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

- Business Model
- Law
Technology

Technology tradeoffs

security  functionality  ease of use  cost

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 DvX, the MPEG-4 compression technology)
- 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, ....

Two Layer Approach

- Traditionally information security has been studied in two layer: policy and mechanism. (Lampson's June 2004 IEEE computer paper)
  - No clear distinction between objective and model
  - models for one policy or objective
- No clear distinction between architecture and mechanism
  - No architectural variation: centralized mainframe system only, no client-server system
OMAM Layered Approach

What?
Objective
Model
Architecture
Mechanism
Assurance

How?

OMAM Examples - MAC

What?
Objective
No Information Leakage
Model
Lattices (Bell-LaPadula)
Architecture
Security Kernel
Mechanism
Security Labels
OM-AM Framework
MAC System
Assurance

OMAM Examples - DAC

What?
Objective
Owner-based Discretion
Model
ACLs, Capabilities, etc.
Architecture
Capability-based systems, etc.
Mechanism
Unix file Sys, etc.
OM-AM Framework
DAC System
Assurance

OMAM Example - RBAC

What?
Objective
Policy Neutral
Model
RBAC96 model
Architecture
User-pull, Server-pull architecture, etc.
Mechanism
Certificates, tickets, etc.
OM-AM Framework
RBAC System
Assurance

OM-AM Examples - UCON

What?
Objective
Policy Neutral
Model
UCONABC Model
Architecture
CORSM, OXID architectures
Mechanism
DRM Technologies, Attribute Certificates, etc.
OM-AM Framework
Usage Control System
Assurance