CN414
Computer Network Security

Week 12:- Digital Right Management

By

Dr. Piya Techateerawat

Digital Right Management

- **DRM Technology**
- DRM Application
- DRM Algorithm Example

Digital Right Management

- Access control technology to limit usage of digital media or devices.
- It may or may not include the copyright protection
- The initial group that use is Sony, Apple, Microsoft and BBC

Digital Right Management

- DRM Technology
- **DRM Application**
- DRM Algorithm Example

Digital Right Management

- DRM is initial proposed with Content Scrambling System (CSS)
- This CSS is used on DVD, player requires a license of CSS playing

Digital Right Management

- Microsoft has PVP (Protected Video Path)
- This PVP allow only signed software to access the content.
- The feature of PVP is able to encrypted data on the transmission to monitor and graphic card.

Digital Right Management

- HD DVD and Blu-Ray use AACS (Advance Access Content System)
- This is the collaborated between Sony, Disney, Intel, Microsoft, Toshiba, IBM, Warner Brothers and Panasonic.

Digital Right Management

- Internet
  - Apple – iTune Store (Apple's Fair Play)
  - Napster music store
  - Sony via Sonic Stage software
  - Adobe (Adobe Protected Streaming)

Digital Right Management

- DRM Technology
- DRM Application
- **DRM Algorithm Example**

Digital Right Management

- MS-DRM version 2
  - Target WMA file
  - Components
    - ECC for public key
    - DES for block cipher
    - RC4 for stream cipher
    - SHA-1 for hash function

Digital Right Management

- Binary data is encoded with Base 64
  - But Microsoft change some character
    - E.g.
      - "*" instead of "/"
      - "/" instead of "@"
      - "!" instead of "%"
      - Therefore it require customize decoding

Digital Right Management

- Files
  - Drmv2clt.dll – basic functionality
  - Blackbox.dll – cyrptography function
  - IndivBox.key – individulaize of blackbox
  - Drmv2.lic – file of license
  - Drmv2.sst – secure state of each license
  - V2ks.bla – public/private keys store
  - V2ksndv.bla – individualized v2 key store

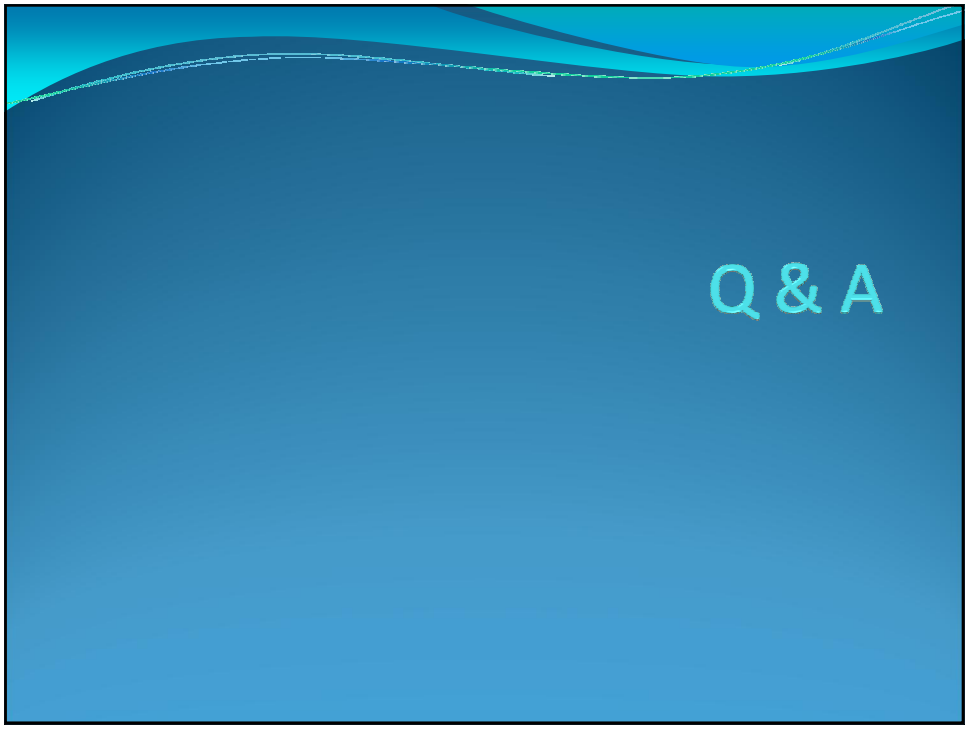
Digital Right Management

- MAC (Message Authentication Code)
  - Using proprietary “MultiSwap”
  - Data cipher block 64 bits
  - Key 12 sets of 32 bits
  - First 6 encode first 32 bit of data where the rest 6 key set encode the last 32 bit of data

$$f(a)=swap(swap(swap(swap(swap(a*k_{[0]})*k_{[1]})*k_{[2]})*k_{[3]})*k_{[4]}) + k_{[5]}$$

Reference

- http://www.spinnaker.com/crypt/drm/freeme/Technical


Q & A