**정보보호특강-사이버 보안 Syllabus**

**Topic in Information Security-Cyber Security**

Fall 2010

Professor : Prof. Kwangjo Kim

N5 R2215, Dep’t of Computer Science, KAIST

(042) 350-3550, 010-9414-1386, [kkj@cs.kaist.ac.kr](mailto:kkj@cs.kaist.ac.kr)

Class Hours and Classroom: 16:00 – 17:15 (Tue, Thu.) and E3-2445

Class Code: CS748

**Class Web Page**: <http://caislab.kaist.ac.kr/lecture/2010/fall/cs748/index.html>

TA: Mr. Jangseong Kim (Ph.D Student), [jskim.withkals@kaist.ac.kr](mailto:jskim.withkals@kaist.ac.kr), 010-7761-5576

**Textbook :**

-Handouts

Recommended Reading Material:

* W. Stallings, “Cryptography and Network Security”, 4th Ed., Pearson Education Inc, ISBN 0-13-187316-4, 2006
* J. Mirkovic, S. Dietrich, D. Dittrich and P. Reiher, “Internet Denial of Service, Attack and Defenses Mechanisms”, 2005, Pearson Education Inc., ISBN 0-13-147573-8

http://www.pearsonhighered.com/educator/academic/product/0,,0131475738,00%2ben-USS\_01DBC.html

* Side Channel Attack: <http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html>
* DETER: <http://www.isi.edu/deter/>

Grading Policy: Midterm (15%), Final (15%), Quiz (5%), HW (10%), Presentation (25%), Term Project(25%), Attendance (5%)

Objective:

This course discusses the latest issues on cyber security beginning with the introduction of basic cryptography to understand how to design authentication primitives covering multi-party cryptographic protocols and core security components for network security, etc. Special presentations on DDoS defenses and secure smart grid are scheduled. The enrolled student must read and present the recommended papers and practice your term project under the guidance of your professor and TA.

Course Schedule

|  |  |  |
| --- | --- | --- |
| Week(Date) | Topic | Remark |
| 1 (9/2,9/7) | Overview/ Basic to Cryptography I |  |
| 2(9/9,9/14) | Basic to Cryptography II | ~9/14: Deadline of course change |
| 3(9/16,9/21) | Side Channel Attack | 9/16:TP Proposal  9/21: No Class |
| 4(9/23,9/28) | Authentication Protocol/ ZKIP | 9/23: No class |
| 5(9/30,10/05) | Paper Presentation #1 |  |
| 6(10/7,10/12) | Multi-party Protocol |  |
| 7(10/14,10/19) | TP Mid-Presentation |  |
| 8(10/21,10/26) | Midterm Exam | 10/21 |
| 9(10/28,11/2) | SSL & TLS |  |
| 10(11/4,11/9) | IPSEC, Firewall, IDS |  |
| 11(11/11,11/16) | DDoS Defenses |  |
| 12(11/18,11/23) | Secure Smart Grid |  |
| 13(11/25,11/30) | Paper presentation #2 |  |
| 14(12/2,12/07) | Car Security |  |
| 15(12/9,12/14) | TP Final presentation |  |
| 16(12/16,12/21) | Final Exam | 12/16 |

\* Schedule can be subject to change slightly depending on the number of enrolled students.