CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

13 NOVEMBER 1996
Revision 0

LECTURE 19

PASSWORDS, PRIVACY, DATA PROTECTION

SUMMARY

For the last 18 lectures of our course, we have looked at Classical Cryptography from the 'what' and 'how' viewpoints. We now look at the 'why' as pertains to passwords, privacy issues, and legal aspects of business and personal data protection. Cryptography is a common security theme for each of these issues. We need to expand our purview to modern or applied cryptography to understand the importance and worldwide scope of cryptography.

I will start with a presentation of Klein's excellent work on password vulnerability. [VACC] We will look at the issue of privacy - and the bundle of rights associated with it. [KENN], [HOFF], [ROSL] [HUTT] We will survey data protection legislation in the business and personal arenas -especially E-Mail systems. [ICC], [BIGE] We will enter the labyrinth of the ITAR and find that recreational and classical cryptography is exempt from ITAR regulations on at least three counts. [NIST], [ITAR] Lastly, I will briefly survey some applied cryptography themes.

PASSWORD VULNERABILITY

We remind ourselves that cryptography is the science of secret writing. Therefore, cryptography is used to protect our vital datafiles and records. It is estimated that more than 85% of all U.S. business, financial and personal records are stored in computer systems. We use passwords (keywords) to enter the maze of security levels to gain access to the various files, records, programs that affect our daily lives. These passwords are cryptographically treated after they are presented to the computer system and stored in that form. Next time you go to your favorite ATM machine, realize that it is cryptography protecting yours and the banks money. The principles that have been presented in this course are used in the same manner on more rigorous algorithms to provide cryptosecurity to modern day machines.

We live in an age of international - no boundary -computer networks capable of performing huge amounts of coordinated work to breach the security of our computer systems and pry open the secrets of lives. But how secure are our systems by virtue of their encrypted passwords? What is the weak link of the cryptosystem - the algorithm, the key or the key management?

Daniel V. Klein of LoneWolf Systems, Pittsburg, Pa. performed a study in 1989 using data from clients in both U.S. and Great Britain that would imply that the key (password) and its management is the weak link. He outlined some of the problems of current password security and demonstrated the ease with which individual accounts may be broken. [VACC] Although his study centered around the UNIX system, his results and conclusions were most general in nature and can not be ignored by users and system administrators of every type of computer system in the country.

UNIX VULNERABILITY

Forgetting for the moment that CPU speeds, computer architectures, and storage capabilities are more than 2 magnitudes of order faster and better in 1996 than what was available when Klein's work was performed in 1989. Klein was interested in the security of accounts and passwords on the UNIX system. Early Unix versions used a password encryption algorithm based on the M-209 U.S. Army cipher machine. The M-209 cipher machine exploits many of the security features we have discussed under aperiodic systems in Lecture 13. On a PDP-11/70, each encryption took approximately 1.25 ms, so that it was possible to check 800 passwords per second. Armed with a dictionary of 250,000 words, crackers could compare encryptions with all those stored in the password file in a little more than 5 minutes. This was a security hole that could be (and was exploited) on government and non-government machines all over the country.

After 1976, versions of UNIX, DES (Data Encryption Standard - to be discussed in a later lecture in detail) was used to encrypt passwords. The user's password was used as the DES key, and the algorithm was used to encrypt a constant.

The algorithm was iterated 25 times, with the results being an 11-character string plus a 2 character "salt." This method was more rigorous and difficult to decrypt. It was complicated through the introduction of one of 4,096 possible salt values and was slower to execute than its predecessor. On a VAX-II machine, a single encryption required about 280 ms, so that the determined cracker could only check about 3.6 encryptions per second. Checking the same 250,000 word dictionary would take 19 hours of CPU time. This reduced the "payoff ratio" for cracking a single password. Checking the passwords on a system with 50 accounts would take , on average, 40 CPU days because of the random selection of salt values practically guarantees that each user's password would be encrypted with a different salt, with no guarantee of success.

In the last 5 years three developments have pushed the problem of password security back into the forefront:

1. CPU speeds are lightning fast and readily available as desktop workstations. Special boards can be made to optimize the password comparisons. With internetworking, many sites have hundreds of individual workstations connected together, and enterprising crackers are discovering that the "divide and conquer" algorithm can be extended to multiple processors, especially at night when those processors are not otherwise being used.

2. New implementations of the DES algorithm have been developed, so that the time it takes to encrypt a password and compare the encryption against the stored value in a password file has dropped below the 1ms mark. Our 250,000 word dictionary can be processed in less than 5 minutes and by dividing the work across multiple workstations, the time required to encrypt these words against all 4,096 salt values is less than an hour. DES has been put into hardware implementation and the time for encryption is further reduced. This means the same dictionary can be cracked in only 1.5 seconds.

3. A study of passwords cracked showed that the user did not readily choose tough passwords but ones that he could remember. Furthermore, surveys show that the user is not concerned with system security but personal privacy. They are not aware that their terminal may become an entry point for a malicious cracker.

COLLECTION

Crackers have been using the same techniques for some time to acquire the password files on UNIX and VAX machines (all open system machines are susceptible):

1. They acquire a copy of the site's /etc/passwd file, either through an unprotected uucp link, well known holes in sendmail or via FTP or tpf or outright theft.

2. They apply the standard or sped up version of DES or the known password encryption algorithm to a collection of words, typically /usr/dict/words, plus some permutations on account and user names, and compare the encrypted results to those found in the purloined /etc/passwd file.

3. If a match is found (and often their are more than one), the cracker has access to the targeted machine. This modus operandi has been known for some time, defended, and still presents a viable alternative for the 'bad guys' for more than 50 per cent of the computers on the market.

KLEIN'S SURVEY

Klein built up a database of approximately 15,000 entries from U.S. and Great Britain of /etc/passwd files in order to try to crack the passwords. Each of the account entries was tested by a number of intrusion strategies. The possible passwords that were tried were based on the users name or account number, taken from numerous dictionaries (including some containing foreign words, phrases, patterns of keys on the keyboard, and enumerations) and from permutations and combinations of words in those dictionaries. After nearly 12 CPU-months of rather exhaustive testing, approximately 25 percent of the passwords have been guessed! 21 percent of the passwords (nearly 3000 passwords) were guessed in the first week and in the first 15 minutes of testing, 368 passwords (or 2.7 percent) had been cracked using what experience had shown would be the most fruitful line of attack (using the user or account names as passwords.)

These statistics are nothing less then frightening. On an average system with 50 accounts in the /etc/passwd file, one could expect the first account to be cracked in under two minutes, with 5 to 15 accounts being cracked by the end of the first day. Even though the root account might not be cracked, all it takes is one account being compromised for the cracker to have a toehold in the system. After that is done, any number of other well-known security loopholes (many of which are published on the network) can be used to access or destroy any information on the machine.

The results did not indicate what all the uncracked passwords were. Rather it showed that users are likely to use words that are familiar to them as their passwords. What new information it did provide, however, was the degree of vulnerability of the systems in question, as well as developing a basis for a proactive password checker. Passwords that can be derived from a dictionary are clearly a bad idea. There are hackers and companies in the business of developing this line of attack on computer systems. I recently downloaded some files in Russian from a site in Moscow that would indicate that others have known this principle too.

SAFE PASSWORDS?

Klein found three classes of 'safer' passwords. One class of more secure passwords was the word pair, where the password consists of two words, separated by a punctuation character. Compuserve uses this technique for their CIS network, but relies on too few punctuation marks too make this an effective deterrent to the clever cracker. Even considering words of only 3 - 5 lowercase characters, /usr/dict/words provide 3000 words for pairing. When a single intermediate punctuation character is introduced, the resulting sample size of 90,000,000 possible passwords is, in theory, rather daunting.

We know from our course that this is not true. Cipher text patterns carry through and are recognizable when using a known algorithm. The 'key space' that must be tested is substantially smaller with a smart dictionary of targeted information. A 'smart' brute force attack will be effective against the fixed length of the password, especially if the number of salt values and/or the number of punctuation marks are limited.

A second type of password introduces upper and lowercase characters into the password to raise the search set size to a magnitude that is more difficult to crack.

The third safe password is one constructed from the initial letters of any easily remembered, but not common, phrase. For example, the phrase "UNIX is a trademark of Bell Laboratories" could give rise to the password UiatoBL. This essentially creates a password that is a random string of upper and lowercase letters. Exhaustively searching this list at 1,000 tests per second with only 7-character passwords would require about 32 CPU-years - a very difficult task.

METHOD OF ATTACK

A number of techniques were used on the accounts in order to determine whether the passwords used for them could be compromised. To speed up the testing, Klein grouped all passwords with the same salt value together. This way, one encryption per password per salt value could be performed, with multiple string comparisons to test for matches. Rather than 15,000 accounts, the problem was reduced to 4,000 salt values. [VACC]

The password tests were as follows:

1. Name Variations

   Try using the users name, initials, account name, and other relevant personal information as a possible password. All in all, up to 130 different passwords were tried, based on this information.

   For the account name klone with a user named "David V. Klein," some of the password tried were: klone, klone0, klone1, klone123, dvk, dvkdvk, dklein, Dklein, leinad, nielk, dvklein, danielk, DvkkD, DANIEL-KLEIN, (klone), KleinD, and so on.

2. Dictionaries

   Try using words from various dictionaries. These included lists of women's and men's names (some 16,000 in all); places (including permutations, so that "spain," "spanish," and "spaniard" would be considered); names of famous people; cartoons and cartoon characters; titles, characters and locations of films and science fiction stories; mythical creatures (garnered from Bulfinch's mythology and dictionaries of mythical beasts); sports (including team names, nicknames, and specialized terms); numbers both as numerals - "2001" and written out - "twelve"); strings of letters and numbers ("a", "aa," "aaa," and so on); Chinese syllables (from the Pinyin Romanization of Chinese, an international standard system of writing Chinese on an English keyboard); the King James Bible; biological terms; common and vulgar phrases (such as "ibmsux" and "deadhead"); keyboard patterns (such as "QWERTY", "asdf" and "zxcvbn"); abbreviations (such as "roygbiv" - the colors in the rainbow, and "ooottafagvah" - a mnemonic for remembering the 12 cranial nerves); machine names (acquired from the /etc/hosts); characters, plays, and locations from Shakespeare; common Yiddish words; the names of asteroids; and a collection of words from various published technical papers. 60,000 separate words were considered per user (with the inter and intradictionary duplicates being discarded.

3. Permutations of Item 2

   Try various permutations on the words from step 2 Make the first letter uppercase or a control character, make the entire word uppercase, reversing the word(with and without the capitalization), changing the letter o to the digit 0, so the word scholar becomes sch0lar, performing similar manipulations on letter z to digit 2, letter s to digit 5. Make the word plural, so dress becomes dresses. Add suffixes of -ed -er -ing to transform words like phase to phased. These 14 to 17 additional tests per word added another 1,000,000 words to the list of possible passwords that were tested for each user.

4. Capitalization

   Try various capitalization permutations on the words in step 2. This included all single-letter capitalization permutations (so that michael would be checked as mIchael, miChael, and so forth,) double letter capitalization (MicHael) and triple letter capitalization (MIchAel). This added 400,000 more words to be tested for single-letter, 1,500,000 for double-letter and 3,000,000 more words for three-letter capitalization checks.

5. Foreign Words

   Try foreign words on foreign language users. Klein used Chinese words on users with Chinese names. Klein made exhaustive one-,two-,three syllable word tests on all 398 Chinese symbols for about 16,158,404 additional tests.

6. Word Pairs.

   Try word pairs. The magnitude of this test was staggering. Klein simplified the test to include words three and four characters in length from usr/dict/words. The number of words was order of magnitude 10**7 X 4096 possible salt values.

Klein used four linked DECstation 3100's to perform 3000 comparisons a second. The study ran for 20 CPU-months. The bulk of the effort was complete in the first 12 CPU-months.

SUMMARY OF RESULTS

The problem with using passwords that are derived directly from obvious words is that when users think "Hah, no one will ever guess this permutation," they are invariably wrong. Klein found a match on the "fylgjas," (guardian creature from Norse mythology. No matter what words or permutations thereof are chosen for a password, if they exist in some dictionary, they are susceptible to direct cracking. Table 19-1 shows the breakdown of passwords cracked in a sample size of 13,797 accounts.

Klein suggests four solutions for the 'key challenge': 1) use a proactive password checker; 2) eradicate easy-to- guess passwords (the user will normally defeat this approach); 3) Assign passwords - nonsense words or random characters (the user dislike this approach also); and 4) use smart cards which respond to electronic challenges from the computer security system.

TABLE 19-1

Passwords Cracked for Sample Set of 13,797 Accounts

Type of Password	Dictionary Size	Duplicates Eliminated	Search Size	Number of Matches	Percent of Total	Cost Benefit Ratio
User/ Account Name	130+	-	130	368	2.7%	2.830
Character Sequences	866	0	866	22	0.2%	0.025
Numbers	450	23	427	9	0.1%	0.021
Chinese	398	6	392	56	0.4%	0.143
Place Names	665	37	628	82	0.6%	0.131
Common Names	2,268	29	2,239	548	4.0%	0.245
Female Names	4,955	675	4,280	161	1.2%	0.038
Male Names	3,901	1,035	2,866	140	1.0%	0.049
Uncommon Names	5,559	604	4,955	130	0.0%	0.026
Myths and Legends	1,357	111	1,246	66	0.5%	0.053
Shakespearean	650	177	473	11	0.1%	0.023
Sports Terms	247	9	238	32	0.2%	0.134
Science Fiction	772	81	691	59	0.4%	0.085
Movies and Actors	118	19	99	12	0.1%	0.121
Cartoons	133	41	92	9	0.1%	0.098

Famous People	509	219	290	55	0.4%	0.190
Phrases and Patterns	998	65	933	253	1.8%	0.271
Surnames	160	127	33	9	0.1%	0.273
Biology	59	1	58	1	0.0%	0.017
/usr/dict/words	24,474	4,791	19,683	1,027	7.4%	0.052
Machine Names	12,983	3,965	9,018	132	1.0%	0.015
Mnemonics	14	0	14	2	0.0%	0.143
King James Bible	13,062	5,537	7,525	83	0.6%	0.011
Misc Words	8,146	4,934	3,212	54	0.4%	0.017
Yiddish Words	69	13	56	0	0.0%	0.000
Asteroids	3,459	1,052	2,407	19	0.1%	0.007
Total	86,280	23,553	62,727	3,340	24.2%	0.053

Table Notes

1. The number of matches is the total number of matches given for the particular dictionary, irrespective of the number of permutations that user applied to it.

2. Duplicate names were eliminated.

3. In all cases, the cost/benefit ratio is the number of matches divided by the search size. The more words that needed to be tested for a match, the lower the cost/benefit ratio.

4. The dictionary used for user/account names checks naturally changed for each user. Up to 130 different permutations were tried for each.

5. Although monosyllabic Chinese passwords were tried for all users (with 12 matches) polysyllabic Chinese passwords were tried only for users with Chinese names. The percentage of matches was 8.0% - a greater hit ratio than any other method but the dictionary size is 16 X 10**6, though, and the cost/benefit ratio is infinitesimal.

Klein's work is a professional success - if we are in the cracking business and a disheartening insight if you are in the security business.

The total size of the dictionary was only 62,727 words (not counting various permutations). This is much smaller than the 250,000-word dictionary postulated at the beginning of this lecture. Yet armed with even this small dictionary, nearly 25% of the passwords were cracked. It is easy to see how a professional organization could increase the dictionary and funding on the machinery and up the cost/benefit ratio significantly.

Table 19-2 shows the length of the cracked passwords.

TABLE 19-2

Length	Count	Percentage
1 Character	4	0.1%
2 Characters	5	0.2%
3 Characters	66	2.0%
4 Characters	188	5.7%
5 Characters	317	9.5%
6 Characters	1160	34.7%
7 Characters	813	24.4%
8 Characters	780	23.4%

The results of the word-pair tests are not included in either of the two tables. They represent another 0.4% of the passwords cracked in the sample.

PRIVACY REFERENCES/RESOURCES

When I started my research on this topic, I thought that there would be a lot of well-organized material available. In my opinion, only the first part of this wish was true. There a fair amount of history, an exciting growth of technology and a legal system that can not keep pace with the issues that have arisen because of the new technology. It would seem that only the money interests have been able to present their cases in the priority list. However, there is plenty of excellent material to work with.

Lance Rose gives a reasonable description of the laws applying to systems operators and on-line owners. [ROSL] Lance J. Hoffman has edited a superior group of papers which define some of the sides of the cryptographic debate. [HOFF] Professor Chandler, et. al. in cooperation with Martin Marietta Energy Systems, Inc. have produced a strong review of the U.S. Laws, Regulations, and Case Law pertaining to commercial encryption products. [CHAN] Charles E. H. Franklin has edited the summary work by ICC on business and private data protection legislation - worldwide. [ICC]

The National Computer Association has 21 proactive forums devoted to current computer security, encryption, privacy, government and civil liberties, legal and other issues. Hult et. al. have produced the definitive Computer Security Handbook; of special value is Professor Robert P. Bigelow's treatment of privacy laws and Dr. Diane E. Levine's treatment of data encryption.

Professor Bigelow discusses the legal aspects of computer privacy in the U.S. He covers a wide variety of topics: databases, state laws, 'The Public's Attitude', the Privacy Act of 1974, social security laws, The Computer Matching Act, Internal Revenue Service, privacy studies, employee privacy -drug testing and E-mail systems, monitoring and surveillance, taxpayer privacy, telecommunications privacy, and caller ID to name just a few. [HUTT], [BIGE]

John Vacca and Derek Atkins, et. al. have produced two of the best internet security books. [VACC], [NEWR] Bruce Schneier has produced the modern reference on professional cryptography algorithms. [SCH2] But James Nechvatal's State of the Art Survey on Public-Key Cryptography for NIST and NCSL is terrific. [NIST90]. Privacy Law and Practice, a three volume treatise edited by Professor George Trubow of John Marshall Law School, is probably the leading source in the United states. ACA's RENARD is a contributor and a very modest expert in the field of intellectual property rights law. NCSA provides an up to date source of information on the encryption legislation. Appendix 2 gives two of the most recent issues of interest: the Bernstein Case and the 56 bit key recovery proposal by the White House. There are other organizations like ACLU, EFF, EPIC and EDUPAGE that update the net regularly regarding privacy. Any netbrowser will find them. Don't forget that the government agencies CIA, NSA, DIA, DOD all have home pages as does the White House and various government- wide security consultants like SAIC.

INTRODUCTION TO PRIVACY ISSUES

Cryptography permits the private citizen to keep his life private. The national debate over cryptographic policy was captured by a speech delivered well before the personal computer was ever invented. In April, 1968, Thomas J. Watson Jr., Chairman of the Board of IBM, was discussing privacy in computer systems in an address to the Commonwealth Club of California.

"... the problem of privacy in the end is nothing more and nothing less than the root problem of the relation of each one of us to our fellow men.

What belongs to the citizen alone?

What belongs to society?

Those, at bottom, are the questions we face - timeless questions on the nature and place and destiny of man..."

These questions work equally well for cryptography.

Professor Robert P. Bigelow says that "we have computer security to protect us from people and people to protect us from computers." [HUTT] Caroline Kennedy points out that the word "privacy" does not appear in the United States Constitution. Yet ask anyone and they will tell you that they have a fundamental right to privacy. They will also tell you that privacy is under siege. [KENN] Professor Hoffman explains that the notion of privacy developed by the Courts grew as a natural process in support of the Bill Of Rights.

The notion that information can be kept secret to any degree vanished with the no territorial limits of cyberspace. Most important, computers assure that whatever is out there is assessable. No more roaming file-to-file. A kid can get in an access your information. What's more, because information exists in cyberspace rather than real space, it can be stolen "copied" without your knowing it. And someday soon, the whole universe of information about you -credit report, insurance records, medical history, employment history, you-name-it may be recorded on "smart cards" that will fit in your wallet. Brave New World surpassed.

Perhaps the biggest threat to our privacy comes in the area know as "information privacy." Information about all of us is collected not only by the old standbys, the IRS and FBI, but also by the MIB, NCOA, and NCIC, as well as credit bureaus, credit unions, credit card companies, mortgagers, banks and employers. We now have cellular phones, (not cordless or real phones), E-mail, Fax, voice mail, talking cars, talking elevators, and even junk mail on something called the Internet. Computers have changed our notion of privacy.

MIB

Actually , there has always been a lot of personal information about ourselves 'out there' but it was the computer that made this information readily available. The chip can store whole books of information for a very long time. The kinds of data are endless (and marketable.) Your medical history is likely to be in your doctors files, insurance companies files, laboratory files, and possibly the Medical Information Bureau (MIB) which collects medical data on some 15 million Americans and makes it available to insurance companies. [KENN]

NCOA

When you fill out a change-of-address card, the U.S. Post Office adds the information to its National Change Of Address (NCOA) database. The Post Office then helpfully passes on the list to list brokers, who license the information to certain direct marketers.

NCIC

The National Crime Information Center (NCIC) database contains over 23 million records identifying people and vehicles sought by the police. NCIC information is available by computer to approximately 71,000 local, state, and federal agencies across the country.

The above are just three examples of the more than 2000 databases that destroy our collective privacy. The Internet is a global network of databases. Our personal profiles are so complete and available, it is like having another self living in a parallel dimension; its a self you can't see, but effects your life just the same. Even if you don't own a computer, you have joined the revolution.

>From the privacy point of view, we are in the most unsettling period in this revolution. Technology is way ahead of the laws. Those well versed in computers already protect their communications with encryption. Many corporations do the same. For every means to secure privacy, we have generated methods to invade it.

The government (especially the FBI) is concerned that if criminals begin communicated electronically and scrambling their messages with cryptography, police cannot just tap in (like the wiretaps used against organized crime.) The government's solution was to come up with Clipper Chip, an approved method of encryption that requires trusted key escrow and permits law enforcement to decode with a warrant and then make the methodology standard in the industry. Privacy advocates are not happy, nor software companies, nor civil libertarians and Internet freedom advocates.

The animating principle of cyberspace is the free flow of information. It is the ultimate democracy, where principles of open records and unfettered speech prevail. This presents a problem to law enforcement, national security interests and intelligence operations.

PRIVACY AND OTHER PERSONAL RIGHTS

The law of privacy originally developed as a protection against individuals private affairs being reported in the press and against the exploitation of their names and pictures for advertising purposes. [HUTT], [BIGE]

The concept of computer informational privacy developed quickly after a proposal by the Bureau of the Budget (circa 1965) to establish a Federal Data Center to receive and store machine readable data in the possession of many branches of the federal government - approximately 30,000 computer tapes and 100 million punched cards. Congress at that time represented the people fairly well. There reaction was to hold hearings on whether such a center could protect individual privacy, since information from the IRS, the Census, the Bureau of Labor Statistics and Social Security might all be included.

Thomas J. Watson, Jr. then Chairman of the board of IBM (the major player in the field for many years) stated:

" Today the Internal Revenue Services has our tax returns. The Social Security Administration keeps a running record on our jobs and our families. The Veterans Administration has medical records on many of us, and the Pentagon our records of military service. So in this scatteration lies our protection. But put everything in one place, computerize it, and add to it without limit, and a thieving electronic blackmailer would have just one electronic safe to crack to get a victims complete dossier, tough as that job may be. And a malevolent Big Brother would not even have to do that: he could sit in his office, punch a few keys and arm himself with all he needed to know to crush any citizen who threatened his power. Therefore, along with the bugged olive in the martini, the psychological tests, and the spiked microphone, the critics have seen "data surveillance" as an ultimate destroyer of the individual American citizen's right to privacy- his right to call his soul his own. "

Think about the abuses of this type of power under Nixon; the hackers who can develop a detailed dossier on you within minutes by phone and modem; the new crime of stealing your "virtual" identity and charging thousands of dollars against your 'new' account at some immediate credit stores. Can you see where encryption would hinder this process abuse?

The public's concern with privacy has been rising steadily over the years. A Lou Harris poll on Americans concern about threats to personal privacy found that in 1970 34 percent were concerned. By 1993 83 percent were very concerned. [Privacy and American Business, October 1993, p3.]

THE FEDERAL PRIVACY ACT

Opposition to the federal data bank, spearheaded by IBM, was responsible for the fact that we do not have such a database (per se) today. With the help of under secretaries Elliot L. Richardson and Casper Weinberger of HEW, and sponsored by Senator Ervin of Watergate fame, and signed by President Ford on 1 January, 1975, The Privacy Act of 1974, P.L. 93-579 became law.

There is a basic rule that government files are open to the public, unless there is a specific reason, enacted by the legislature, saying that certain files are not available. At the federal level, this principle is demonstrated by the Freedom Of Information Act (FOIA) 5 U.S.C. sec. 552, under which a citizen or organization can obtain most governmental records. The Privacy Act, most of which is codified at 5 U.S.C. sec 552a, applies only to records maintained by certain branches of the federal government, specifically executive departments, independent regulatory agencies, government corporations, and government-controlled corporations such as the Federal Reserve Banks. It is not applicable to Congress (of course) or to the District of Columbia. When corporations do business under federal agency contracts, the contractors employees are subject to the same rules under the Privacy Act, including criminal penalties for failure to comply with the act.

The act defines a "record" that is subject to it very broadly:

"Any item, collection, or grouping of information about an individual that is maintained by an agency,including, but not limited to , his education, financial transactions, medical history, and criminal or employment history and that contains his name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or a voice print or a photograph."

Agencies can maintain information about individuals only when it is relevant and necessary to accomplish the agency's purpose. The act prohibits the disclosure of any record except within the agency maintaining it unless the individual makes a written request for the data; there are exceptions. The agency must give public notice of the existence of each record system, (The 1993 listing of records systems of just the DOD consumed 935 pages of the Federal Register.) including any proposal to match the record against those of another federal or state agency, keep track of certain disclosures, and establish rules of conduct for those who design, and operate the systems. [58 Fed Reg. 10002-10935, 22 February 1993] [The Computer Matching and Privacy Act of 1988, P.L. 100-503, added subsections (0) to 5 U.S.C. sec. 552a.]

The act also states:

"{agency must} establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." [subsection (e)(10)] [HUTT]

Investigative records maintained by CIA, FBI and other law enforcement agencies as well as national defense secrets are completely except from the act's operation.

If an individual proves that an agency intentionally or willfully violated the Privacy Act, fines up to $5,000 per individual violation may be recovered as damages.

The act also established specific rules prohibiting any federal, state or local governmental agency from denying an individual benefits or privileges because he/she refused to disclose a Social Security Number. [P.L. 93- 579, sec. 7. requires the governmental agency asking for the SSN to "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."] This also shows what significance is put on the SSN as a entry key to most federal databases. It also gives you the prime target of data or ID thieves. A effective countermeasure would be to encrypt the information. The notable exception to the rule is the requirement for SSN's for drivers licenses.

Out of this act has come a Privacy Protection Commission to make recommendations to Congress. (most not passed!) and an outgrowth called privacy implications of the National Information Infrastructure Superhighway system. Vice President Al Gore is currently leading the charge on this one. The OMB has published an interesting report on protecting intellectual property and privacy called "National Information Infrastructure:Draft Principles for Providing and Using Personal Information and Commentary," 60 Fed. Reg. 4362, 20 January, 1995.

STATE ACTS AND REGULATIONS

Like the FOIA, most states have Public Records Acts modelled after it and whose basic thrust is to make all records available to the citizen, subject to exceptions for law enforcement, trade secrets, and the like. Several states have enacted Fair Information Practices Acts regulating the information that state agencies could maintain about individuals. several states have enacted Uniform Information Practices Code and one municipality, Berkeley, California has enacted a citywide ordinance on privacy.

EMPLOYEE RIGHTS

In addition to the legal protections against discrimination available to all employees, and the right to advance warning in layoff situations, serious problems have arisen from electronic E-Mail and drug testing. With respect to E-mail (hence a push for PGP and PEM cryptosystems to protect the mail) invasion of privacy claims for employees have been for the most part unsuccessful. Drug testing suits have been partially successful against the employer.

INTERNATIONAL PRIVACY

A number of European countries also have privacy acts covering both governmental and private corporate records. Most of the laws apply to computerized data banks, which must be licensed by a governmental authority.

The rules of disclosure are quite strict, and there are particular prohibitions against the transfer of information in these databanks across national boundaries. [ICC: this reference is the 'bible' of business and data protection legal requirements in foreign countries.]

A DEEPER LOOK AT ELECTRONIC MAIL

Federal law prohibits the intentional interception of wire, oral or electronic communications. This does not, however, require that telephone companies offering cellular service provide for the encryption of such conversations, even though they can be intercepted. [Shubert v Metrophone, Inc., 898 F. 2d 401 (3d Cir 1990)] The Electronic Communications Privacy Act of 1980, (47 U.S.C. 551) is strictly interpreted; in one case the disclosure by an attorney to the district attorney and to the court of illegal acts of police officers, as shown by their intercepted telephone calls, resulted in his being fined $20,000. [Rodgers v Wood. 910F. 2d 444 (7th Cir. 1990)]

It is not yet clear whether this law applies to the intentional reading by those in control of a bulletin board or a company's electronic mail of the messages sent over the system. In Thompson v Predaina [S.D. Indiana, #88-93C, dismissed voluntarily August 10, 1988] plaintiff, a law student, alleged that the defendant, a bulletin board operator, saved and distributed messages that the plaintiff had ordered deleted. The complaint includes counts under 18 U.S.C. 2520 and 2707. [Detail analysis 41 Fed Comm. L.J. 17 (November 1988)] It has been held that the operator of an electronic bulletin board is not liable for defamation absent actual knowledge of the allegedly defamatory statement. [Cubby v Compuserve, Inc. F. Supp. 3 CCH Comp. Cas. para 46,547 (S.D.N.Y. 1991)]

In March 1990 Alana Shoars sued her former employer, Epson America, alleging that her supervisor read and printed out her electronic mail (and that of other employees), and she was fired when she complained. A class action suit was filed in July, 1990. [The damages were $75,000,000. The case was widely covered in the trade press. see BIGE or HUTT]. A similar action against Nissan was file in January, 1991 and a suit has been filed against the FBI to determine whether it is monitoring the bulletin boards of political organizations. [HUTT] Suit has been threatened against the Prodigy network as a bulletin board to complain against the rate increase to cover monitoring of offensive language and denial of service to those who use it or send insults.

DATA PROTECTION AND DATA ENCRYPTION: A VIEW OF MODERN CHALLENGES

The previous section on E-Mail shows that people get angry when their mail is intercepted - who owns the mail system or on-line service doesn't matter. It is not surprising that encryption of E-Mail has grown to major proportions. With the advent of the computer and telecommunications, the most effective means of secreting messages is through the use of cryptology or a cryptosystem. We know that. We have studied classical cryptosystems for the last several months. The focus has been on private key (password; keyword) systems. These are also known as symmetric key or private key systems.

Trusted Information Systems

Cryptography is big business. Trusted Information Systems (TIS) conducted a survey of companies making products that employ cryptography both within and outside the U.S. Appendix 1 presents companies and countries reported in their survey as of June 1996. TIS identified 1262 products worldwide. The TIS survey is summarized by company and location.

The detailed products listing and company contact information may be found at:

http://www.tis.com/crypto/

This is not a static list. TIS updates it weekly. I read in the (11 November 1996) Edupage that Phelps Dodge plans to market in Japan a scrambler/decoder that works on 128 bit keys. Since 40 bits is the maximum (56 bits under the temporary position of the White House proposal) under ITAR regulations, and the government supports a trusted third party key escrow via the Clipper chip, I suspect that Phelps may have a challenge on its hands. Since I have brought up the subject of ITAR, lets take a brief side trip.

CLASSICAL CRYPTOGRAPHY / RECREATIONAL CRYPTOGRAPHY

The U.S. International Trade in Arms Regulations (ITAR)

All modern cryptography is subject to the famous ITAR regulations that put cryptography on the munitions list and requiring licensing prior to export. A license is required regardless of the manner in which the technical data is transmitted, whether the transfer is in person, by telephone, through correspondence or electronically. [22 C.F.R. para 125.2] Appendix 3 presents some of the pertinent sections. The entire ITAR file of 125 pages has been transmitted to the Crypto Drop Box for the student to download. Appendices 2 and 4 illustrate current issues in the debate about modern cryptography. The export license is required for the export of unclassified technical data. Category XIII (b) 1 of the Munitions Control List covers cryptographic equipment.

ITAR EXCEPTIONS

ITAR govern what products can and cannot be subjected to export controls. These regulations clearly define a set of conditions in which information considered to be in the "public domain" can not be subject to these controls. In the ITAR itself, public domain is defined as information published and that is generally accessible or available to the public:

o through sales at bookstores

o at libraries

o through patents available at the patent office, and

o through public release in any form after approval by the cognizant U.S. Government department or agency.

Recreational and Classical Cryptography, i.e. everything taught in my class, falls under the first two and last exception to the ITAR regulations. [ITAR], [HOFF]

PURPOSE OF ENCRYPTION

Recall from Lecture 1 that in a cryptosystem plaintext is acted upon by a known algorithm (set of mathematical rules to determine the transformation process to cipher-text) and a key which controls the encryption / decryption algorithm to transform the data into cipher-text. In a system using a key, the message cannot be transformed without the key. Two types of key systems exist: symmetric or private key systems and asymmetric, or public key systems.

The basic purpose of encryption (beyond enjoyment for some of us as in ACA recreational cryptography) is to protect sensitive data from unauthorized disclosure. When computer systems are involved, this data can be data stored within the system or data transmitted across insecure public carriers.

A sender authorizes a transmission medium to carry a message to a receiver. The message is exposed during the transmittal and subject to possible eavesdropping and /or alteration. Any intruder who intercepts the message might be able to interrupt it or modify it (which includes possibly fabricating a false but authentic -looking message.)

The availability of the message is affected if the intruder successfully interrupts the transmission. The confidentiality, or secrecy, of the message is affected when it is intercepted because the intruder can read it, know its intentions, plan countermeasures or modify the message for his own advantage. If the authentic- looking but false message is successful substituted, then we have an integrity issues as well.

Modern encryption methods are used to prevent the exposures previously defined and offer desirable features such as:

Data Confidentiality, or Secrecy, since messages must be decrypted in order for information to be understood.

Data Integrity because some algorithms additional protect against forgery or tampering.

Authentication of Message Originator, if the key has not been compromised and remains secret.

Authentication of System User takes place by the user performing a cryptographic function with a unique cryptographic key.

Electronic Certification and Digital Signature, using cryptographic algorithms to protect against unauthorized modification and forgery of electronic documents.

Nonrepudiation, using secret key where either the sender alone or only the sender and recipient can generate "signed" messages. This is very important in the making of electronic contracts.

MODERN CRYPTOGRAPHY: USING PRIVATE AND PUBLIC CRYPTOGRAPHIC KEYS

Classical Cryptography Course, Volume I and II concentrate on symmetric ciphers of increasing levels of difficulty. The two basic types of encryption are substitution and transposition. We have studied cases where both are applied to the cipher to increase its security.

Most complex ciphers do not use either simple substitutions or permutations (transpositions), relying instead on a secret key (K) which controls a long sequence of complicated substitutions and permutations. The ciphertext message then depends on both the plaintext message and the key value, as demonstrated by equation 1:

$$C = E(K, P) \qquad \text{eq. 1}$$

The key (K) modifies the specific encryption algorithm (E), which is then applied to transform the plaintext (P) into ciphertext (encrypted message) (C).

Use of a key provides additional security because its value, as well as the encryption algorithm, is required in order to decrypt information. Two types of systems use keys: private key and public key systems.

Private key systems (symmetric) use a single key to both encrypt and decrypt information. A separate key is needed for each pair of users. Security depends on protection and secrecy of the key. The best known private key system is the Data Encryption Standard, first introduced to the public in 1977.

Public key systems, (asymmetric) or two-key, systems use a public and a private key. The public key is publicly known, even published, but the user must keep the private key completely secret. The best known public key system is the Rivest, Shamir, and Adelman (RSA) algorithm.

In public key systems, the public and private keys are mathematically related. Messages may be encrypted with the public key, but only can be decrypted by the recipient using the private key. great care must be exerted in protecting the keys because we always assume that the algorithm is known to a system perpetrator.

DATA ENCRYPTION STANDARD (DES)

DES is a private key 56-bit algorithm. The DES algorithm is published by the National Institute of Standards and Technology as Federal Information Processing Standard (FIPS) 46-2. (download from our CDB) It is the only published secret key system approved for protection of Federal unclassified information and adopted by American National Standards Institute (ANSI) for commercial applications. In 1986, the ISO organization recommended the use of DES as an international standard called DEA-1. The recommendation was withdrawn soon after. DES is widely used in financial applications to protect trillions of dollars of electronic funds transfers weekly. The key is a sequence of 8 bytes, each containing 7 key bits and one parity bit; it is crucial that the key remain secret.

DES uses substitution and transposition techniques applied alternatively. When DES encrypts a single block, the characters are scrambled 16 times ("rounds"), under control of the key, and this results in 64 bits of ciphertext. DES accommodates about 72 quadrillion key combinations.

DES is embedded in many commercial products and is popular with both government agencies and private companies. NSA publishes a list of evaluated endorsed DES products (NEDESPL). [HUTT]

KEY DISTRIBUTION DRAWBACK

A major problem with encryption is the secure distribution of encryption keys to multiple users across networks. Two parties using a secret key system have to agree on the key. Because it is not safe to transmit the key over the communication channel, the parties have to meet personally to agree on the key or exchange keys via a courier. There are vulnerabilities in both of these techniques. Alternatively, if the key itself is encrypted using a different (public key) algorithm, the key may be transmitted over a communications link.

RIVEST, SHAMIR, AND ADLEMAN ALGORITHM (RSA)

The best known public key algorithm is RSA. The keys are generated mathematically, in part by combining prime numbers. Each user has a public and a private key. Devised in 1978 at MIT, this system has 512 bit, and 1024 bit (in some commercial versions higher) keys and provides authentication in addition to encryption.

Typically, the sender encrypts his message using a secret-key algorithm. Next, the sender uses a public-key system to encrypt the secret key with the receiving party's public key. The sender transmits both the encrypted message and the encrypted key across the communication channel. The recipient decrypts the secret key first, by using his public key. Once the secret key has been decrypted, the recipient uses it to decrypt the main message. This type of cryptographic system is a hybrid.

With public-key cryptography, any party can use any public key to send an encrypted message. However, that message can only be decrypted by a party having the corresponding private key. [LEVD], [HUTT]

CRYPTOGRAPHIC NETWORKS

To form a cryptographic network, each network user should be provided with the same algorithm but with different keys so that messages sent by one node in the network can only be deciphered by the intended recipient node. Figures 19-1 to 19-3 show three different cryptographic networks. Each Kn represents a different key.

Figure 19-1
A Fully Connected End-To-End Network

```
ZDDD?      K6       ZDDD?
3 2 3 <---------->  3 4 3DDDD? K4
@DDDYD?             @DDDY    3
 3K1  @?K2           3 K5    3
 3     @DDDDDD?      3       3
ZDDD?       K3@DDDDDZDDD?    3
3 1 3 <-----------> 3 3 3    3
@DBDY               @DDDY    3
  @DDDDD<DDDDDD>DDDDDDDDDDDDDY
```

When end-to-end encryption is used, both the sender and receiver must be equipped with compatible hardware. After validating each other, the two units exchange encryted data. Messages are encrypted by the sender and decrypted only at the final destination.

Figure 19-2
A Link Encrypted Network

```
ZDD?    K1    ZDD?   K2      ZDD?   K3      ZDD?
31 3 <DDDDDD> 32 3 <DDDDDD>  33 3 <DDDDDD>  3 43
@DDY          @DDY           @DDY           @DDY
```

Link encryption involves a series of nodes, each of which decrypts, reads, and then re-encrypts the message as it is transmitted through the network. With link encryption, both source and the destination remain private, and no synchronization of special equipment is required. However, more nodes = more possibilities of the message being intercepted and/ or modified.

Figure 19-3
A Hybrid Network

```
      ZDD?    K1                K5  ZDD?
      32 3 >DDD?                ZDD<36 3
      @DDY     3                3   @DDY
               3                3
ZDD?    K2    ZDD?   K4       ZDD?   K6      ZDD?
31 3 DDDDDDD> 33 3 <DDDDDD->  35 3 <DDDDDDD  3 73
@DDY          @BDY            @DDY           @DDY
               3                3
      ZDD?     3                3   ZDD?
      34 3 >DDDY                @DD<38 3
      @DDY     K3               K7  @DDY
```

In a hybrid network, there is communication between a large number of secondary stations and a single main station all using separate master keys. A few stations intercommunicate with each other.

Figure 19-4
A Central Key Distribution Facility

```
                     ZDD?
           ZDDDDDDDDD 32 3   DD DD D?
                     @DDY          3
           3          3
                      3 K1         3
           3          3
                     ZDD?          3
           3         31 3
                     @DDY          3
           3          3
                      3            3
           3          3
          ZDD?   K2   3  K3       ZDD?
          34 3 D D D DAD D D DD   33 3
          @DDY                    @DDY
```

It would seem that preferable to use a public-key system for cryptography, because of its versatility, it is slower that the equivalent private key cryptosystems, by order of 10,000 times or more. The new t3-100 Cray machine can do 3 trillion operations a second! Think how that will effect cryptographic searches in the future. The hybrid system uses the best of both kinds of systems. The speed advantage of the private key cryptography is used for encrypting and transmitting. Public key transactions are for the smaller transmissions. A typical combination (for a hybrid) is to employ a public dual key for encryption and for the distribution of the private keys, and the private-key system for bulk data.

The central key facility is useful when it is undesirable to entrust individual stations with control of cryptographic keys. Two stations wishing to communicate request a session key from the central station. The key generated at the central station is sent to both stations encrypted in each stations master key. The master key list is known only to the central station. [HUTT] (LEVD)

PRETTY GOOD PRIVACY (PGP)

This system is a public-key system invented by Phillip Zimmerman and draws upon the International data Standard (IDEA) and RSA algorithms. By far the defacto standard for the Internet and public. NSA has not endorsed it. Amateurs swear by it. It appears to be out of the legal hassle mode. More on this system in a future lecture.

PRIVACY ENHANCED MAIL (PEM)

A system that uses both message encryption and digital signatures, PEM encrypts messages and authenticates senders of E-mail. PEM was a child of DARPA and uses DES on the front-end for encryption and RSA for sender authentication. Trusted Information Systems introduced it commercially. The federally funded Clipper/Skipjack is now recommended as a substitute for PEM. [LEVD]

KEY MANAGEMENT AND DISTRIBUTION

Key management involves the secure generation, distribution, storage, journaling, and eventual disposal of encryption keys. The adequacy of key management is a significant factor in using encryption as a security method. Keys can be either distributed via escorted courier, magnetic media, or via master keys that are then used to generate additional keys.

Cryptographically protected data is dependent on the protection of the encryption keys. The entire system can be compromised by the theft, loss or compromising of a key. Standards for key management have been developed by ISO, ANSI, federal government and the American Banking Association. Key management is crucial to maintaining good, cost-effective, and secure communications between a large number of users.

IMPLEMENTATION CONSIDERATIONS

Media

Cryptography can take place in software, hardware, or firmware. The least efficient and cheapest media is software.

Configurations

In-line, off-line, embedded, and stand-alone are four different types of configurations, each with its own requirements, need to considered when implementing cryptosystems.

1. Inline. The communications equipment is external to the cryptosystem. The handoff occurs after encryption to the communications device.

2. Off-line. The source controls all encryption, storage, and communications facilities.

3. Embedded. Configurations may be off or on line. The main requirement is that the cryptographic module be embedded or contained within the computer and the interface with that computer.

4. Stand-alone. These require that the cryptographic module is separately enclosed outside of the host and physically secured.

NIST FIP's 140-1 is entitled "Security Requirements in Cryptographic Modules," describes four levels of security ranging from commercial grade security to penetration/tamper resistant.

ONE-TIME CIPHER KEYS

Discussed in Volume I in detail.

DIGITAL SIGNATURES AND NOTATIONS

RSA and DSA are the best known digital signature algorithms. The latter was invented by NSA and approved for government use. NIST has supported the DSA algorithm. Both are tools for authenticating the user and origin of the message and the identity of the sender. A digital signature is unforgeable, verifies the signer, is not reusable, cannot be repudiated and proves that the sender did not sign an altered document. DSA is based on the SHA (Secure Hashing Algorithm) and is described in FIPS PUB 180 "Secure Hash Standard."

CARTE A MEMOIR (Memory Card)

The French invented the smart card which contains a chip to process information in protected memory. They are used for access control and for end-to-end encryption schemes.

CYBER NOTARIES

The American Bar Association has developed rules for electronic notaries for commerce that incorporate digital signatures. Ben Wright of NCSA is the leading authority on this kind of commerce.

KERBEROS

Among the commercial authentication systems, the most popular is Kerberos. Developed at MIT, it verifies the user and incorporates unique session keys for client /server communications via a ticket-granting server. Scientific American described the system accurately and vividly in August 1994.

TEMPEST

This program was established in 1950's to shield electronic equipment from electromagnetic radiations (Van Ek emissions) that could be intercepted and "read". TEMPEST is an entire vendor evaluation program for the equipment that contains emanations via a special shield.

THE CLIPPER/SKIPJACK CHIP CONTROVERSY

In October 1985, NSA announced plans to phase out DES in favor of the technique of "embedding" cryptography into electronic communications within the United States.

The Clipper Chip, renamed Skipjack because of a trademark conflict, is a U.S. Government-sponsored tamper resistant chip for voice encryption that employs a classified algorithm and a key escrow facility. Capstone, which uses the Skipjack algorithm, is a data encryption chip that adds digital signatures and key exchange enhancements. Each chip contains an 80-bit key that is split into two parts immediately following manufacture. Each half of the key is deposited into custody of a trusted "escrow agent." NSA designed it during the Reagan Administration and proposed it in April 1993 for both government and public use.

Once installed in telephones, by use of a secret military algorithm, the chip would turn the telephones into gibberish for everyone but the speaker and the intended listener. [Similar to the STU-III secure system in some ways.] The uniqueness and the controversy of Skipjack lies in the LEAF (law enforcement access field) that allows law enforcement, with cooperation of the two parties, to listen under certain circumstances and to decipher Clipper-encrypted traffic. Any government agency desiring to legally listen to the owner of a communications device that contains the chip, the government agency would present evidence of lawful authority to the escrow holders, who would then reveal the key pairs that the agency would join in order to begin listening to the conversations. Notification of the target (subject) is not necessary.

When Clipper Chip was announced, it was stated that there was no plan to legislate Clipper as the only means to protect telecommunications. However, Clipper Skipjack can only achieve its stated objectives if everyone uses it. Manufacture of the chips would be closely controlled with "trusted" companies. Mykotonx was chosen to program the chips, VLSI was chosen to manufacture the chips, and NSA would design the algorithms and protocols. Additional points of compromise would be the trusted facilities, which hold the keys, and the FBI, which actually decrypts the Clipper traffic.

The American public, EFF (Electronic Frontier Foundation) and a consortium of companies DEC, HP, IBM, SUN, MCI, Microsoft, Apple, and AT&T opposed the Clipper Chip and submitted 118 questions to the White House.

The NIST, on July 30, 1993 issued a request for public comments on its proposal to establish Clipper/Skipjack as a FIP. Clipper/Skipjack can not be implemented in software, which closed out more of the commercial market. RSA data security had more than a million packages licensed by 1992 and another million expected because of the Macintosh OS and Novell Netware 4.0 deals.

There was such a controversy over Clipper/Skipjack that by July 1994, the government announced that it was no longer seeking to make this the standard form of encryption, although NIST officials do not intend to issue the DES standard again in its current form.

The Clinton Administration has taken up the cause and issued numerous trial balloons to force the issue. See Appendix 4 for a recent balloon.

When separated from the government's proposed implementation of Clipper/Skipjack, the concept of key escrow cryptography does have applicability for commercial use. Business managers fear possible extortion by unsavory employees who would hold corporate data for ransom by withholding encryption keys. Key escrow cryptography could eliminate this problem, but in addition to the friction created by the government's proposed implementation, there appear to be too many vulnerabilities involved with the Clipper/Skipjack to make the system acceptable in its current form.

LECTURE 18 SOLUTIONS

18-1. Unidecimal square root. (Three words 0-E) MARSHEN

LO'SE gives root it; - KF = EKSE; - ERRE = EWH

Answer: HE WORKS LIFT

18-2. Duodecimal division. (Two words, 0-E) CODEX

BRIDGE / CLUBS = CC; - DUHRE = BRHEE; - DUHRE = BOLO

Answer: ORCHID BUGLES

Appendix 1

TIS Worldwide Survey of Cryptographic Products

Crypto Survey - Domestic Products:Summary listing of domestic cryptographic products as of 7/25/96

2010 Software Corp.
3Com Corp.
ADT Security Systems
ASC Systems
ASD Software, Inc.
AT&T Bell Laboratories
AT&T Datotek, Inc.
Acma
Adobe Systems, Inc.
Advanced Encryption Systems
Advanced Engineering Concepts, Inc.
Advanced Micro Devices, Inc.
Advanced Network Services, Inc.
Aladdin Software Security, Inc.
Alcatel TITN Inc.
Alsoft, Inc.
American Computer Security
Antelope Production, Inc.
Apple Computer
Applied Software, Inc.
Argus Systems Group Inc.
Arkansas Systems, Inc.
Arkhon Technologies, Inc.
Ashton Tate
Atalla Corp.
Atemi Corporation
Automated Design Systems Inc.
Axent Technologies
BCC
BOE Corp.
Bankers Trust Company
Banyan Systems Inc.
Bellcore
Bi-Hex Co.
Bill Dorsey, Pat Mullarky, and Paul Rubin
Borland
Braintree Technology
Burroughs
CDSM Inc.
COGON Electronics, Inc
COM & DIA, L.L.C.
Casady and Greene
Centel Federal Systems, Inc.
Central Point Software
Certus International
Cettlan Corp.
CheckPoint Software Technologies
Cincinnati Microwave Communications, Inc.
Clarion
Codex Corp.
Cohesive Systems
Collins Telecommunications Products Division
Comm Touch Software Inc.
Command Software Systems
Commcrypt
Communication Devices, Inc.
Complan
Computer Associates International, Inc.
Connect, Inc.
Cordant
Cray Communications, Inc.
Cryptall
Cyber-Safe
CyberSafe Corporation
Cybernetics
Cycomm Corp.
Cylink Corp.
Cyno Technologies Inc.
Cypress Data Systems
DSC Communications
DataEase International
Datakey, Inc.
Datamedia Corporation
Datawatch, Triangle Software Division
Digital Crypto
Digital Delivery, Inc.
Digital Enterprises, Inc.
Digital Equipment Corp.
Digital Pathways
Digital Secured Networks Technology Inc.
Dolphin Software
Dowty Network Systems
E-Systems
Eave Stopper
Enigma Logic, Inc.
Enterprise Integration Technology
Enterprise Solutions Ltd.
Ergomatrix
Everett Enterprises
Software Corporation
Fairchild Semiconductor
Fifth Generation Systems, Inc.
Fischer International
Front Line Software
Funk Software
Gemplus Card International
General Electric Company
General Kinetics, Inc.
General Magic
Gerald J. DePyper
Glenco Engineering
Group Technologies
Harcom Security Systems Corp.
Harris Computer Systems Corporation
Hawkeye Grafix, Inc.
Helpful Programs, Inc.
Hilgraeve, Inc.
Hughes Aircraft Company
Hughes Data Systems, Inc.
Hughes Network Systems - Maryland

Hydelco, Inc.
Ilex Systems Inc.
Info Security Systems
Info Tel Corp.
Info-ZIP
InfoNow Corporation
Information Resource Engineering (IRE)
Information Security Associates, Inc.
Information Security Corp.
Innovative Communications Technologies, Inc.
Inside Technologies, Inc.
Intel
Intelligent Security System Inc.
Inter-Tech Corp.
International Business Machines, Inc. (IBM)
International Micro Industries (IMI)
Interscan Corp.
Isocor
J.G. Van Dyke & Associates, Inc.
John E. Holt and Associates
John Walker
Jones Futurex
KarlNet, Inc.
Kensington Microware Ltd.
Kent Briggs
Kent Marsh Ltd.
Key Concepts
Kinetic Corp.
Kommunedata
Lassen Software, Inc.
Lattice, Inc.
Lexicon, ICOT Corporation
Litronic Industries (Information Systems Division)
Livermore Software Laboratories, Inc. (LSLI)
Lockheed Martin Advanced Technology Laboratories
Lotus Development Corp.
MARX International, Inc.
MCTel
Maedae Enterprises
Magna
Marathon Computer Press
Marcor Enterprises
Mark Riordan
Massachusetts Institute of Technology (MIT)
Matsushita Electronic Components Co.
Mergent International
Merritt and Colstan
Micanopy MicroSystems, Inc.
Micro Card Technologies, Inc.
Micro Security Systems, Inc.
Microcom Inc. (Utilities Product Group)
Microlink Technologies, Inc.
Microrim
Microsoft
Mike Ingle
Morning Star Technologies
Morse Security Group, Inc.
Motorola
Mykotronx, Inc.
National Semiconductor
NetPro Computing Inc.
Netscape Communications Corporation
Network Systems Corporation
Network-1, Inc.
Networking Dynamics Corp.
Nixdorf Computer Corporation
Norton
Novell, Inc.
Open Commerce
Open Computing Software Group, Inc. (OCSG)
Open Software Foundation
Optimum Electronics, Inc.
Oracle
Otocom Systems, Inc.
PC Dynamics, Inc.
PC Guardian
PC Plus, Inc.
PKWARE Inc.
PMC Electronics
Pacific Communication Sciences, Inc.
Paradyne Corporation
Paralon Technologies
Personal Computer Card Corp.
Pinon Engineering, Inc.
Premenos
Pretty Good Privacy, Inc.
Prime Factors
Qtrain Corporation
RSA Data Security, Inc.
Racal-Guardata
Radix2 Software Engineering
Rainbow Technology
Raptor Systems, Inc.
Raxco
Retix
Ross Engineering, Inc.
Rothenbuhler Engineering
Rudaw/Empirical Software Products Ltd.
S Squared Electronics
SCO
SOS Corporation
SPRY/CompuServe
SVC
Safe Call
Safetynet
Samna Corp.
Scrambler Systems Corp.
Scrambler Technologies, Inc.
Sector Technology
Secur-Data Systems, Inc.
Secura Technologies
Secure Computing Corporation
Secure Systems Group International, Inc.
SecureWare, Inc.
Security Microsystems, Inc.
Semaphore Communications Corporation
Sentry Software
Sentry Systems, Inc.
Silver Oak Systems
SmartDisk Security Corp. (SDSC)
Smartstuff Software
Software Directions, Inc.

Software Solutions, Inc.
Solid Oak Software
So phCo, Inc.
Sota Miltope
Spyrus, Inc.
StarNine Technologies, Inc.
Stellar Systems, Inc.
Sterling Software Inc. (System SW Mktg. Div.)
Sterling Software Interchange Software Division
Steven Ryckman
Sun Microsystems, Inc.
SunSoft
Symantec
Techmar Computer Products, Inc.
Techmatics, Inc.
Technical Communications Corp. (TCC)
Tecsec, Inc.
Telenetics Corporation
Telequip Corp.
Telos Corp.
Terisa Systems
Terry Ritter
Texas Instruments, Inc.
The Exchange
Thumbscan, Inc.
Titan Linkabit
Tracor Aerospace Inc.
Tracor Ultron
TradeWave
Transcrypt International
TriTeal Corp.
Trigram Systems
Triton Systems
Trusted Information Systems, Inc.
UNISYS Corp.
UTI-MACO
UUNet Technologies, Inc.
United Software Security
UsrEZ Software, Inc.
V-ONE Virtual Open Network Enviroment Corp.
VLSI Technology, Inc.
Vasco Data Security, Inc.
Verdix Corp. (Secure Products Division)
VeriSign, Inc.
ViaCrypt
Visionary Electronics
WRQ, Inc.
WTShaw
Wang Laboratories
Wells Fargo Security Products
Western DataCom Co., Inc.
Western Digital Corporation
Will Price
WordPerfect Corp
XTree
Xetron Corp.
Zoomit International
ZyXE L

Crypto Survey - Foreign Products Summary listing of foreign cryptographic products as of 7/25/96

ARGENTINA
Hugo D. Scolnik
Newnet S.A.

AUSTRALIA
Cybanim Pty Ltd.
Eracom Pty Ltd.
Eric Young
Microlock
Mosaic Industries
News Datacom
Randata

AUSTRIA
Siemens AG Austria

BELGIUM
CNET
Highware, Inc.
Lintel Security
UTI-MACO Belgium

CANADA
Border Network Technologies, Inc.
CRYPTOCard Corporation
Certicom
Chrysalis ITS
Compression Technologies, Inc.
FSA
Isolation Systems
Micro Tempus, Inc.
Milkyway Networks Corporation
Northern Telecom Canada Ltd. (Data Comm. Products)
Northern Telecom Canada Ltd. (Secure Networks)
Okiok Data
Queen's University
Secured Communications Inc. (SCI)
Sierra Wireless
The Enigma Group
TimeStep Corporation
Tundra Semiconductor Corp.
Zoomit Corporation

CZECH REPUBLIC
Decros spol. s r .o.

DENMARK
Aarhus University, Computer Science Department
CryptoMathic
GN Datacom
LSI Logic/Dataco AS

FINLAND
Antti Louko
Jetico, Inc.
SSH Communications Security Oy

FRANCE
ActivCard
Atlantis
Digital Equipment Corp. (DEC), Paris Research Lab
Hewlett Packard France
Philips Communication Systems

GERMANY
Andreas Kupries
Baller & Huwig
CE Infosys GmbH
Celticon
DataSafe
EZI GmbH
FAST ComTec GmbH
GMD
Gliss & Herweg
Jurgen Meyer, Frank Gadegast
Karl Huwig
KryptoKom
SIT
Siemens-Nixdorf
Stefan D. Wolf
TeleSecurity Timmann
Telenet Kommunikation Systeme
UTI-MACO GmbH

HONG KONG
Triple D Ltd.

INDIA
Bharat Electronics Ltd.
Chenab Info Technology

IRAN
Communications Industries Group

IRELAND
Baltimore Technologies Ltd.
Eurologic Systems, Ltd.
Systemics Ltd.

ISRAEL
Aladdin Knowledge Systems, Ltd.
Algorithmic Research Ltd.
Aliroo Ltd.
Carmel Software Engineering Ltd.
Elementrix Technologies Ltd.
EliaShim Microcomputers Ltd.
Secure Network Systems, Ltd.

ITALY
AMTEC SPA
CERT-IT
Eutron Spa

JAPAN
Fujitsu Labs Ltd.

MEXICO
The King of Hearts

NETHERLANDS
Concord Eracom Nederland BV
DigiCash
Incaa Datacom BV
Philips Crypto B.V.
Pijnenburg
Verspeck & Soeters b.v.

NEW ZEALAND
LUC Encryption Technology, Ltd. (LUCENT)
Peter Gutmann

POLAND
Enigma Information Security Systems

RUSSIA
Ancort
Askri
Elias Ltd.
INFORM -RTG
LAN Crypto
ScanTech
TELECRYPT, Ltd.

SOUTH AFRICA
Denel Informatics
NetSec
Sentera

SWEDEN
AU-System Communication AB
Ardy Elektronics
Business Security AB
COST Computer Security Technologies International
DynaSoft
Henry Padilla
SECTRA AB
SONNOR Crypto AB
Stig Ostholm

SWITZERLAND
ASCOM Tech AG
Crypto AG
Gretacoder Data Systems AG
Omnisec AG
Safeware AG

UK
Apricot Computers, Ltd.
Avant Guardian Ltd.
British Telecom
Data Innovation Ltd.
DataSoft International Ltd.
Digital Crypto
Finansa
GEC-Marconi Secure Systems
Global CIS Ltd.
ICL Secure Systems
IQ International
International Data Security, Ltd.
J.R.Ward Computers Ltd.
J.S.A. Kapp
JPY Associates Ltd.
Jaguar Communications Ltd.
Microft Technology Ltd.
PC Security Ltd.
Plessy Crypto
Plus 5 Engineering Ltd.
Portcullis Computer Security Ltd.
Protection Systems Ltd.
Racal Airtech Computer Security
S&S International PLC
Sophos Ltd.
University College London
Zergo, Ltd.
Zeta Communications Ltd.

Appendix 2

BERNSTEIN v UNITED STATES CRYPTO CASE

The complexity of the constitutional privacy issues are demonstrated by the current Bernstein Case.

Case Background

While a graduate student at the University of California at Berkeley, Bernstein completed development of an encryption equation (an "algorithm") he called "Snuffle." Bernstein wished to publish a) the algorithm, (b) a mathematical paper describing and explaining the algorithm, and (c) the "source code" for a computer program that incorporates the algorithm. Bernstein also wished to discuss these items at mathematical conferences, college classrooms and other open, public meetings. The Arms Export Control Act and the International Traffic in Arms Regulations (the ITAR regulatory scheme) required Bernstein to submit his ideas about cryptography to the government for review, to register as an arms dealer, and to apply for and obtain from the government a license to publish his ideas. Failure to do so would result in severe civil and criminal penalties. Bernstein believed this was a violation of his First Amendment rights and sued the government.

In the first phase of this litigation, the government argued that since Bernstein's ideas were expressed, in part, in source code, they were not protected by the First Amendment. On April 15, 1996, Judge Marilyn Hall Patel in the Northern District of California rejected that argument and held for the first time that computer source code is protected speech for purposes of the First Amendment.

Because of its far-reaching implications, the Bernstein case is being watched closely by privacy advocates, the computer industry, the export and cryptography communities, and First Amendment activists. In fact, several members of these communities provided declarations that were submitted in support of Bernstein's motion.

On 26 July 1996, Bernstein filed a motion for partial summary judgment in his suit against the State Department that could strengthen his claim that government restrictions on information about cryptography violate the First Amendment's protections for freedom of speech. In his 45-page memorandum in support of his motion, Bernstein set forth several First Amendment arguments:

Legal Arguments

* Any legal framework that requires a license for First Amendment protected speech, which may be granted or withheld at the discretion of a government official, is a prior restraint on speech. In order for this framework to be acceptable, the government has the burden of showing that publication will "surely result in direct, immediate, and irreparable damage to our Nation or its people" and that the regulation at issue is necessary to prevent this damage. The government has not met this burden regarding the ITAR legal framework.

*   Because restrictions on speech about cryptography are content-based, the court must apply a strict scrutiny test in determining whether individuals can be punished for engaging in this speech. A strict scrutiny test requires that a regulation be necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end. The ITAR regulatory scheme has adopted the *most* restrictive approach by prohibiting all speech in the area of cryptography.

*   The ITAR regulatory framework lacks the necessary procedural safeguards. Grants of administrative discretion must be limited by clear standards, and judicial review must be available. "Quite simply, the ITAR Scheme allows its administrative agencies to make inconsistent, incorrect and sometimes incomprehensible decisions censoring speech, all without the protections of judicial review or oversight."

*   The ITAR framework is unconstitutionally vague. The government doesn't even seem to know what its regulations include and exclude! Here, the lack of standards has allowed the government to misuse a statute aimed at commercial, military arms sales to limit academic and scientific publication.

*   The ITAR regulatory scheme is overbroad. In an internal memo written almost 20 years ago, the government's own Office of Legal Counsel concluded that the ITAR's licensing standards "are not sufficiently precise to guard against arbitrary and inconsistent administrative action." The OLC specifically warned that the coverage was so broad it could apply to "communication of unclassified information by a technical lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest." This is exactly what is happening here, and it is unconstitutional.

Full text Available

The legal arguments expressed above in the Bernstein case are taken from material available from the Electronic Frontier Foundation (EFF) online archives. Full text of the lawsuit and other paperwork filed in the case is available from EFF's online archives:

http://www.eff.org/pub/EFF/Policy/Crypto/
ITAR_export/Bernstein_case/ ftp.eff.org,
pub/EFF/Policy/Crypto/ITAR_export/Bernstein_case
/ gopher.eff.org,
1/EFF/Policy/Crypto/ITAR_export/Bernstein_case/

Appendix 3

FEDERAL REGISTER
VOL. 58, No. 139
Rules and Regulations
DEPARTMENT OF STATE
Bureau of Politico-Military Affairs
22 CFR Parts 120, 121, 122, 123, 124, 125, 126, 127, 128, and 130
[Public Notice 1832]
Amendments to the International Traffic in Arms Regulations
Part II
58 FR 39280

DATE: Thursday, July 22, 1993

ACTION: Final rule.

SUMMARY: This rule amends the regulations implementing section 38 of the Arms Export Control Act, which governs the import and export of defense articles and services. The rule clarifies existing regulations and reduces the regulatory burden on exporters of defense articles and services.Although this is a final rule public comment is welcome and will be taken into account to the extent possible.

EFFECTIVE DATE: This final rule is effective July 22, 1993.

FOR FURTHER INFORMATION CONTACT: Information regarding this notice may be obtained from James Andrew Lewis, U.S. Department of State, Bureau of Politico- Military Affairs (202-647-4231), Mal Zerden or Allan Suchinsky, U.S. Department of State, Office of Defense Trade Controls (703-875-6644).

SUPPLEMENTARY INFORMATION: The regulations implementing section 38 of the Arms Export Control Act were last revised substantially in November 1984. A proposed rule was published on May 7, 1992 (57 FR 19666), for public comment. This Final Rule clarifies and simplifies the current regulations. Certain sections are consolidated while others are revised in the interests of clarity and consistency. To the extent possible, related sections are cross-referenced. In amending the regulations, public comments and suggestions from industry and other U.S. agencies have been considered and in many cases incorporated into the regulations.

The most significant changes are an increase in the validity period of a license from three to four years and a revision of the policy used by the Department for designating defense articles that takes into account civil application and functional equivalence. Several new exemptions from licensing requirements are also established. These exemptions will cover exports under approved manufacturing or technical assistance agreements; spare parts valued at $ 500 or less; intra-company transfers of components being sent abroad for assembly; temporary imports for repair and servicing; and items which were previously licensed for temporary export to trade shows.

Other changes include a clarification of the commodity jurisdiction process, which establishes a review period and specifies the appeal process. The definition of public domain is expanded and clarified. An exception allows for the re-export of certain U.S.-origin components to the Governments of NATO countries, and the Governments of Japan and Australia without prior U.S. approval for components which are not significant military equipment or controlled for purposes of the Missile Technology Control Regime and do not require Congressional notification.

PART 121-THE UNITED STATES MUNITIONS LIST

Category XIII-Auxiliary Military Equipment

(a) Cameras [including space cameras] and specialized processing equipment therefor, photointerpretation, stereoscopic plotting, and photogrammetry equipment which are specifically designed or modified for military purposes, and components specifically designed or modified therefor;

(b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including:

(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:

(i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.

(ii) Specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.

(iii) Employing only analog techniques to provide the cryptographic processing that ensures information security in the following applications:

(A) Fixed (defined below) band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

(B) Fixed (defined below) band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

(C) Fixed (defined below) frequency inversion and in which the transpositions change not more frequently than once every second;

(D) Facsimile equipment;

(E) Restricted audience broadcast equipment;

(F) Civil television equipment.

Note: Special Definition. For purposes of this subparagraph, fixed means that the coding or compression algorithm cannot accept externally supplied parameters (e.g., cryptographic or key variables) and cannot be modified by the user.

(iv) Personalized smart cards using cryptography restricted for use only in equipment or systems exempted from the controls of the USML.

(v) Limited to access control, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password of PIN protection.

(vi) Limited to data authentication which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication.

(vii) Restricted to fixed data compression or coding techniques.

(viii) Limited to receiving for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions.

(ix) Software designed or modified to protect against malicious computer damage, (e.g., viruses).

Note: A procedure has been established to facilitate the expeditious transfer to the Commodity Control List of mass market software products with encryption that meet specified criteria regarding encryption for the privacy of data and the associated key management. Requests to transfer commodity jurisdiction of mass market software products designed to meet the specified criteria may be submitted in accordance with the commodity jurisdiction provisions of S 120.4.

Questions regarding the specified criteria or the commodity jurisdiction process should be addressed to the Office of Defense Trade Controls. All mass market software products with cryptography that were previously granted transfers of commodity jurisdiction will remain under Department of Commerce control. Mass market software governed by this note is software that is generally available to the public by being sold from stock at retail selling points, without restriction, by means of over the counter transactions, mail order transactions, or telephone call transactions; and designed for installation by the user without further substantial support by the supplier.

(2) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment.

(3) Cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components or software.

(4) Systems, equipment, assemblies, modules, integrated circuits, components or software providing certified or certifiable multi-level security or user isolation exceeding class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) and software to certify such systems, equipment or software.

(5) Ancillary equipment specifically designed or modified for paragraphs (b) (1), (2), (3), (4) and (5) of this category;

Appendix 4

CLINTON'S ENCRYPTION PLAN WITH KEY RECOVERY SYSTEM

The New York Times reported in its section C1, on 1 October 1996, that:

-- Attempting to compromise with critics of its "key escrow" approach to data encryption, the Clinton Administration now plans to begin allowing U.S. computer companies to export software using powerful encryption codes (or "keys") up to 56 bits long. However, the government will require those companies to develop, within two years, a "key recovery" system allowing U.S. law enforcement or anti-terrorist groups armed with a search warrant to get the key from the several third-party companies, each of which would hold one part of the key. IBM and some other large companies are supporting the plan, but other companies are expected to oppose it. The system will be successful only if the Administration can convince other countries to adopt the same kind of system.