

Sociological Issues in Cryptography

Dean Sabella

Introduction

- Should cryptography distribution be controlled?
- What role does the government play in cryptography?
- How can we balance privacy and security?

Historical role of government

- Traditionally government (through military) was main user of cryptography.
- Now far more widespread, hence perceived need for regulation
- Presents new challenge for government

Importing Cryptography

- There are no restrictions!

Domestic Cryptography

- Generally fine to use cryptography in Australia
- Encryption equipment connected to PSTN may need ACA certification
- Governmental communications may need DoD clearance

Export restrictions

- Cryptography can be considered munitions
- Many countries (including Australia) are signatories to Wassenaar Arrangement

The Wassenaar Arrangement

- Oversees export and distribution of weaponry & “dual use goods”
- Agreed to by 33 countries, including Australia, in 1996
- Replaced COCOM, which ended in 1994
- Waiver for non-specialised software (GSN)
- Australia refuses to apply GSN in full

Australian Legislation

- **Customs Act 1901**
 - Pt VI The Exportation of Goods
 - Division 1 Prohibited Exports, Section 112, 2AB
- **Customs (Prohibited Exports) Regulations, Regulation 13E**
 - Items on *Defence and Strategic Goods List* prohibited – enforced by Customs Act.

Exporting Cryptography

- Need license to export crypto
- Administered by the Defense Signals Directorate
- No appeal mechanism, opaque process
- No provision for FOI requests
- Generally no problem with ≤ 56 bits

US Export Controls

- Generally considered problematic for business
- Export restrictions relaxed in 2000 as a result
- Applied Cryptography, by Bruce Schneier
 - Legal to export source listings in book, but not floppy disk
 - “defence article under category XIII(b)(1) of the United States Munitions List”
- PGP source exported in hardcopy

Anti-circumvention restrictions

- Copyright Amendment (Digital Agenda) Act 2000
- Like USA's DMCA, implements WIPO Copyright treaty
- Allows for breaking crypto to be a criminal offence
- e.g. Sklyarov and DMCA

How can governments intercept

- Data encrypted using some algorithm
- Can be decrypted by authorized agency
- Relies on a trusted third party
- Usually through a process called *key escrow*.

Key escrow details

- 3 main components:
 - User Security Component (USC)
 - Key Escrow Component (KEC)
 - Data Recovery Component (DRC)

See *Communications of the ACM*, Vol. 39, No. 3, March 1996 for more detail

User Security Component

- Encrypt/decrypt data
- Applies to communications and stored data
- Stores identifiers and keys for emergency decryption
- Binds Data Recovery Field (DRF) to encrypted data
- Can be implemented in hardware or software

Key Escrow Component

- Stores data recovery keys
- Part of key management infrastructure
- Operated by trusted parties
- Keys can be split among several parties
- All usual considerations apply as for CAs
- Authorize and validate requests from DRC

Data Recovery Component

- Recovers plaintext using KEC and DRF
- Acquires K for real- or nonreal-time
- May need to use brute force if KEC only provides partial keys
- Need safeguards on what is done with keys

Escrow systems

- **Best known example – Clipper Chip**
 - Tamper resistant IC, implements EES.
 - Developed by NSA
 - Classified protocol, so cryptanalysis not possible
 - Half the recovery key stored with NIST and half with Treasury
 - Has unique key and Law Enforcement Access Field (LEAF)
- **Many others available**
 - <http://www.cosc.georgetown.edu/~denning/crypto/Appendix.html> for descriptions

Clipper operation

- Each end agrees on 80-bit session key (using any method, e.g., RSA)
- Message encrypted and sent
- LEAF field attached
 - Exact details classified
- Receiver then verifies LEAF and decrypts message

Clipper Interception

- $LEAF = E[KF](E[KU](KS) \parallel UID \parallel EA)$
- How can DRC intercept?
 - Decrypts LEAF with family key
 - Provides serial number to KEC
 - ? Now knows serial number and encrypted session key
 - Gets warrant for serial number, obtains KU
 - Uses KU to obtain session key
 - Uses session key to decrypt message

Clipper Politics

- Original proposal was all interaction with US Government required Clipper
- Voluntary for all other transactions
- Officially abandoned in 1998

Arguments for Clipper:

- Government needs to be able to intercept criminal communications
- Key splitting reduces illegal access
- Requires court order for recovery, protecting privacy
- Voluntary standard

Arguments against Clipper

- Communications not totally private
- Could be manipulated for political reasons
- Complexity of system scares industry
- Smart criminals won't use clipper, or pre-encrypt
- Open to abuse even with safeguards
- Once keys released, can intercept indefinitely
- Will it stay voluntary?

Escrow in Australia?

- **Pro-escrow paper written in 1995**
 - Steve Orłowski, (Assistant Director, Attorney-General's Department)
 - Personal paper, not necessarily view of Government
- **Walsh report 1997 casts doubts on workability and desirability of escrow**

Privacy considerations

- Mechanism for generating own keys
- Anonymous transactions
- Public Key Registers
 - Used to link private data together?
 - Requires unique ID info – what availability?
 - How to stop malicious CRL entries
 - Ability to accumulate multiple keys discreetly
 - New rights and laws probably needed

Implications of key escrow

- Do we trust third party?
 - Can't use to combat tyrannical regime
 - Electoral sabotage
 - No longer true privacy
- Governments can regulate communications

What, if not escrow?

- Focus seems to be on legally enforceable surrender of keys
- Regulation of Investigatory Powers Act
 - UK, 2000
- Cybercrime Bill
 - Australia, 2001
 - Based on European convention
 - Also prohibits cracking tools
- Freedom not to incriminate yourself?

Conclusion

- **Governments want to regulate strong crypto exports**
 - Will become more widespread with Wassenaar Arrangement
- **Want to listen to internal communications**
 - Escrow out of favour for now, could still make a comeback
 - Current fashion is key recovery through legal channels
- **Want crypto that's legally secure as well as crypto secure**
 - As per WIPO guidelines

Sociological Issues in Cryptography

Questions?