Key Recovery

Steven M. Bellovin
smb@research.att.com
973-360-8656

Issues

- Protocol Design
- System Issues

Protocol Design

- Cryptographic protocol design is *hard*.
- New bugs are still being found in the oldest published protocol.
- Key recovery is a new problem, without a long history of work.
- Not surprisingly, key recovery protocols have had bugs, too.

System Issues

- Protocol design is the easy part of key recovery.
- All aspects of the total system design must be scrutinized, including the human element.
- Can an attacker go around the cryptography?

Authorizations

- How do key recovery centers recognize almost 900,000 members of 17,000 different U.S. law enforcement agencies (1992 figures)?
- Are all law officers incorruptible?
  - Just today's AP wire listed at least four different stories of illegal activities by government officials.
- How are authorized requests communicated to many different key recovery centers, by many different law enforcement agencies? How are they validated?

Running a Key Recovery Center

- What if it is hacked?
- What if someone breaks in?
- What if one of its employees is corrupted or blackmailed? (Our top intelligence and law enforcement agencies have suffered these types of failures.)
- Recovery centers are prime targets for many different kinds of attacks.

Corporate Key Recovery

- No need at all for recovery of communications keys.
- Storage key recovery is almost always done with the co-operation of the key owner.
- Authorization is local, and generally done by personal knowledge and recognition.
- Companies make their own risk/benefit tradeoffs.

Benefits of Secure Cryptosystems

- Cryptography is an absolute necessity to secure the Internet.
  - It's even necessary in corporate Intranets.
- Corporate secrets can be safeguarded, including against attacks by foreign intelligence agencies.
- Personal privacy can be protected.
- In short, many crimes can be prevented.