Motivation

- Conflict between an individual’s right to privacy and the government’s need to invade privacy to uphold the law
- Complicated by digital data, encryption and wireless communications
Codes of Ethics

- ACM
  - Respect the privacy of others
  - Honor confidentiality
- AITP Code of Ethics
  - Protect the privacy and confidentiality of all information entrusted to me
- Software Engineering Code of Ethics
  - Work to develop software and related documents that respect the privacy of those who will be affected by that software

U.S. Constitution

- Fourth Amendment (abridged)
  - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.
- Fifth Amendment (abridged)
  - No person shall be compelled in any criminal case to be a witness against himself.
Privacy and Cyber-Utopia

- Global, seamless and secure e-commerce
- New encryption standard required
  - Individual privacy preserved
  - Law enforcement surveillance possible
  - U.S. computer industry globally competitive
  - Ability of national governments to regulate the nation preserved

Wiretapping

- Law enforcement eavesdropping on communication without informing the people who are communicating
- U.S. Supreme Court *Olmstead v. U.S.* (1928): wiretaps did not require special authorization if no trespassing necessary
- U.S. Supreme Court (1967): wiretaps, even of public phone booths, require prior judicial authorization
Authorizing a Wiretap

- Law-enforcement agency must convince a judge that
  - There is “probable cause” to believe a serious crime is involved
  - The wiretap should produce evidence relevant to prosecuting the crime
  - There is no other practical means of obtaining the evidence
- Usage statistics reported to congress

If the court agrees
  - Court issues a court order to the law enforcement agency
  - Phone company lawfully obligated to facilitate the wiretap
- Wiretaps authorized for a maximum of 30 days; extendable
- After wiretap completed, government must inform subject that they were wiretapped
Effectiveness of Wiretapping

- Activity since 1968 (EPIC)
- Each wiretap actually enabled monitoring many conversations
- Computerization complicates wiretapping
  - Digital data
  - Computer switching
  - Optical fiber transmission
  - Need to know data structures, formats and algorithms used in communication systems

Digital Telephony Standards

- 1994 mandate that communications systems equipment be designed to allow practical wiretapping by law enforcement
- Isolate the communications stream of an individual
- $500M allocated for conversion
- Communications Assistance for Law Enforcement Act (CALEA)
Digital Telephony Standards: Issues

- Most effective way to fight crime?
- Increase government’s “big brother” power?
- Security problems?
- Hindering technological advance?
- Who pays for the cost?
- Effect on U.S. industry competitiveness?
- Mandated capabilities useful?

Encryption

- Wiretapping encrypted digital communication of no use
- Solutions
  - Break encryption scheme
  - Legislate encryption
Private-Key Encryption

- Also called secret key or symmetric
- Algorithm public; key private
- Easy to break if number of possible keys is small
- Problems
  - How to securely distribute private key
  - Ensuring authenticity of messages

Data Encryption Standard (DES)

- Developed at IBM in 1977
- Private-key encryption
  - 56-bit key \(2^{56} = 72 \times 10^{15}\) keys
- Key chosen randomly for each message
- Applies 56-bit key to each 64-bit block of data
- Multiple passes for stronger encryption
  - Triple DES still in use \(2^{56+56+56}\) keys
- RSA code-breaking effort
Public-key Encryption

- Also called asymmetric
- Each person generates a public and private key
- Everybody knows public keys
- Only individual A need know their own private key
- $\text{private}_A(\text{public}_A(M)) = M$
- $\text{public}_A(\text{private}_A(M)) = M$

Public-key Encryption

- Digital signatures
- Person A encrypts message M with their private key to get M’
- Person A encrypts M’ with B’s public key to get M’’, which is sent to B
- Person B decrypts M’’ with private key to get M’
- Person B decrypts M’ with A’s public key to get M, but only if from A
- $\text{public}_A(\text{private}_B(\text{public}_B(\text{private}_A(M)))) = M$
Generating Public/Private Key Pairs

- RSA algorithm (patented)
- \( \text{encrypt}_A(M) = M^e \mod n \)
- \( \text{decrypt}_A(M) = M^d \mod n \)
- Public key = (e,n)
- Private key = (d,n)
- \( n = p*q \), where p and q are large random primes
  - e and d chosen based on p and q
- Security rests on difficulty to factor product n of two large primes

Government Encryption Policy

- Government’s position
  - Public-key encryption too difficult to wiretap
  - Limit export of encryption
  - Design own tap-able encryption scheme
- Industry’s position
  - Use widely-accepted, strong encryption standard
  - Freely export standard
Escrowed Encryption Standard

- EES developed by U.S. government in 1993
- Skipjack algorithm implemented on the Clipper and Capstone chips
- Private-key encryption
- Each chip has an 80-bit unit key U, which is escrowed in two parts to two different agencies
- Chip also includes a 30-bit serial number and an 80-bit family key F common to all Clipper chips

Two devices agree on an 80-bit session key K to communicate
- Message is encrypted with key K and sent
- Law-Enforcement Access Field (LEAF) appended to message, including
  - Session key K encrypted with unit key U
  - Serial number of sender
  - All encrypted with family key F
ESS Wiretapping

- Use family key to obtain LEAF
- Now have serial number of sending device and encrypted session key
- Upon authorization, two agencies present their two escrowed portions of the unit key U
- Use unit key U to decrypt session key K
- Use K to decrypt message

EES Issues

- Circumvention
- Security
  - Skipjack algorithm
  - Escrowed keys
- Both escrow agents governmental
- U.S. industry competitiveness
- “Forgetting” unit keys
- EES dropped due to public opposition
Advanced Encryption Standard

- AES to be U.S. government’s next encryption standard beginning 2001
- Rijndael algorithm selected from among several candidates
  - Efficient block cipher
  - Variable block and key length
    - AES supports 128, 192 and 256 bits
- See http://www.nist.gov/aes

Current Issues

- Encryption export limitations
  - Relaxed January 2000
- Key recovery (escrowed) encryption
- Any encrypted message must be decryptable by law enforcement with proper authorization
  - Encrypter must provide means to decrypt message
  - Fifth amendment issues
Case Study: Pretty Good Privacy

- Pretty Good Privacy (PGP)
  - www.pgp.com
  - web.mit.edu/network/pgp.html
- Uses patented, export-restricted RSA public-key encryption algorithm
- Philip Zimmerman develops PGP for encrypted email in 1990
  - Not licensed from RSA
  - “Anonymous friend” posts code to Internet

Points to Remember

- Law enforcement using new wiretap legislation to monitor email
- Escrowed key approaches likely to never catch on
- AES holds promise
- Law enforcement needs mechanism to decrypt information pertinent to criminal activity
- There is no specific “right to privacy” in the U.S. Constitution
Resources

- Electronic Privacy Information Center
  - www.epic.org
- Electronic Frontier Foundation
  - www.eff.org