**DEPARTMENT/PROGRAM**: Computer Science  

**COURSE PREFIX/NUMBER**: CSC/ECE 774  

**DATE OF LAST ACTION**:  

**COURSE TITLE**: Advanced Network Security  

**ABBREVIATED TITLE**: ADV_NET_SECURITY  

**SCHEDULING**:  
- Fall  
- Spring  
- Summer  
- Every Year  
- Alt. Year Odd  
- Alt. Year Even  
- Other  

**CREDIT HOURS**: 3  

**OFFERED BY DISTANCE EDUCATION ONLY**:  

**CONTACT HOURS**:  
- Lecture/Recitation  
- Seminar  
- Laboratory  
- Problem  
- Studio  
- Independent Study/Research  
- Internship/Practicum/Field Work  

**GRADING**: ABCDF  

**CONTACT HOURS**:  
- Lecture/Recitation  
- Seminar  
- Laboratory  
- Problem  
- Studio  
- Independent Study/Research  
- Internship/Practicum/Field Work  

**OFFERED BY DISTANCE EDUCATION ONLY**:  

**GRADING**: ABCDF  

**S/U**:  

**CONTENT**:  
- Review of cryptographic techniques; internet key management protocols; electronic payments protocols and systems; intrusion detection and correlation; broadcast authentication; group key management; security in mobile ad-hoc networks; security in sensor networks.  

**PREREQUISITE(S)**: CSC/ECE 570, CSC/ECE 574  

**COREQUISITE(S)**:  

**PRE/Corequisite For**:  

**RESTRICTIVE STATEMENT**:  

**CURRICULA/MINORS**  
- Required  
- Qualified Elective  
- MCS, MS, MSCN  

**PROPOSED EFFECTIVE DATE**: Fall 2004  

**APPROVED EFFECTIVE DATE**:  

**CATALOG DESCRIPTION**: A study of network security policies, models, and mechanisms. Topics include: network security models; review of cryptographic techniques; internet key management protocols; electronic payments protocols and systems; intrusion detection and correlation; broadcast authentication; group key management; security in mobile ad-hoc networks; security in sensor networks.  

**RECOMMENDED BY**:  

**ENDORSED BY**:  

**APPROVED**:  

**DEAN**: Date  

**COLLEGE DEAN(S)** Date  

**CHIEF**: Date  

**DEPARTMENT HEAD/DIRECTOR**: Date  

**COORDINATOR**: Date  

**OFFICE**: Date  

**PROGRAM**: Date  

**ADVISOR**: Date  

**SPECIALIST**: Date  

**DEPARTMENT**: Date  

**DIVISION**: Date  

**SCHOOL**: Date  

**COLLEGE**: Date  

**UNIVERSITY**: Date

**NOTE**: Click once on shaded fields to type data. To check boxes, right click at box, click “Properties”, and click “Checked” under Default Values.
CSC/ECE 774 Advanced Network Security

A. Course Justification

Information security has become increasingly important as society switches from a paper world to an electronic world. Industry, government agencies and various other organizations have an increasing demand for well-trained engineers who are prepared to secure these organizations’ information systems. The Computer Science Department recognized this need several years ago and is currently offering two graduate level courses on information systems (CSC 574) and network security (CSC 774) as well as two undergraduate level courses on introductory computer security (CSC 405) and information systems security (CSC 474, piggybacked with CSC 574).

As a discipline, information security has been studied for several decades and has many more topics than can be covered in these courses. For example, design and development of secure and reliable operating systems are not covered in the current courses, though they are briefly touched upon in CSC 474/574. Trust management is not discussed in any of these courses as well. Indeed, a typical curriculum on information security covers the information security topics in at least four courses. For example, the College of Computing at Georgia Institute of Technology offers seven courses on information security (Please see http://www.gtisc.gatech.edu/education.html).

With two new faculty members (Dr. Jun Xu and Dr. Ting Yu) joining the department in Fall 2003, the Computer Science Department has an opportunity to expand its offerings in information security. Under the leadership of Dr. Peng Ning, Dr. Jun Xu, and Dr. Ting Yu, the Computer Science Department has developed two new courses: CSC 716 Design of Secure and Reliable Systems, and CSC 743 Database Security (CAFs are still being written.) In CSC 743, we plan to cover the fundamental as well as advanced topics on database and distributed systems security, and to prepare the students for conducting successful research related to information system security. In CSC 716, we plan to teach algorithms/techniques in both security and reliability fields that are related to system level design issues, including how systems fail, how algorithms can be compromised, how protocols can be attacked, and ultimately, how the failures can be uncovered and fixed. In addition, we plan to revise the current two graduate level security courses, CSC 574 (Information Systems Security) and CSC 774 (Network Security), to offer a more consistent and coherent information security curriculum.

B. Proposed Revision with Reasons

The revision of the existing security courses is mainly due to the creation of CSC 743 (Database Security). As the title of CSC 743 suggests, it is more appropriate to cover database specific security techniques in CSC 743 rather than in CSC 574. Consequently, the database security portion (except for the introductory content) of CSC 574 (Information Systems Security) is being moved into CSC 743 (Database Security). Specific revisions include:

- Moving the discussion of classical network security techniques (firewalls, IP security, secure socket layer (SSL)) from CSC 774 (Network Security) into CSC 574;
- Changing the title of CSC 574 from “Information Systems Security” to “Information Systems and Network Security” to reflect the above change;
- Adding the following advanced network security topics into CSC 774:
  - group key management (for secure group communication);
  - security changes, which are listed below:
    - Moving the in mobile ad-hoc networks, and security in sensor networks;
    - Changing the title of CSC 774 from “Network Security” to “Advanced Network Security” to reflect the above changes.

The ECE Department has requested to cross-list CSC 574 and CSC 774 as ECE courses to give ECE students more exposure to security courses. After consulting with the head of the Computer Science Department, the Computer Science DGP, and the interdepartmental networking group about the availability of resources and the appropriateness of the courses for both programs, it was decided to support the ECE Department’s request. Thus, this CAF requests cross-listing CSC 574 and CSC 774 as ECE courses.

C. Course Objectives

By the end of this course, successful students will be able to:

1. List the common threats and vulnerabilities of networked systems.
2. Describe network security goals, existing network security mechanisms and services.
3. Explain 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 common and different features of the above key management protocols along with the advantages and disadvantages of each protocol.
8. Describe the following electronic payment systems: NetBill, PayWords, MicroMint, and fair exchange protocols.
9. Explain the basic concepts of network intrusion detection and the challenges the intrusion detection community is facing.
10. Describe at least three methods for correlating intrusion alerts.
11. Apply an existing intrusion detection system (Snort, which is a free intrusion detection system) to perform intrusion detection.
12. Describe and give examples of broadcast authentication protocols.
13. Explain the two types of group key management techniques: group key agreement and group key distribution.
14. Describe the following group key management protocols: Group Diffie-Hellman protocol, Tree-based Group Diffie-Hellman protocol, LKH, and SDR.
15. Explain at least one secure MANET routing protocol.
16. Explain at least one approach for detecting selfish nodes in MANET.
17. Describe μTESLA, the broadcast authentication protocol for sensor networks.
18. Explain the following key pre-distribution protocols for sensor networks: random key predistribution scheme, q-composite scheme, random pair-wise keys scheme, and polynomial pool based random key predistribution scheme.
19. Apply one-way function chains and collisions of one-way function images to provide authentication.
20. Identify flaws in cryptographic protocols.

D. Enrollment Last 5 Years
This course was offered for the first time in Spring 2003. The enrollments in Spring 2003 and Spring 2004 were 18 and 28 respectively.

E. New Resources Required
Reallocation of existing department resources will permit offering this course on the proposed schedule.

F. Catalog Description

Previous:
A study of network security policies, models, and mechanisms. Topics include: network security models; network access control, firewalls; review of cryptographic techniques; IP layer security; internet key management protocols; transport layer security; application layer security, email security, web security; intrusion detection techniques.

Proposed:
A study of network security policies, models, and mechanisms. Topics include: network security models; review of cryptographic techniques; internet key management protocols; electronic payments protocols and systems; intrusion detection and correlation; broadcast authentication; group key management; security in mobile ad-hoc networks; security in sensor networks.

G. 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:
   (See B above)

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 28 lectures (or 14 weeks).)
1. Introduction to network security (1 lecture)
   o Basic concepts: security services, security mechanisms, etc.
   o Scope of course
2. Review of cryptography and traditional network security techniques (1 lectures)
   o Secret key and public key cryptosystems
   o One-way hash function
   o Authentication
   o Key distribution (Key distribution center, Certificated based key distribution)
   o Traditional network security techniques (Firewalls, IPsec, and SSL)
3. Internet key management protocols (3 lectures)
   o Basic concepts of key management (Session key security principles, Perfect Forward Secrecy, etc.)
   o Manual key management
   o Automatic key management (SKIP, Oakley, ISAKMP, IKE)
4. Electronic payment systems (2 lectures)
   o Electronic billing systems
   o Micropayments
   o Fair exchange protocols
5. Network intrusion detection (2 lectures)
Intrusion alert correlation

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

7. Group key management (3 Lectures)
   o Basic concepts in group key management
   o Group key agreement protocols (GDH, B-D protocols, TGDH)
   o Group key distribution protocols (LKH, secret-sharing based protocols, SDR)

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

9. Security in sensor networks (3 lectures)
   o Broadcast authentication
   o Key management for sensor networks
   o Secure location verification

10. In-class presentations of advanced topics (5 lectures)
    o Topics selected by the instructor on a per-semester basis
    o Students present the above topics individually or in group (depending on enrollment)
    o 25 minutes per presentation (3 presentations per lecture)
    o See Section 15. 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: determined by the university

7. Grading:
   Homework 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%
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/ECE Computer Networks, CSC/ECE 574 Information Systems & Network 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.

15. **“Grading Policy for In-Class Presentations.”**
Grading Form for In-class Presentation

In class presentation counts for 10% of the final grade.

Preparation (20 points)
- Preparation of Slides (10 points): _______________
- Preparation of Question (10 points): _______________

In-class Presentation (60 points)

Clarity of the content (30 points)
- Does the presenter discuss the basic techniques logically and clearly?
  - Introduction (5 points): _______________
  - Related work (5 points): _______________
  - Main techniques (20 points): _______________

Clarity of oral presentation (5 points)
- Does the presenter speak clearly?

Coverage (10 points)
- Does the presenter cover the essential techniques in the paper?

Future Work (5 points)
- Does the presenter have a clear idea what could be done based on the results in the paper?

Questions and Answers (10 points)
- Does the presenter give satisfactory answers to audiences’ questions?

Maintenance of Discussion Board (20 points)
(This section will be evaluated at the end of semester.)
- _______________

F. Previous Syllabus

1. Instructor:
   Dr. Peng Ning,
   Office: 453 EGRC, Centennial Campus
   Phone: (919) 513-4457
   Email: ning@csc.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, student 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 application of cryptography to network security problems
   4. Explain the network access control mechanisms, including the basic concepts of firewalls, packet filters, application gateways, and typical firewall configurations
   5. Design firewall configurations and rules to protect a given network
   6. Outline the protocols, i.e., AH and ESP protocols, for IP Security and the two modes for both protocols.
   7. Explain in their own words the goals of IP Security protocols (AH and ESP), the
   8. Use combinations of IP security protocols to achieve a given security goal (e.g., source authentication, content authentication, traffic confidentiality, etc.)
   9. Describe the basic concepts of key management (e.g., session key security principles, Perfect Forward Secrecy, Back Traffic Protection, etc.)
   10. Explain the principles of key managements
   11. Describe the following key management protocols: manual key management, MKMP, SKIP, Photuris, SKEME, ISAKMP/Oakley
   12. Explain the common and different features of the above key management protocols, and the advantage and disadvantage of each protocol.
   13. Explain SSH, SSL, and TLS protocols.
   14. Apply the above protocols to protect transport-layer communication.
   15. Describe PGP, S/MIME, and SET.
16. Apply the above protocols to protect WWW transactions
17. Describe the following electronic payment systems: ECash, ECheck, Micropayment system, fair exchange protocols.
18. Explain the basic concepts of network intrusion detection and the challenges intrusion detection community is facing
19. Explain the following anomaly detection techniques: NIDES/STAT, System Call Trace-based approach, specification-based approach (a.k.a. execution monitoring).
20. Explain the following misuse detection techniques: STAT, rule-based misuse detection, abstraction-based intrusion detection, data mining based method.
21. Apply an existing intrusion detection system (Snort, which is a free intrusion detection system) to perform intrusion detection.

3. Textbook:
   - 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)
      o Security services
      o Security mechanisms
      o Security management
   2. Review of cryptographic techniques (3 lectures)
      o Secret key and public key cryptosystems
      o One-way hash function
      o Authentication
      o Key distribution (Key distribution center, Certificated based key distribution)
   3. Network access control (3 lectures)
      o Basic concepts (firewall policy)
      o Packet filters
      o Application gateways
      o Firewall Configuration
   4. Internet layer security (4 lectures)
      o IP Sec architecture
      o Authentication Header (AH) protocol
      o Encapsulating Security Payload (ESP) protocol
   5. Internet key management protocols (6 lectures)
      o Basic concepts of key management (Session key security principles, Perfect Forward Secrecy, etc.)
      o Manual key management
      o MKMP
      o SKIP
      o Photuris
      o SKEME
      o ISAKMP/Oakley
   6. Transport layer security (3 lectures)
      o Secure Shell (SSH)
      o Secure Sockets Layer (SSL)
      o Transport Layer Security (TLS)
   7. Application layer security (3 lectures)
      o Security enhanced protocols
o Secure email (PGP, S/MIME)
  o WWW Transactions

8. Electronic payment systems (3 lectures)
  o Electronic Cash
  o Electronic Checks
  o Credit card Payments
  o Micropayments
  o Fair exchange protocols

9. Network intrusion detection (4 lectures)
  o Basic concepts of intrusion detection (anomaly detection, misuse detection, false positive, false negative, etc.)
  o Anomaly detection techniques
  o Misuse detection techniques

5. Schedule of Reading Assignments:

- Topic 1: Chapters 1, 3
- Topic 2: Chapters 4
- Topic 3: Chapters 5, 6, 7, 8
- Topic 4: Chapters 9.1 – 9.3
- Topic 5: Chapter 9.4, handouts 1, 2, 3
- Topic 6: Chapter 10
- Topic 7: Chapter 11
- Topic 8: Chapter 13, handouts 4, 5
- Topic 9: Chapter 14, handouts 6, 7.

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

   There are six 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: topics 1 and 2, due by week 4
   - Homework 2: topics 3, due by week 6
   - Homework 3: topics 4, 5 due by week 8
   - Homework 4: topics 5 and 6, due by week 11
   - Homework 5: topics 7 and 8, due by week 13
   - Homework 6: topics 9, due by week 15
   - Mid-term exam: week 8
   - Research project report: due by week 15
   - Final exam: decided by the university.

7. Grading:

   - Assignments 30%, project 20%, midterm 25%, final 25%. 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+: >= 65% and < 70%
     - C: >= 60% and < 65%
     - C-: >= 55% and < 60%
     - F: < 55%

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

13. Laboratory Safety or Risk Assumption: Not Applicable.


15. Grading Policy for In-Class Presentations

<table>
<thead>
<tr>
<th>Grading Form for In-class Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>In class presentation counts for 10% of the final grade.</td>
</tr>
</tbody>
</table>

Preparation (20 points)
- Preparation of Slides (10 points):
- Preparation of Question (10 points): ____________

In-class Presentation (60 points)

Clarity of the content (30 points)
- Does the presenter discuss the basic techniques logically and clearly?
- Introduction (5 points): ____________
- Related work (5 points):
- Main techniques (20 points):

Clarity of oral presentation (5 points)
- Does the presenter speak clearly?
- ________________

Coverage (10 points)
- Does the presenter cover the essential techniques in the paper?
- ____________

Future Work (5 points)
- Does the presenter have a clear idea what could be done based on the results in the paper?
- ____________

Questions and Answers (10 points)
- Does the presenter give satisfactory answers to audiences’ questions?
- ____________

Maintenance of Discussion Board (20 points)
(This section will be evaluated at the end of semester.)
- ____________