



Satuan Acara Pengajaran

EEC320803 - Keamanan Jaringan Komputer

Pengajar

Muhammad Salman S.T., MIT

Tujuan Perkuliahan

This course covers: Introduction to security and privacy; basic concept of confidentiality, integrity and authentication; security model and access control; network and web security; intrusion detection and prevention; vulnerabilities and attacks; risk analysis and security policies issue.

Minggu 1

Materi COURSE INTRODUCTION
This session discusses some issues related to the objective of the course, the references used, the assessment and the lesson plan (SAP = Satuan Acara Pengajaran) which will be conducted. The housekeeping and Class Rules are also presented.

Media * PPT Slide Presentation
* Web based Lecture @SCELE (<http://scele.ui.ac.id>)

Referensi * Computer Security, D. Gollmann, Willey, 1998
* Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
* Principles of Information Security, M.E.Whitman, Thomson Course, 2003

Aktivitas * Lecture and Discussion

Minggu 2

Materi DISCUSSION & WATCHING DOCUMENTARY VIDEO
TITLE: HACKER - ANGEL AND OUTLAW (Discovery Channel Production)

This alarming program reveals the daily battle between the Internet's outlaws and the hackers who oppose them by warding off system attacks, training IT professionals and police officers, and watching cyberspace for signs of imminent infowar. Through interviews with frontline personnel from the Department of Defense, NYPD's computer crime squad, private detective firm Kroll Associates, X-Force Threat Analysis Service, and several notorious crackers, the program provides penetrating insights into the millions of hack attacks that occur annually in the U.S. including one that affected the phone bills of millions and another that left confidential details of the B-1 stealth bomber in the hands of teenagers. The liabilities of wireless networks, the Code Red worm, and online movie piracy are also discussed.

Media - Video CD Presentation (51 minutes) - Short Movie
- Web based Lecture @SCELE (<http://scele.ui.ac.id>)

Referensi VCD VIDEO TITLE:
HACKER - ANGEL AND OUTLAW
(Discovery Channel Production)

Aktivitas * Case Study (Problem based Learning)
* Group Discussion

Minggu 3

Materi ACCESSABILITY AND SECURITY
The whole meaning of networking is to share programs, but granting others to access a computer device reveals an open window for securities threats. It is important to have the right balance between network security and user access.

Media - Slide Presentation
- Web based Lecture @SCELE

Referensi # Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
Principles of Information Security, M.E.Whitman, Thomson Course, 2003

Aktivitas Group Assignment (2 students per group):

Find any video related to any security issue. By next week, the students have to show their video in front of the class and give some comments.

Upload your assignment as a short resume paper which contains:

- * group name and members
- * video file URL (the video has to be uploaded to any video website such as youtube etc)
- * the background of the story and comment on those security issue

Note:

- * the video also has to be added as a video link at the Facebook group (join first to the Group "Fundamental of Network Security Class EEC320803").
- * Write on a comment field: group name, video title and short description of video.
- * Please also try to give comment to your friend's video.

Minggu 4

Materi

AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

An authentication factor is a piece of information used to authenticate or verify a person's identity on appearance or in a procedure for security purposes and with respect to individually granted access rights.

Factors are generally classified into three classes (in the order of strength of allocation):

- * The ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)
- * The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN))
- * The inherence factors: Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier).

Media

- * Slide Presentation
- * Web based Lecture @SCELE

Referensi

- * Computer Security, D. Gollmann, Willey, 1998
- * Website <http://www.cert.org>

Aktivitas

- * Case Study
 - * Lecture and Discussion
-

Minggu 5

Materi

PRIVACY & ENCRYPTION

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Media

- * PPT Slide presentation
- * Web based Lecture @SCELE

Referensi

Principles of Information Security, M.E. Whitman and H.J. Mattord, Thomson Course, 2003

Aktivitas

- * Case Study
 - * Lecture and Discussion
-

Minggu 6

Materi CASE STUDY: EMAIL SECURITY AND PGP

"If all the personal computers in the world - 260 million - were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message." (William Crowell, National Security Agency, March 20, 1997) -

An unencrypted email is like a postcard. Everybody can read it. Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It was originally created by Philip Zimmermann in 1991.

PGP supports message authentication and integrity checking. The latter is used to detect whether a message has been altered since it was completed (the message integrity property), and the former to determine whether it was actually sent by the person/entity claimed to be the sender (a digital signature). In PGP, these are used by default in conjunction with encryption, but can be applied to plaintext as well. The sender uses PGP to create a digital signature for the message with either the RSA or DSA signature algorithms. To do so, PGP computes a hash (also called a message digest) from the plaintext, and then creates the digital signature from that hash using the sender's private keys.

-
- Media**
- * Slide presentation
 - * Web based Lecture @SCELE
 - * PGP Software (<http://www.pgp.com>)

-
- Referensi**
- * Computer Security, D. Gollmann, Willey, 1998
 - * PGP (Pretty Good Privacy) Tutorial
 - * PGP Desktop User Guide

-
- Aktivitas**
- * Create Public and Private Key
 - * Create Keyring on PGP Keyserver
 - * Encrypt secure email by implementing Asymmetric Encryption
 - * Implement the Digital Signature to the message

Minggu 7

Materi MID TERM ASSIGNMENT

Topic on Symmetric & Asymmetric Encryption, and also building own Encrypted Message using any Classical Cryptography model (substitution, transposition, steganography etc)

-
- Media**
- * PPT Slide presentation
 - * Web based Learning @SCELE
-

Referensi # Crypto tools: <http://www.cs.iit.edu/~cs549/>
Secret Language: <http://www.exploratorium.edu/ronh/secret/secret.html>
Enigma rotor machine: <http://enigmaco.de/enigma/enigma.swf>

Aktivitas Part A:
Write a short paper to answer the following questions:
1. Explain the difference between Symmetric and Assymmetric Encryption, and which one you think is better and more secure? and Why? Give example!

2. Find example of the Encryption Algorithm, one for each of Symmetric and Asymmetric Encryption. Describe briefly the concept of each algorithm. Do not forget to mention your references!!

Part B:
Create your own Encrypted Message using any Classical Cryptography model (substitution, transposition, steganography etc). Using your model, show how the plaintext is encrypted, and how to decrypt it back to its original text.

Build as a simple application (you can use any preferred tools that you feel convenience from as simple as MS-Excel, Javascript or any other tools.

Prepare a short presentation and demo for Part B only.
All files (both parts) are uploaded as a single ZIP file on SCELE.

Minggu 8

Materi **BACKUP RECOVERY MANAGEMENT**

Backups are one of the most critical, but often neglected, tasks in proper data management. Both home users and network administrators have lax attitudes towards backups until the day comes when they lose data, especially important business-related data. With the refinements in hardware and software technologies backups are easy and relatively inexpensive, even for the small office and home users.

Full backup

A full backup is a complete copy of everything on the source drive to the backup media. Most users and administrators run a full backup on a weekly or monthly basis.

Incremental backup

An incremental backup only copies the data that has changed since the last backup. Administrators will run incremental backups on a daily basis to capture the data files added or updated during the day.

Differential backup

A differential backup copies the data that has changed since the last full backup. It is important to understand the difference between an incremental and differential backup. Administrators use differential backups to facilitate more complex tape rotation schemes and sometimes in database environments.

Media * PPT Slide presentation
 * Web based Lecture @SCELE

Referensi * Computer Security, D. Gollmann, Willey, 1998
 * Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
 * Principles of Information Security, M.E.Whitman and H.J.Mattord, Thomson Course, 2003

Aktivitas * Case Study
 * Lecture and Discussion

Minggu 9

Materi COMPUTER SECURITY FORENSIC

Computer security forensics -- still a rather new discipline in computer security -- is a rapidly growing discipline and an even faster growing business. It focuses on finding digital evidence after a computer security incident has occurred. The goal of computer security forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it.

There are essentially three phases for recovering evidence from a computer system or storage medium. Those phases are: (1) acquire, (2) analyze, and (3) report. Often, the results of a forensic investigation are used in criminal proceedings.

Computer criminals always leave tracks, it's "just" a matter of finding these tracks. But this part is not always easy. The evolution in computer technology goes on, computers and other communication systems become very complicated and better connected through all kinds of networks. At the same time, computer crime techniques become more sophisticated and better coordinated. If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

-
- Media**
- * PPT Slide presentation
 - * Web based Lecture @SCELE

-
- Referensi**
- * Computer Security, D. Gollmann, Willey, 1998
 - * Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
 - * Principles of Information Security, M.E.Whitman and H.J.Mattord, Thomson Course, 2003

-
- Aktivitas**
- * Case Study
 - * Lecture and Discussion

Minggu 10

Materi DEMO and PRESENTATION

This is a session to present student's assignment on creating a simple application of Classical Encryption. Each group has only 10-15 minutes to do the presentation.

There are 13 groups of students who had submitted the assignments and scheduled for 3 (three) weeks.

-
- Media**
- * PPT Slide Presentation
 - * PC for encryption software demo
 - * Web based Learning @SCELE
-

- Referensi**
- * Computer Security, D. Gollmann, Willey, 1998
 - * Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
 - * Principles of Information Security, M.E.Whitman and H.J.Mattord, Thomson Course, 2003
-

- Aktivitas**
- * Student presentation and demo
 - * Discussion
-

Minggu 11

Materi DEMO and PRESENTATION (Cont'd)

This is a session to present student's assignment on creating a simple application of Classical Encryption. Each group has only 10-15 minutes to do the presentation.

There are 13 groups of students who had submitted the assignments and scheduled for 3 (three) weeks.

- Media**
- * PPT Slide Presentation
 - * PC for encryption software demo
 - * Web based Learning @SCELE
-

- Referensi**
- * Computer Security, D. Gollmann, Willey, 1998
 - * Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
 - * Principles of Information Security, M.E.Whitman and H.J.Mattord, Thomson Course, 2003
-

- Aktivitas**
- * Student presentation and demo
 - * Discussion
-

Minggu 12

Materi DEMO and PRESENTATION (Cont'd)

This is a session to present student's assignment on creating a simple application of Classical Encryption. Each group has only 10-15 minutes to do the presentation.

There are 13 groups of students who had submitted the assignments and scheduled for 3 (three) weeks.

- Media**
- * PPT Slide Presentation
 - * PC for encryption software demo
 - * Web based Learning @SCELE
-

- Referensi**
- * Computer Security, D. Gollmann, Willey, 1998
 - * Corporate Computer and Network Security, R.R.Panko, Prentice-Hall, 2004
 - * Principles of Information Security, M.E.Whitman and H.J.Mattord, Thomson Course, 2003
-

- Aktivitas**
- * Student presentation and demo
 - * Discussion
-

Minggu 13

Materi CASE STUDY:
INFORMATION SECURITY RECOMMENDATION REPORT

This is a group assignment. The goal of this assignment is to produce a Network Security Recommendation Report which contains a series of recommendations to the school addressing matters as follows:

- * Assessment of school environment and description of what need to be protected;
 - * Advance plans for what to do in an emergency or disaster;
 - * Methods and tools to protect the networks against attacks from the outside world.
 - * Ways to backup and recovery the data and information;
-

- Media**
- * PPT Slide presentation
 - * Web based Learning @SCELE
-

- Referensi**
- * Internet resources
 - * Paper and Journal related to security issue
-

- Aktivitas**
- * Group discussion
 - * Writing recommendation report
-