Introduction to Secure Electronic Commerce

ISA 767, Secure Electronic Commerce
Xinwen Zhang, xzhang6@gmu.edu
George Mason University
Fall 2005

Learning Secure Electronic Commerce

- Available learning programs
  - Master degree program, graduate certificate program, graduate and undergraduate course, single lecture, etc.
- Usual coverage and fundamental issues
  - Cryptography, Access Control, Internet and network security, security protocols, PKI, certificate, etc.
Our Coverage

- We skip details of technologies and mechanisms that can be found in previous, prerequisite classes.
- The details of these issues can be found in textbooks without difficulty.
- Our focus goes beyond them and covers various advanced issues that are found in recent literature.

Electronic Commerce

- Using electronic (networked) connections.
- Virtually everything available in physical world as well as digital goods and services are available in e-marketplace.
- Trades of digital goods and services
  - New technologies
  - New business models
  - New legislations
- More in-depth study in INFS 640 Intro to E-commerce
3 Success Factors for E-commerce

Technology
- Enabler for e-commerce.
- Provides functionality and security
- New business models with new technology
- No bullet proof security yet. (not in near future either)
- Technology does not guarantee any success in e-commerce
  - But can be a key problem to success
Technology

- Technology tradeoffs

Security  Functionality  Cost
Ease of use

Business Model

“A business model is the method of doing business by which a company can sustain itself - that is, generate revenue.” by Michael Rappa, NCSU.

- Bridges/converts technology input to economic value output

Technical Inputs  Business Model  Economic Outputs

Business Model (continued)

- Successful so far
  - Apple iTune service and iPod

- Not so successful
  - Circuit city’s Divx (Digital Video Express) movie rental service (not DivX, the MPEG-4 compression technology)
    - [http://hometheater.about.com/library/weekly/aa062199.htm](http://hometheater.about.com/library/weekly/aa062199.htm)

- In Business
  - Wal-Mart and Netflix DVD rental subscription services

Law

- New legislation for new technology
  - Promises and problems

- Illegal case
  - Previous Napster
  - 321 Studios lawsuit (Aug. 2004)
  - Morpheus and Grokster

- Supreme court’s new decision
  - peer-to-peer companies such as Grokster could be held responsible for the copyright piracy on their networks
  - BitTorrent for legal content
  - Microsoft Avalanche
Our Focus and Approach

- We are focusing on Technology as an enabler
  - Neutral position
  - Security aspects
- Layered approach
  - Traditional, intuitive approach in IT and CS communities
  - E.g., OSI 7 layers, Policy and Mechanism (two layers) approach, .....
OMAM Layered Approach

What?    Objective
  Model
  Architecture
  Mechanism
How?      Assurance

OMAM Examples - MAC

<table>
<thead>
<tr>
<th>What?</th>
<th>Objective</th>
<th>No Information Leakage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Lattices (Bell-LaPadula)</td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td>Security Kernel</td>
<td></td>
</tr>
<tr>
<td>Mechanism</td>
<td>Security Labels</td>
<td></td>
</tr>
</tbody>
</table>

OM-AM Framework    MAC System    Assurance
### OMAM Examples - DAC

<table>
<thead>
<tr>
<th>What?</th>
<th>Objective</th>
<th>Owner-based Discretion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model</td>
<td>ACLs, Capabilities, etc.</td>
</tr>
<tr>
<td></td>
<td>Architecture</td>
<td>Capability-based systems, etc</td>
</tr>
<tr>
<td></td>
<td>Mechanism</td>
<td>Unix file Sys, etc</td>
</tr>
</tbody>
</table>

**OM-AM Framework** | **DAC System** | **Assurance**

### OMAM Example - RBAC

<table>
<thead>
<tr>
<th>What?</th>
<th>Objective</th>
<th>Policy Neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model</td>
<td>RBAC96 model</td>
</tr>
<tr>
<td></td>
<td>Architecture</td>
<td>User-pull, Server-pull architecture, etc.</td>
</tr>
<tr>
<td></td>
<td>Mechanism</td>
<td>Certificates, tickets, etc.</td>
</tr>
</tbody>
</table>

**OM-AM Framework** | **RBAC System** | **Assurance**
OM-AM Examples - UCON

<table>
<thead>
<tr>
<th>What?</th>
<th>Objective</th>
<th>Policy Neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Model</td>
<td>UCON$_{NEC}$ Model</td>
</tr>
<tr>
<td></td>
<td>Architecture</td>
<td>CRM/SRM, CDID architectures</td>
</tr>
<tr>
<td></td>
<td>Mechanism</td>
<td>DRM Technologies, Attribute Certificates, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How?</th>
<th>OM-AM Framework</th>
<th>Usage Control System</th>
<th>Assurance</th>
</tr>
</thead>
</table>

17