CSE 5473: Network Security

Prof. Yinqian Zhang

Class Meetings: MWF 1:50 – 2:45pm

Location: Bolz Hall 316

Course homepage: http://www.cse.ohio-state.edu/~zhang.834/courses/cse5473/index.html

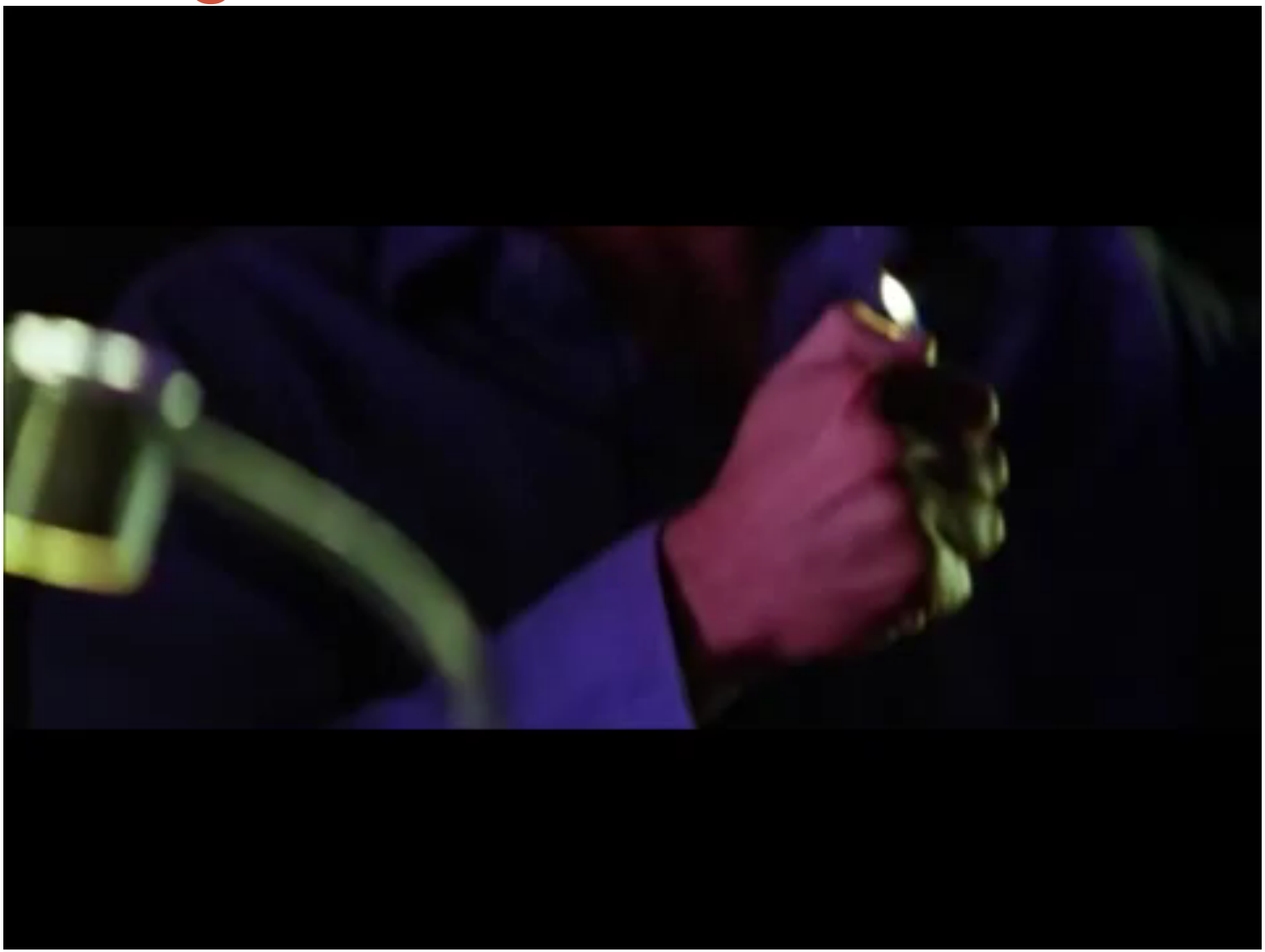
Introduction of the Instructor

- Yinqian Zhang, Ph.D.
  - Assistant Professor, CSE & ECE
  - A security researcher
- Research Area: Computer security & privacy
  - Cloud computing security
  - Virtualization/OS security
  - Network security
  - And a lot others….
- Introduce yourself..

Why do you choose Network Security

- A. This is a required class. I have to take it to graduate.
- B. Only course available. I have no other choices.
- C. I think hacking is cool. I want to learn to be a hacker.
- D. I want to understand concepts and techniques of network security attacks and countermeasures. I want to get familiar with some fundamentals of cryptography, network security designs using available secure solutions, and state-or-the-art security issues and technologies. I want to get some exposure to research in network security.
- E. The professor is awesome and I like to spend hours in his class.

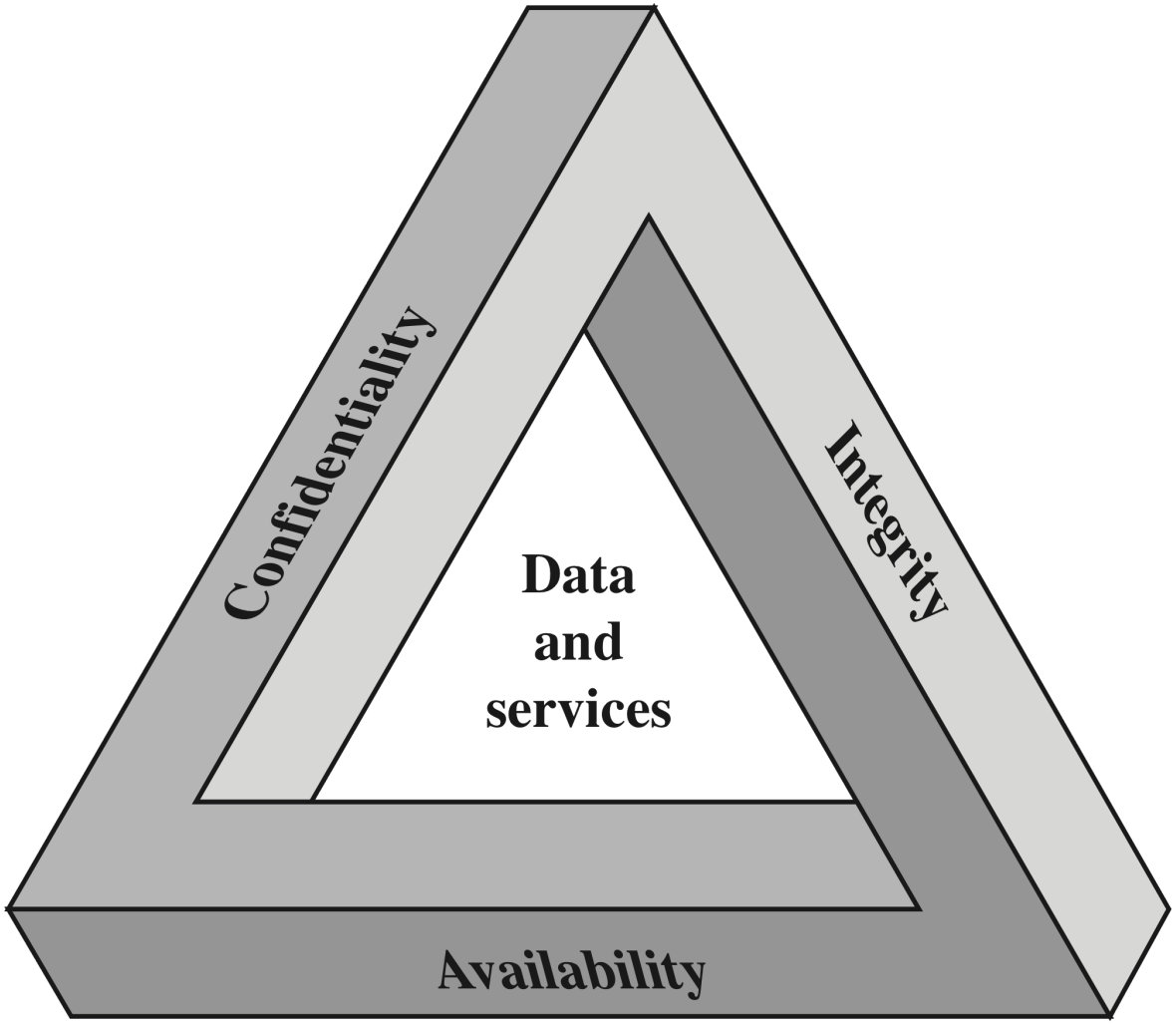
Hacking Like a Pro?



Computer security

- The NIST *Computer Security Handbook* defines the term computer security as:
  - “the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources” (includes hardware, software, firmware, information/ data, and telecommunications)

What is security



Security objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Model for network security

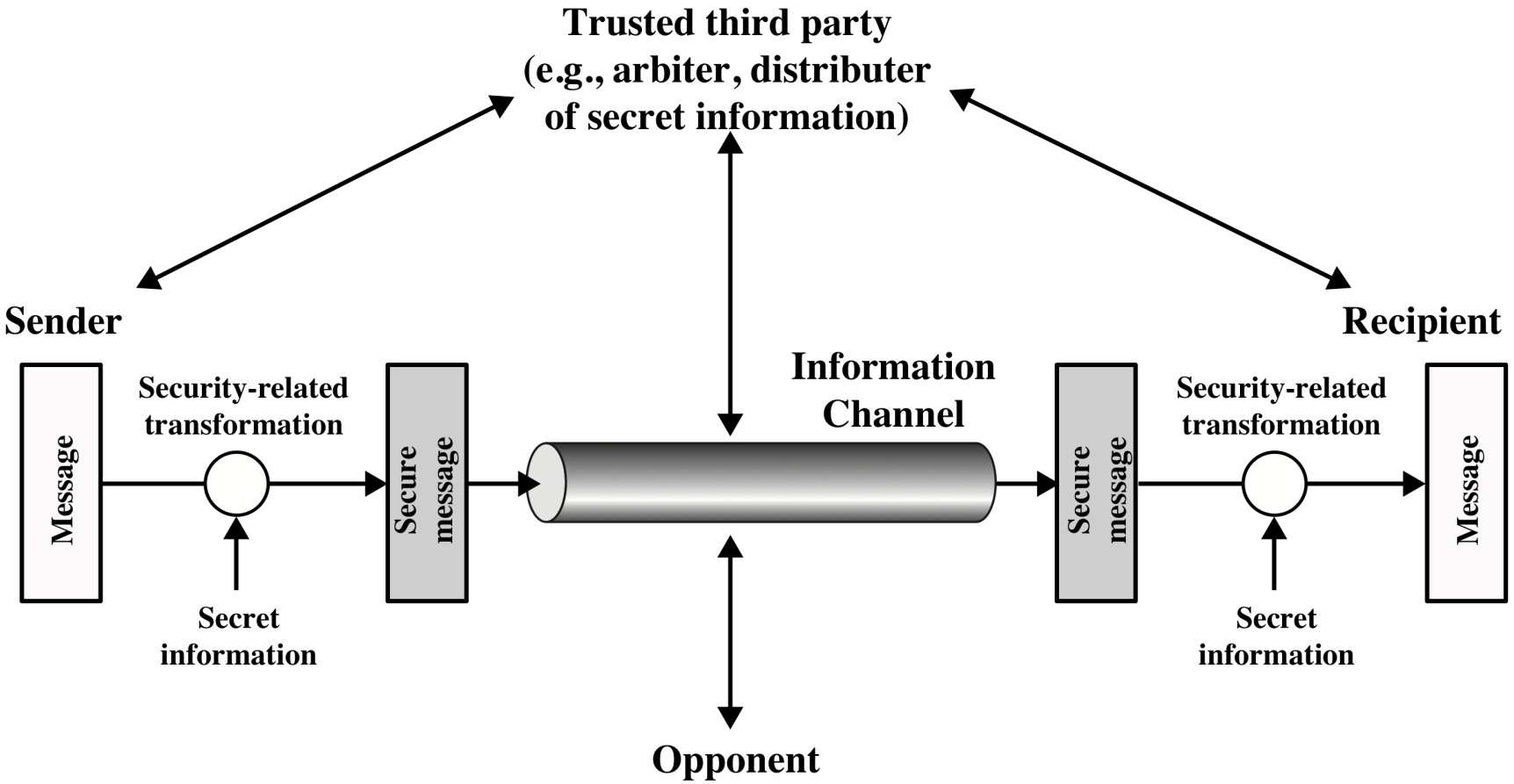
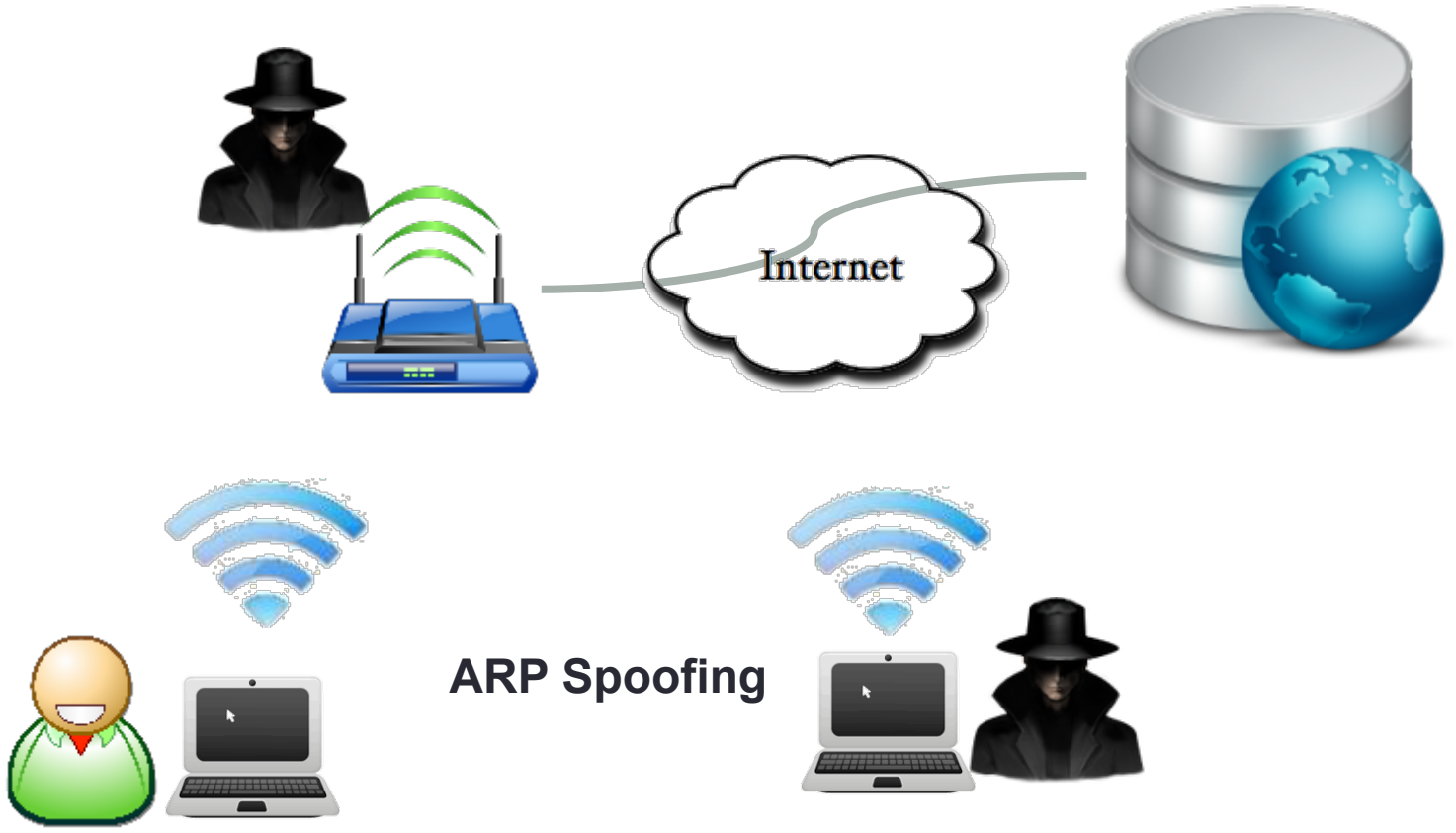


Figure 1.2 Model for Network Security

Threats and attacks

- Threats
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is possible danger that might exploit a vulnerability
- Attacks
  - An assault on system security that derives from an intelligent threat; that is, an intelligent act that is deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Why do we need network security



Topics of the course

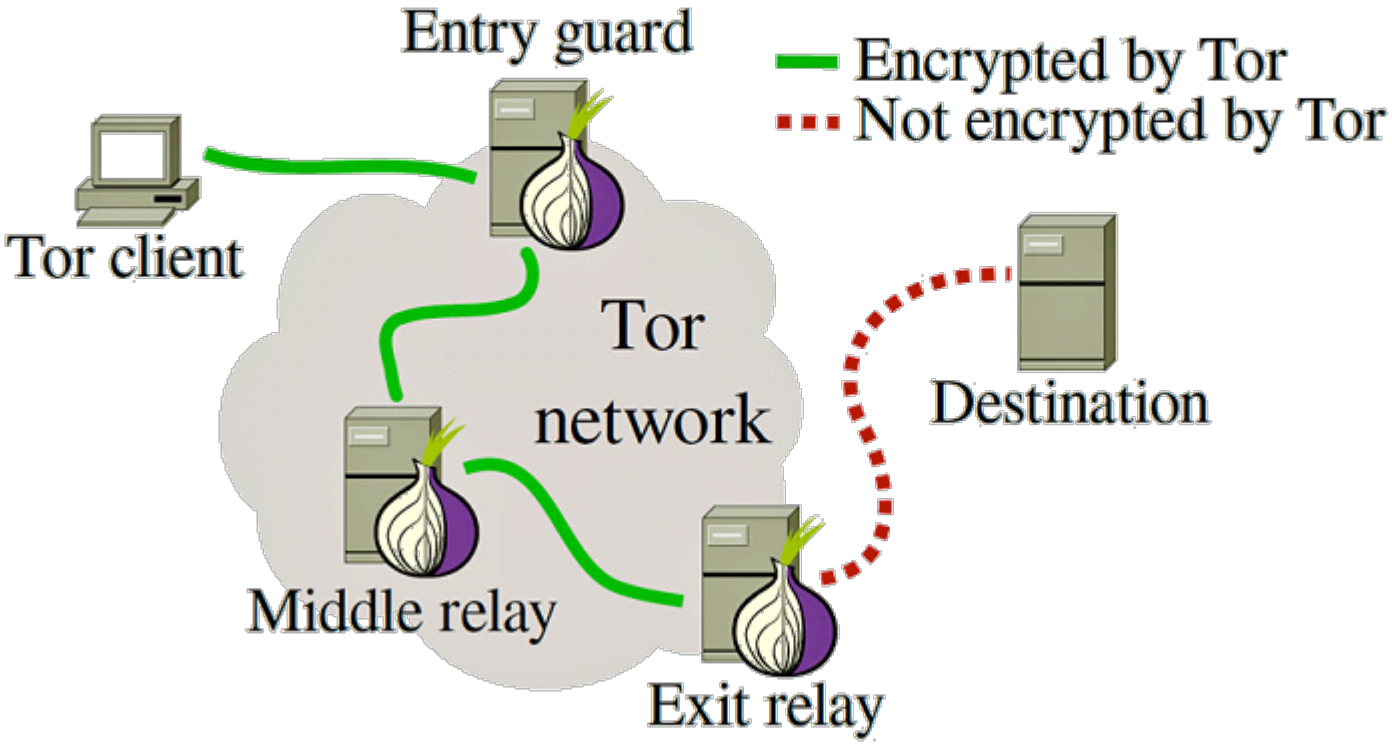
- Cryptography
  - Symmetric ciphers (DES, AES)
  - Asymmetric ciphers (RSA, DH)
- Security protocols
  - Key distribution and management
  - Data integrity and message authentication codes
  - Non-repudiation and digital signatures
- Network and Internet security
  - Transport-level security: SSL and TLS
  - Wireless network security
  - Email security: Pretty Good Privacy (PGP)
  - IP security: IPSec and VPN
- Special topics

Special topic: anonymous communications

- Network communications among parties concealing parties' identity and existence of communications
  - IP address
  - Web user tracking (cookie, browser/OS fingerprinting, etc)
  - Websites you visit
- Who's your enemy?
  - Local network administrators
  - Internet Service Providers
  - Government agency (e.g, NSA)

Anonymous communication (Con't)

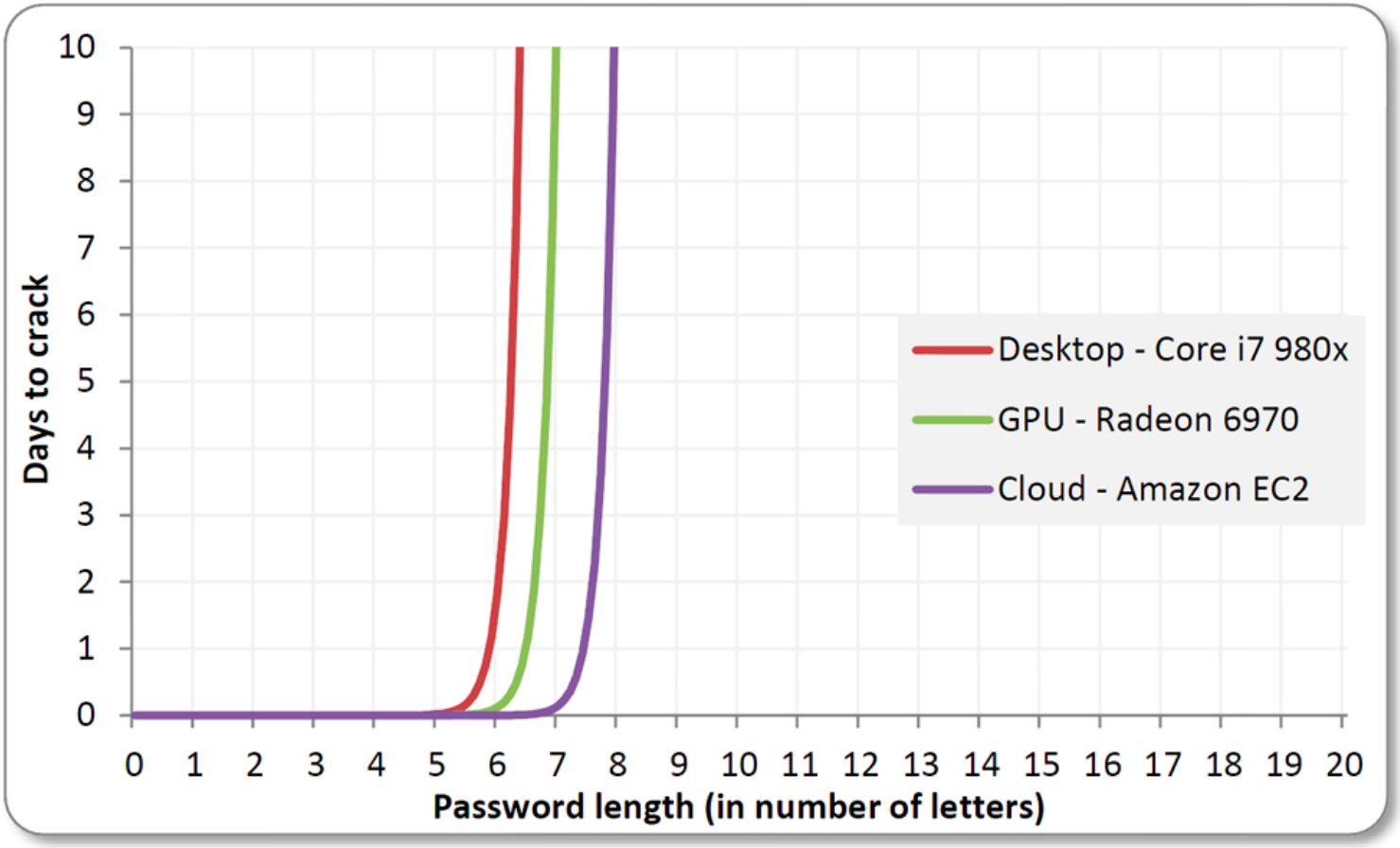
- Tor (The Onion Router)
  - A free software for anonymous communication



Special topic: password security

"I don't know how my site keeps getting hacked. Everybody I give my password to says it's very secure."

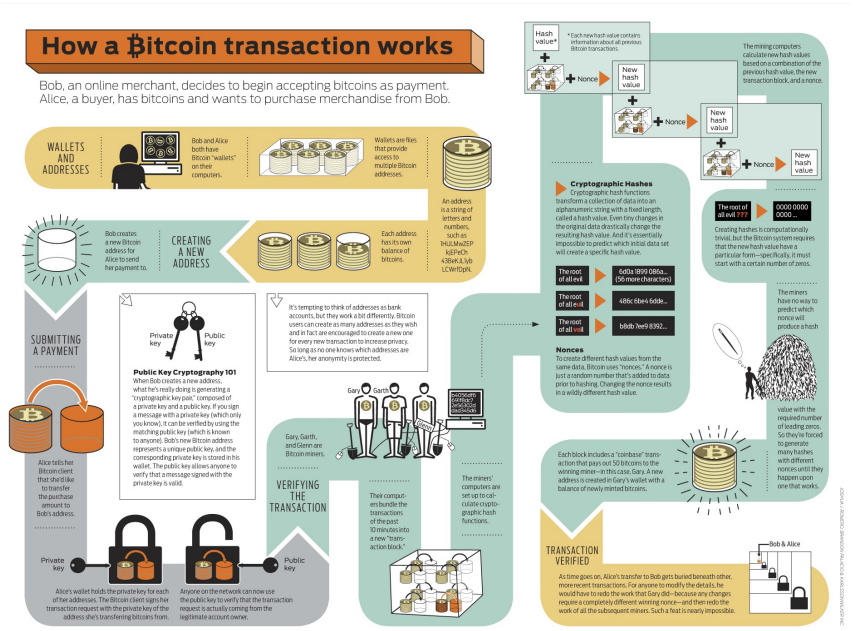
Password security (Con't)



http://blog.erratasec.com/2012/08/common-misconceptions-of-password.html

Special topic: bitcoins

- Decentralized digital currencies:
  - No central point of control over the money supply
- Bitcoin: An open-source peer-to-peer payment network
  - Using **digital signatures** & **encryption**
    - decentralization is the basis for Bitcoin's security and freedom
- How bitcoin works



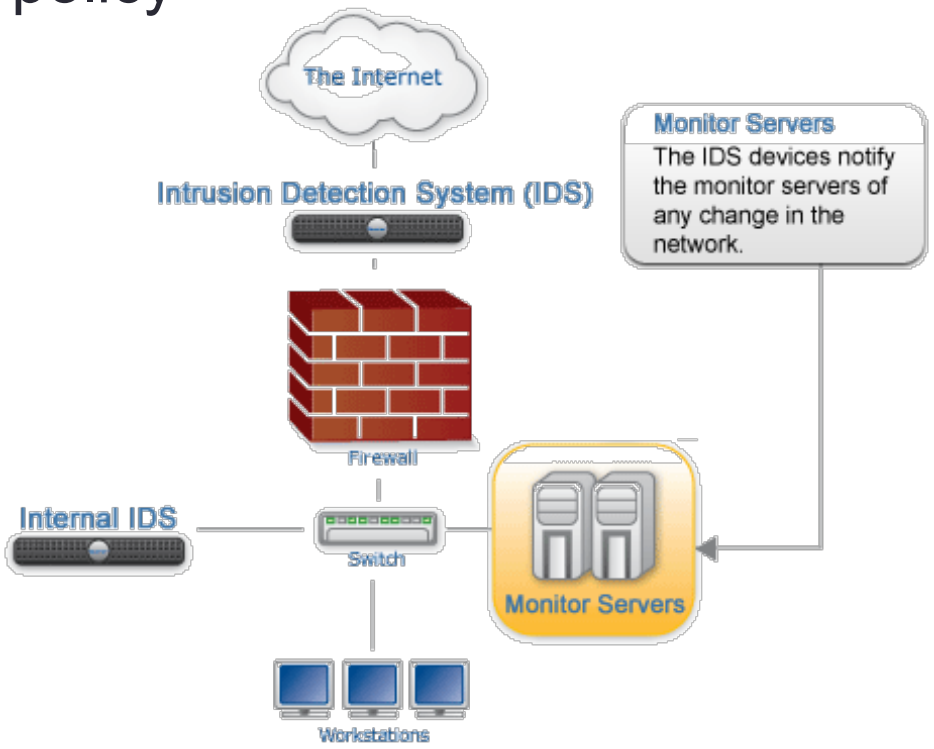
Special topic: remote exploitation

- Network (port) scanning
  - Probe a server or host for open ports
  - OS or service fingerprinting

- Vulnerability exploitation
  - Sending maliciously-crafted network packet to remote open ports
  - Buffer overflow and control flow hijacking
  - Remote backdoor for attacker to login

Special topic: intrusion detection

- A device or software application that monitors network activities for malicious activities or policy violations.
- Types of IDS
  - Host-based
  - Network-based
- Detection techniques
  - Anomaly detection
  - Misuse detection



Special topics: network attacks

- Sniffing
  - IP sniffing
  - TCP session sniffing
  - HTTP password sniffing
- Network spoofing
  - IP Address spoofing
  - ARP spoofing
  - DNS spoofing
  - Email spoofing
  - Search engine poisoning
- DOS attacks
  - SYN flood attack
  - ICMP flood attack
  - Ping of Death (PoD)
  - Smurf Attack
- Web security
  - SQL injection
  - Session Hijacking
  - Cross-side scripting (XSS)
  - Man-in-the-middle Attack

What we will NOT cover

- Mathematics underlying cryptographic
- System security
  - Secure operating system designs
  - Access control mechanisms
  - Memory integrity attacks and defenses (e.g., ROP/JOP, ALSR, CFI)
- Malware: virus, rootkit, adware
- Computer forensics
- Security management and practice in large enterprises
- Security product configuration and installation
- Others

Security courses at OSU

- CSE 4471: Information Security
  - A big picture perspective: introduction to digital information threats and attacks, attack detection and responses; cryptography
- CSE 5351: Introduction to Cryptography
  - Foundations of cryptography; mathematical formulations/proofs of security goals; zero-knowledge proof systems; cryptographic protocols.
- CSE 5472: Information Security Projects
  - Team-based projects: solve information security problems
- **CSE 5473: Network Security**
  - **Applied cryptography, security protocols, network attacks and defenses**
- CSE 5479: Topics on Computer Security
  - Computer security (research seminar)

Prerequisite

- Knowledge of network protocols
  - IP, ARP, TCP, UDP, DNS, HTTP, etc.
- Programming skills
  - C/C++, Java, or scripting languages (e.g., Python)
  - Talk to me if you know nothing about programming
- A personal computer
  - Run lab experiments in virtual machines (e.g., VirtualBox)
  - Don’t mess up your own computer!
  - What if I cannot bring a laptop to class?
    - Find a teammate and always sit together!
    - Talk to me if you cannot do either.

Course materials

- Syllabus, schedule, and announcements
  - http://www.cse.ohio-state.edu/~zhang.834/courses/cse5473/
- Slides and assignments
  - Download from Piazza
  - https://piazza.com/class/jc6bq11gaw71kp
- Textbook
  - William Stallings, Cryptography and Network Security: Principles & Practice:
    - 6th Ed., Pearson, 2013, ISBN:0133354695
    - 5th Ed., Prent. Hall, 2010, ISBN:0136097049
    - 4th Ed., Prent. Hall, 2002, ISBN:0131873164

Communication

- Upload reports and code
  - CARMEN (https://carmen.osu.edu/)
- Ask questions online
  - Piazza
- Need help with Labs
  - Grader office hour
- Need help with assignments or exams
  - Instructor office hour

Grading

- Percentage distribution
  - Assignments: 50%
  - Course project: 25%
  - Mid-term exam: 20%
  - Attendance: 5%
- Grading is relative
  - You might get an A at 75% (if most of the other students are less than 75%)
  - Your final grade will only get better than the points you earned

Letter	Percentage
A	93-100
A-	90-92.9
B+	87-89.9
B	83-86.9
B-	80-82.9
C+	77-79.9
C	73-76.9
C-	70-72.9
D+	67-69.9
D	60-66.9
E	0-59

Homework assignments

- 4 homework assignments
  - Solve puzzles and answer questions
  - Prepare your answers to the questions using **Word** or other text editing tools and submit **pdf** files!
  - No programming needed
  - Goal: help you prepare the mid-term exam.
- 20% of your final grades
  - Single-person job, you are on your own

Lab exercises

- 6 lab exercises
  - Performing network attacks
  - Security analysis of software programs
  - Experiments with network defense tools
  - **Programming tasks**
- 30% of your final grades
  - 1~2 students per team
  - If you are not familiar with VirtualBox, find someone who does!
  - If you are a terrible programmer, find someone who is not!
  - Clearly document individual contributions, team members may have (slightly) different points for the same lab report

Extra Credits

- Philosophy: Everyone should be able to finish the assignments within reasonable amount of time
- Questions that require extra thinking, research and time deserve extra credits
- Each assignment *may* include questions for extra credits that is worth of up to 20% of the assignment
  - That is, you have a chance to earn 50% * 120% + 50% = 110%
  - Still >93% for A
  - Grades are relative to your classmates and will only get higher …

Exams

- **One mid-term exam** (20%)
  - 1 hour, during one of the class meetings
  - Closed book
  - No teamwork allowed
  - Time: March 30th, Friday. 1:50pm ~ 2:45pm (tentative)
- No final exam

Course projects

- A coding project that aim to be open-sourced
  - A few topics to be selected from
- Team up with fellow students (up to 4 students per team)
  - Clearly document individual contribution, so each team member will receive (slightly) different points
- 25% of your final grades
  - Monthly project progress presentation
    - One slides presentation to describe your progress
  - Code and manual
    - A working tool with clearly documented manual
  - Project demo

Attendance

- You are expected to attend every class meeting
- Attendance record will be *sampled*
- 5% of your final grades
- In reality, if 10 attendance checks in total, you will get the 5% if your name appears on 8 of them
  - Sampling errors will be considered!
  - You don’t need to inform me if you are only absent for just once!

A summary

- This is a course that requires you to
  - Spend hours to conduct lab experiments
  - Write programs for homework or course project
  - Learn and *memorize* concepts and techniques of network security and cryptography
  - Attend almost every class meeting
- If you have no prior experience in basic Linux administration and/or programming, and you don't want to learn
  - Please drop the class early
- Waitlisted students: come to me after class

Questions

- Office Hours (DL798): MF 3:00 – 4:00pm, or by appointment
- Next class meeting: Wednesday, Jan 10th, 1:50pm
- Email me: yinqian@cse.ohio-state.edu
- Email subject: [cse5473] your subject here
  - But try not to email me unless absolutely necessary.

- Email our grader: Hansey Chen (chen.4800@osu.edu)
  - Office hour: W 3:00 – 4:00pm

Today's homework

- Bring a laptop to class on Wed, or team up with someone who can.
- Finish Lab 0 (Step 1-4) before next class meeting on Wed.
- Piazza -> resources -> Resources -> Labs -> Lab_0.pdf