

Outline

- ◆ Encrypting files
- ◆ Encrypting communication
- ◆ Encrypting music
- ◆ Encrypting videos

Encrypting Files

- ◆ Attacks on standard file protection:
 - Boot computer with a new operating system CD
 - Steal hard drive
- ◆ File encryption
 - Files are stored in encrypted form on disk
 - Only owner and other authorized users has the secret key for decrypting the file
- ◆ Issues:
 - Which encryption scheme should be used?
 - Should every file be encrypted with the same key?
 - Where should the secret key be stored?
 - Should authorized users share the same secret key?
 - Should administrators always have the secret key?

Simple File Encryption

- ◆ A simple file encryption method consists of
 - Encrypting each file to be protected with symmetric-key encryption (e.g., AES)
 - Using a different key for each file
 - Distributing keys to authorized users
- ◆ Advantages
 - Symmetric-key encryption is efficient and faster than public-key encryption
- ◆ Disadvantages
 - Storage of multiple keys (one per file)
 - Distribution of keys to authorized users
 - Key has to be shared with each authorized user
 - Revoking access by a user to a file requires
 - ◆ re-encrypting the file
 - ◆ distributing a new key to the authorized users of the file

Better File Encryption

- ◆ More efficient key management in file encryption:
 - Using symmetric encryption (e.g., AES), encrypt each file with a different **file encryption key (FEK)**
 - Using public-key encryption (e.g., RSA), encrypt FEK with the public key of each authorized user
 - Store encrypted versions of FEK with file
 - This approach is used in Windows XP, Linux, and PGP
- ◆ Advantages:
 - File encryption and decryption is efficient
 - Each user stores a single private key and makes available a single public key
- ◆ Disadvantages:
 - Revoking access by a user to a file requires re-encrypting the file (but no key distribution is needed)

Encrypting Communication

- ◆ Alice and Bob communicate over the internet
 - Communication between browser and web server
 - Remote shell connection
- ◆ Typical approach, used in TLS and SSH
 - Alice and Bob use public-key cryptography to agree on
 - ◆ stream-encryption key s
 - ◆ content-integrity key c
 - The communication stream is partitioned into blocks
 - For each block b , the following is transmitted
$$E_s(b \mid H(c \mid b))$$
 - Hashing the block with the content-integrity key defends against modifications of the block
 - Encrypting with the stream-encryption key defends against eavesdropping

Digital Rights Management

- ◆ Digital Rights Management (DRM) refers to hardware and software systems providing access control for digital content (e.g., music and video files)
- ◆ DRM aims at preventing the illegal altering, sharing, copying, printing, and viewing of digital media
- ◆ Copyright owners claim DRM is needed to prevent revenue lost from illegal distribution of copyrighted material
- ◆ Most DRM schemes used in practice are
 - poorly designed
 - easily broken

Digital Millennium Copyright Act

◆ DMCA highlights

- Illegal to circumvent anti-piracy measures built into software
- Unlawful to create, sell, distribute, or publish information about devices that illegally copy software
- Some exemptions for research purposes
- Provides exceptions to nonprofit libraries, archives, and educational institutions in some cases

◆ DMCA was highly lobbied by the media industry

Music Encryption

- ◆ Software music players (e.g., iTunes) encrypt purchased songs
- ◆ Typical DRM encryption approach
 - Songs are stored encrypted on disk
 - Decryption keys stored within player
 - Keys shared with a limited number of trusted devices
- ◆ Attacks on poorly designed DRM encryption
 - Capture unencrypted song while being transmitted
 - Reverse-engineer player to find decryption key
 - Write rogue player
 - Brute force decryption

Video Encryption

- ◆ Key management for trusted video players
 - A controller distributes protected content to a collection of n players
 - The players share a common symmetric key with the controller
 - Each movie is encrypted with the shared key and broadcast to all the devices
- ◆ Some devices (traitors) are cloned or used to illegally copy and distribute protected content
- ◆ Problems:
 - Identifying traitors
 - Revoking traitors

