CSC 774 Network Security

Syllabus

1. Instructor:
   Dr. Peng Ning,
   Office: 250 Venture III, 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: Tuesdays and Thursdays, 3:00 pm – 4:00 pm

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 network security goals, existing network security mechanisms and services
   3. Explain the various applications of cryptography to network security problems
   4. Describe the basic concepts of key management (e.g., session key security principles, Perfect Forward Secrecy, Back Traffic Protection, etc.)
   5. Explain the principles of key management
   6. Describe the following key management protocols: manual key management, SKIP, Oakley, ISAKMP, and IKE.
   7. Explain the common and different features of the above key management protocols, and the advantage and disadvantage of each protocol.
   8. Describe PGP, S/MIME, and SET.
   9. Apply the above protocols to protect WWW transactions
   10. Describe the following electronic payment systems: NetBill, PayWords, MicroMint, fair exchange protocols.
   11. Explain the basic concepts of network intrusion detection and the challenges intrusion detection community is facing
   12. Describe at least three methods for correlating intrusion alerts.
   13. Apply an existing intrusion detection system (Snort, which is a free intrusion detection system) to perform intrusion detection.
   14. Describe and give examples of broadcast authentication protocols.
   15. Explain the two types of group management techniques: group key agreement and group key distribution.
   16. Describe the following group key management protocols: Group Diffie-Hellman protocol, Tree-based Group Diffie-Hellman protocol, LKH, and SDR.
   17. Explain at least on secure MANET routing protocol.
   18. Explain at least one approach to detecting selfish nodes in MANET.
   19. Describe µTESLA, the broadcast authentication protocol for sensor networks.
   20. 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.
21. Apply one way function chains and collisions of one way function images to provide authentication.
22. Identify flaws in cryptographic protocols.

3. Text:
   • No textbook is required.
   • Handouts (All handouts are available on-line through NCSU library):


• Optional readings:

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. Review of cryptography and traditional network security techniques (1 lectures)
   - Secret key and public key cryptosystems
   - One-way hash function
   - Authentication
   - Key distribution (Key distribution center, Certificated based key distribution)
   - Traditional network security techniques (Firewalls, IPsec, and SSL)

3. Internet key management protocols (4 lectures)
   - Basic concepts of key management (Session key security principles, Perfect Forward Secrecy, etc.)
   - Manual key management
   - Automatic key management (SKIP, Oakley, ISAKMP, IKE)

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

5. Network intrusion detection (2 lectures)
   - Intrusion alert correlation

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

7. 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)

8. Security in mobile ad-hoc networks (MANET) (3 lectures)
   - Secure ad-hoc routing protocols
   - Detecting selfish or malicious nodes

9. Security in sensor networks (4 lectures)
   - Broadcast authentication
   - Key management for sensor networks
   - Secure location verification

10. In-class presentations of advanced topics (6 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:

   - Topic 1: No reading required;
   - Topic 2: No reading required;
   - Topic 3: Papers 1 – 5;
• Topic 4: Papers 6 – 10;
• Topic 5: Papers 11 & 12;
• Topic 6: Papers 13 – 15;
• Topic 7: Papers 16 – 20;
• Topic 8: Papers 21 – 22;
• Topic 9: Papers 23 – 26;
• Topic 10: Recent research papers selected on a per-semester basis.

6. Schedule of homework due dates, quizzes and exams:
There are five homework assignments and three 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: topic 3, due by week 4
• Homework 2: topics 4 and 5, due by week 7
• Homework 3: topics 6 and 7, due by week 10
• Homework 4: topics 8 and 9, due by week 13
• Homework 5: topic 10, due by week 16
• Research project report: due by week 16
• Mid-term exam #1: week 5
• Mid-term exam #2: week 10
• Final exam: decided by the university.

7. Grading:
Assignments: 10%; midterm #1: 15%; midterm #2: 15%; final: 30%; research paper: 20%; 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](http://www.fis.ncsu.edu/ncsulegal/41.03-codeof.htm) from the Office of Student Conduct, or from the following URL.

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.**