Key Escrow and its risks

(an illustration of organizational and other issues

Presented by

Magnus Almgren

(slides adapted from Erland Jonsson)

Key Escrow System

- Other names are Key Recovery, Data recovery, Exceptional Access and Trusted Third Party (Fullmaktssystem, Depositionssystem)
- **Main characteristics/definition**:
  - A System for Law-Enforced Covert Surveillance
  - A mechanism through which a third party can get access to the clear text of encrypted data without the knowledge of the user.
  - Requires the existence of one or many very sensitive keys that must be protected for very ling times

Requirements from authorities

- Access to keys must be possible without end-user knowledge or consent
- Access to communicated as well as stored data
- Ubiquitous adoption/International coverage
- High Availability (less than 2h, around the clock, all year)
- Key escrow should be possible for long times afterwards
- Cp “Self-Escrow” (e.g. for employees in a company)

Risks with Key Escrow (1)

There are a number of fundamental new risks with a system of the type suggested for Key Escrow.

1. Introduces of new vulnerabilities (i.e. a risk for the basic functionality of the system)
   - new potential (illicit) access to data
   - insider misuse
   - new (very valuable) targets for attacks
   - destroys Forward Secrecy
   - transmission and storage of the keys

Risks with Key Escrow (2)

2. Complexity
   - hard to design such systems (several bugs found in the former “US Escrowed Encryption Standard, based on the Clipper chip).
   - scale factors
   - operational complexity
   - authorization for Key Recovery new potential (illicit) access to data

Risks with Key Escrow (3)

3. Costs
   - operational costs (for agents)
   - product design costs
   - costs for authority control, evaluation, accreditation, etc
   - end-user costs

Summary

- The suggested Key Escrow system is a good example of the problems that arise when attempting to construct very large, complex systems that have to be secure.
- See “The Risks of Key Recovery, Key Escrow, Trusted Third Party and Encryption”
  http://www.cdt.org/crypto/risks98/