I433 System & Protocol Security and Information Assurance

Yan Huang

Credit: Vitaly Shmatikov, UT Austin

Course Personnel

- Instructor: Yan Huang
  - Office: Lindley 330C
  - Open door policy – don't hesitate to stop by!
- AI: Shruti Shivaramakrishnan
  - Office hours: Friday after class or by appointment
- Watch the course website
  - Assignments, reading materials, lecture notes

Prerequisites

Computer Programming (C and JavaScript)

Introduction to Computer Security

Cryptography

Compilers and/or Operating Systems

Computer Networks

Course Logistics

- Lectures
  - Monday, Wednesday 12:20-1:10 BH317
  - Attend lectures! Lectures will cover some material that is not in the textbook – and you will be tested on it!
- Quiz (20% of the grade)
- Labs (40% of the grade)
  - Friday 10:10-11:00, 11:15-12:05 Info East 009
  - Security is a contact sport!
- Midterm (15% of the grade)
- Final (25% of the grade)
- IU Student Honor Code will be strictly followed

No make-up or substitute exams!
If you are not sure you will be able to take the exams in class, do not take this course!

Late Submission Policy

- Each lab assignment is due before class on the due date
- You have 3 late days to use any way you want
  - You can submit one assignment 3 days late, 3 assignments 1 day late, etc.
  - After you use up your days, you get 0 points for each late assignment
  - Partial days are rounded up to the next full day

Course Materials

- Textbook:

  Kaufman, Perlman, Speciner. "Network Security"
  - Lectures will not follow the textbook
  - Lectures will focus on "big-picture" principles and ideas of network attack and defense
  - Attend lectures! Lectures will cover some material that is not in the textbook – and you will be tested on it!
- Katz, Lindell "Introduction to Modern Cryptography"
  - Recommended
- Occasional assigned readings

Other Helpful Resources

- Ross Anderson's "Security Engineering"
  - Focuses on design principles for secure systems
  - Wide range of entertaining examples: banking, nuclear command and control, burglar alarms
- "The Shellcoder's Handbook"
  - Practical how-to manual for hacking attacks
- Kevin Mitnick's "The Art of Intrusion"
  - Real-world hacking stories
  - Good illustration for many concepts in this course
- Conference Proceedings (freely accessible)
  - ACM CCS, IEEE S&P, NDSS, USENIX Security

Main Topics of the Course

- Cryptography
  - Definitions & Applications
- Software Security
  - Memory attacks
- Web Security

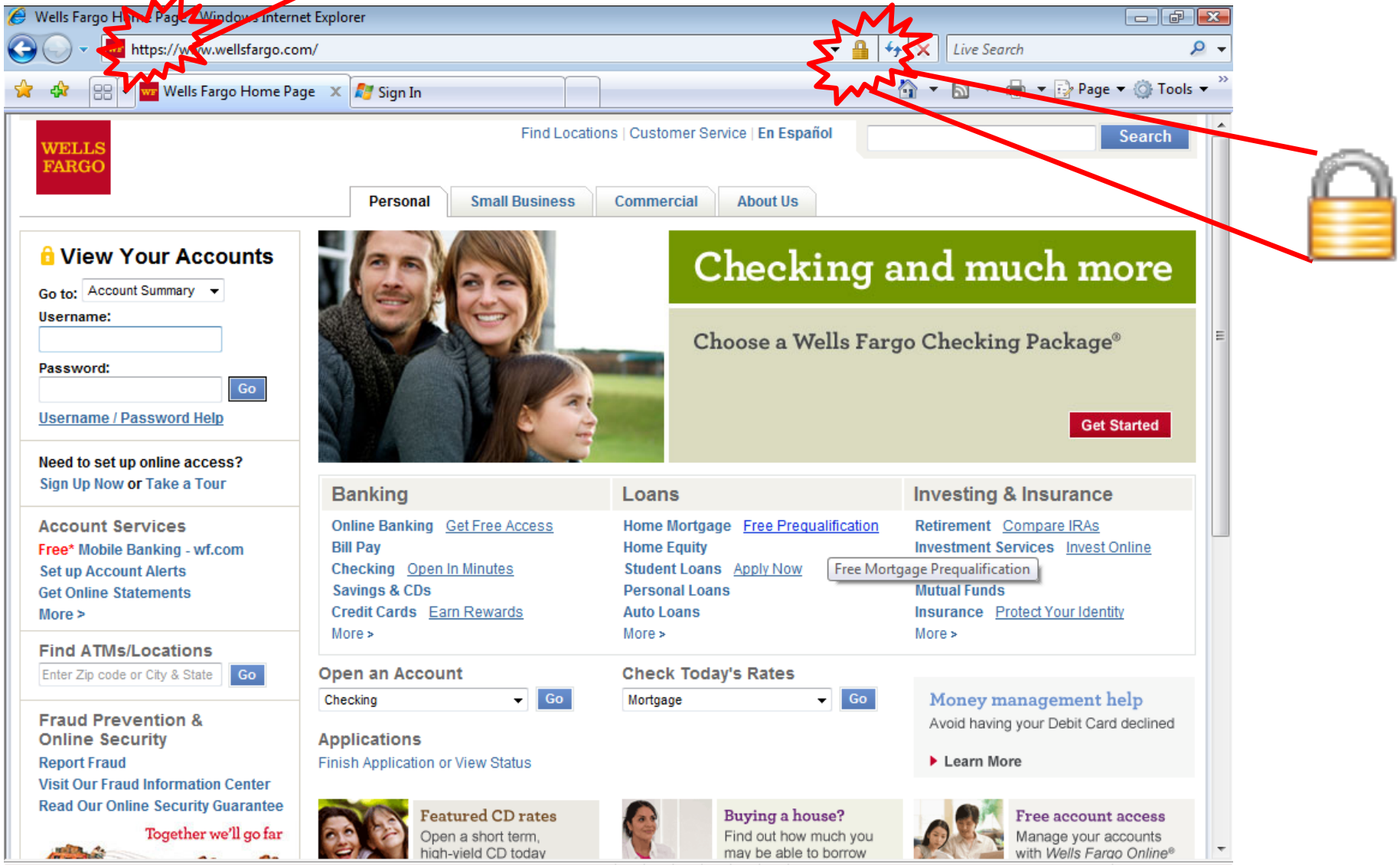
- Network Security

What This Course is Not About

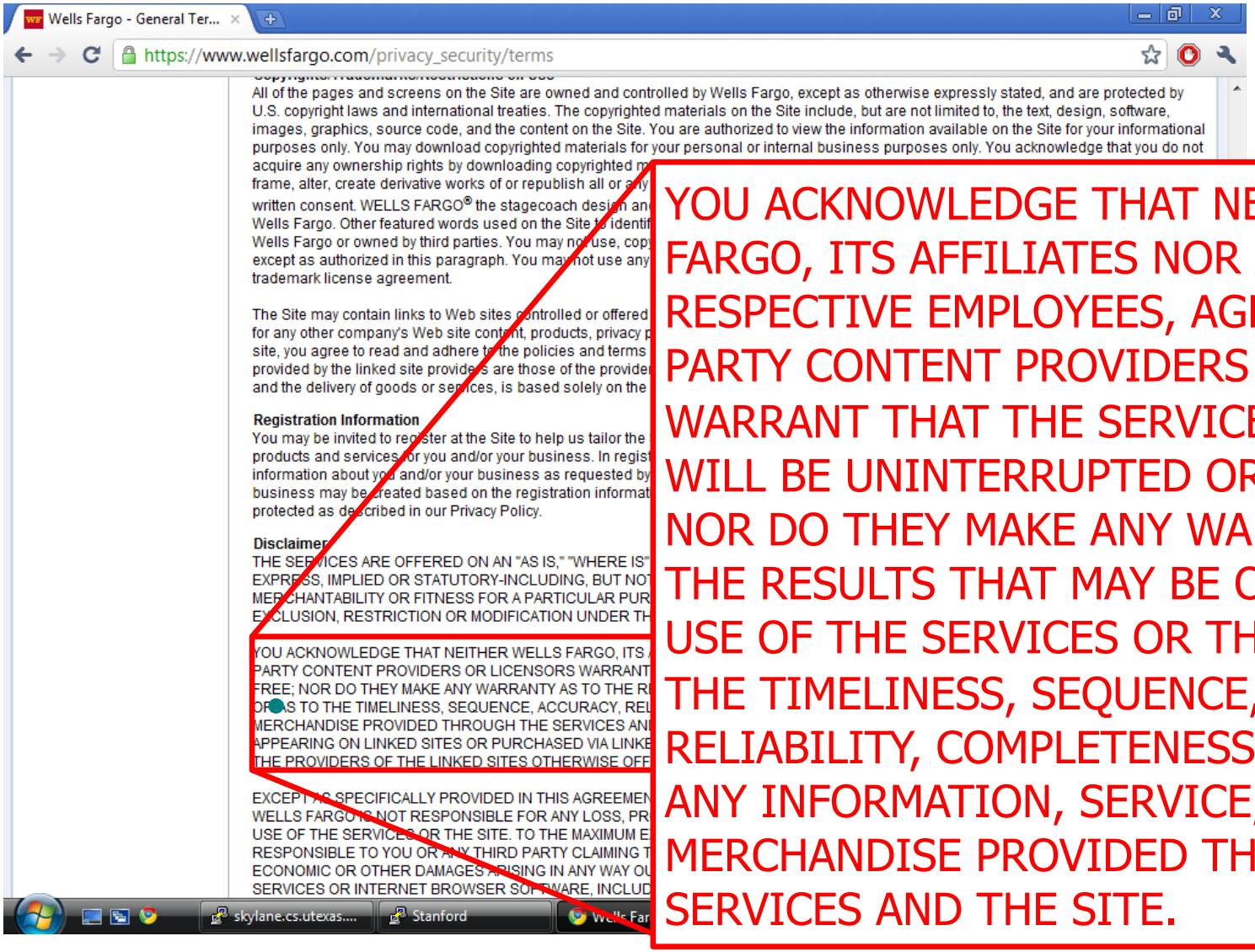
- Not a comprehensive course on computer security
- Not a course on ethical, legal, or economic issues
  - No file sharing, DMCA, piracy, free speech issues
  - No surveillance
- Only a basic overview of cryptography
  - Take I538 for deeper understanding
- Only some issues in systems security
  - Very little about OS security, secure hardware, physical security, security of embedded devices…

Motivation

https://



Excerpt From "General Terms of Use"



"Privacy, Security and Legal"

"As a Wells Fargo customer, your privacy and security always come first."

- Privacy policies
  - Privacy policy for individuals
  - Online privacy policy
  - Social Security Number protection policy
  - International privacy policies
- Your online security
  - How we protect you
  - Online security guarantee
- Fraud information center
  - How fraudsters operate
  - How to protect yourself
- USA PATRIOT ACT information

What Do You Think?

What do you think should be included in "privacy and security" for a banking website?

Desirable Security Properties

- Authenticity
- Confidentiality
- Integrity
- Availability
- Accountability and non-repudiation
- Access control
- Privacy of collected information

…

What Drives the Attackers?

- Put up a fake financial website, collect users' logins and passwords, empty out their accounts
- Insert a hidden program into unsuspecting users' computers, use it to spread spam or for espionage
- Subvert copy protection for music, video, games
- Stage denial of service attacks on websites, extort money
- Wreak havoc, achieve fame and glory in the blackhat community

Marketplace for Vulnerabilities

- Option 1: bug bounty programs
  - Google: up to $3133.7 in 2010, now up to $20K per bug
  - Facebook: up to $20K per bug
  - Microsoft: up to $150K per bug
  - Pwn2Own competition: $10-15K
- Option 2: vulnerability brokers
  - ZDI, iDefense: $2-25K
- Option 3: gray and black markets
  - Up to $100-250K reported (hard to verify)
  - A zero-day against iOS sold for $500K (allegedly)

It's a business!

- Several companies specialize in finding and selling exploits
  - ReVuln, Vupen, Netragard, Exodus Intelligence
  - The average flaw sells for $35-160K
  - $100K+ annual subscription fees
- Nation-state buyers
  - "Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too" -- NY Times (Jul 2013)

Marketplace for Stolen Data

[Dell SecureWorks, 2013]

- Single credit card number: $4-15
- Single card with magnetic track data: $12-30
- "Fullz": $25-40
  - Full name, address, phone, email addresses (with passwords), date of birth, SSN, bank account and routing numbers, online banking credentials, credit cards with magnetic track data and PINs
- Online credentials for a bank account with $70-150K balance: under $300

Prices dropped since 2011, indicating supply glut

Marketplace for Victims

[Trend Micro, “Russian Underground 101”, 2012]

- Pay-per-install on compromised machines
  - US: $100-150 / 1000 downloads, “global mix”: $12-15
  - Can be used to send spam, stage denial of service attacks, perform click fraud, host scam websites
- Botnets for rent
  - DDoS: $10/hour or $150/week
  - Spam: from $10/1,000,000 emails
- Tools and services
  - Basic Trojans ($3-10), Windows rootkits ($300), email, SMS, ICQ spamming tools ($30-50), botnet setup and support ($200/month, etc.)

Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows are the “vulnerability of the decade”
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.

Better News

- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem"
  - Many security holes are based on misunderstanding
- Security awareness and user "buy-in" help
- Other important factors: usability and economics

Reading Assignment

- Read Kaufman 2.1-4 and 4.2