SYLLABUS:

Date / Revision	April 2017/September 2017/IT
Faculty	Engineering
Study Program	Computer Science

SUBJECT: IT SECURITY 2

1 Basic Information

1.01	**Subject Name**	**IT SECURITY 2 (Network Security)**
1.02	**Semester**	5
1.03	**Level**	1
1.04	**SKS**	2
1.05	**Mandatory / Curriculum**	D-05
1.06	**Subject Code**	OTSE
1.07	**Subject Code**	CSE-D-OTSE-217
1.08	**Year**	2017
1.09	**Quality Control**	Final Test, see evaluation
1.10	**Limitations**	Min 12 and Max 32 students in one class
1.11	**Combined with**	
1.12	**Perquisite**	IT Security 1 (Information Security)
1.13	**Responsible**	
1.14	**Revision**	September 2017

2 Description of Subject

This course contains network security topics. It will discuss general threat, confidentiality, integrity, and availability. Defensive technologies and including authentication/authorization, access control, segmentation, log/traffic monitoring, reputation-based security, and secure protocol (SSH, TLS, DNSSEC). Practical activities is part of the course.

PO Box 150, BSD CPA 15330
Tel. +62 85212318000
info@iuli.ac.id
www.iuli.ac.id
IULI – Eco Campus, The Breeze
Jl. BSD Grand Boulevard
BSD City 15345
Island of Java

3 Objectives

To provide student with knowledge, skill and experience about network security, and the its future development.

4 Competency

- To understand the basic principles and practices in computer and network security.
- To understand the foundational theory about computer security and threats
- To be able to design and implement network security in a life system

5 Learning Approach / Methodology

- Lectures/ Class contact (time-tabled) supplemented with interactive questions and answers;
- Student Study Effort: homework/assignment; preparation for test/quizzes/ examination.

6 Evaluation

5.1	**Absence maximum**	25%
5.2	**Participation in Discussion**	05 Points
5.3	**Homework / Classwork**	05 Points
5.4	**Presentation /Simulation**	10 Points
5.5	**Daily Quiz**	20 Points
5.6	**Final Examination**	60 Points
	Total	100 Points

7 Text Book and Reference

1	**Main Text Book:** Network Security: Private Communication in a Public World, Kaufman, Perlman and Speciner, Prentice Hall, 2002, ISBN-10: 0-13-046019-2
2	**Supplement Textbooks:** Computer Security: Principles and Practice, 3rd Edition, William Stallings and Lawrence Brown, Pearson, 2014, ISBN-13: 978-0133773927

PO Box 150, BSD CPA 15330
Tel. +62 85212318000
info@iuli.ac.id
www.iuli.ac.id
IULI – Eco Campus, The Breeze
Jl. BSD Grand Boulevard
BSD City 15345
Island of Java

8 Content / Topics of Lecture

Week	Content/Topics of Lecturing	Text Book Chapter	Rem
1	Encrypting a Large Message, Generating MACs, Multiple Encryption DES, Nifty Things to Do with a Hash, MD2, MD4, MD5, SHA-1, HMAC	Modes of Operation , Hashes and Message Digests	
2	Modular Arithmetic, RSA, Diffie-Hellman, Digital Signature Standard (DSS), How Secure Are RSA and Diffie-Hellman?, Elliptic Curve Cryptography (ECC), Zero Knowledge Proof Systems	Public Key Algorithms	
3	Modular Arithmetic, Primes, Euclid's Algorithm, Chinese Remainder Theorem, Zn*, Euler's Totient Function, Euler's Theorem, Notation, Groups, Fields, Mathematics of Rijndael	Number Theory , Math with AES and Elliptic Curves	
3	Password-Based Authentication, Address-Based Authentication, Cryptographic Authentication Protocols, Who Is Being Authenticated?, Passwords as Cryptographic Keys, Eavesdropping and Server Database Reading, Trusted Intermediaries, Session Key Establishment, Delegation	Overview of Authentication Systems	
4	Passwords, On-Line Password Guessing, Off-Line Password Guessing, How Big Should a Secret Be?, Eavesdropping, Passwords and Careless Users, Initial Password Distribution, Authentication Tokens, Physical Access, Biometrics	Authentication of People	
5	Login Only, Mutual Authentication, Integrity/Encryption for Data, Mediated Authentication (with KDC), Nonce Types, Picking Random Numbers, Performance Considerations, Authentication Protocol Checklist	Security Handshake Pitfalls	
6	Tickets and Ticket-Granting Tickets, Configuration, Logging Into the Network, Replicated KDCs, Realms, Interrealm Authentication, Key Version Numbers, Encryption for Privacy and Integrity, Encryption for Integrity Only, Network Layer Addresses in Tickets, Message Formats	Kerberos V4	
7	ASN.1, Names, Delegation of Rights, Ticket Lifetimes, Key Versions, Making Master Keys in Different Realms Different, Optimizations, Cryptographic Algorithms, Hierarchy of Realms, Evading Password-Guessing Attacks, Key Inside Authenticator, Double TGT Authentication, PKINITÂPublic Keys for Users, KDC Database, Kerberos V5 Messages	Kerberos V5	
8	**Midterm Break**		
9	Some Terminology, PKI Trust Models, Revocation, Directories and PKI, PKIX and X.509, X.509 and PKIX Certificates, Authorization Futures	PKI (Public Key Infrastructure)	
10	What Layer?, Session Key Establishment, Perfect Forward Secrecy, PFS-Foilage, Denial-of-Service/Clogging Protection, Endpoint Identifier Hiding, Live Partner Reassurance, Arranging for Parallel Computation, Session Resumption, Plausible Deniability, Data Stream Protection, Negotiating Crypto Parameters	Real-Time Communication Security	
11	Overview of IPsec, IP and IPv6, AH (Authentication Header), ESP (Encapsulating Security Payload), So, Do We Need AH?, Comparison of Encodings, Photuris, SKIP, History of IKE, IKE Phases, Phase 1 IKE, Phase-2 IKE: Setting up IPsec SAs, ISAKMP/IKE Encoding	IPsec: AH and ESP IPsec: IKE	
12	, Using TCP, Quick History, SSL/TLS Basic Protocol, Session	SSL/TLS	

PO Box 150, BSD CPA 15330
Tel. +62 85212318000
info@iuli.ac.id
www.iuli.ac.id
IULI – Eco Campus, The Breeze
Jl. BSD Grand Boulevard
BSD City 15345
Island of Java

	Resumption, Computing the Keys, Client Authentication, PKI as Deployed by SSL, Version Numbers, Negotiating Cipher Suites, Negotiating Compression Method, Attacks Fixed in v3, Exportability, Encoding, Further Reading		
13	, Distribution Lists, Store and Forward, Security Services for Electronic Mail, Establishing Keys, Privacy, Authentication of the Source, Message Integrity, Non-Repudiation, Proof of Submission, Proof of Delivery, Message Flow Confidentiality, Anonymity, Containment, Annoying Text Format Issues, Names and Addresses, Verifying When a Message was Really Sent, Key Distribution, Efficient Encoding, Certificate and Key Revocation, Signature Types, Your Private Key, Key Rings, Anomalies, Object Formats	Electronic Mail Security, PGP (Pretty Good Privacy)	
14	Structure of a PEM Message, Establishing Keys, Some PEM History, PEM Certificate Hierarchy, Certificate Revocation Lists (CRLs), Reformatting Data to Get Through Mailers, General Structure of a PEM Message, Encryption, Source Authentication and Integrity Protection, Multiple Recipients, Bracketing PEM Messages, Forwarding and Enclosures, Unprotected Information, Message Formats, DES-CBC as MIC Doesn't Work, Differences in S/MIME, S/MIME Certificate Hierarchy	PEM &S/MIME	
15	**Final Examination**		

PO Box 150, BSD CPA 15330
Tel. +62 85212318000
info@iuli.ac.id
www.iuli.ac.id
IULI – Eco Campus, The Breeze
Jl. BSD Grand Boulevard
BSD City 15345
Island of Java