San José State University

Department of Computer Science

CS 166, Information Security, Section 02 (47860), Fall 2017

Course and Contact Information

Instructor: Kwang-Pill Sung

Office Location: Student-Faculty Conference Room, MH229

Telephone: 408-460-1059

Email: kwang-pill.sung@sjsu.edu

Office Hours: Tuesday 9:15-10:15 am

Class Days/Time: Tuesday and Thursday 10:30-11:45 am

Classroom: MH 233

Prerequisites: CS 146 (with a grade of "C-" or better) and either CS 47 or CMPE 102 or CMPE 120 (with a grade of "C-" or better); or instructor consent.

Course Description: Fundamental security topics including cryptography, protocols, passwords, access control, software security, and network security. Additional topics selected from multilevel security, biometrics, tamper-resistant hardware, information warfare, e-commerce, system evaluation and assurance, and intrusion detection.

This course covers topics about Introduction and overview, IPSec with Cisco Packet Tracer, Crypto basics, Symmetric key cryptography, Public key cryptography, Cryptographic hash function and related topics, Authentication, Authorization, Network security basics, Simple authentication protocols, Real-world security protocols, Software flaws and malware, Additional software security topics.

Additionally, Post-Quantum Cryptography, DDos, VPN, PKI, Wireless, SSL, Smart Card, Cloud Computing Security, IoT Security, IPSec, ZFW, Tools, Server Side Attacks, Trojan Horses, IDS, Hacking Techniques, Web Security Vulnerabilities, etc

Course Learning Outcomes (CLO) (Required) After completing this course you should be knowledgeable of the major technical security challenges in each of the following four areas: cryptography, access control, protocols, and software.

Required Texts/Readings

Textbook: We will use a manuscript that will eventually become **the 3rd edition** of the textbook Information Security: Principles and Practice, Mark Stamp

(2nd Edition Errata: http://www.cs.sjsu.edu/~stamp/infosec/Errata_2d.pdf)

(1st Edition Errata: http://www.cs.sjsu.edu/~stamp/infosec/Errata.pdf)

Other Readings

 A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security, Tobias Klein, No Starch Press, 2011. Lots of interesting real-world examples of vulnerable code.

 Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski and Andrew Honig, No Starch Press, 2012. An excellent book for information on reverse engineering (whether for malware analysis or other purposes). Includes many hands-on exercises.

 Software Reverse Engineering (SRE) (Links to an external site.) at http://reversingproject.info/. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.

 Network Security: Private Communication in a Public World, second edition, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 2002, ISBN: 0-13-046019-2. This book provides good coverage of cryptography and excellent coverage of several security protocols.

 Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, John Wiley & Sons, Inc., 2001, ISBN: 0-471-38922-6; see Ross Anderson's Security Engineering (Links to an external site.) at http://www.cl.cam.ac.uk/~rja14/book.html, where you can obtain a free (and legal) copy of the 1st edition of the book. This is an excellent book for an overview of security in general, but it is not too focused or technically detailed.

 Security in Computing, third edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2003, ISBN: 0-13-035548-8. The strength of this book is its coverage of the security issues related to software. In particular, operating systems and some

aspects of secure software engineering are covered well. This book also has some good, basic information on viruses.

 Applied Cryptography: Protocols, Algorithms and Source Code in C, second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9. For better or for worse, in industry, this is the standard reference for all things cryptographic.

 Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Ed Skoudis with Tom Liston, Prentice Hall, 2006, ISBN: 0-13-148104-5. There are many books that claim to provide information on how to foil hackers, but this is by far the best that I have seen. This is an updated version of the original Counter Hack, published in 2001.

 Computer Viruses and Malware, John Aycock, Springer, 2006, ISBN: 0387302360. This book gives a good introduction to research topics related to malware. The book is well-written and surprisingly easy reading, given the technical nature of the material.

 Additional relevant material:

 Previous semester lecture videos are available on You Tube (Links to an external site.) at http://www.youtube.com/playlist?list=PLQEAKfSI2JLOzrgaQOgF6S3PqXs2zR614

 Class-related discussion will be posted on Piazza. You are strongly encouraged to participate by asking questions, as well as by responding to questions that other students ask. At the start of the semester, you should receive an email asking you to join this discussion group—if not, contact your instructor via email.

 Quantum Computer/Post-Quantum Cryptography

https://www.youtube.com/watch?v=UiJiXNEm-Go

https://www.youtube.com/watch?v=g_IaVepNDT4

https://www.youtube.com/watch?v=S52rxZG-zi0

https://www.research.ibm.com/ibm-q/

https://www.youtube.com/watch?v=0dXNmbiGPS4

Course Requirements and Assignments

 NOTE that University policy F69-24 (Links to an external site.) at http://www.sjsu.edu/senate/docs/F69-24.pdf states that "Students should attend all

meetings of their classes, not only because they are responsible for material discussed therein, but because active participation is frequently essential to insure maximum benefit for all members of the class. Attendance per se shall not be used as a criterion for grading."

More guidelines on grading information and class attendance can be found from the following two university policies:

- University Syllabus Policy S16-9 (http://www.sjsu.edu/senate/docs/S16-9.pdf)

- University policy F15-12 (http://www.sjsu.edu/senate/docs/F15-12.pdf)

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/

==========

From the first class, please download the following files asap:

http://www.kwangnet.com/kpsung/CS166/CS166-Section2-F17.docx

http://www.kwangnet.com/kpsung/CS166/ 050.jpg

http://www.kwangnet.com/kpsung/CS166/IPsec summary (SJSU).ppt

http://www.kwangnet.com/kpsung/ PacketTracer60_Build45_setup.exe

http://www.kwangnet.com/kpsung/CS166/ Ipsec-KWANG.pkt

http://www.kwangnet.com/kpsung/CS166/ R1_IPSEC_CONFIG.txt

http://www.kwangnet.com/kpsung/CS166/ R3_IPSEC_CONFIG.txt

http://www.kwangnet.com/kpsung/CS166/ probs1.pdf

http://www.kwangnet.com/kpsung/CS166/Intro.pptx

http://www.kwangnet.com/kpsung/CS166/ 1_Crypto.pptx

http://www.kwangnet.com/kpsung/CS166/ 2_AccessControl.pptx

http://www.kwangnet.com/kpsung/CS166/ 3_Protocols.pptx

http://www.kwangnet.com/kpsung/CS166/ 4_Software.pptx

http://www.kwangnet.com/kpsung/CS166/ Conclusion.pptx

http://www.kwangnet.com/kpsung/CS166/ qqqqqqqqqqq.gif

http://www.kwangnet.com/kpsung/CS166/ ipcalc11.exe

https://www.mysterytwisterc3.org/en/

http://users.telenet.be/d.rijmenants/en/enigmasim.htm

https://enigma.hoerenberg.com/

https://www.wireshark.org/#download

https://sourceforge.net/projects/stegtool/?source=typ_redirect

http://www.kwangnet.com/kpsung/CS166/ Quantum Cryptography (SJSU).ppt

http://www.kwangnet.com/kpsung/CS166/ Why_Quantum.jpeg

http://www.kwangnet.com/kpsung/CS166/ Quantum_2.jpg

http://www.kwangnet.com/kpsung/CS166/ Cryptography Overview (SJSU).ppt

==========

Homework ANSWERS (Will be available after your due date)

http://www.kwangnet.com/kpsung/CS166/ANS_HW_1.doc

http://www.kwangnet.com/kpsung/CS166/ANS_HW_2.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_3.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_4.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_5.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_6.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_7.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_8.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_9.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_10.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_11.docx

http://www.kwangnet.com/kpsung/CS166/ANS_HW_12.docx

==========

Schedule (subject to change)

Week 1 --- Syllabus, IPSec with Cisco Packet Tracer

Week 2 --- Introduction and overview (Chapter 1)

Week 3 --- Crypto basics (Chapter 2)

Week 4 --- Symmetric key cryptography (Chapter 3)

Week 5 --- Public key cryptography (Chapter 4)

Week 6 --- Cryptographic hash function and related topics (Chapter 5)

Week 7 --- **1 MIDTERM**, **100 points** **(Date: Tuesday, October 3)**

Week 8 --- Authentication (Chapter 6)

Week 9 --- Authorization (Chapter 7)

Week 10 --- Network security basics (Chapter 8)

Week 11 --- Simple authentication protocols (Chapter 9)

Week 12 --- Real-world security protocols (Chapter 10)

Week 13 --- Software flaws and malware (Chapter 11)

Week 14 --- Additional software security topics (Chapter 12) (THANKSGIVING WEEK)

Week 15 --- Additional software security topics (Chapter 13)

Week 16 --- **Special Topics / Student Presentation**

Week 17 --- **Special Topics / Student Presentation**

Week 18 --- **1 Final, 150 points (Monday, December 18 09:45-noon)**

- **http://info.sjsu.edu/static/policies/final-exam-schedule-fall.html**

Project Paper (less than 10 pages) (50 points) / Presentation Slides (50 points) will be due by MIDNIGHT, on December 18 (FINAL), 100 points - PLEASE START EARLIER, and Email me at kwang-pill.sung@sjsu.edu

Zip your Project Paper (less than 10 pages) / Presentation Slides into a file named **project.zip.**

Email your work to **kwang-pill.sung@sjsu.edu by midnight on December 18 (FINAL).**

The subject line of your email must be of the form:

CS166 (or SE166) yourlastname last4digitofyourstudentnumber

That is, the subject line must consist of 3 identifiers.

There is no space within an identifier and each identifier is separated by a space. I will confirm your message. (If you don't get my confirmation, you need to resend)

==========

- **Homework is due (include source code, but not executable files) by class starting time on the due date on your papers.** Each assigned problem requires a solution and an explanation (or work) detailing how you arrived at your solution. Cite any outside sources used to solve a problem.
- **12 Homeworks (on your papers), 120 points (10 points each assignment) (subject to change)**
  - **Assignment 1**: **Due Tuesday, August 29 (VERY EASY)**
  - **Assignment 2**: **Due Thursday, August 31**
    (2nd Edition: Chapter 1, problems 1, 11, 13, 15, 17. The problems for Chapter 1 are available at http://www.cs.sjsu.edu/~stamp/other/chap1/probs1.pdf.

(3rd Edition: Chapter 1, problems 1, 8, 9, 11, 13)

- **Assignment 3**: **Due Thursday, September 7**
  (2nd Edition: Chapter 2, problems 1, 2, 5, 6, 9, 11, 18, 22) Use your program from problem 11 when you solve the simple substitution in problem 9.

- (3rd Edition: Chapter 2, problems 1, 2, 5, 6, 8, 10, 16, 18) Use your program from problem 10 when you solve the simple substitution in problem 8.

- **Assignment 4: Due Thursday, September 14**

  (2nd Edition: Chapter 3, problems 3, 9, 11, 12, 20, 21, 25, 29, 30)

  (3rd Edition: Chapter 3, problems 2, 7, 9, 10, 17, 18, 20, 23, 24)

- **Assignment 5**: **Due Thursday, September 21**
  (2nd Edition: Chapter 4, problems 1, 2, 5, 7, 8, 12, 18, 19, 23)

  (3rd Edition: Chapter 4, problems 1, 2, 4, 6, 7, 9, 13, 14, 18)

- **Assignment 6: Due Thursday, September 28**
  (2nd Edition: Chapter 5, problems 4, 10, 14, 15, 19, 20, 22, 24, 34, 37)

  (3rd Edition: Chapter 5, problems 3, 8, 12, 13, 17, 18, 20, 21, 30, 33)

- **1 MIDTERM**, **100 points** **(Date: Tuesday, October 3)**

- **Assignment 7**: **Due Thursday, October 12**
  (2nd Edition: Chapter 7, problems 6, 10, 14, 21, 23)

  (3rd Edition: Chapter 6, problems 4, 8, 11, 17, 18)

- **Assignment 8**: **Due Thursday, October 19**
  (2nd Edition: Chapter 8, problems 1, 2, 3, 5, 7, 8, 13, 15, 19)

  (3rd Edition: Chapter 7, problems 1, 2, 3, 4, 6, 7, 12, 14, 17)

- **Assignment 9**: **Due Thursday, October 26**
  (2nd Edition: Chapter 9, problems 4, 6, 7, 9, 15, 16, 24, 25, 32)

  (3rd Edition: Chapter 9, problems 3, 6, 7, 9, 12, 13, 21, 22, 28)

- **Assignment 10**: **Due Thursday, November 2**
  (2nd Edition: Chapter 10, problems 1, 10, 11, 12, 15, 21, 23, 24, 28, 33, 34, 37)

  (3rd Edition: Chapter 10, problems 1, 7, 8, 9, 12, 18, 20, 21, 25, 29, 30, 33)

- **Assignment 11**: **Due Thursday, November 9**
  (2nd Edition: Chapter 11, problems 6, 11, 14, 15, 23, 33, 34)

  (3rd Edition: Chapter 11, problems 4, 7, 9, 10, 15, 25, 26)

- **Assignment 12**: **Due Thursday, November 16**
  (2nd Edition: Chapter 12, problems 1, 2, 3, 7)

  (3rd Edition: Chapter 12, problems 1, 2, 3, 7)

- **1 Final, 150 points (Monday, December 18 09:45-noon)**

- **Project Paper (less than 10 pages) / Presentation Slides will be due by MIDNIGHT, on December 18 (FINAL), 100 points - PLEASE START EARLIER and Email me kwang-pill.sung@sjsu.edu**

==========

- NOTE that University policy F69-24 at http://www.sjsu.edu/senate/docs/F69-24.pdf states that "Students should attend all meetings of their classes, not only because they are responsible for material discussed therein, but because active participation is frequently essential to insure maximum benefit for all members of the class. Attendance per se shall not be used as a criterion for grading."

- **Grading Policy**

  - **1 MIDTERM, 100 points (Date: Tuesday, October 3)**

  - **12 Homeworks (on your papers), 120 points (10 points each assignment)**

- **1 Final, 150 points (Monday, December 18 09:45-noon)**
  - **http://info.sjsu.edu/static/policies/final-exam-schedule-fall.html**

  Project Paper (less than 10 pages) (50 points) / Presentation Slides (50 points) will be due by MIDNIGHT, on December 18 (FINAL), 100 points - PLEASE START EARLIER and Email me at kwang-pill.sung@sjsu.edu

  No make-up tests will be given and ***no*** late homework (or other work) will be accepted.

- Nominal Grading Scale:

Percentage	Grade
92 and above	A
90 - 91	A-
88 - 89	B+
82 - 87	B
80 - 81	B-
78 - 79	C+
72 - 77	C
70 - 71	C-
68 - 69	D+
62 - 67	D
60 - 61	D-
59 and below	F

- Note that "All students have the right, within a reasonable time, to know their academic scores, to review their grade-dependent work, and to be provided with explanations for the determination of their course grades." See University Policy F13-1 at http://www.sjsu.edu/senate/docs/F13-1.pdf for more details.

- The last day to drop is **Wednesday, September 6,** and the last day to add is **Wednesday, September 13**