

TERMINOLOGIES CONT.

Lecture 4a

COMPSCI 726

Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

July 26, 2021

SECURITY MECHANISMS



- Encryption
 - A process of encoding messages in such a way that only authorised parties can read it
- Digital signature
 - A cryptographic technique that allows recipients to validate message authenticity
- Access control mechanism
 - Techniques for enforcing access rights
- Notarisation
 - Using a trusted party to assure data exchange
- Password
 - A secret word or phrase known to an authorised party

RELATIONSHIP BETWEEN SECURITY SERVICES AND MECHANISMS

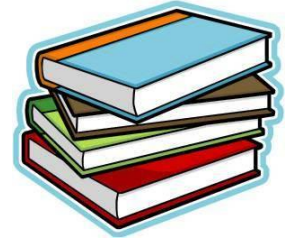
| Services | Encryption | Digital Signature | Access Control Mechanism | Notarisation | Password |
|---------------------------|------------|-------------------|--------------------------|--------------|----------|
| Authentication | ✓ | ✓ | | | ✓ |
| Access Control | | | ✓ | | |
| Confidentiality (Message) | ✓ | | | | |
| Confidentiality (Header) | ✓ | | | | |
| Data Integrity | ✓ | ✓ | | | |
| Non-repudiation | | ✓ | | ✓ | |
| Availability | | | | | |

SUMMARY



- Network security provides a secure platform for performing critical operations
- The OSI security architecture consists of security attacks, services, and mechanisms
- Security services are offered for preventing attacks
- There could be different mechanisms to implement a security service
- One mechanism can offer multiple security services

RESOURCES



- Read Chapter 1 of
Network Security Essentials – Applications and Standards
Fourth Edition
William Stallings
Prentice Hall
ISBN 0-13-706792-5



Questions?

Thanks for your attention!