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
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 managements
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):

1. A. Aziz, "Simple Key Management for Internet Protocol (SKIP)", in *Proceedings of INET 95*, June 1995.
2. H. Krawczyk "SKEME: a versatile secure key exchange mechanism for Internet," in *Proceedings of the Symposium on Network and Distributed System Security*, Page(s): 114 –127, 1996.
3. H. Orman, "*The OAKLEY Key Determination Protocol*," *IETF Request For Comment 2412*, November 1998.
4. D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," *IETF Request For Comment 2408*, November 1998.
5. D. Harkins, D. Carrel, "*The Internet Key Exchange*," *IETF Request For Comments 2409*, November 1998.
6. B. Cox, J.D. Tygar, and M. Sirbu. "Netbill Security and Transaction Protocol," In *The First USENIX Workshop on Electronic Commerce*, pages 77--88, July 1995.
7. R. Rivest and A. Shamir, "PayWord and MicroMint: Two simple micropayment schemes," in *Proceedings of Security Protocols Workshop*, pages: 69 – 87, 1996.
8. S. Micali and R. Rivest. "Micropayments revisited". In Bart Preneel, editor, *Progress in Cryptology --- CT-RSA 2002*, Lecture Notes in Computer Science, Vol. 2271. Springer-Verlag, February 18—22, 2002.
9. N. Asokan, M. Schunter, and M. Waidner. "Optimistic Protocols for Fair Exchange," In *Proceedings of 4th ACM Conference on Computer and Communications Security*, Zurich, April 1997.
10. P. Liu, Peng Ning, Sushil Jajodia, "Avoiding Loss of Fairness Owing to Failures in Fair Data Exchange Systems", *Decision Support Systems*, 31(3):337-350, 2001.
11. B. Mukherjee, L.T. Heberlein, and K.N. Levitt. "Network Intrusion Detection," *IEEE Network*, 8(3): 26-41, May 1994.
12. P. Ning, Y. Cui, D. S. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts," in *Proceedings of the 9th ACM Conference on Computer & Communications Security*, pages 245--254, Washington D.C., November 2002.
13. A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," in *Proc. of IEEE Security and Privacy Symposium*, May 2000.
14. A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and Secure Source Authentication for Multicast," in *Proceedings of Network and Distributed System Security Symposium*, February 2001.
15. A. Perrig, "The BiBa One-Time Signature and Broadcast Authentication Protocol," in *Proceedings of the ACM Conference on Computer and Communications Security*, November 2001.

16. M. Steiner, G. Tsudik, and M. Waidner, “Diffie-Hellman Key Distribution Extended to Group Communication,” in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pages 31--37, 1996.
17. Y. Kim, A. Perrig and G. Tsudik, “Simple and fault-tolerant key agreement for dynamic collaborative groups,” in *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 235 -- 244, 2000.
18. H. Harney and E. Harder, “Logical Key Hierarchy Protocol,” Internet Draft, draft-harney-sparta-lkhp-sec-00.txt, 1999.
19. D. Naor, M. Naor, and J. Lotspiech, “Revocation and Tracing Schemes for Stateless Receivers,” in *Lecture Notes in Computer Science, Vol. 2139*, pages 41 – 51, 2001.
20. Donggang Liu, Peng Ning, Kun Sun, “Efficient Self-Healing Group Key Distribution with Revocation Capability,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pages 231--240, Washington D.C., October, 2003.
21. Y. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad~Hoc Networks,” in *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002),* September, 2002.
22. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 255 -- 265, 2000.
23. A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, “SPINS: Security Protocols for Sensor Networks,” in *Proceedings of Seventh Annual International Conference on Mobile Computing and Networks*, July 2001.
24. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41 -- 47, November, 2002.
25. H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” in *Proceedings of IEEE Symposium on Research in Security and Privacy*, pages 197—213, May 2003.
26. D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pages 52--61, Washington D.C., October, 2003.

- Optional readings:
  - Rolf Oppliger, Internet & Intranet Security, 2/e. Artech House, 2002. ISBN: 1580531660.
  - Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 1995. ISBN: 0-13-061466-1.
  - William Stallings, Cryptography and Network Security: Principles and Practice, 3/e, Prentice Hall, 2003. ISBN: 0-13-091429-0.

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:

- A+: >= 95%
- A: >= 90% and < 95%
- A-: >= 85% and < 90%
- B+: >= 80% and < 85%
- B: >= 75% and < 80%
- B-: >= 70% and < 75%
- C+: >= 66% and < 70%
- C: >= 63% and < 66%
- C-: >= 60% and < 63%
- D+: >= 56% and < 60%
- D: >= 53% and < 56%
- D-: >= 50% and < 53%
- 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/

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.

13. Laboratory Safety or Risk Assumption: Not Applicable.

14. "Pass-through" Charges: Not applicable.