Network Security
CEN 5542-01
formerly CIS 5357

Administrative
• TR, 8:00-9:15 am
• 103 James Jay Love Building
• www.cs.fsu.edu/~yasinsac/ns03/main.html
• Will establish and use a class mailing list

My Information
• Alec Yasinsac
• 262 James Jay Love Building
• 644-6407
• yasinsac@cs.fsu.edu
• Office hours: TBA

Course Focus
• Network Security Theory
• Network Security Mechanisms
  – Cryptographic Protocols
  – Public Key Infrastructures
  – Intrusion Detection
• How to do Research
• A Few Network Security Applications

Text

Evaluation
• Participation 25% 25%
• Chapter Exams 2 x 15% 30%
• Term Paper 25% 25%
• Final Exam 20% 20%

100%
Participation
- Attendance
  - Be here (1 pt/class)
  - You may print slides from the course home page
- Homework
- Lab Assignments
- Quizzes

Homework
- From text or instructor
  - Counts as two quizzes
  - May be quiz from reading assignment
  - Others are listed on the Course Calendar
  - May drop one of these

Exams
- Two one hour exams
- Roughly equivalent new content quantity
- Final will cover new material and the previous exams

The Term Paper
- 25% of the course grade
- Target: Research quality
- List of topics provided on course web page or,
  - Bring other topics to me for approval
- Milestones
  - Topic, bibliography, outline, draft, final

Laboratory Exercises
- Six total labs
- Three will be required
- Three will be optional

Quizzes
- 8-10
- Unannounced
- Beginning of class
- Will not drop any quiz grades
- Can replace up to 3 quiz grades with the optional lab exercises
Admin Notes

- Now on the Course Web Page:
  - The slides for class 1. (From the main page select calendar, complete calendar, then the class topic)
  - A bibliography for the course: (resources, course bibliography)
  - A tentative paper list: (assignments, paper list)
  - Syllabus (Access it from the main page.)

Some Predictions

- C's will be pretty easy to get
- A's will be pretty hard to get
- There will be some F's
- You will wait until the last minute for most everything

Course Evaluation Comments

That I Am Going For:
1. I got my money's worth, e.g.
   - I learned volumes about Network Security and how to do research
   - I will apply much of what I learned
2. The instructor was on time, prepared, and energetic
3. Class was worth going to
4. I got what I earned

Eval Comments That I Do NOT Expect to See

1. I REALLY enjoyed those exciting reading assignments!
2. This Network Security stuff is all perfectly clear to me now.
3. The instructor knew every answer to every question
4. The instructor is obviously an Information Security Expert.

Finally:

We Will Start On Time

- We go by my watch
- Quizzes are first thing

This Semester

- Cryptography (~40%)
  - Application
  - Algorithms
- Security Protocols (~20%)
- Web/IP Security (30%)
- Miscellaneous Security Issues (10%)
Today's Discussion

1. Introduction to Information Security

Information Security

- Privacy
- Integrity
- Non-repudiation
- Denial of service

Information Security Strategies

- Privacy ➢ Protect
- Integrity ➢ Protect/detect
- Non-repudiation ➢ Protect/detect
- Denial of service ➢ Detect

Information Security

- Dealing with malicious behavior
  - Before
  - During
  - After

Goals

- Before
  - Prevent attack
- During
  - Minimize damage
- After
  - Recover
  - Put them in jail

Security Services

- Confidentiality
- Authentication
- Access control
- Integrity
- Non-repudiation
Authentication
• Concerned with user identity
• What is the essence of identity?
  – Your being :-)
  – Your name/address/IP
  – Your physical self - fingerprint, retinal scan
  – Your password
    • Something you know
    • If someone else knows your password, they are you!
• The essence of your identity must be:
  – Unique
  – Uncopyable

Access Control/Authorization Control
• Concerned with what users are authorized to do
• Three parties: Owner, User, Custodian
  – Not necessarily mutually exclusive
  – Discretionary AC: The owner decides who gets access
  – Mandatory AC: Classification determines who gets access

Access Control/Authorization Control
• Access Control
  – Owner provides ACL/M to custodian
  – Custodian must
    • Authenticate User
    • Match user ID against the access list for the resource
• Authorization control
  – Owner provides certificate to user
  – User presents certificate to gain access

Confidentiality
• Protecting
  – Files
  – Communication
  – Computation
  – Traffic analysis
  – Identity

Non-repudiation
• Authentication allows you to KNOW who someone is
• Non-repudiation allows you to PROVE who does something
• Digital signatures

Security Threats
• Viruses
• Loss of Privacy
• Masquerade
• Deletion of data
• Changing of data
• Stealing cycles
• Denial of service/access

Not all Inclusive
Definition of Hacking

• Classic: Elegant programmer
• Present: Programmer good enough to use services in unintended ways to do things that they probably shouldn't.
  – IP capabilities (ICMP)
  – Application holes (Word Macros)

Viruses

• Piggyback artists
• Identified by their "signature"
• Norton, McAfee update signature files every 48 hours (at my last check)
• Trojan Horse is very similar
• Worst is yet to come [still]

Review

• Administration
• Intro to Network Security

Preview

• Networking primer
• Secure Channels
• Security models