonymity may not be either good or not good, but the *outlawing* of anonymity would require a police state to enforce, would impinge on basic ideas about private transactions, and would foreclose many options that some degree of anonymity makes possible.
- "People should not be anonymous" is a normative statement that is impractical to enforce.

6.7.2. Speaking of the isolation from physical threats and pressures that cyberspace provides, Eric Hughes writes: "One of the whole points of anonymity and pseudonymity is to create immunity from these threats, which are all based upon the human body and its physical

surroundings. What is the point of a system of anonymity which can be pierced when something "bad" happens? These systems do not reject the regime of violence; rather, they merely mitigate it slightly further and make their morality a bit more explicit...I desire

systems which do not require violence for their existence and stability. I desire anonymity as an ally to break the hold of morality over culture." [Eric Hughes, 1994-08-31]

6.7.3. Crypto anarchy means prosperity for those who can grab it, those competent enough to have something of value to offer for sale; the clueless 95% will suffer, but that is only just. With crypto anarchy we can painlessly, without initiation of aggression, dispose of the nonproductive, the halt and the lame. (Charity is always possible, but I suspect even the liberal do-gooders will throw up their hands at the prospect of a nation of

mostly unskilled and essentially illiterate and innumerate workers being unable to get meaninful, well-paying jobs.)

6.7.4. Crypto gets more important as communication increases and as computing gets distributed

- with bits and pieces of one's environment scattered around
  - have to worry about security
- others have to also protect their own products, and yet still provide/sell access
  - private spaces needed in disparate locations...multinationals, teleconferencing, video

6.8. Crypo Needed for Operating Systems and Networks

6.8.1. Restrictions on cryptography--difficult as they may be to enforce--may also impose severe hardships on secure operating system design, Norm Hardy has made this point several times.

- Agents and objects inside computer systems will likely need security, credentials, robustness, and even digital money for transactions.

6.8.2. Proofs of identity, passwords, and operating system use

- ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)

- operating systems and databases will need more secure procedures for access, for agents and the like to pay for services, etc.
  - unforgeable tokens

6.8.3. An often unmentioned reason why encyption is needed is for the creation of private, or virtual, networks

- so that channels are independent of the "common carrier"

- to make this clear: prospects are dangerously high for a consolidation under government control of networks
  - in parallel with roads
  - and like roads, may insist on equivalent of licenses
    - is-a-person
    - bans on encryption

- The Nightmare Scenario: "We own the networks, we won't let anyone install new networks without our approval, and we will make the laws about what gets carried, what encryption can be used, and how taxes will be collected."
- Fortunately, I doubt this is enforceable...too many ways to create virtual networks...satellites like Iridium, fiber optics, ways to hide crypto or bury it in other traffic
  - cyberspace walls...

- more than just crypto: physical security is needed (and for much the same reason no "digital coin" exists)

- processes running on controlled-accesss machines (as with remailers)
  - access by crypto
  - a web of mutually suspicious machines may be sufficient
- robust cyberspaces built with DC-Net ("dining cryptographers") methods?

6.9. Ominous Trends

6.9.1. Ever-increasing numbers of laws, complexities of tax codes, etc.

- individuals no longer can navigate

6.9.2. National ID cards

- work permits, immigration concerns, welfare fraud, stopping terrorists, collecting taxes
  - USPS and other proposals

6.9.3. Key Escrow

6.9.4. Extension of U.S. law around the world

- Now that the U.S. has vanquished the U.S.S.R., a free field ahead of it for spreading the New World Order, led of course by the U.S.A. and its politicians.
  - treaties, international agreements
  - economic hegemony
  - U.N. mandates, forces,

6.9.5. AA BBS case means cyberspace is not what we though it was

6.10. Loose Ends

6.10.1. "Why don't most people pay more attention to security issues?"

- Fact is, most people never think about real security.
- Safe manufacturers have said that improvements in safes (the metal kind) 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.)
- Crypto is economics. People will begin to really care when it costs them.

6.10.2. What motivates an attackers is not the intrinsic value of the data but his perception of the value of the data.

6.10.3. Crypto allows more refinement of permissions...access to groups, lists

- beyond such crude methods as banning domain names or "edu" sorts of accounts

6.10.4. these general reasons will make encryption more common, more socially and legally acceptable, and will hence make eventual attempts to limit the use of crypto anarchy methods moot

6.10.5. protecting reading habits..

- (Imagine using your MicroSoftCashCard for library checkouts...)

6.10.6. Downsides

- loss of trust
- markets in unsavory things
- espionage

- expect to see new kinds of con jobs
  - confidence games
  - "Make Digital Money Fast"

6.10.7. Encryption of Video Signals and Encryption to Control Piracy

- this is of course a whole technology and industry
- Videocypher II has been cracked by many video hackers
- a whole cottage industry in cracking such cyphers
- note that outlawing encryption would open up many industries to destruction by piracy, which is yet another reason a wholesale ban on encryption is doomed to failure

---

Revision #1
Created 23 June 2022 03:44:47 by c0mmando
Updated 23 June 2022 03:45:43 by c0mmando