COMP 3355
Cyber Security

K.P. Chow

University of Hong Kong

Security Threats

- Eavesdropping: intercepting and reading messages intended for other users
- Masquerading: sending and receiving messages using another user's identity
- Message tampering: intercepting and altering messages intended for other users
- Replaying: using previously sent messages to gain another user's privileges
- Infiltration: abusing an user's authority in order to run hostile or malicious programs
- Traffic analysis: observing the traffic to/from a user
- Denial of service: preventing authorized users from accessing various services

Risk Analysis

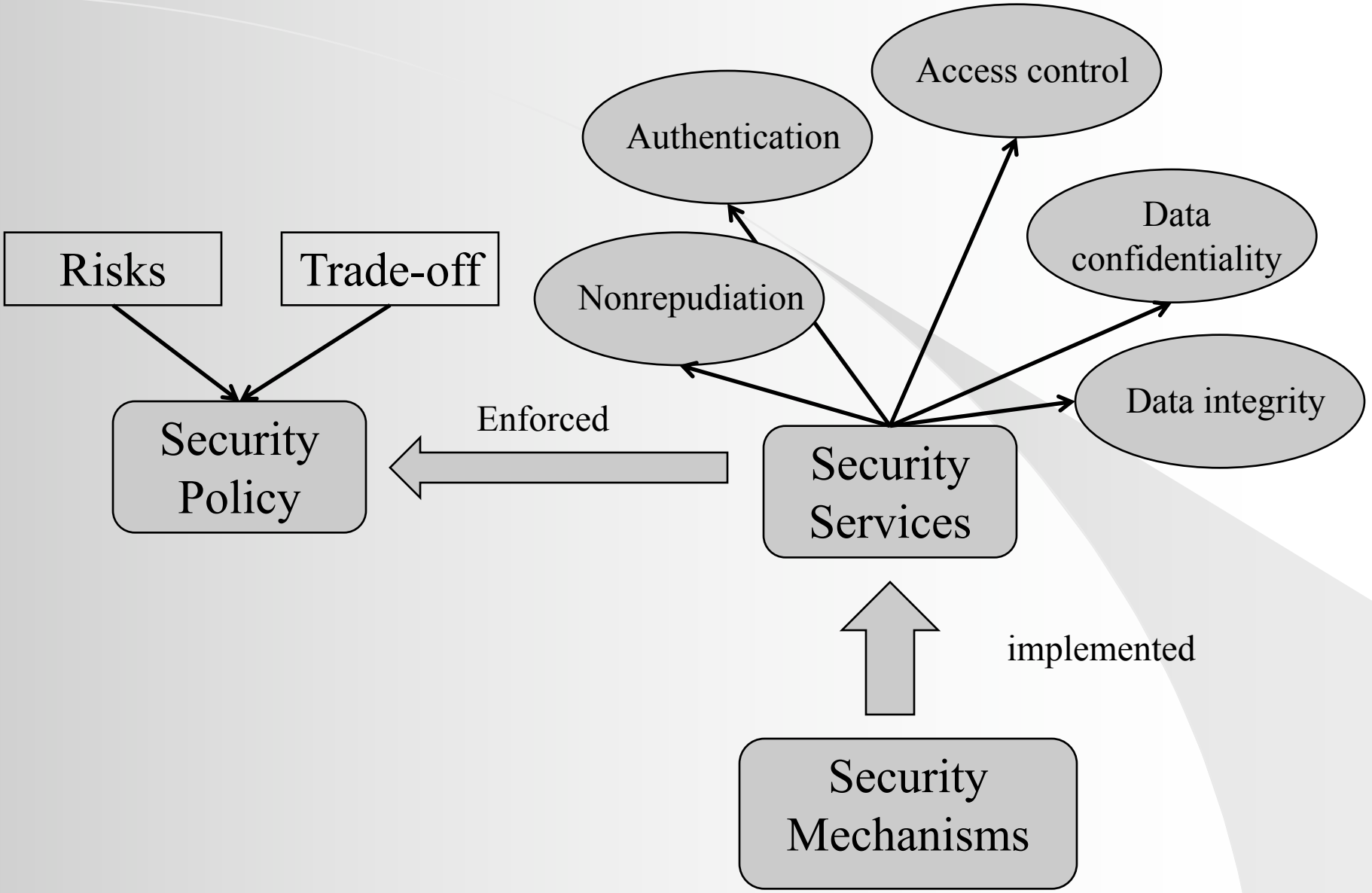
- Starting point to enhance security: risk analysis
  - Evaluates the relationship between
    - the serious of a threat (the cost of repairing any damage caused by a successful attack)
    - its frequency of occurrence (probability), and
    - the cost of implementing a suitable protection mechanism

	Threat Probability		
Seriousness	**Seldom**	**Not often**	**Often**
Not serious	1	2	3
Serious	4	5	6
Very serious	7	8	9

Risk Levels 1 – 9

Security Services

- Risk analysis → security policy
- Should security policy cover all possible risks?
  - NO: a reasonable trade-off between risks and available resources
- How to enforce the security policy? Security services (ISO Security architecture)
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
- Security services are implemented by security mechanisms


Access control
Authentication
Data confidentiality
Nonrepudiation
Data integrity
Risks
Trade-off
Security Policy
Enforced
Security Services
implemented
Security Mechanisms

Security Services = Basic Computer Security Concepts (CIA)

- Confidentiality: prevention of unauthorized disclosure of information
- Integrity: prevention of unauthorized modification of information

Cryptography

- Availability: prevention of unauthorized withholding of information or resources
- Authenticity: able to verify the origin of data
- Accountability: audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party

Access Control

Objectives

- This course introduces the principles, mechanisms and implementation of cyber security and information protection. Knowledge about cyber-attacks and defense are included.

Course Aims

- Be able to understand the principles and objectives of information security, encryption, cyber-attacks and defense
- Be able to understand security models and to apply the model to achieve the security objectives
- Be able to understand the basic principles of security design and to apply the principles
- Be able to understand the security issues of a real-life Internet applications
- Be able to implement a practical Internet application in a secure manner

Course Information

- Lecturer: KP Chow (chow@cs.hku.hk)
- Tutor: Crida Wei (ycwei@cs.hku.hk) & Terry Wang (tywang@cs.hku.hk)
- Tutor Office Hour: Tue 4:00pm-6:00pm
- Lecture: Tue 1:30-3:20 (MB167), Fri 2:30-3:20 (MB167)
- Assessment
  - 50% Final Exam
  - 50% Continuous Assessment
    - Mid-term test(s)
    - Assignments and Lab exercises
- References:
  - Dieter Gollmann, *Computer Security*, Wiley; 3rd edition
  - H.X. Mel & D. Baker, *Cryptography Decrypted*, Addison-Wesley, 2001

Teaching Plan

- Network and Internet security and protection
- Cryptography: Symmetric key cryptography and public key cryptography
- Authentication techniques
- Access control methods
- Application and web security
- Analysis and models of secure systems
- Cyber threat assessment and penetration testing
- Mobile code security

- First lecture:

Sep 6th (Friday) 2:30-3:20pm (MB167)