Network Security

CSCI368

Dr. Khoa Nguyen
University of Wollongong

Contact details

Dr. Khoa Nguyen

khoa@uow.edu.au

If you email me, please include the subject and topic in the subject line: For example: CSCI368: A1.

- This way I can tell if an email is about almost due assessment or similar important matters.
- While I generally reply to emails within a couple of working days there will be times when other activities will take priority.
- **If possible, use your university account for email.**

About Me

- 2014: PhD in Cryptography (Nanyang Technological University, Singapore)
- 2014-2021: (Senior) Researcher at Nanyang Technological University
- August 2021– present: Senior Lecturer, SCIT, UOW.

- Research Areas: Cryptography, Information Security and Cybersecurity, Privacy-Preserving Cryptographic Protocols
- More information: https://sites.google.com/view/khoantt/

What is CSCI368 about

- Covering a wide range of topics in computer network security
  - From cryptography to network protocols
  - From security programming to protocol design
- Knowledge required
  - Basic cryptography (will be introduced briefly)
  - Basic computer network knowledge
  - Programming: C, C++, or Java

Aims

- Understand network vulnerabilities and network-based attacks
- Apply a range network security technologies for securing networks
- Use appropriate security standards and network security tools to enhance security of a distributed system
- Evaluate, compare, and recommend network security applications and systems

Contents

Topic	Description
1	Subject Introduction, Network Basics, Cryptography Basics
2	Public Key Infrastructure
3	Secure Message Transmission, Email Security
4	Authentication and Key Establishment Protocols
5	Centralised Authentication Systems, Kerberos
6	Internet Protocol Security (IPSec), Internet Key Exchange (IKE)
7	Secure Sockets Layer (SSL)/ Transport Layer Security (TLS), Secure Shell (SSH)
8	Wireless & Mobile Security, Wi-Fi Protected Access (WPA), GSM/3GPP

Textbook and References

- William Stallings, Cryptography and Network Security, 7th edition, Pearson, 2016
- Other references:
  - C. Kaufman, R. Perlman, and M. Speciner, Network Security: PRIVATE communication in a PUBLIC world, 2nd edition, Prentice Hall, 2002.
  - William Stallings, Network Security Essentials, 6th edition, Pearson, 2016
  - Colin Boyd, Anish Mathuria, Douglas Stebila, Protocols for Authentication and Key Establishment, 2nd Edition, Springer, 2020

Assessments

Assignment 1, programming	20%	Due: 02 Aug 2024 23:55 (SG Time)
Assignment 2, protocol design & analysis	20%	Due: 23 Aug 2024 23:55 (SG Time)
Final Exam	60%	04 Sep 2024

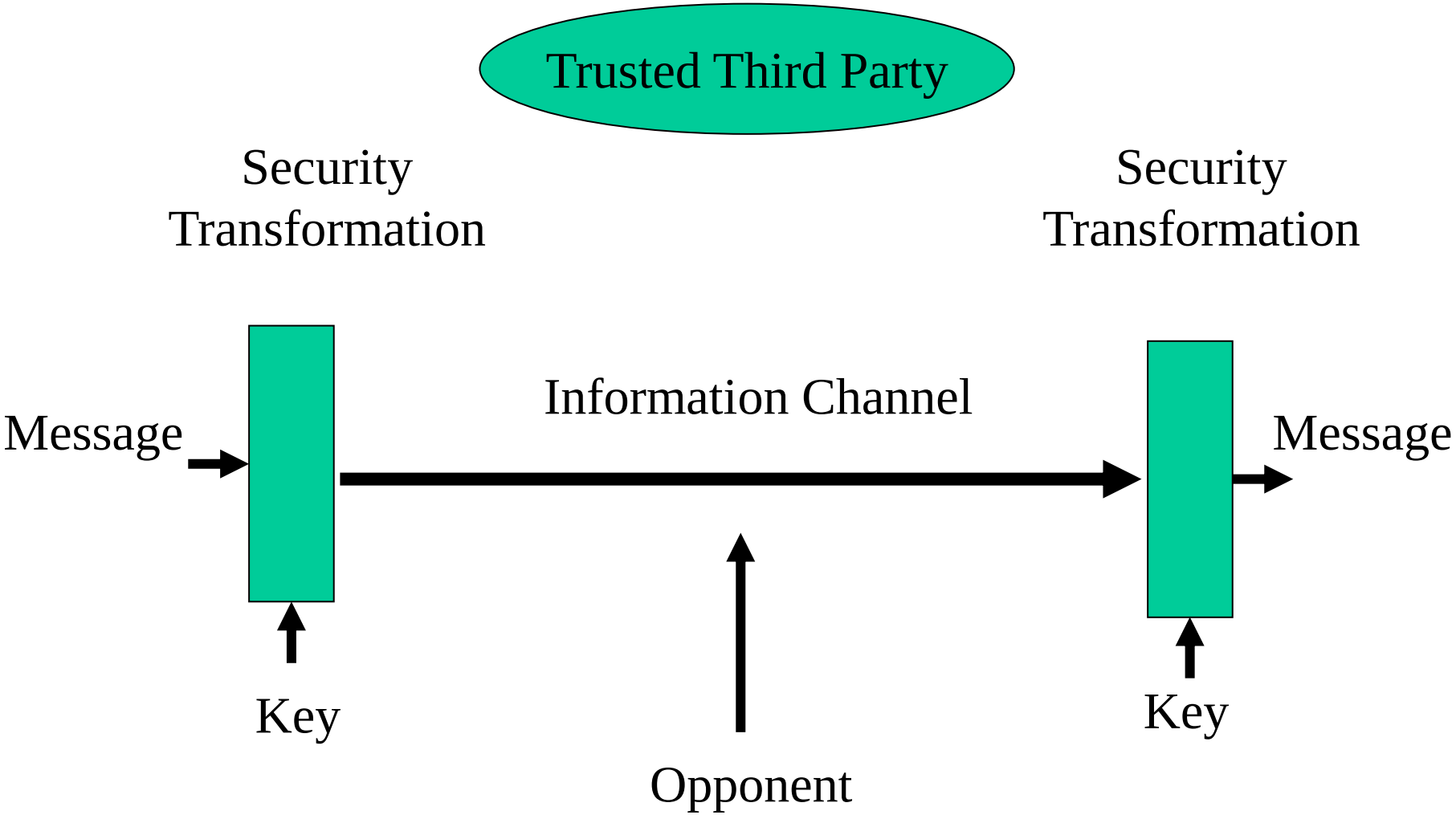
Assessment

- Assignments must be submitted via Moodle.
- It is the student's responsibility to keep a backup of his/her work. There will be no extension granted due to any circumstance related to the failure of students' own equipment.
- Penalties apply to all late work, except if student **academic consideration** has been granted.
- Late submissions will attract a penalty of 5% of the assessment mark per day including weekends. Assignments more than 4 days late **will not be accepted**.
- Students who copy an assignment may receive zero for that assignment. This also covers assignments which may be the product of community effort by several students. Working together is acceptable, but the final coding should be the work of the individual student, as assessment is a measure of your ability. All students involved in plagiarism will have a zero mark for that assessment task.
- **At least 40% in the final exam, otherwise TF may be given.**

Network Security

- Computer network is vulnerable to attackers.
- Network Security is important because computers rely on computer network for communication.
- There are many remote applications: e-commerce, distributed & clouding computing, mobile communications, IoT, etc.
- Network security provides protection to network and applications

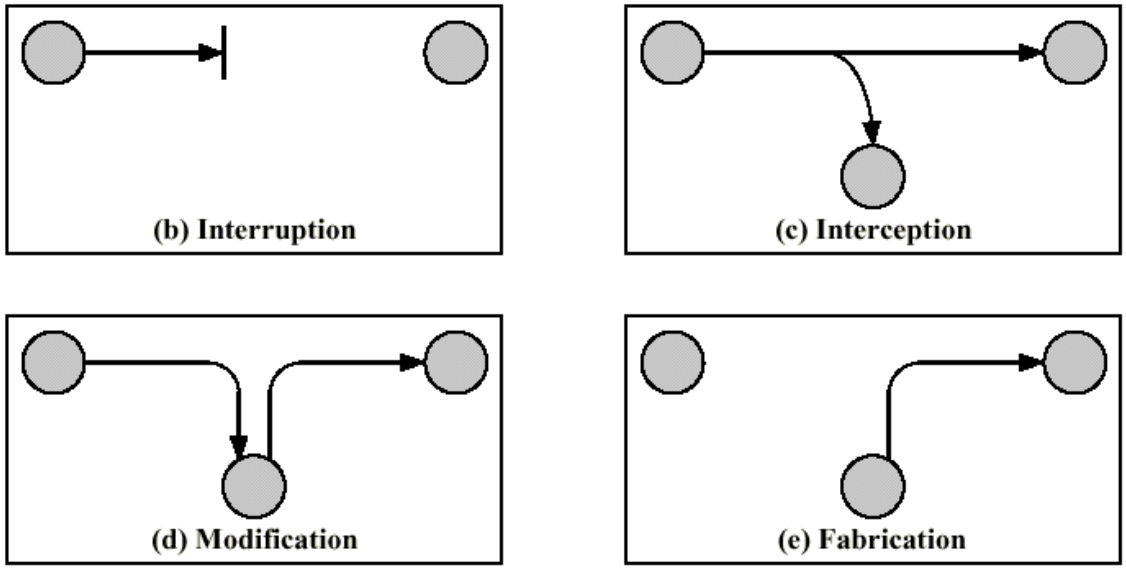
The abstract communication model



Security Requirements: Fundamental

- **Confidentiality**: Stored or transmitted information should be accessible only by authorised parties.
- **Integrity**: Information should be protected from unauthorised modification - alteration, insertion, or deletion.
- **Authenticity**: The origin of a message should be assured.
- **Availability**: Information should be accessible to authorised parties.

Security Issues



- Interruption: an attack on availability (Active).
- Interception: an attack on confidentiality (Passive).
- Modification: an attack on integrity (Active)
- Fabrication: an attack on authenticity (Active)

Common Attacks

- Passive Attacks:
  - Eavesdropping communications and releasing of messages.
  - Traffic analysis on the identities, locations, frequency etc of communications.
- Active Attacks:
  - Masquerade (impersonation) attack
  - Modification of message
  - Denial of service
  - ……

Security methods: Cryptography

- Encryption:
  - Symmetric Cryptosystems – Secret key
    - AES, DES, RC4, ...
  - Asymmetric Cryptosystems – Public key
    - RSA, ElGamal, ...
- Digital signature:
  - RSA, DSS, ElGamal.
- (Keyed) Hash:
  - MD5, SHA-1/2/3, HMAC, etc.

Security protocols

- Protocols are agreed upon rules or standards enabling connection and interaction between parties.
  - They can specify data formats.
  - Rules of exchange, who does what when?
  - Specify termination or error rules or handling conditions.

Network Security is …

- … about securing computer networks to meet the security requirements:
  - Confidentiality, availability, integrity etc.
- … using security protocols/systems:
  - VPN, SSL, Kerberos, IPSec, …