CS 6431

Security and Privacy Technologies

Vitaly Shmatikov

http://www.cs.utexas.edu/~shmat/courses/cs6431/

Course Logistics

- Lectures: Wednesday, 7:30-9:25pm
- Alternating between New York and Ithaca
- Instructor: Vitaly Shmatikov
  - Email: shmatikov@cornell.edu
  - Office hours by appointment
- No textbook; we will read a fair number of research papers
- Watch the course website for lecture notes, assignments, and reference materials

Grading

- Homeworks: 40% (4 homeworks, 10% each)
  - Homework problems will be based on research papers
- Project: 60%
  - Computer security is a contact sport – the best way to understand it is to get your hands dirty
  - Projects can be done individually or in small teams
  - Project proposal due October 1
  - You can find a list of potential project ideas on the course website, but don't hesitate to propose your own

Prerequisites

- PhD students only
  - Except by permission of instructor (rarely granted)
- Basic understanding of operating systems and memory management
  - At the level of an undergraduate OS course
- Some familiarity with cryptography
  - Cryptographic hash functions, public-key and symmetric cryptosystems
- Ask if you are not sure whether you are qualified to take this course

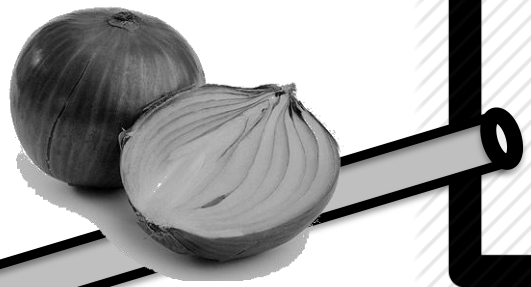
What This Course is Not About

- Not a comprehensive or "fundamentals" course on computer security
- Not a course on cryptography
  - We will cover some crypto when talking about secure network protocols and privacy
- Not a seminar course
  - We will read and understand state-of-the-art research papers, but you'll also have to do some actual work ☺
- Focus on several specific research areas
- You have a lot of leeway in picking your project

Syllabus

❹ Anonymity networks

❷ Application security: Web, mobile, hybrid



❸ Network security: SSL, DNS, BGP; network telescopes

❺ Data privacy, anonymity, online tracking

❻ Side channels

❶ Memory and code security

Start Thinking About a Project

- A few ideas are on the course website
- Many ways to go about it
  - Build a tool that improves software security
    - Analysis, verification, attack detection, attack containment
  - Apply an existing tool to a real-world system
  - Demonstrate feasibility of some attack
  - Do a substantial theoretical study
  - Invent something of your own
- Start forming teams and thinking about potential topics early on!

A Few Project Ideas

- Privacy-preserving augmented reality, computer vision, image recognition
- Program analysis for finding security bugs in multi-protocol network stacks
- Side channels in cloud infrastructure
- Security and privacy of genetic data
- Censorship resistance and steganography
- Security and privacy of consumer devices
- Security of mobile APIs
- Choose something that interests you!