CIS 6930/CNT 4411 Computer and Network Security Syllabus

1. Instructor:

Dr. Yao Liu,
Office: ENB 336
Phone: 813-974-1079
Email: yliu@cse.usf.edu
URL: http://www.cse.usf.edu/~yliu/
Office hour: WM 1:30am – 3:00pm
Class meetings: WM 9:30pm - 10:45pm in CIS 2084

2. Teaching Assistant:

Mr. Xiaoshan Wang
Office: ENB 213
Email: xiaoshanwang@mail.usf.edu
Office hour: TBD

3. Course Prerequisites:

- Prior knowledge of networking fundamentals would be helpful.

4. Course Description

The course is a study of fundamental concepts and principles of computing and network security. The course covers basic security topics, including symmetric and public key cryptography, digital signatures, cryptographic hash functions, authentication pitfalls, and network security protocols.

5. Course Objectives

The course covers basic security topics, including symmetric and public key cryptography, digital signatures, hash functions, and network security protocols. By the end of this course, students will understand basic security terms such as plaintext, cipher-text, encryption/decryption, and authentication. Students will be able to explain the basic number theory required for cryptographic applications, and manually encrypt/decrypt and sign/verify signatures using cryptographic approaches. Students will be able to identify typical security pitfalls in authentication protocols, and outline the protocols, i.e., AH and ESP protocols, for IP Security.

6. Student Learning Outcomes:

By the end of the course, students will: 1. be tested on core network security problems in the tests or quizzes. 2. Implement at least two key security algorithms regarding public key and symmetric key cryptographic operations as part of their assignments. 3. Finish

at least four homework assignments. 4. Design, implement, or use security techniques learned in the course as part of their project.

7. Textbook:

Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*, *2nd Edition*, Prentice Hall, 2002, ISBN: 0-13-0460192.

8. Tentative Schedule:

(These will be adjusted based on the actual progress in a semester.)

T1. Basic Security Concepts (1 lecture)

- Confidentiality, integrity, availability
- Security policies, security mechanisms, assurance

T2. Basic Cryptography (1 lecture)

- Historical background
- Transposition/Substitution, Caesar Cipher
- Introduction to Symmetric crypto primitives, Asymmetric crypto primitives, and Hash functions

T3. Secret Key Cryptography (5 lectures)

- Data Encryption Standard (DES)
- Encrypting large messages (ECB, CBC, OFB, CFB, CTR)
- Multiple Encryption DES (EDE)

T4. Message Digests (3 lectures)

- Applications
- Strong and weak collision resistance
- The Birthday Paradox
- MD5, SHA-1

T5. Public Key Cryptography (5 lectures)

- Number theory: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totent functions, multiplicative and additive inverse
- RSA, Selection of public and private keys

T6. Authentication (4 lectures)

- Basic concepts of identification and authentication
- Password authentication
- Authentication protocols

T7. Trusted Intermediaries (2 lecture)

- Public Key infrastructures
- Certification authorities and key distribution centers
- Kerberos

T8. Real-time Communication Security (5 lectures)

- IPsec: AH and ESP
- IPsec: IKE

9. Grading:

• Assignments 20%, project 20%, midterm 20%, final 30%, quiz 10%
• The final grades are computed according to the following rules:

- A+: >= 95%;
- A: >= 85% and < 95%;
- A-: >= 80% and < 85%;
- B+: >= 75% and < 80%;
- B: >= 70% and < 75%;
- B-: >= 66% and < 70%;
- C+: >= 63% and < 66%;
- C: >= 60% and < 63%;
- C-: >= 56% and < 60%;
- D: >= 53% and < 56%;
- E: >= 50% and < 53%;
- F: < 50%.

11. Policies on late assignments:

Late homework will be accepted until the solution is posted or the homework is discussed in class. A 15% reduction in grade for each day applies.

12. Policies on absences and scheduling makeup work:

There will be no makeups for homework assignments. Make-up exams will not normally be permitted. Exceptions will be made if a student presents a police report or a doctor's note that shows some emergency situation.

13. Academic integrity:

The university policies against academic dishonesty will be strictly enforced. A student must complete his/her tests, projects and assignments on his/her own. A student's signature on any tests, projects and assignments indicates that the student neither gave nor received unauthorized aid. An FF grade will be assigned to a student who is caught cheating for this class. Example cheating behaviors include but not limited to: direct and

indirect plagiarizing another student's work or online resources, and modifying incorrect test and homework answers for regrading.

14. USF policy on working with students with disabilities:

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, student must identify himself or herself to Students with Disabilities Services and provide documentation of a disability. For more information on USF's policy on working with students with disabilities, please see

http://www.sds.usf.edu/index.asp

**Every part of this syllabus is subject to adjustment as the semester progresses. If you are dissatisfied with the course policies, grading, and assignments, please contact the instructor. Reasonable requests for modifications may be accommodated at the instructor's discretion.*