Lecture 14: Key Managements, Standard, and Emerging Technology

Ching-Yung Lin
Department of Electrical Engineering
Columbia University, New York, NY 10027

Course Outline

- Multimedia Security:
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – Confidential MM
  - Watermarking – Uninfringible MM
  - Authentication – Trustworthy MM

- Security Applications of Multimedia:
  - Audio-Visual Person Identification – Access Control, Identifying Suspects
  - Media Sensor Networks – Event Understanding, Information Aggregation
  - Standard and Emerging Technologies
Evolution of Digital Media Applications, Challenges, and Standards

Signals → Features → Semantics → Knowledge

Recent Past

Near Future

Applications

- MPEG-1, -2, -4
  - Video storage
  - Broadband
  - Streaming video and delivery
- MPEG-4, -7
  - Content-based retrieval
  - Multimedia filtering
  - Content Adaptation
- MPEG-7
  - Semantic-based analysis and retrieval
  - Enterprise content management
- MPEG-21
  - E-commerce of electronic content
  - Flexible business models
  - Digital items

Problems and Innovations

- Compression
- Coding
- Communications
- Similarity-based searching
- Object-based coding
- Modeling and classification
- Personalization and summarization
- Media mining
- Decision support
- Rights management

MPEG-21 Multimedia Framework: "Transactions of Digital Items"

- Users and participants in the content value chain seamlessly exchange content in form of "digital items" across networks and devices
- Framework supporting all forms of electronic content/intellectual property (video, music, learning objects, on-line reports, etc.)
- Digital Item = bundling of:
  - Essence (i.e., media resources)
  - Metadata
  - Rights expressions
  - Identifiers
- Example: Digital music package
**MPEG-21 Standard Framework**

- “Interoperable Multimedia Framework”
- “E-Commerce for E-Content”
- “Digital Audio-Visual Framework”
- **Vision:** “To enable transparent and augmented use of multimedia resources across a wide range of networks and devices.”
- **Goal:** Integration of technologies for content identification and consumption
- **Output:** ISO technical report and technical specification (International Standard in 2003)

**Authorization using MPEG-21 Rights Expression Language**

- **Rights Expression Language (REL):**
  - Specifies a language for declaring rights and permissions associated with use of digital items.
  - The rights expressions use terms as defined in the Rights Data Dictionary.
- **Rights Data Dictionary (RDD):**
  - Specifies a model and dictionary for clearly and consistently defining terms for use in rights expressions.
Rights Expression Language (XrML) (I)

- XrML 2.0:
  - developed by Xerox
  - adopted by MPEG-21
- Issuer(s) + Grant(s) = License
- Schemas:
  - Core Schema
  - Stand Extension Schema
  - Content Extension Schema

- Mandatory Elements in Core Schema:
  - Principal: all Principal, key holder
  - Right: Issue, Revoke, Possess Property, Obtain
  - Resource: Digital Resource
  - Condition: all Conditions, validity Interval, revocation Freshness, exist Right, pre-requisite Right

- Optional Elements in Standard Schema:
  - Grant: exercise limit, seek approval, track report, territory, valid time, etc.
  - Fee: cash, payment per use, best price under, etc.
  - Name Extensions: email, dns, common, x509 subject, etc.
  - Revocation Extension: revocable

A sample XrML Grant

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<license xmlns="http://www.xrml.org/schema/2001/11/xrml2core" >
  <grant>
    <keyHolder>
      <info>
        <dsig:KeyValue>
          <dsig:RSAKeyValue>
            <dsig:Modulus>Fa7wo6NYfmvGqy4ACSWcNmuQfbejSZx</dsig:Modulus>
            <dsig:Exponent>AQABAA==</dsig:Exponent>
          </dsig:RSAKeyValue>
        </dsig:KeyValue>
      </info>
    </keyHolder>
    <possessProperty />
    <sx:commonName>Alice Richardson</sx:commonName>
  </grant>
</license>
```

Rights Expression Language (XrML) (II)

- Optional Elements in Standard Schema:
  - File Management Rights: access, backup, delete, execute, restore, etc.
  - Transport Rights: copy, loan, transfer
  - Derivative Works Rights: edit, embed, extract
  - Render Rights: export, play, print
  - Configuration Rights: install, uninstall
  - Extension to Resources: digital Work, Metadata, security Level,
  - Extension to Condition: destination, source, helper, renderer, watermark
MPEG IPMP Extension

- Applied to any MPEG multimedia representation
- Objectives:
  - Allow the same protected content to be consumed on different vendors’ Terminals.
  - Allow the same content to be protected by different vendors’ IPMP Tools.

**Architecture Diagram**

**DVD Content Scramble System Overview**

- Content De-scrambling Process:
  - Mutual Authentication
  - Decoding disk
  - Send disk and title keys
  - Send sectors
  - Host decodes the title key using the disk key
  - The host decodes the sector using the title key and the sector key
DVD Content Scramble System

Linear Feedback Shift Register (LFSR):  
- generating pseudo-random bit stream  
- use this bit stream to XOR it with the original stream  
- the decoder uses XOR again to get the original stream

Disk and Player Keys  
- each player has a small number of keys  
- each disk is encoded by a disk key.  
- each disk contains a hidden sector  
- the hidden sector contains the disk key encrypted with all 409 possible player keys.  
- it holds the disk key encrypted with the disk key.  
- the player decrypts the appropriated entry and then verifies that it has correctly decoding the disk key, by decoding the decrypted disk key.

Encryption and Key Managements

- **5C DTCP (Digital Transmission Content Protection):**  
  - Authentication and data encryption with a digital bus (primarily the IEEE 1394 Firewire bus).  
  - Supported by Hitachi, Intel, Matsushita, Sony and Toshiba.

- **Cisco OCCAM (Open Conditional Content Access Management):**  
  - Public key infrastructure with a central authority  
  - One-way protocols lead to more robust implementations

- **IBM xCP Cluster Protocol**  
  - Broadcast encryption  
  - Derived from Content Protection for Recordable Media (supported by IBM, Matsushita, Intel and Toshiba).
Broadcast Encryption

- Algorithmic Lineage
  - Broadcast encryption - Fiat and Naor, Crypto ’93
  - Tracing traitors - Chor et al., Crypto ’94

- Alternative to Public Key Encryption
  - 2 or 3 orders of magnitude less overhead
  - One-way protocols lead to more robust implementations

- Supports key revocation
  - Unlike global secret schemes in which a single hacking event breaks the whole system

Cluster Model

- mkbserver
- authTable
- Content + usage rules
- client
- MKB
- authTable
- Content + usage rules
Media Key Blocks

- Scheme is large matrix of random keys
- Each device assigned one key from each column

MKB is data structure w/multiple ciphers of same media key under different device keys

Digital Item Adaptation using MPEG-7 and MPEG-21

- Media Description
  - MPEG-7 Description Schemes
- Usage Environment
  - MPEG-7 User Preferences
  - MPEG-21 Usage Environment
- Content Adaptability
  - MPEG-7 Media Resource Requirement
  - MPEG-21 Media Resource Adaptability
A Personalization and Summarization System Architecture

- **Database Server**
  - Content Sources
  - MPEG-7 Media Descriptions
  - MPEG-21 Rights Expression
  - Content Adaptability

- **Media Middleware**
  - Select Personalized Contents in Personalization Engine
  - Retrieve and Adapt Contents in Adaptation Engine

- **User Client**
  - Request for Personalized Content
  - Communicate Usage Environment

---

**Database Server**

- **Media Descriptions**
  - MPEG-7 DS

- **Rights Expression**
  - MPEG-21 RE

- **Content Adaptability**
  - MPEG-7 Media Resource Requirement
  - MPEG-21 Media Resource Adaptability

- **VideoAnnEx**
  - MPEG-7 Annotation Tool

- **VideoSue**
  - MPEG-21 MRA

- **VideoEd**
  - MPEG-21 MRA

- **VideoAnn**
  - MPEG-7 MRR

- **VideoMPEG**
  - MPEG-7

---

**Server**

- Media Descriptions
- Rights Expressions
- Content Adaptability

**Middleware**

- Personalization Engine
- Adaptation Engine

**Client**

- Usage Environment
- User Query
- Display Client
Media Middleware

**Personalization Engine**
- Content Selection
  - Video selections
  - Scene selections
- Format Selection
  - Format, frame rate, display size, color

**Content Adaptation Engine**
- Format Transcoder
  - Video, Image, Audio, Text
- Scale Transcoder
  - Frame rate, display size, color
- Presentation Composer
  - Spatial composition, temporal ordering

**User Client**

- **Usage Environment**
  - Persistent Data
  - User Profile
    - English speaker, NYC resident
  - Device Profile
    - Color display, audio capability
  - Transmission Profile
    - 56K modem, ethernet

- **User Query**
  - User Specific Preferences
    - Keyword search, CBR

**Middleware**

**Personalization Engine**
- DID Parser
- Request Parser

**Processing Engine**
- Summarization
- Semantic Query
- Feature-Based Query
- Content Selection
  - Format Decision

**Adaptation Engine**

**User Client**

**Usage Environment**
- User Profile
- Device Profile
- Transmission Profile

**User Query**
- Topic Preference
- Query Keywords
- Time Constraints

**Display Client**
- PCs (Browser, Application)
- PDA (Palm, Win_CE)
- Phones/Watches (WAP, Jini)
Media Middleware
Video Summarization on Usage Environment

\[
P = \text{user preference vector, where } p_i \text{ denotes the preference weighting for concept } i.
\]

\[
A = \text{attribute matrix, where score } a_{ij} \text{ is defined as the relevance of concept } i \text{ in shot } j.
\]

\[
W = \text{weighted importance vector, where } w_i \text{ is the weighted concept for shot } i.
\]

\[
W = \begin{bmatrix}
w_1 & w_2 & \ldots & w_M
\end{bmatrix}
\]

\[
A = \begin{bmatrix}
a_{1,1} & a_{1,2} & \ldots & a_{1,N} \\
a_{2,1} & a_{2,2} & \ldots & a_{2,N} \\
\vdots & \vdots & \ddots & \vdots \\
a_{M,1} & a_{M,2} & \ldots & a_{M,N}
\end{bmatrix}
\]

\[
P = \begin{bmatrix}
p_1 \\
p_2 \\
\vdots \\
p_M
\end{bmatrix}
\]

A is generated manually, semi-automatically, or automatically.

Media Middleware
Compressed-Domain MPEG Editing Tool

- Run-time user selection of video shots
- Fast creation of personalized summaries
- On-line preview of editing results
- Compatible with MPEG-1 and MPEG-2
- Demo: http://sapphire.watson.ibm.com/VideoEd
User Client
PDA Devices

- Browsing
  - Channels
  - Links
- Preferences
  - Video Source
  - Preferences
  - Time Constraint
- Queries
  - Topics
  - Keyword Search
  - Time Constraints

User Client
IBM Websphere Portal Server

- Usage Environment
  - User Preference Topics
    [news, entertainment, education]
  - Device [terminal, PDA]
  - Network Constraint
- User Query
  - Topic Preferences
  - Keyword Search
  - Time Constraint
Interoperable Multimedia Content Management: Relevant Standards – MPEG-7 and MPEG-21

Metadata is critical for describing essential aspects of content:
- Main topics, author, language, publication, etc.
- Events, scenes, objects, times, places, etc.
- Rights, packaging, access control, content adaptation, etc.

Conformity with open metadata standards will be a vital:
- Allows faster design and implementation
- Interoperability with broad field of competitive standards-based tools and systems
- Leveraging of rich set of standards-based technologies for critical functions such as content extraction, advanced search, and personalization

Relevant critical standards for interoperable multimedia CM:
- MPEG 7 Multimedia Content Description Interface
- ISO/IEC standard for multimedia metadata (XML-Schema based)
- MPEG 21 Multimedia Framework
- ISO/IEC standard for transactions of digital items, rights management, and content adaptation

Summary of benefits:
- MPEG-7 allows interoperability of systems and tools for multimedia content analysis, annotation, indexing, searching, and filtering
- MPEG-21 allows interoperable transactions of digital multimedia content

---

Summary of Video Personalization and Summarization

Video Personalization and Summarization System allows universal access and personalized content of rich media to any user environment at anytime and anywhere

Innovations
- Standards-based (MPEG-7 & MPEG-21) interoperable solution
- Off-line semi-automatic MPEG-7 XML content annotation
- Digital item adaptation and transactions using MPEG-21
- Optimized content adaptation to user query and user environment
- Real-time compressed domain video composer for MPEG contents

Applications
- Enterprise rich media (e.g., e-Learning, video conferencing, news, communications)
- Wireless (i.e., personalized video clips, image slide shows)

Conclusion
- Methods for automatic rich media annotation, indexing, retrieval, and optimized
Emerging Technologies

- **Complex Network Analysis**

An example of complex network: Power-Law Network


\[
p_k = e^{-\mu} \cdot \frac{m^k}{k!}
\]

The probability distribution of the number of links \(k\) for a random network.

\[
p_k = C \cdot k^{-\tau} e^{-k/\kappa}
\]

Another example of complex network: Small-World Network

Six Degree Separation:
- adding long range link, a regular graph can be transformed into a small-world network, in which the average number of degrees between two nodes become small.

from Watts and Strogatz, 1998

What is a complex network?

- Most real-world networks have complex topological features:
  - Heavy-tail in the degree distribution
  - High clustering coefficient
  - Assortativity or Disassortativity among vertices
  - Community structure at many scales
  - Self-similar hierarchical structure

- Simple networks:
  - Typically represented by graphs such as a lattice or a random graph.
  - Topology structure roughly the same in any part of network.
  - Does not posses the above features

- Examples:
  - Social Networks – studied in sociology, public health, commerce, communication.
  - Computer Networks – WWW, security,…
  - Biological Networks – neurons, genes, protein, animals,…
  - Others: sensor network, river network, power lines, …
Relationships are multi-dimensional and uncovered through network questions

**Actions**
- Communication: How often do you communicate with this person?
- Innovation: How often do you turn to this person for new ideas?
- Advice: How often do you seek advice from this person before making an important decision?

**Awareness**
- Awareness: I am aware of this person’s knowledge and skills
- Valued Expertise: How likely are you to turn to this person for specialized expertise
- Learning: How likely are you to rely on this person for advice on new methods and processes

**Emotional**
- Trust: I believe there is a high personal cost in seeking advice or support from this person
- Access: I believe this person will respond to my request in a reasonable and timely manner
- Energy: I generally feel energized when I interact with this person

Group and Roles

**Central people**
- Sam: Could be a bottleneck or holding group together

**Peripheral people**
- Earl: Goes to others but no one goes to him for information. At risk for leaving. Potentially unrealized expertise

**Sub-groups**
- Group split by function. Very little information shared across groups
Some Roles are especially critical

What happens if Sam leaves the group through layoffs, job reassignment, attrition, merger, retirement?

Attributes can create barriers to collaboration

The connections show that very little communication occurs between countries.
Revealing problems can provoke solutions

A follow-up SNA 14 months later showed great improvement.

Some examples of Degree Distribution

- (a) scientist collaboration: biologists (circle) physicists (square), (b) collaboration of movie actors, (d) network of directors of Fortune 1000 companies
Social Network of Switchboard-2 Dataset

- 679 nodes ➔ edges = 4472
Switchboard-2 Network Degree Distribution

- 679 nodes (actors)
- Out degrees → Normal. In degrees → Abnormal.

The Most Difficult Challenge: State-of-the-Arts?

- Our Objectives: Find important people, community structures, or information flow in a network, which is dynamic, probabilistic and complex, in order to allocate resources in a large-scale mining system.

  - Social Networks in sociological and statistic fields: focus on (1) overall network characteristics, (2) dynamic random graphs, (3) binary edges, etc. 
    - Not consider probabilistic nodes/edges or individual nodes/edges.

  - Epidemic Networks & Computer Virus Network: focus on (1) overall network characteristics – when will an outbreak occurs, (2) regular / random graphs. 
    - Not focus on individual nodes/edges.

  - (Computer) Communication Networks: focus on (1) packet transmission – information is not duplicated, or (2) broadcasting – not considering individual nodes/edges or complex network topology.

  - WWW: focus on (1) topology description, (2) binary edges and ranked nodes (e.g., Google PageRank) → Not consider probabilistic edges.
What is a Dynamic Probabilistic Complex Network?


### Modeling a Dynamic Probabilistic Complex Network

**[Assumption]** A DPCN can be represented by a Dynamic Transition Matrix \( P(t) \), a Dynamic Vertex Status Random Vector \( Q(t) \), and two dependency functions \( f_M \) and \( g_M \).

\[
P(t) \triangleq \begin{bmatrix}
p_{1,1}(t) & p_{1,2}(t) & \cdots & p_{1,N}(t) \\
p_{2,1}(t) & p_{2,2}(t) & \cdots & p_{2,N}(t) \\
\vdots & \vdots & \ddots & \vdots \\
p_{N,1}(t) & p_{N,2}(t) & \cdots & p_{N,N}(t)
\end{bmatrix},
\]

\[
Q(t) \triangleq \begin{bmatrix}
q_1(t) \\
q_2(t) \\
\vdots \\
q_N(t)
\end{bmatrix},
\]

where

\[
p_{kl}(t) \triangleq \begin{bmatrix}
\text{Pr}(y_{kl}(t) = SE_1) \\
\text{Pr}(y_{kl}(t) = SE_2) \\
\vdots \\
\text{Pr}(y_{kl}(t) = SE_{K_k})
\end{bmatrix},
\]

\[
q_l(t) \triangleq \begin{bmatrix}
\text{Pr}(x_l(t) = SY_1) \\
\text{Pr}(x_l(t) = SY_2) \\
\vdots \\
\text{Pr}(x_l(t) = SY_{Y_l})
\end{bmatrix},
\]

\[
\sum_{\omega \in \Omega_i} \text{Pr}(y_{ij}(t) = SE_{\omega}) = 1,
\]

\[
\sum_{\omega \in \Omega_j} \text{Pr}(x_j(t) = SY_{\omega}) = 1,
\]

and \( x_i(t) \): the status value of vertex \( i \) at time \( t \).

\( y_{ij}(t) \): the status value of edge \( i \rightarrow j \) at time \( t \).
Modeling a Dynamic Probabilistic Complex Network – cont’d

- Also the Network Topology should follow the characteristics of complex network:

  Network topology follows power-law:

  \[
  \Pr(\sum_i u(p_{i,j}) = l) \sim S \cdot l^{-d}
  \]

  where \( u(p_{i,j}) = \begin{cases} 
  1, & \text{if } \exists t, \Pr(y_{i,j}(t) \neq \text{null}) > 0 \\
  0, & \text{else} \end{cases} \)

  \( d \) is typically in the range of 2 ~ 2.5.

  and the clustering coefficient \( C \) is typically > 0.2.

  \[
  C = \Pr(u(p_{j,k}) = 1 \mid u(p_{i,j}) = 1, u(p_{i,k}) = 1)
  \]

Edges are Markov State Machines, Nodes are not

- State transitions of edges: S-D-A-R model. (Susceptible, Dormant, Active, and Removed) This indicates the time-aspect changes of the state of edges.

  Edge view

- States of nodes: S-A-I model. (Susceptible, Active, and Informed)

  Trigger occurs when the start node of the edge changes from state S to state I:

  Node view

  Network view
Advanced Modeling -- Dynamic Probabilistic Social Network [Lin 2006]

- Social networks are usually evolving -- that the relationships and actions of actors are dynamic and probabilistic.

Dynamic Probabilistic Social Network Analysis

- Predict Information Flow based on DPSN analysis – e.g. Phone calls of 679 Midwest universities students.
Predicting behavioral information flow based on DPSN

If information starts spreading from Actor 100, what are the probabilities that the other people got informed?

The Probabilities of the Nodes Receives Information

SmallBlue Ego-- Who does a person know and collaborate?
SmallBlue Find-- find an expert with *useful* knowledge in corporate

SmallBlue Connect – Link people’s knowledge, expertise and social connections
References


Review of Course

- Multimedia Security:
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – Confidential MM
  - Watermarking – Uninfringible MM
  - Authentication – Trustworthy MM

- Security Applications of Multimedia:
  - Audio-Visual Person Identification – Access Control, Identifying Suspects
  - Media Sensor Networks – Event Understanding, Information Aggregation
  - Standard and Emerging Technologies
Final Project

- Due on May 12 (Friday).
- If you are a graduating student, please submit your final project to TA and me by noon May 12.
- Presentation on May 10. Format is similar to the project proposal.
- Demo or online webpages will be welcome.