CS 419 Computer Security

Week 0: About the Class

Paul Krzyzanowski

Welcome to computer security

About Me

MASON SHOE DEALER CERTIFICATION

This Is To Acknowledge That

P KRZYZANOWSKI

Has Been Approved and Accepted As An Authorized Mason Dealer And. Upon Reviewing the Mason Shoe Material. Is Qualified To Accept Orders For All Mason Products.

Victor T. Mason
President
MASON SHOE
COMPANY

DEALER MASON SHOE CERTIFICATION

Web site and contact

Canvas: https://rutgers.instructure.com/courses/160949

web: www.cs.rutgers.edu/~pxk/419

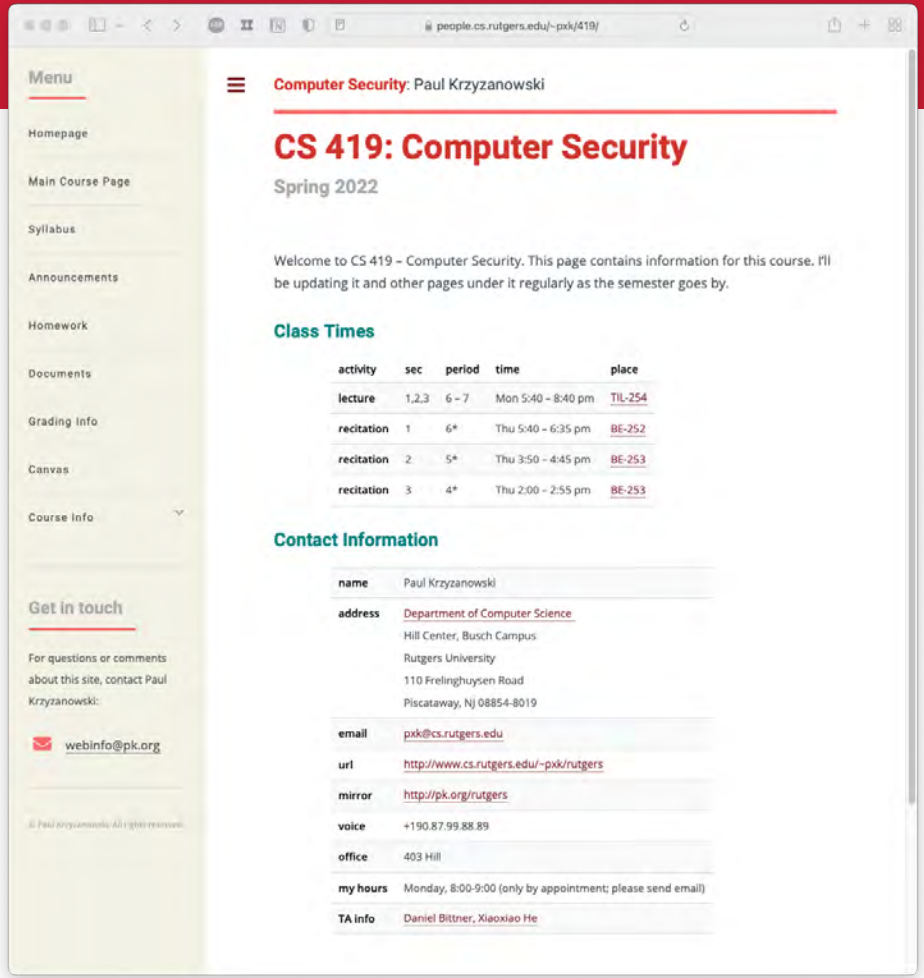
mirror: www.pk.org/419

email: pxk@cs.rutgers.edu

phone: +190.87.99.88.89

Class info

- **Contact info**
- **TA info**
- **Syllabus**
- **Lecture notes**
- **Canvas links to:**
  - Class news
  - Homework



Class meetings

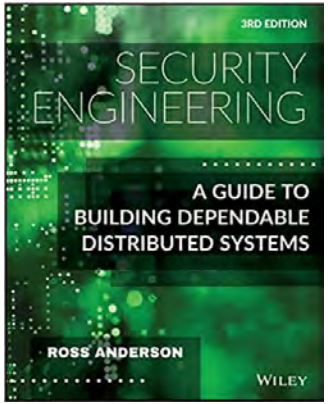
- **Classes will be held via Zoom (initially)**
- **Lecture recordings will be made available**
  - Canvas
- **You can take classes asynchronously when they're remote**
  - I'll be around for questions
  - Send via zoom chat, email, etc.
  - I will post FAQs and corrections if needed

Text

None required – but we will use several sources

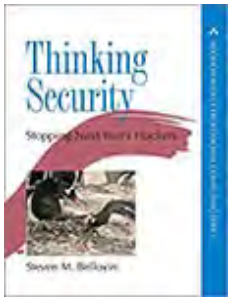
Security Engineering: A Guide to Building Dependable Distributed Systems
3rd Edition
by Ross J. Anderson

https://www.cl.cam.ac.uk/~rja14/book.html



But mostly…

- Other reading material on the web
- Lecture slides
- Lecture notes/summaries



Policy

- **If classes are remote:**
  - Weekly quizzes: 5-6 questions; 15 minutes

  else
  - 3-4 in-class quizzes, no final
- **Short programming assignments (~4)**
  - Individual assignments
  - Due prior to the due date
- **Written assignments**
  - Due prior to the due date
- **Collaboration & academic integrity**
  - Individual assignments – no copying!

Grades

- Quizzes ~ 40%
- 6-10 written assignments ~ 25%
- ~4-5 programming assignments ~35%

What this course IS

- **Security engineering**
- **Understand why systems have weaknesses**
- **How do we deal with these weaknesses?**
  - People, devices, networks, operating systems, applications
  - Cryptographic algorithms
  - Authentication & key distribution protocols
  - Ensuring integrity & confidentiality

Things we'll cover

- **Intro: threats, risks, security needs**
- **Access control**
  - Core OS mechanisms for access control
  - Mandatory vs. discretionary access control
- **Code injection**
  - Buffer overflow, shell scripts, input validation
- **Client-side risks & protection**
  - Viruses, worms, trojans
  - Human factors
- **App confinement**
  - Jails, virtual machines, sandboxes
- **Cryptography**
  - Encryption
- **Integrity & key distribution**
  - Public keys, hashing, digital signatures
- **Authentication**
  - Passwords, tokens, biometrics
- **Cryptocurrency**
  - Bitcoin, proof of work, proof of stake
- **Network security**
  - Switches, routers, services
- **Network protection**
  - Firewalls, VPNs, Zero Trust
- **Web security**
- **Mobile security**
- **Anonymous communication**
  - Tor
- **Content protection**
  - Steganography, watermarking, DRM
- **IoT**
  - Security risks in embedded software
- **Forensics**

What this course is NOT

- **How to write viruses/trojans/malware**
- **How to break into systems**
- **How to be a hacker**
- **Rigorous mathematics on systems, security, or cryptography**

The End