Legal and social issues in privacy and security

Security and privacy, legal issues

- Rapid developments computer systems, networks and give rise for
  - New threats for security and privacy ;
  - New defensive measures;
- We have seen various technical means to protect security and privacy in computer systems and networks;
- In real life they should be accompanied by law regulations.

International and national politics issues

- US Export control on cryptographic software:
  - was the main reason to separate JCA and JCE in Java cryptographic library implementation
- Recent discussions in British Parliament:
  - the government proposal on 90 (...42...28)days detention was motivated in a part by necessity to have more time for decryption of intercepted correspondence

Legal Restrictions on Cryptography

- The legal landscape of cryptography is complex and constantly changing.
- Many aspects:
  - Cryptography and patent system
  - Cryptography and Trade secret Law
  - National and International regulations of cryptography
  - Digital Rights management
  - ...

Cryptography and Patent System

- Early development of cryptographic protocols and systems was influenced by patent law;
- Many important techniques, including *public key cryptography* have been patented, including:
  - Diffie-Hellman key exchange algorithm (expired 1997);
  - RSA encryption algorithm (expired 2000).
- In general, one of the results of the patent protection appeared to be reduced use of the invention

Cryptography and Trade Secret Law

- Until recently many encryption algorithms were kept as proprietary, secret and protected by the trade secret provisions;
- The idea was that one could achieve *additional security for the encrypted data by keeping the encryption algorithms themselves secret;*
- Most experts does not support such idea:
  - It is almost impossible to keep the details of successful algorithm secret: example of RC2 and RC4 data encryption algorithms;
  - If the algorithm has a hidden flaw, then it is could be discovered too late: example of CSS algorithm for protecting DVD content (reverse
- There are still many patented algorithms and they are protected by law

Legal Regulations of Cryptography

- Motivations (at national level):
  - Cryptography can be used to hide criminal activities;
  - Strong cryptography can make difficult, or almost impossible to conduct search warrants by legal authorities;
- Motivations (at international level):
  - Strong cryptography can make impossible to decrypt correspondence by military, economical, etc competitors, or, in general, unfriendly countries.

US regulatory efforts

- 1980s: special costly, time consuming licences for export machines or programs implementing cryptography;
- 1992: free export of cryptographic programs, but with the restriction on key size: no more than 40 bits;
- 1992-1996 Proposals by US administration to use *key escrow* techniques: Clipper chip, and software key escrow.

Clipper chip

- Escrowed Encryption Standard (Clipper Chip);
- A cheap tamper-proof chip,each with unique ID;
- A classified encryption algorithm;
- A back door is embedded and government has a copy of a key used in every such a chip, so when authorized, every encrypted message can be decrypted
- Mechanisms to ensure security of keys and no unauthorized use of the “back door”;
- 1997: Leading cryptographers and computer scientists published a report: “… government encryption plan is risky and impractical”.

Potential problems with Clipper Chip

- The potential for insider abuse;
- The creation of new vulnerabilities and targets for attack;
- Scaling;
- The difficulties of properly authenticating requests for keys;
- The cost;

US regulations

- January 2000, new regulations:
  - Allowed export of cryptographic products with *any key* length after a technical review to any country that was not specifically listed a terrorist country;
  - Essentially, export control on strong cryptography was eliminated;

International agreements on cryptography

- **Wassenaar Arrangement** on Export Control fro Conventional Arms and Dual-Use Goods and Technologies;
- 1996 – Present;
- Allows export of mass-market software;
- Allows export of all products that use encryption to protect intellectual property

Digital Rights Management

- Digital Millennium Copyright Act (US, 1998):
  - criminalizes production and dissemination of technology for circumventing the control access for the copyrighted works
  - Controversy: Dmitry Sklyarov case (2001) and Edward Felten case (2000)
  - Copyright protection vs legality of cryptanalytic research?
- Copyright Directive (EU 2001)

International agreements on cryptography

- Council of Europe Recommendation 95 (13), 1995-Present; recommendations on use of cryptography;
- European Union Council Regulation 1334/2000:

  export to other EU countries unrestricted; export to other countries may require an authorization, or license;

Privacy Protection: OECD Guidelines

- In 1980, the Organization for Economic Development and Cooperation (OECD) adopted a set of privacy guidelines;
- **Aim:** to harmonize the growing number of privacy regulations throughout the industrialized world;
- The guidelines were specifically designed to deal with growing problem of *transborder data flows;*
- The guidelines consist of eight main principles.

OECD Guidelines: main principles

- **Collection Limitation Principle:** there should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means;
- **Data Quality Principle:** personal data should be relevant to the purposes for which it is to be used, should be accurate, complete, and kept up to date.

OECD Guidelines: main principles

- **Purpose Specification Principle:** the purposes for which personal data is collected should be specified not later that at the time of data collection and the subsequent use limited to the fulfilment of those purposes;
- **Use Limitation Principle:** Personal data should not be disclosed, made available, or otherwise used for purposes others that those specified in advance, except:
  - With the consent of the data subject; or
  - By authority of law

OECD Guidelines: main principles

- **Security Safeguards Principle:** personal data should be protected by reasonable security safeguards again such risks as loss, unauthorized access, destruction, etc.;
- **Openess Principle:** there should be a general policy of openess about developments, practices and policies with respect to personal data.

OECD Guidelines: main principles

- **Individual Participation Principle:** an individual should have the right:
  - To obtain the data from a data controller, or confirmation of whether or not the data controller has data relating to him;
  - To be given reasons if a request made specified as above is denied, and to be able to challenge such denial; and
  - To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.

OECD Guidelines: main principles

- **Accountability principle:** a data controller should be accountable for complying with measures which give effect to the principle stated above

---

The OECD Guidelines do not have the force of law, but are instead used as guidelines for each OECD member country (30 countries at the moment, including UK) when passing its own laws

European Data protection

European Union Directive 95/46/EC, the Directive on Protection of Personal Data:

http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm

UK data protection act

Data protection act 1998:

http://www.opsi.gov.uk/acts/acts1998/19980029.htm

Three ballot voting system

New secure voting system by Ronald R.Rivest (autumn 2006)

"I am not filing for any patents on this approach, and I encourage others who work on extensions, improvements or variations of this approach to act similarly. Our democracy is too important. . . R.Rivest"

See details at
http://theory.lcs.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf