Encryption and Interception of Communications

Daniel M German
Copyright

- Originally based on the slides for “A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet” (2nd Edition), created by Sherry Clark Copyright 2003 Prentice Hall
- Further extended by Daniel M. German
Encryption and Interception of Communications

- Overview of the Controversies
- Intercepting Communications
- Cryptography and Its Uses
- Fundamental Issues
Overview of the Controversies

- Communications Privacy Affected by:
  - Interception of communications, including:
    - Telephone, E-mail, and Web activity.
  - Restrictions on secure encryption.
    - Exportation of strong encryption was viewed as a threat to national security.
  - Communications technology must assist law enforcement, not hinder.

- Global surveillance systems.
  - The constitutionality of domestic systems and the necessity of international systems are under question.
Intercepting Communications

- Wiretapping
  - Telephone:
    - Pre-1934: used widely by government, businesses, and private sector.
    - 1934: the Federal Communications Act disallowed unauthorized wiretaps; many ignored the law.
Intercepting Communications

Wiretapping

New Technologies:

- 1986: Electronic Communications Privacy Act (ECPA) and its amendments restricted government interception of e-mail, cell-phones, etc..
- 2001: USA Patriot Act loosened restrictions on government wiretapping and communications interception.
Intercepting Communications

Designing Communications Systems for Interception and Tracking

Obstacles to interception:
- Incomplete pen-registers as a result of long distance service.
- Packet-mode communications (e-mail, file transfers, Internet phones).

Solutions:
- CALEA: Requires telecommunications equipment be designed to ensure interception by law enforcement (with court order).
Intercepting Communications

- Designing Communications Systems for Interception and Tracking (cont’d)

- CALEA
  - Costs include modified hardware, software, and overuse by authorities.
  - Wiretappable systems vulnerable to criminal hacking, industrial spies, etc..
  - Competition weakened due to restricted changes and diversities.
  - Civil liberties threatened by nationwide standard for surveillance.
Intercepting Communications

- Carnivore
  - FBI’s system to intercept e-mail with a court order.
    - Pro: Law enforcement needs this tool to fight crime.
    - Con: All e-mail goes through FBI’s Carnivore system.
Intercepting Communications

- NSA and Echelon
  - NSA (National Security Agency):
    - Collects and analyzes communications to find threats to national security.
  - Echelon:
    - Member nations intercept communications for each other.
Cryptography and Its Uses

- **Cryptography**
  - Definition:
    - Hiding data in plain sight.
  - Terms:
    - Plaintext: Original, readable message or data.
    - Cyphertext: Modified, unreadable message or data.
    - Encryption: The act of converting plaintext into cyphertext.
    - Decryption: The act of reverting cyphertext back to readable, plaintext.
Cryptography and Its Uses

Public Key Cryptography

How it works:
- User creates a mathematically-related key pair (public and private keys).
- Public keys are shared publicly; private keys are kept secret.
- Public keys are used to encrypt message or data.
- Private keys are used to decrypt message or data.

Benefits:
- No secret keys need be shared or transmitted.
- Very secure.
Cryptography and Its Uses

- Encryption
  - Used by:
    - Military personnel.
    - Financial institutions.
    - Human-rights activists.
    - Government agencies.
    - Anyone wanting to keep messages or data private.
Cryptography and Its Uses

- Steganography
  - Definition:
    - Hiding data so that its existence is not known.
  - Examples:
    - Digital watermarks.
    - Hiding text in image files.
  - Used by:
    - Military,
    - Publishers,
    - Anyone wishing to hide messages or data.

- Secrecy and Export Controls
  - Control of Secrecy
    - The NSA designs unbreakable codes for the U.S. government.
    - The NSA attempts to break codes used by other governments.
    - In the past, the NSA also controlled the funding for and publishing of cryptographic research.
Secrecy and Export Controls

Control of Exportation

- Early U.S. policy prevented the exportation of strong encryption.
- Meanwhile, foreign production and use of strong encryption negatively impacted U.S. competition in the world market.
- Cryptographic researchers, privacy advocates, and others successfully challenged exportation restrictions.

- Domestic Encryption
  - Key Escrow
    - Third-party entrusted with non-public encryption keys.
  - Real-time Access to Plaintext
    - Immediate decryption of encrypted data.
    - Long-time goal of the FBI.
  - Key Recovery
    - The ability to recover encrypted files if necessary.
    - Used by some businesses.
Fundamental Issues

- **Role of Secrecy**
  - U.S. Policy Keeps Secret:
    - Cryptographic research.
    - Wiretap ease or difficulty.
    - Encryption algorithms.
    - Software (e.g. Carnivore).
    - Global endeavors (e.g. Echelon).
  - **Problems:**
    - Secret algorithms cannot be tested by experts.
    - ’Backdoors’ might exist.
    - NSA-influenced wiretap and encryption exportation bills.
Fundamental Issues

The Ever-changing Status Quo

Past:
- Simple codes and cyphers.

Present:
- 512-bit RSA encryption.
- AES (Advanced Encryption Standard).

Future:
- Quantum computing.
- Quantum cryptography.
Fundamental Issues

- Trust in Government
  - Appropriate or Abusive?
    - Wiretapping by FBI and local police.
    - Wiretapping by NSA.
    - Strong encryption restrictions.
    - Clipper Chip and Key Escrow.
    - Roving wiretaps.
    - Cell-phone tracking
    - Key logger systems.
    - Development of a nationwide standard for surveillance.
    - Immediate decryption technology built in to the Internet.
Canada

What is the situation in Canada?
Lawful access

- **Lawful Access.** The lawful interception of communications and the lawful search and seizure of information, including computer data.
  - “used to investigate serious crimes, such as drug trafficking, money laundering, smuggling, child pornography, and murder”.
  - “essential tool for the investigation of threats to national security, such as terrorism”.
  - (From the Lawful access FAQ, Dept. of Justice)
Communications that can be intercepted

- Wireline technologies (telephone)
- Wireless technologies (cellular telephones, satellite communications, pagers)
- Internet technology (email, Web)
Who can use Lawful Access

- RCMP
- Canadian Security Intelligence Services (CSIS)
- Provincial police
- Municipal police
- Competition bureau
Data Preservation and ISPs

- ISPs might be required to preserve data of an individual **before** a warrant is issued
Lawful access

- It is not a law (yet). It is under consultation
- If it becomes one:
  - Canada’s telecommunications service providers (TSPs) will be required to install equipment in their networks to allow for real-time interception of communications,
  - to have the capability of simultaneously intercepting multiple transmissions, and
  - to provide detailed subscriber information to law enforcement authorities without a court order within 72 hours.
  - TSPs will be subject to inspections and
  - required to provide the government with reports on the technical capabilities of their networks.
Email interception

- When is email collected? During
  - Typing
  - transmission to the sender’s ISP
  - transmission to the recipient’s ISP
  - transmission from ISP to recipient
  - When it is read

- When it is stored?
  - Sender
  - ISPs
  - Recipient

- Is it interception (Part VI of the criminal code), or
- Is it seizure (Part XV of the criminal code)
USA: Reading your email

“Last week a Federal District Court in Boston decided that when someone reads your private e-mail without your permission and before you receive it, it doesn’t violate federal wiretap law. The ruling perfectly illustrates how we can frustrate the entire purpose of a statute simply by reading it too carefully.”

- The ISP had a bookstore business too
- The ISP filtered Amazon’s email
- The messages were not “intercepted” during transmission
USA: Keystroke loggers

“A federal judge in Los Angeles has dismissed charges against a California man who used a keystroke logger to spy on his employer, ruling that use of such a device does not violate federal wiretap law.” (Security Focus)
Wiretapping in Canada

- Who should pay?
- In 2004, the Canadian Association of Chiefs of Police proposed a $0.25/month surcharge to help pay for wiretaps
Eavesdropping by individuals

The interception of domestic “private communications” is illegal:

“184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.” (Criminal Code)

Some argue that Canada’s Criminal Code does not make it illegal to intercept and record communications between foreigners!
Echelon: Canada

- Station in Leitrim, Quebec, alleged to be surveying Latin America’s communications.

- “private communication” means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it; (Criminal Code)
Canada’s policy on Cryptography

- Support for Electronic Commerce
  - Canadians are free to develop, import and use whatever cryptography products they wish.
  - The Government will not implement mandatory key recovery requirements or licensing regimes.
  - The Government encourages industry to establish responsible practices, such as key recovery techniques for stored data.
  - The Government will act as a model user of cryptography through the practices of the Government of Canada Public Key Infrastructure (GOC PKI).
  - The Government encourages and supports industry-led accreditation of private sector certification authorities.
  - Sidenote, for many years I was not allowed to use Netscape or Internet Explorer with strong crypto.
Canada: Export / International Agreements

- Canada will continue to implement cryptography export controls in keeping with the framework of the international Wassenaar Arrangement.

- Canada will take into consideration the export practices of other countries and the availability of comparable products when rendering export permit decisions.

- The export permit application process will be made more transparent and procedures will be streamlined to ensure the least regulatory intervention necessary.
Canada: Crypto and Criminal Code

The Government proposes amendments to the Criminal Code and other statutes as necessary to:

- criminalize the wrongful disclosure of keys;
- deter the use of encryption in the commission of a crime;
- deter the use of cryptography to conceal evidence; and
- apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances.
Electronic Docs and signatures: Canada

- Defined in the “Personal Information Protection and Electronic Documents Act” Chapter 5 (Bill C-6)
  - Defines what an electronic document is,
  - The validity of secure electronic signatures
  - When and how electronic documents are accepted as evidence: “31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.”
Certificate Authorities in Canada

- Canada Post: PosteCS
  - Heralded as the first comprehensive solutions for digital signatures/encrypted communication in Canada
  - Most people and organizations never cared
  - Provides:
    - A signing authority
    - Carrier
PosteCS: How it works

- PosteCS uses SSL applications:
  - Sender uploads messages or documents, with choice of security levels, to the PosteCS server via https
  - PosteCS server sends out an email notification which contains a unique URL (a patented technology)
  - Recipient clicks on the unique URL to get to the message and documents stored on the secure PosteCS server
PosteCS: Pricing/Services

Services:

- Real-time tracking
- Electronic Postmark (The official date and time stamp and to prove non-tampering of documents)
- 128-bit transmission encryption (This requires an SSL enabled browser)
- 1024-bit server level encryption
- Password protection
- Unlimited file size attachments
- Up to 10-day storage on the secure PosteCS server

Cost: from $0.6 to $3.5 per message
Is listening to a wireless network legal in Canada?

It is illegal to use the wireless network!