CS457 INFORMATION SECURITY

Section 001 - Three Crediдt Hours
Fall 2015

COURSE INFORMATION

Time	:	14:30 ˜ 15:20 MWF (three credit hours)
Place	:	HHS 1202

INSTRUCTOR INFORMATION

Name	:	Dr Xunhua (Steve) Wang
E-Mail	:	wangxx@jmu.edu (put CS457 in the subject line)
Phone	:	(540) 568-3668
Fax	:	(540) 568-2745 (add Attn: Xunhua Wang)
Office	:	ISAT/CS 213
Web Site	:	http://users.cs.jmu.edu/wangxx/web/2015Fall-cs457/index.html
Office Hours	:	12:50 - 14:20, 15:25 - 15:55 Monday; 13:20 - 14:20, 15:25 - 15:55 Wednesday; 12:50 - 14:20 Friday or by appointment

COURSE CATALOG DESCRIPTION

This course covers the basic issues of information system security. The roles of planning, management, policies, procedures, and personnel in protecting the confidentiality, integrity, and availability of information are described. Specific threats (malicious code, network attacks, and hostile content) and widely used countermeasures (access control mechanisms, firewalls, intrusion detection systems) are also discussed.

COURSE GOALS

After taking this course, students should be able to

1. exhibit a security mindset
2. explain services provided by information security and how information security achieves them with fundamental security building blocks
3. use security techniques to improve network/system/application security

Detailed course objectives can be found in the detailed course objectives section toward the end of this document.

COREQUISITES

CS 361 Computer Systems II or the permission of the instructor

TEXTBOOKS

Required : Bruce Schneier. *Secrets and Lies*. Wiley Computer Publishing. 2004. ISBN: 0471453803. (Also ISBN: 0471253111, 2000; This book is called SL hereafter.)

: Notes, provided in electronic format throughout the semester

GRADING

Your grade in the course will be earned / calculated as follows:

Projects	40%
Middle Term Exam 1	15%
Middle Term Exam 2	15%
Final exam	30%

GRADE		POINT RANGE	DESCRIPTION
A	→	[93 – 100]	Superior
A^-	→	[89 – 93)	
B^+	→	[86 – 89)	
B	→	[82 – 86)	Good
B^-	→	[78 – 82)	
C^+	→	[74 – 78)	
C	→	[72 – 74)	Average
C^-	→	[69 – 72)	
D^+	→	[65 – 69)	
D	→	[60 – 65)	Passing
D^-	→	[58 – 60)	
F	→	[0 – 58)	Failure

Notes:

1. There will be *no* "incomplete" grade for this course. If you intend to drop, it is your responsibility to do it before the deadline.
2. This grading policy is subject to change, depending on the overall class performance. Notice will be given if this is necessary.

UNIVERSITY POLICIES

Adding/Dropping Course Policy

Students are responsible for adding and dropping courses via e-campus. The last day to add a course for the Fall 2015 semester is September 17th, 2015 (Thursday)(signatures required after September 8th, 2015 (Tuesday)). The last day to drop a course for the Fall 2015 semester with a "W" grade is October 29th, 2015 (Thursday). I do not give "WP" or "WF" grades to students requesting a drop after the deadline except in extraordinary circumstances. The Office of the Registrar http://www.jmu.edu/registrar/wm_library/fall_2015_bookmark.pdf has other relative dates and deadlines.

Cancellations

The JMU's cancellation policy (http://www.jmu.edu/JMUpolicy/1309.shtml) provides details of information dissemination for inclement weather and other emergencies.

Honor Code

Students are expected to comply with the JMU Honor Code as stated in the Student Handbook and available from the Honor Council Web site: http://www.jmu.edu/honor/code.shtml.

Consulting with other students about problems and solutions is not a violation of the Honor Code provided that the ultimate work turned in for an assignment is your own. This means that everything written down and turned in for an assignment must come from your head and not someone else's. When in doubt, ask me. Copying another student's software in any form is a violation of the Honor Code.

Religious Observation Accommodations

If you can not satisfy a requirement of the course for religious reasons you must let me know at least 2 weeks in advance. In some cases you will be required to "make up" the requirement, in other cases the distribution of requirements will be changed.

Disability Accommodations

If you need an accommodation based on the impact of a disability, you should contact the Office of Disability Services (Wilson Hall, Room 107, www.jmu.edu/ods, (540-568-6705) if you have not previously done so. Disability Services will provide you with an Access Plan Letter that will verify your need for services and make recommendations for accommodations to be used in the classroom. Once you have presented me with this letter, you and I will sit down and review the course requirements, your disability characteristics, and your requested accommodations to develop an individualized plan, appropriate for CS457.

PROJECT ASSIGNMENTS

1. Project submission:
   (a) Projects must be submitted in two ways.
      i. In electronic form to the JMU Canvas system: The electronic submission is intended to prove you have submitted by the deadline. Your electronic submissions can be either in Microsoft Word or RTF and they must follow the following rules:
         A. For project *i* (such as 1, 2, 3, ...), use *your-last-name_your-first-name_project_i* as the file name.
         B. Put your official name (the name on university records) and e-mail address in the header/footer of your Word document.
         C. Use anti-virus software to scan your document before you submit.
      ii. A hard copy due *before* the class meeting on the due date. I will grade the hard copy.

(b) **Honor pledge:** Your project submissions must start with the following pledge: "*This work complies with the JMU honor code. I did not give or receive unauthorized help on this assignment.*" Any submission without this pledge will be rejected!

2. There will be *no* extensions to projects or exams unless arrangements are made beforehand **and** students can provide convincing evidences (such as documented medical or family emergencies).

ATTENDANCE

Attendance is not required but highly recommended. I do take attendance for each meeting and please remember to sign up for each class. This will help me track students' progress. With a poor attendance record, you will *not* get my sympathy if you perform poorly in this course.

IMPORTANT DATES

These dates are for your information ONLY. It is your responsibility to contact the university to get the official dates. You can find the university calendar at http://www.jmu.edu/registrar/wm_library/fall_2015_bookmark.pdf

First class	:	August 31st, 2015 (Monday)
Free add deadline	:	September 8th, 2015 (Tuesday)
Force add deadline	:	September 17th, 2015 (Thursday)
Free drop deadline	:	September 8th, 2015 (Tuesday)
Drop-with-an-W deadline	:	October 29th, 2015 (Thursday)
Midterm exam 1	:	To be announced
Midterm exam 2	:	To be announced
Last class	:	December 11th, 2015 (Friday)
Final Exam	:	1:00 - 3:00 pm, Monday, Dec. 14, 2015

TENTATIVE SCHEDULE

Table 1 gives the tentative schedule for this course.

DETAILED COURSE OBJECTIVES

By the end of this semester, you should be able to

1. explain in your own words the following terminologies:

   (a) security, safety, threat, vulnerability, asset, security policy, preventive/detection/corrective security mechanism, risk, intruder, insider threat, risk avoidance, risk management, risk acceptance, accountability, security through obscurity, identity theft, physical security, cost/benefit analysis, risk analysis, TEMPEST, domain, security perimeter, audit trail, auditing, shredding

   (b) confidentiality, integrity, availability, reliability (fault/error/failure, buffer overflow, race condition), authentication, non-repudiation, cryptology, cryptography, cryptanalysis, symmetric key cryptography, one-time pad, public key cryptography, digital signature, hash function, cryptographic hash function, C-MAC, HMAC, DES, AES, ECB, CBC, RSA

Table 1: Course Content (Tentative)

UNIT	TOPIC	SUBTOPIC	TEXT	PROJECTS	EXAMS
1	Syllabus & Overview		SL-Chap {1 ~ 5}, Notes-Chap 1		
2	Security mindset	Common sense & the subtle	SL-Chap {1 ~ 5},		
3	Confidentiality I	Classical ciphers	SL-Chap 6:85-92,	Project I	
		Ideal cipher	Notes-Chap2		
4	Confidentiality II	AES & modes of operation	SL-Chap 6:94-96,	Project II	
		RSA encryption	Notes-Chap 3		
5	Integrity	MAC	SL-Chap 6:92-94,		
6	Non-repudiation	RSA digital signatures	SL-Chap 6:96-101,		
7	Key Management	Digital certs & PKI	SL-Chap 6:96-101,		
					Exam 1
8	Entity Authentication	In general	SL-Chap 9,	Project III	
		Password	Notes-Chap 6		
		Token & biometric			
9	Access Control		SL-Chap 8, Notes-Chap 7		
10	Security Models		SL-Chap 8, Notes-Chap 7		
11	OS Security		SL-Chap 14, Notes-Chap {8, 9}		
					Exam 2
12	Security Development		SL-Chap {13, 15}	Project IV	
13	Security Evaluation		Notes-Chap 10		
14	Network Attacks		SL-Chap {10, 11, 12}, Notes-Chap 11;	Project V	
15	Intrusion Detection		Notes-Chap 12		
16	Network Defense	NAT	Notes-Chap 13		
		Firewall	Notes-Chap 13		
		IPsec	Notes-Chap 13		
17	Channel Security	SSL/TLS, SSH	Notes-Chap{14,16}	Project VI	
18	Security as Business				
19					Final Exam

(c) authentication factors: authentication by possession/knowledge/property/location, biometrics, false rejection rate (FRR), false acceptance rate (FAR)

(d) password, dictionary attack, password aging, proactive password checking, password shadow, salt, Unix password security, one-time password

(e) access control: MAC (entities, security level, security categories, security labels, subject, object clearance, classification, dominate), DAC, RBAC, access control matrix (sparse)/list, authorization policy

(f) policy, mechanism, confidentiality model (BLP model, the simple security property, the *-property), integrity model (Biba model, the simple integrity property, integrity *-property, Clark-Wilson integrity model), Chinese wall model, security architecture, policy composition

(g) the least privilege principle, need-to-know principle

(h) operating system security: TCB, reference monitor, host intrusion detection, covert channel, privi-

leged instructions, permissions, privileges (user rights); tamper proof/resistant/evident

(i) information assurance, TCSEC, CC (protection profile, security target, target of evaluation)

(j) malicious logics, mobile code, computer virus, Trojan horse, Internet worm, logic bomb, backdoor, side channel attacks (timing, power), Cinderella attack, fault analysis, traffic analysis, information warfare, social engineering, honeyspot, passive/active attacks, DoS, DDoS, SYN flooding, smurf attack, e-mail bombing, spoofing attack (IP spoofing, DNS spoofing, sequence number guessing, session hijacking)

(k) signature/knowledge-based network intrusion detection

(l) security planning, business continuity, disaster recovery

(m) firewall, packet filtering firewall, circuit replay firewall, application gateway; IPsec, ESP, AH, tunnel mode, transport mode

(n) SSL/TLS, SSH, HTTPS

(o) E-mail security: PGP/GPG, S/MIME

2. Explain how AES encryption, decryption, and key scheduling work
3. Explain how RSA encryption and digital signature work
4. Explain how C-MAC and HMAC work
5. Describe the different factors for authentication
6. Explain what dictionary attacks are and how to mitigate them. Explain why one-way hash and salt are used in password-based authentication
7. Explain the differences between MAC and DAC
8. Explain, in the BLP model, what simple security property and star-property are
9. Explain, in the Biba model, what simple integrity property and integrity star-property are
10. Explain why writing-up violates integrity in the Biba model
11. Explain the differences between military security model and commercial security model
12. Explain how CC works
13. Explain the difference between worm and computer virus
14. Explain how packet filtering firewall, circuit relay firewall and application gateway work
15. Explain how IPsec ESP and AH work and how they can be used to protect computer networks
16. Explain how SSL/TLS and SSH work and how they can be used for network security

STUDY HINTS

- Exams are based on the course objectives. If you master the objectives, you will do well in exams. Also, restudying your course objectives from time to time may help a lot.
- For each project/exam, after it is returned, please see me after class (rather than later) if you have any questions about it.

- The course slides are designed to help you master the important points quickly. They are not intended to replace the textbook and you are required to read the textbook.

QUOTES

"Cliff, you're an old fart; Why do you care so much that someone's frolicking in your system? That could have been you, in your distant youth. Where is your appreciation of creative anarchy?"
— Darren Griffith, in 1987, to Cliff Stoll, defending non-malicious hacking

"Forget your perfect offering
There is a crack, a crack in everything"
— Leonard Cohen

"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it."
— Robert Morris

"World War III is a guerrilla information war with no division between military and civilian participation."
— Marshall McLuhan, 1970, in "Culture Is Our Business"

"I know I'm paranoid, but I worry about whether I'm paranoid enough."
— Sandy Harris

"Only the paranoid survive."
— Andrew S. Grove

"I believe in the fallibility of human nature. We continually step on our best aspirations. We're humans. Given a chance to screw up, we will."
— Brent Scowcroft, 10/31/2005, National Security Advisor for Presidents Ford and George H.W. Bush

"We're always chasing the bad guys - the good guys are never ahead. We're not the ones who wrote these exploits. They are often found in the wild and the defenders are generally following the black hats."
— HD Moore

"Robust defense is based on realistic threats, and realistic threats are identified via attackers' perspective."
— Coderman@gmail.com, 09/23/2013

"Hackers don't steal credit card numbers one by one across the network; they steal them in bulk — by the thousands or even millions — by breaking into poorly protected networks."
— Bruce Schneier

"Although he practiced good computer security and used an anonymous relay service to protect his identity, he slipped up. ... Monsegur slipped up once, and the FBI got him."
— Bruce Schneier, 03/16/2013

"There are two ways to design a system. One is to make it so simple there are obviously no deficiencies. The other is to make it so complex there are no obvious deficiencies."
— C. A. R. Hoare