# Key Management

- Choosing long, random keys doesn't do you any good if your clerk is selling them for $10 a pop at the back door
- Or if you keep a plaintext list of them on a computer on the net whose root password is "root"
- Proper key management is crucial

# Desirable Properties in a Key Management System

- Secure
- Fast
- Low overhead for users
- Scaleable
- Adaptable
  - Encryption algorithms
  - Applications
  - Key lengths

# Users and Keys

- Where are a user's keys kept?
- Permanently on the user's machine?
  - What happens if the machine is cracked?
- But people can't remember random(ish) keys
  - Hash keys from passwords/passphrases?
- Keep keys on smart cards?
- Get them from key servers?

# Key Servers

- Special machines whose task is to generate, store and manage keys
- Generally for many parties
- Possibly Internet-wide
- Obviously, key servers are highly trusted

# Security of Key Servers

- The key server is the cracker's holy grail
  - If they break the key server, everything else goes with it
- What can you do to protect it?

# Security for Key Servers

- Don't run anything else on the machine
- Use extraordinary care in setting it up and administering it
- Watch it carefully
- Use a key server that stores as few keys permanently as possible
  - At odds with need for key storage
- Use a key server that handles revocation and security problems well

# Single Machine Key Servers

- Typically integrated into the web browser
  - Often called *key chains* or *password vaults*
- Stores single user's keys or passwords for various web sites
- Usually protected with an overall access key
- Obvious, encrypted versions stored on local disk

# Security Issues for Single Machine Key Servers

- Don't consider one that doesn't store keys encrypted
- Issues of single sign-on
  - If computer left unattended
  - In case of remote hacking
    - Anything done by your web browser is "you"

# Local Key Servers

- Can run your own key server machine
  - Stores copies of all keys you use
- Possibly creates keys when needed
- Uses careful methods to communicate with machines using it
- E.g., Sun StorageTek Crypto Key Management System

# Key Storage Services

- Third party stores your keys for you
  - In encrypted form they can't read
- ANSI standard (X9.24) describes how third party services should work
- Not generally popular
- HyperSafe Remote Key System is one example
- Variants may become important for cloud computing

# The Dark Side of Key Storage

- Governments sometimes want your crypto keys
- Since they might not be able to read your secret data without them
- They'd often prefer you didn't know they asked . . .
- *Key escrow* services can allow this

# Key Escrow, Clipper, and Skipjack

- In the 1990s, US government tried to mandate key escrow
  - For encrypted network communications
- Based on a new cipher (Skipjack)
- Implemented in a special chip (Clipper)

# Basic Idea Behind Clipper

- Encrypted messages would carry special information
- Privileged parties could use it to retrieve the crypto key used
- Governments would be among those parties
- But, of course, they'd never abuse it . . .

# What Happened to Clipper?

- Totally fried by academic security community
  - Experts united in their scorn for both idea and particular implementation
- Chips were built
- Nobody used them
- The idea is now dead, but . . .

# The NSA and Key Services

- Snowden revelations have shown that the NSA frequently goes after keys
- Will commercial key escrow services give keys to the NSA?
- If not, will the NSA try to get them, anyway?
- Key servers are a big, fat target for folks like the NSA