CSC 774 Advanced Network Security

Syllabus

1. **Instructor:**
   
   Dr. Peng Ning,
   
   Office: 3258 EB II, Centennial Campus
   
   Phone: (919) 513-4457
   
   Email: pning@ncsu.edu
   
   URL: [http://www.csc.ncsu.edu/faculty/ning](http://www.csc.ncsu.edu/faculty/ning)
   
   Office hours: See course website

2. **Course Objectives:**

   By the end of this course, students will be able to:
   
   1. List the common threats and vulnerabilities of networked systems
   2. Describe the following electronic payment systems: NetBill, PayWords, MicroMint, fair exchange protocols.
   3. Describe and give examples of broadcast authentication protocols.
   4. Explain the two types of group management techniques: group key agreement and group key distribution.
   5. Describe the following group key management protocols: Group Diffie-Hellman protocol, Tree-based Group Diffie-Hellman protocol, LKH, and SDR.
   6. Explain at least one secure MANET routing protocol.
   7. Describe security mechanisms for secure routing in MANET.
   8. Explain at least one approach to detecting selfish nodes in MANET.
   9. Describe μTESLA, the broadcast authentication protocol for sensor networks.
   10. Explain the following key pre-distribution protocols for sensor networks: random key predistribution scheme, q-composite scheme, random pairwise keys scheme, polynomial pool based random key predistribution scheme.
   11. Explain the techniques for secure and resilient location estimation in wireless sensor networks.
   12. Explain client puzzle and its effects on denial of service (DoS) attacks.
   13. Use client puzzles to mitigate potential DoS attacks.
   14. Use one-way function chains, collisions of one-way function images, and Merkle hash tree to provide authentication.
   15. Identify flaws in cryptographic protocols.

3. **Text:**

   - No textbook is required.
   - Handouts (All handouts are available on-line):
     
     

### 4. Course Organization and Scope:

(Assume each lecture takes 75 minutes. The following topics need 30 lectures (or 15 weeks).)

1. Introduction to network security (1 lecture)
   - Basic concepts: security services, security mechanisms, etc.
   - Scope of course
2. Network Security Primitives (5 lectures)
   - Absolute basics: Secret key and public key cryptosystems (RSA, DSA, Diffie-Hellman key exchange), one-way hash function
- One-way key chain, Merkle hash tree
- Traditional key distribution techniques (Key distribution center, Certificate based key distribution)
- Client puzzles
- Zero-knowledge proof
- Bloom filter
- Secret sharing
- ID-based cryptography
- Secret handshake
- Rabin’s information dispersal algorithm

3. Electronic payment systems (3 lectures)
   - Electronic billing systems
   - Micropayments
   - Fair exchange protocols

4. Broadcast authentication (2 lectures)
   - TESLA and EMSS
   - BiBa

5. Group key management (4 Lectures)
   - Basic concepts in group key management
   - Group key agreement protocols (GDH, B-D protocols, TGDH)
   - Group key distribution protocols (LKH, secret-sharing based protocols, SDR)

6. Security in ad-hoc networks (4 lectures)
   - Secure ad-hoc routing protocols
   - Detecting selfish or malicious nodes
   - Broadcast authentication
   - Key management for sensor networks
   - Secure location verification

7. Network intrusion detection (1 lecture)
   - Intrusion alert correlation

8. In-class presentations of advanced topics (10 lectures)
   - Topics selected by the instructor on a per-semester basis
   - Students present the above topics individually or in group (depending on enrollment)
   - 25 minutes per presentation (3 presentations per lecture)
   - See Section H for grading policy for in-class presentations

5. Schedule of Reading Assignments:

   • See schedule of classes on course website.

6. Schedule of homework due dates, quizzes and exams:

   There are five homework assignments and two exams. Quizzes are given in the form of pop-up quizzes. Pop-up quizzes are adopted to encourage the students to study during the non-exam weeks. The results are not counted in the final grade.
   • Homework 1: See schedule of classes on course website.
   • Mid-term exam #1: week 6
• Mid-term exam #2: week 12
• Term paper: end of semester.

7. Grading:
Assignments: 10%; midterm #1: 25%; midterm #2: 25%; research paper: 30%; in-class presentation: 10%. The final grades are computed according to the following rules:
   o A+: >= 95%
   o A: >= 90% and < 95%
   o A-: >= 85% and < 90%
   o B+: >= 80% and < 85%
   o B: >= 75% and < 80%
   o B-: >= 70% and < 75%
   o C+: >= 66% and < 70%
   o C: >= 63% and < 66%
   o C-: >= 60% and < 63%
   o D+: >= 56% and < 60%
   o D: >= 53% and < 56%
   o D-: >= 50% and < 53%
   o F: < 50%.

8. Policies on incomplete grades and late assignments:
Homework and project deadlines will be hard. Late homework will be accepted with a 10% reduction in grade for each class period they are late by. However, once a homework assignment is discussed in class, submissions will no longer be accepted. All assignments must be turned in before the start of class on the due date.

9. Policies on absences (excused and unexcused) and scheduling makeup work:
   • You may be excused from an exam only with a university approved condition, with proof. For example, if you cannot take an exam because of a sickness, we will need a doctor's note.
   • Events such as going on a business trip or attending a brother's wedding are not an acceptable excuse for not taking an exam at its scheduled time and place.
   • You will have one chance to take a makeup exam if your absence is excused. There will be no makeup for homework assignments.

10. Course prerequisites:
CSC 570 Computer Networks, CSC 574 Information Systems Security

11. Academic integrity:
The university, college, and department policies against academic dishonesty will be strictly enforced. You may obtain copies of the NCSU Code of Student Conduct from the Office of Student Conduct, or from the following URL.
http://www.fis.ncsu.edu/ncsulegal/41.03-codeof.htm.
12. **NC State 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, students must register with Disability Service for Students at 1900 Student Health Center, Campus Box 7509, 515-7653.

[http://www.ncsu.edu/provost/offices/affirm_action/dss/](http://www.ncsu.edu/provost/offices/affirm_action/dss/)

For more information on NC State’s policy on working with students with disabilities, please see [http://www.ncsu.edu/provost/hat/current/appendix/appen_k.html](http://www.ncsu.edu/provost/hat/current/appendix/appen_k.html).

13. **Laboratory Safety or Risk Assumption: Not Applicable.**

14. **“Pass-through” Charges: Not applicable.**