

# IT 4823

## Information Security Administration

### Introductions

### About Computer Security



Notice: This session is  
being recorded.

# Syllabus

- The syllabus is in electronic format.
- See “Start Here” in the D2L section for this course.

# Introductions

## **Bob Brown**

- 30 years' experience in managing information technology
- Experienced in teaching both hardware and software courses
- Master's degree in CS from SPSU
- Ph.D. in computer information systems from Nova Southeastern University



## Expectations of University Students

- **Critical thinking:** The ability to analyze a situation, impose order on it, and extract facts and probabilities.
- **Writing:** organization, spelling and grammar, proper use of others' work.
- **Work outside class:** Two outside hours for each class hour. For this class, that's about 15 hours per week, five in class and ten outside.

# Expectation for this Class

- You will be in your seats at the start of the class period.
- You will remain in class for the full period.
- You will keep cell phones and other gear quiet
- Only one person will talk at a time
- If you bring food, bring enough for everyone!



**What do you notice about this list?**

# Expectation for this Class

- You will be in your seats at the start of the class period.
- You will remain in class for the full period.
- You will keep cell phones and other gear quiet
- Only one person will talk at a time
- If you bring food, bring enough for everyone!



**These are all about being courteous to your classmates!**

# Some More Expectations

- You will come to class prepared by having done the assigned reading.
- You will do your own work.  
There are severe penalties for cheating. You will complete your work on time.

# What You Can Expect of Me

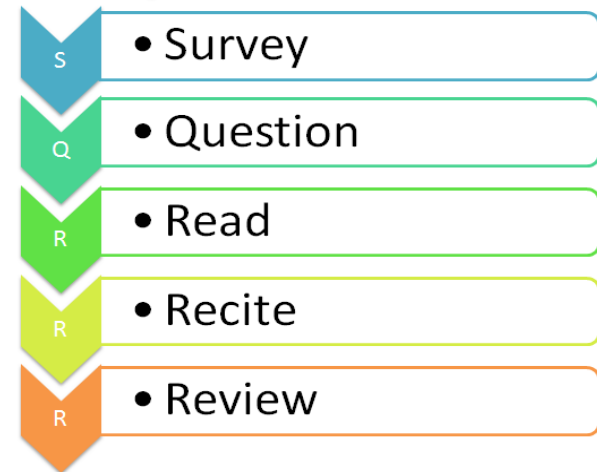
- I will be in class on time, every time.
- I will be prepared to cover the scheduled material thoroughly.
- Your work will be graded and returned promptly; generally within a week.
- I will listen respectfully to your opinions.
- I will answer your questions promptly and carefully; if I do not know an answer, I'll find out.
- I will help you succeed.



# How To Succeed in this Class

- Read the syllabus
- Read the textbook  
An effective reading technique: SQ3R  
*Survey • Question • Read • Recite • Review*
- Come to class and  
*pay attention!*
- Take notes (the pen is mightier than the laptop)
- Do the homework
- Allow enough time





## SQ3R



# Another Word About Workload

- You are in class five hours per week.  
You should expect to spend about twice that (or ten hours) outside class on reading, preparation, study, and homework.
- That's fifteen hours per week total.
- If you are not ready for that, you have some deciding to do!

# A Recent Student Rating

RATING	CLASS	COMMENT
07/29/2015	 IT 3123	TOUGH GRADER TESTS ARE TOUGH LECTURES ARE LONG
 <b>POOR</b>	For Credit: Yes Attendance: Mandatory	Unprofessional will mark the feedback on book but for
1 HELPFULNESS	Textbook Use: Barely cracked it open	<div><p><i>Textbook use:</i> <b>Barely cracked it open.</b> <i>Grade received:</i> <b>D-</b></p></div>
1 CLARITY	Rater Interest: Really into it	
1 EASINESS	Grade Received: D-	
		 1 person found this useful  1 person did not find this useful
		<a href="#">report this rating</a>

Moral: You are going to have to study to earn a satisfactory grade.

# Syllabus Review

- Textbook
- Appointments
- Class schedule
- Exam Schedule: exams *will* happen as scheduled. Be there!

# Objectives

- Build a sensitivity to the threats and vulnerabilities of personal, organizational, and national security information systems;
- Build a working knowledge of principles and practices in information security.
- Design, execute, or evaluate personal or organizational security procedures and practices.
- Identify the key areas of information security and how they work.

Detailed objectives are in the syllabus

# Goal: Mastery of the Material

- Your job: master this material. “Own” it so that you can use it in your profession.
- My job: help you to do that.
- Another job for me: measure your mastery. That means grades. *Grades are not the objective* of this class; they are a measure of how well you achieved the objectives!
- Take care of mastery and the grade will take care of itself.

# Grading Plan

- 30 % Homework
- 15% Quizzes
- 30 % Exams (two @ 15%)
- 25% Final exam

You cannot earn a satisfactory grade without doing the homework

# When People Submit Homework

- 1-2 days before deadline: 5% (*These are the people who earn grades of A.*)
- 3-24 hours before: 10%
- 1-2 hours: 10%
- **less than 1 hour: 65%**
- emails in distress after the deadline has expired: 10% (or nothing at all)

} Most unsatisfactory grades are from this group



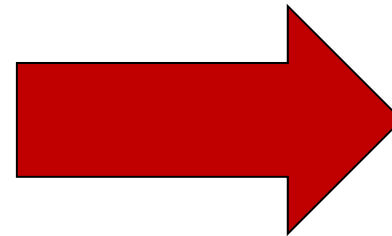
# “Due” Means Due

- Late homework will not be graded (and you’ll get a zero)
- Submitted to D2L only
- No email, no paper, no excuses!

# Keeping Track of Due Dates

## Course Syllabus

Kennesaw State University Information Technology Department IT 3123 — Hardware and Software Concepts — Spring, 2016 Course Syllabus			
Instructor: Bob Brown (470) 578-7505 <a href="mailto:Bob.Brown@kennesaw.edu">Bob.Brown@kennesaw.edu</a> <a href="http://bbrown.kennesaw.edu/it123/2016_02/">http://bbrown.kennesaw.edu/it123/2016_02/</a>			
Office hours: (J-282) Tuesday and Thursday, 9:15 – 10:45 AM and 12:15 – 1:45 PM; also by appointment. I will try to respond to email within 24 hours during the work week if you include "IT 3123" in the subject.			
<b>Course calendar:</b>			
Date	Topic	Reading	Due Today
Jan 12	Introductions and Overview	Chapter 1	
Jan 14	Concepts and Systems Architecture	Chapter 2	
Jan 19	Number Systems	Chapter 3	Assignment Zero
Jan 21	Data Formats	Chapter 4	Assignment 1
Jan 26	Integer and Floating Point Numbers	Chapter 5	Quiz 1
Jan 28	Digital Logic	Supplement	
Feb 2	The Little Man Computer	Chapter 6	Assignment 2
Feb 4	From LMC to a "Real" Computer		Quiz 2
Feb 9	Instructions at the Machine Level		
Feb 11	The CPU and Memory I	Chapter 7	
Feb 16	The CPU and Memory II	Chapter 8	Assignment 3, Quiz 3
Feb 18	<b>Exam 1</b>		
Feb 23	Input and Output	Chapter 9	
Feb 25	Computer Peripherals	Chapter 10	
Mar 1	Modern Computer Systems	Chapter 11	Quiz 4
Mar 3	March 2 is the last day to withdraw with a grade of W. Overview of Networks and Data Communications	Chapter 12	Assignment 4
Mar 8	Ethernet and TCP/IP	13.1 - 13.5	
Mar 10	Network Names and Addresses, Other Protocols	13.6-13.10	
Mar 15	Communication Channels	Chapter 14	Assignment 5, Quiz 5
Mar 17	<b>Exam 2</b>		
Mar 22	Overview of Operating Systems	Chapter 15	
Mar 24	User's View of Operating Systems	Chapter 16	
Mar 29	File Management	Chapter 17	
Mar 31	The Internet Operating System	18.0-18.6, 18.8-18.10	
Apr 5-7	No meeting — Spring Break		
Apr 12	Virtual Memory	18.7	Assignment 6
Apr 14	Virtualization of Multiple Systems	18.11	
Apr 19	Operating System Examples	Supplement	Quiz 6
Apr 21	Programming Tools	Supplement	
Apr 26	About Computer Security		
Apr 28	Review for Final		
May 5	<b>Final Exam: 10:30-12:30 (Note changed time)</b>		



## Your Gear



# Submitting Homework

- All homework will be submitted using Desire2Learn. **No other method is acceptable.**
- Homework is due by 11:59 PM on the date given in the syllabus.
- You must prepare your homework in a form that I can read with Microsoft Word.
- LibreOffice is a free program that can write Word-compatible files.

# Handwritten Work

- In a few cases, I will allow handwritten or hand drawn work. (For example, a network diagram.)
- You may still type this work if you like.
- If you choose handwriting, you must **scan your handwritten work**. (Scanners are available in the CSE lab.)
- You must paste the scanned image into the proper place in your Word document. **Multiple documents will not be accepted.**

# Homework Grading

- I will mark your homework on a “points off” basis.
- This is a *major change* from the way I’ve marked homework in the past. If you’ve had other classes from me, take note!

# More About the Homework

- The teacher knows the answers (usually.)
- There are two purposes to homework:
  - To allow you to practice what you've learned
  - To allow you to demonstrate that you've learned it.
- Cut-and-paste homework will not do.
- And it might get an academic misconduct penalty!

# Quizzes

- We will have about 6 quizzes this term.
- Quizzes cover the assigned reading as well as the lectures!
- Quizzes will be administered using D2L.

# About Exams

- Exams will be given on the dates shown in the syllabus.
- If you miss an exam without making arrangements with me *in advance*, you will earn a grade of zero.
- “Making arrangements” does not mean leaving voice mail or sending email; it means we have had a two-way discussion and agreed on when you will take the exam.



# Narrated Slides

- Lecture slides will be posted to D2L in the appropriate module as PDF files a day or so after each lecture.
- There is information about printing the slides in D2L.
- The lectures are recorded and will be available as video files with slides and audio synchronized.
- These are **not a substitute** for coming to class!

# About the Narrated Slides

- They're intended for people taking this course; you paid big bucks for the course material.
- Every now and then, someone decided to “help” me and list the podcasts with the iTunes Store. **Please don't do that!**
- Apple does not care about the rights of others, and does not respond to requests to remove such podcasts.
- The only thing I can do in that case is password the files, which will be a pain in your side!

# What Does “Secure” Mean?

- A system that does what it is intended to do and *nothing else.* – *Charles Pfleeger*
- “A computer is secure if you can depend on it and its software to behave as you expect.”  
– *Garfinkle and Spafford*
- “The protection afforded to an automated information system in order to attain the objectives of preserving confidentiality, integrity, and availability.” – *NIST*

# Thinking About Security

[Do not fall into] the classic security misapprehension error: the idea that either you're "secure" or you're not.

The real question, as we all know, should be, "against what sort of attacks am I vulnerable?"

*—Curt Sampson*

# Specifying Security

- Security is specified by *policy*.
- Policies are organizational laws; they state what must happen, what may happen, and what must not happen.
- A system the behavior of which does not violate organizational policies is, by definition, secure.
- So, effective security is impossible in the absence of policy.

# Example: Student Grades

- Policy: Only authorized persons may alter student grades.
- OK... who's authorized?

# Example: Student Grades

- Policy: Only authorized persons may alter student grades.
- OK... who's authorized?
- Authorized persons:
  - University registrar
  - Full-time employees of the registrar's office, if designated by the registrar.
- These are *policy* questions, not “security” questions.

# Policies and Mechanisms

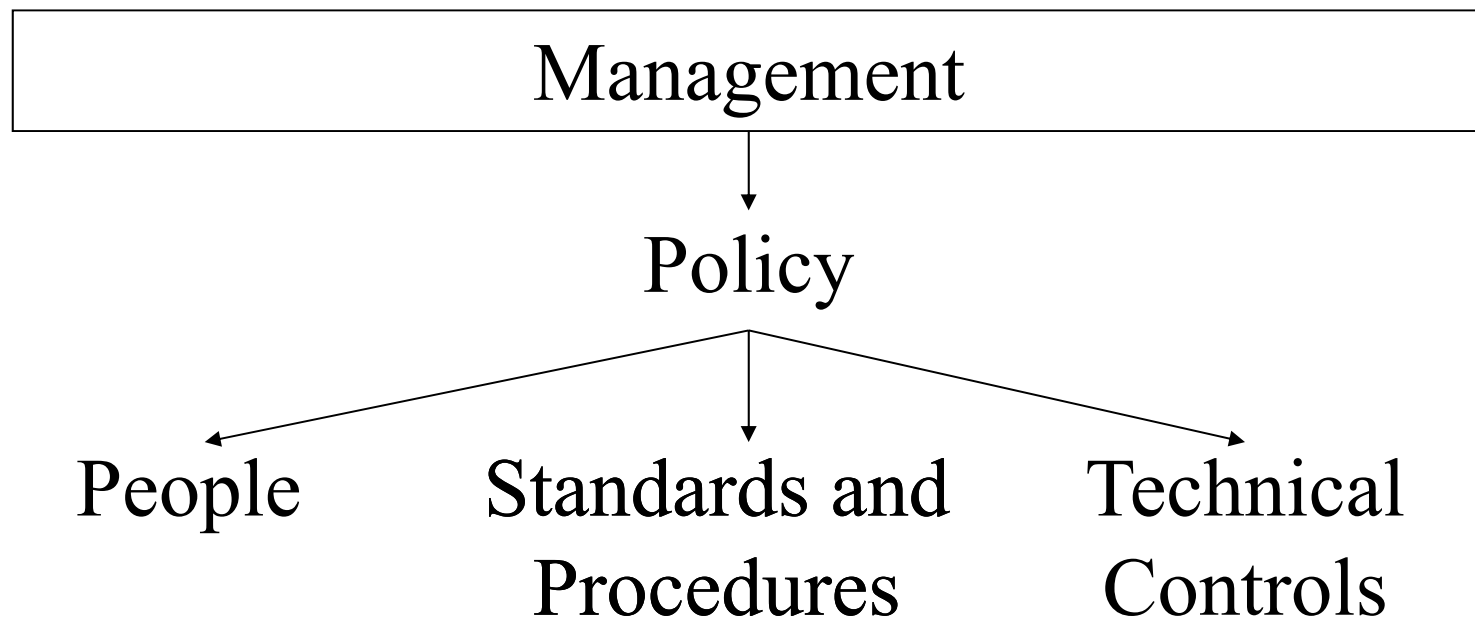
- Policy says what is, and is not, allowed
  - What *must* happen, what *may* happen, what *must not* happen.
  - This defines “security” for the site/system/*etc.*
- Mechanisms enforce policies
- Application of mechanism in the absence of supporting policy could be *detrimental* to security!
- “Security at the expense of usability comes at the expense of security” – Avi D



# Policy Considerations

- Value of assets protected
- Vulnerabilities
- Threats
- Trade-offs
  - Security vs. ease of use
  - Cost of security vs. cost of failure and recovery

# A Structure for Security



# Properties of Information Security

- **Confidentiality**
  - Keeping data and resources hidden from unauthorized personnel
- **Integrity**
  - Data integrity (integrity)
  - Origin integrity (authentication)
- **Availability**
  - Enabling access to data and resources when and where they are needed.

Your book calls this the Security Requirements Triad.

# Confidentiality

- **Data confidentiality:** Information considered confidential (by policy) is not disclosed to unauthorized persons.
- **Privacy:** Assurance that individuals control what data are collected about them and how those data are used and disclosed.

# Integrity

- **Data integrity:** Data agree with the source from which they are derived, and data and programs are changed only in authorized (by policy) manners.
- **System integrity:** A system performs its intended function (and nothing else) unimpaired and free from unauthorized manipulation.
- **Origin integrity:** We can be sure that data came from the ostensible source.

# Availability

A system is:

- Available to authorized users
- When and where they need it
- With a suitably good response time.

# Authenticity and Accountability

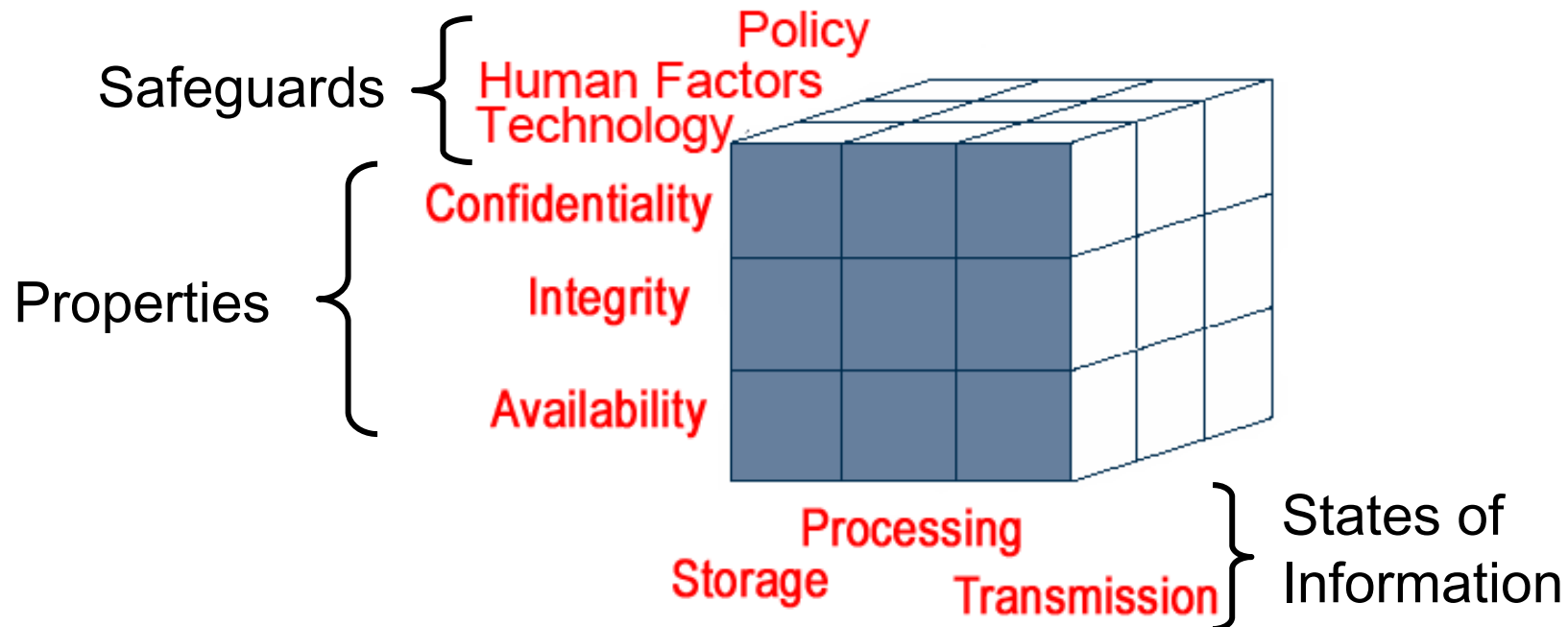
- **Authenticity:** The ability to verify the source of data, messages, etc. (This is really *origin integrity*.)
- **Accountability:** We can tie actions to a particular entity. (This is *origin integrity* again.)

# How Bad Is It?

- NIST divides security failures into three levels of impact.
  - Low: Minimal adverse effect
  - Moderate: An organization can perform its primary functions, but with reduced effectiveness.
  - High: Performance of an organization's mission is significantly impaired.



# McCumber Security Model



Consider not only the properties of security, but also the states of information and the controls available.

*National Security Telecommunications and Information Systems Security Committee*

# Assets to be Protected

- Hardware
- Software
- Data
- Infrastructure (including communications facilities)
- People

# The Attacker's Triad: DAD

- Disclosure: compromises confidentiality
  - Outside attackers
  - Insiders
  - Programming or other errors
- Alteration: compromises integrity
  - Accidental or malicious alteration
  - Programming or equipment failure
- Denial: compromises availability
  - Deliberate attacks
  - Failures of systems or environment

# Stallings's List

- Disclosure (failure of confidentiality)
- Deception (failure of origin integrity)
- Disruption (failure of availability)
- Usurpation (this one is more a mechanism than a consequence; usurpation will lead to one or more of the consequences above.)

# Who Are These Attackers Anyway?

- Intelligence and law enforcement agencies
- Criminals
- Corporate spies
- Misguided insiders
- Vandals
- Poorly-socialized adolescents
- Others...

# Where Are They?

- Outsiders
  - Network-based attacks
  - Physical attacks
- Malicious insiders
  - May have authorized access to systems they attack
  - May be in positions of trust
- Other insiders
  - Non-malicious mistakes made by those with authorized access.

# Vulnerabilities, Threats, Risks

- **Threat:** something bad that can happen. A potential violation of security policy.
- **Vulnerability:** a weakness that could allow a system to enter a state not permitted by policy.
- **Exploit:** a mechanism for taking advantage of a vulnerability.
- **Risk:** the probability that a particular threat (violation of policy) to a particular asset will be realized. Implies a vulnerability that can be exploited.

# Goals of Information Security

- **Prevention**
  - Prevent violations of security policy
- **Detection**
  - Detect violations of security policy
- **Response and Recovery**
  - Stop the violation, assess and repair damage
  - Continue to function correctly even if security policy is violated
  - Return system to a state consistent with policy



# Trust and Assumptions

- Underlie *all* aspects of security
- Policies are assumed to:
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms are assumed to:
  - Enforce policy
  - Work correctly

# Trust Comes From Assurance

- Assurance is a formal evaluation of a system, with more or less rigor.
  - Specification assurance
    - Requirements analysis
    - Statement of desired functionality
  - Design assurance
    - How system will meet specification
  - Implementation assurance
    - Programs/systems carry out the design
    - A system does what is was designed to do...
  - *and nothing else!*

# Computers and Networks

- Previously, computer systems could be secured by locking them up.
- Most computers are now connected to networks, and to the Internet.
- So, threats can be physically remote.

# Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

# Challenges

- It's not that simple!
- Security design must consider potential attacks.
- Physical and logical placement of security mechanisms may not be obvious.
- Mechanisms have operational challenges, *e.g.* key distribution.
- It's a battle of wits.
- Not everyone sees the benefit.

# More Challenges

- Effective security requires constant monitoring
- Security can be an afterthought.
- Strong security may be viewed as an impediment to getting work done.

# Security Trends

- Vulnerabilities up
- Incidents up
- Losses up
  - Virus contamination
  - Data disclosure
  - Hardware theft
- Attacks becoming more sophisticated (and knowledge needed by attackers decreasing.)

# Focus and Bias

- Current information security focuses primarily on mitigation.
- There is a bias toward technological mechanisms
- There is a bias in favor of logical rather than physical mechanisms



# Questions

