Welcome to the Dark Arts!

Instructor:

- Dr. Joseph Gersch
  - Background in industry, computer security and academia
- CSB 464
- Office hours:
  - Tuesday/Thursday 1-2PM
  - Email: gersch@cs.colostate.edu
TAs

- Graduate TAs
  - Sachini Weerawardhana
  - Vignesh Pagadala

- Undergraduate TA
  - Noah Cain
Website: [http://www.cs.colostate.edu/~cs356](http://www.cs.colostate.edu/~cs356)
- Syllabus
- Progress page
  - Assignments
  - Lecture slides and notes
- Deter

Canvas
- Assignments
- Submissions
- Grades
Grading policy

- Class Participation – 10%
  - Newshound Reports on “Security in the news”
  - Other miscellaneous items as they come up
- Homework / quizzes – 15%
- Projects – 25%
- Midterm – 25%
- Final – 25%
Late policy

- In general, there isn’t one. Turn things in ON TIME!!

- Homework
  - Due Tuesday by 2PM (beginning of class)

- Projects
  - As specified in assignment
  - 50% penalty for limited-time late submissions (typically 1 week)

- Exams
  - No late exams

- ... Unless prior arrangement are made for extenuating circumstances. Emergency situations will be accommodated.

- Authors: William Stallings & Lawrie Brown

- (3rd & 4th editions ok, but be careful during homework assignments: the chapter questions could be numbered differently)

- Be careful in homework between “Problems” and “Review Questions” or you will be answering the wrong question!!!
“News hounds”
  - 3 newshounds per class period
  - Selected at beginning of class
  - Random

- Take notes and send to cs356@cs.colostate.edu
  - PDF form
  - Will be posted to website
  - Newshound notes and presentation due in next class

- Grade based on quality and completeness
Weekly assignments

- Reading assignments
  - Due before topic covered in class
  - Occasional quizzes
- Chapter quizzes
  - Due class time on Tuesday
- Homework assignments
  - Due class time on Tuesday
  - PDF format
  - Checked into Canvas
Cheating

- Don’t.
- Academic Integrity will be notified.
- You will fail the class.
Respect

- Student to student
- Student to TA
- TA to Student
- Professor to Student
- Student to Professor
Cell Phones and Laptops

- No cell phones – no exceptions
- Laptops for note taking only.

- This is a pet peeve of mine: you (or your parents) are paying a lot of money for you to be here. If you don’t plan on paying attention, drop now and let someone else get a slot in the class.

- I’m going to do my best to make this class very worthwhile for you. I’ll be doing demos and bring in real-world stories. SO... be here and be engaged in what we are doing.
Posted to the progress page
Available before class
Feel free to print and take notes
What do we cover

- Phase 1: the fundamental concepts, tools and techniques

- Phase 2: “It takes a thief to catch a thief”, so let’s learn how the bad guys work and learn how to hack.
  - Techniques, demos, “bank robbery” and other assorted break-ins

- Phase 3: Learn how to defend
What do we cover

- Chapter 1 – Overview
- Chapter 2 – Cryptographic Tools
  - Hash Functions
  - Encryption (public/private, symmetric)
  - Digital signatures
- BitCoin & Block Chain  *(new this semester)*
- Chapter 3 – User authentication
  - Passwords
  - Tokens
  - Biometric
What do we cover?

- Chapter 4 – Access control
  - Concepts
  - DAC (Discretionary)
  - RBAC (Role-based)

- Chapter 5 – Database Security
  - Relational Databases
  - Inference
  - Statistical
What do we cover?

- Chapter 6 – Malicious software
  - Types of malware
  - Propagation
  - Payload
  - Countermeasures

- Chapter 7 - Denial of service
  - Flooding
  - Distributed
  - Reflector
Chapter 8 – Intrusion Detection
   - Host-based
   - Distributed
   - Network

Chapter 9 – Firewalls and Intrusion Prevention
   - Types of firewalls
   - Characteristics
   - Location and configurations
What do we cover?

- Chapter 22 – Internet Security
  - Secure email
  - SSL
  - HTTPS

- Chapter 23 – Internet Authentication
  - X.509
  - Identity Management

- Chapter 24 – Wireless Network Security
What do we cover?

- As time permits
  - Chapter 10 – Buffer overflow
  - Chapter 11 – Software security
  - Chapter 12 – Operating system
  - Chapter 20 – Symmetric Encryption
  - Chapter 21 – Public Key Encryption
Projects

- 1-2 programming assignments
- 2-3 DETER projects