

CE 441/Computer and Network Security

30 Shahrivar, 1398

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology





What is Security?

- Confidentiality (محرمانگی)
 - Not the same as privacy (حریم خصوصی)
- Integrity (صحت)
- Availability (دسترس پذیری)
 - Turning off a computer provides confidentiality and integrity, but hurts availability. . .



More Definitions

- **vulnerability** (آسیب پذیری): An error or weakness in the design, implementation, or operation of a system
- **threat** (تهدید): An adversary that is motivated and capable of exploiting a vulnerability
- **attack** (حمله): A means of exploiting some vulnerability in a system

(Definitions from Trust in Cyberspace)



Threats (تهدیدات)

- script kiddies
- Hacking for profit
 - The primary motivation for most current attacks is money (i.e. spammers)
- Industrial espionage
 - Professionals are more likely to use non-technical means, too: social engineering, bribery (رشوہ), wiretaps, etc.
 - Professionals tend to know what they want



Threats (تهدیدات)

- Inside jobs
 - insiders know what you have and your weak points
 - Insiders are on the inside of your firewall
- Government backed attackers
 - Governments may want your technology (Boeing vs. Airbus)
 - Well-funded attackers
 - Is cyber-warfare a threat?



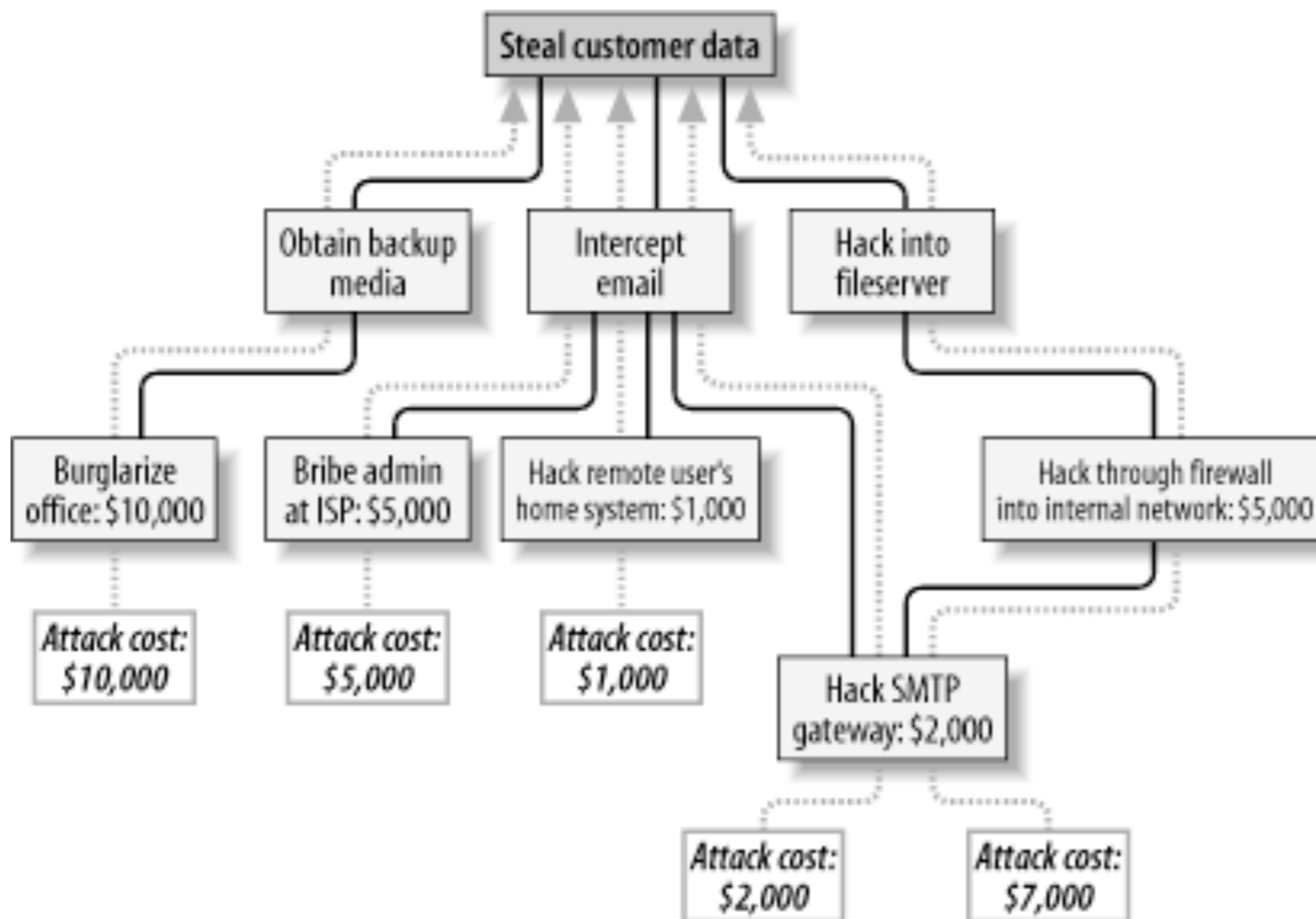
Why Do Threats Matter?

- You can't design a security system unless you know who the enemy is
- Security is fundamentally a matter of economics
 - Cost vs. Reward
- Defender:
 - How much security can you afford?
 - How much do you need?
- Attacker:
 - How much can you spend?
 - How much do you gain?

- ATM with 50,000 IR or 500,000 IR



Attack Tree

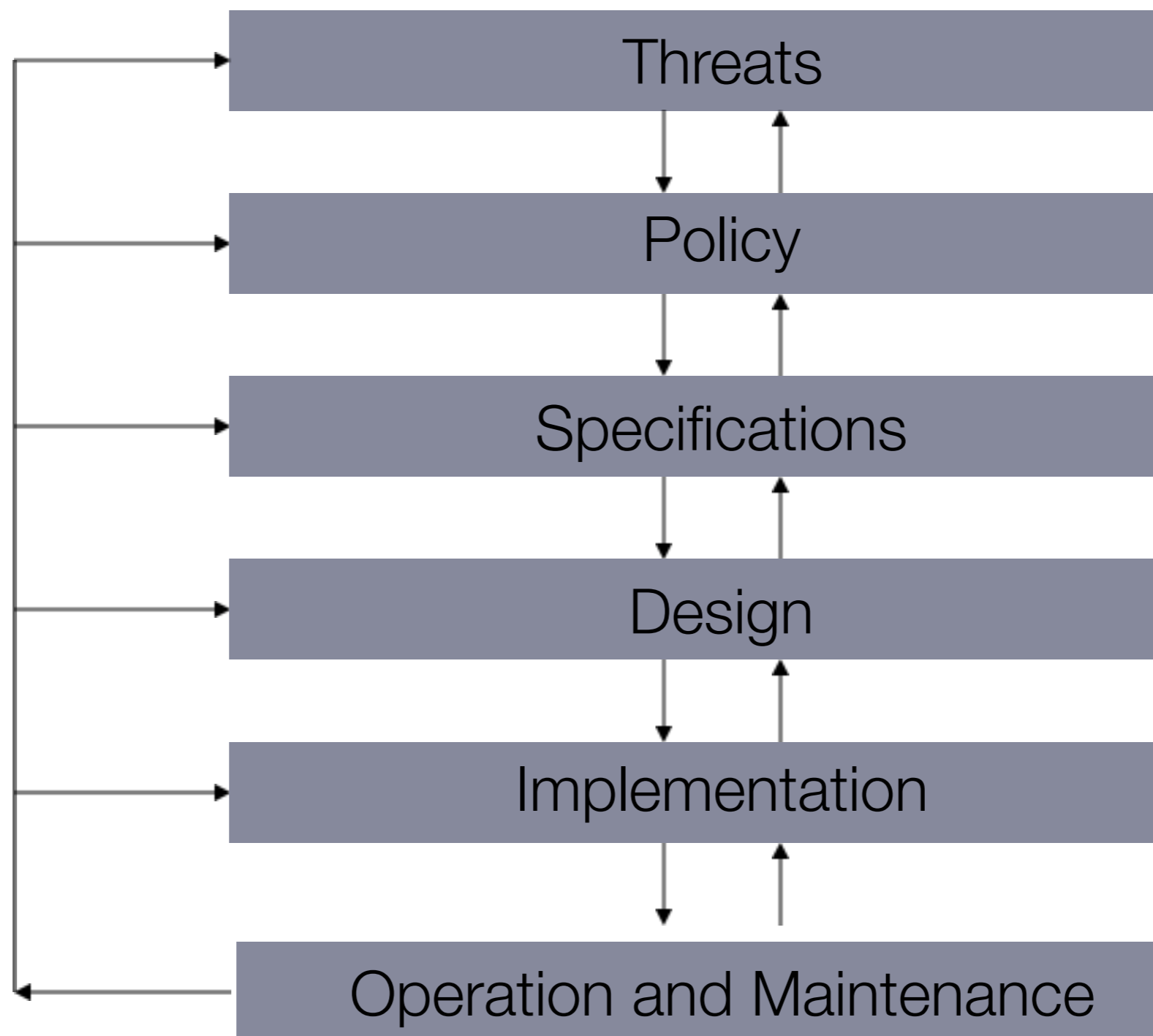


Be Realistic About Modeling Threats...



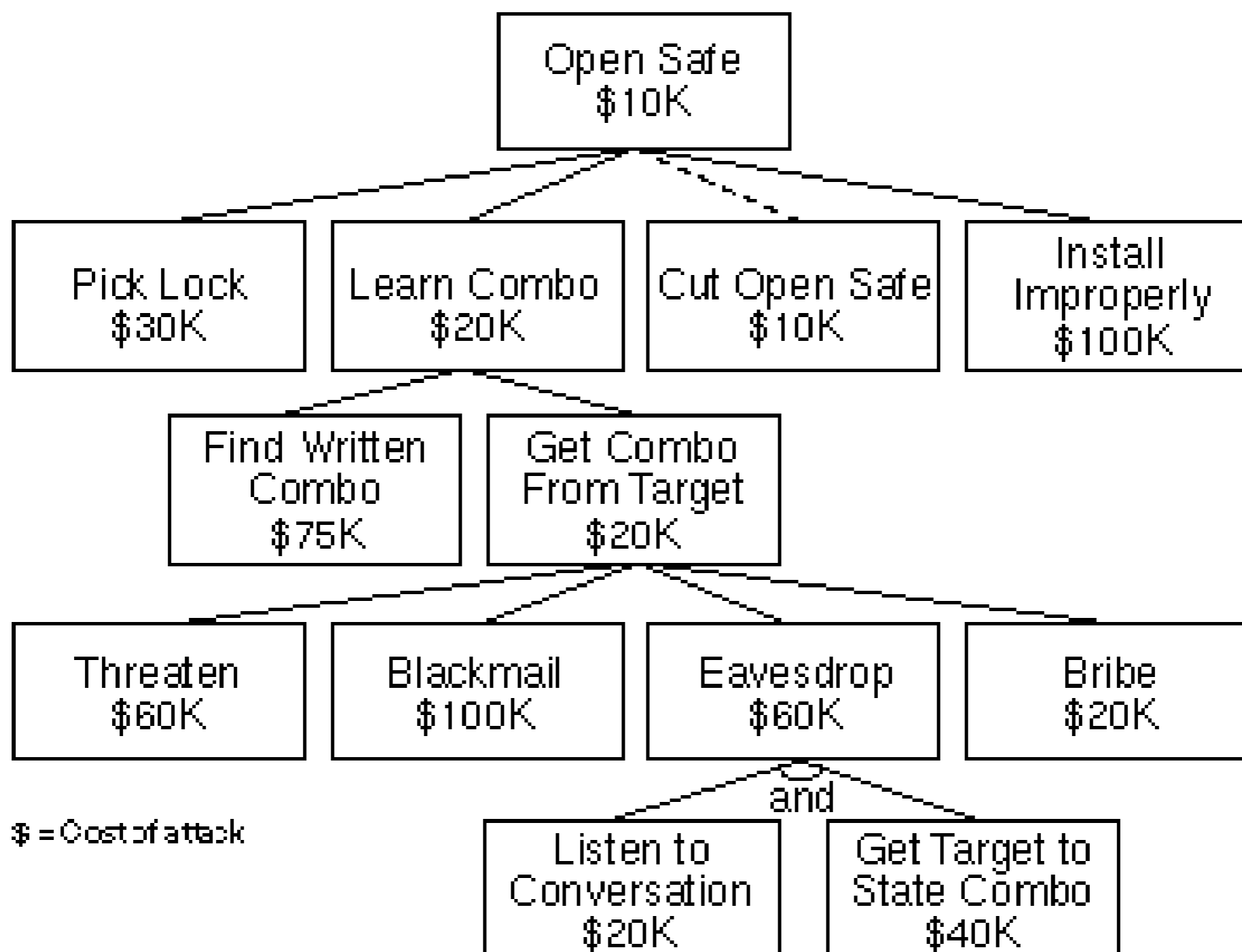


Security Life Cycle





Attack Tree





Attacks



Eavesdropping (شنود)

- Attack on confidentiality
- Cryptography is a defense
- What about traffic analysis?
 - Pentagon Pizza deliveries
 - Language identification in encrypted VoIP traffic
- Some times you want to avoid encryption
 - Steganography
 - Prisoner problem
 - Covert channels
 - CPU usage



Creative attacks!

- Can I find out what links you have visited?
 - Use javascript to get the color of the links on the page
 - Can find out if you have visited a specific link (This was fixed)!
 - Set the background color to that of the visited link color, and employ Captchas



4 + 5 = 9; 4 + F = A; 5 + F = 6; 4 + 5 + F = 8

FA4A SA8A A-65 A9-5



Phishing

- Attack on integrity
- Which site is authentic?

<http://www.tejaratbank.ir/en/>

<http://www.tegaratbank.ir/en/>

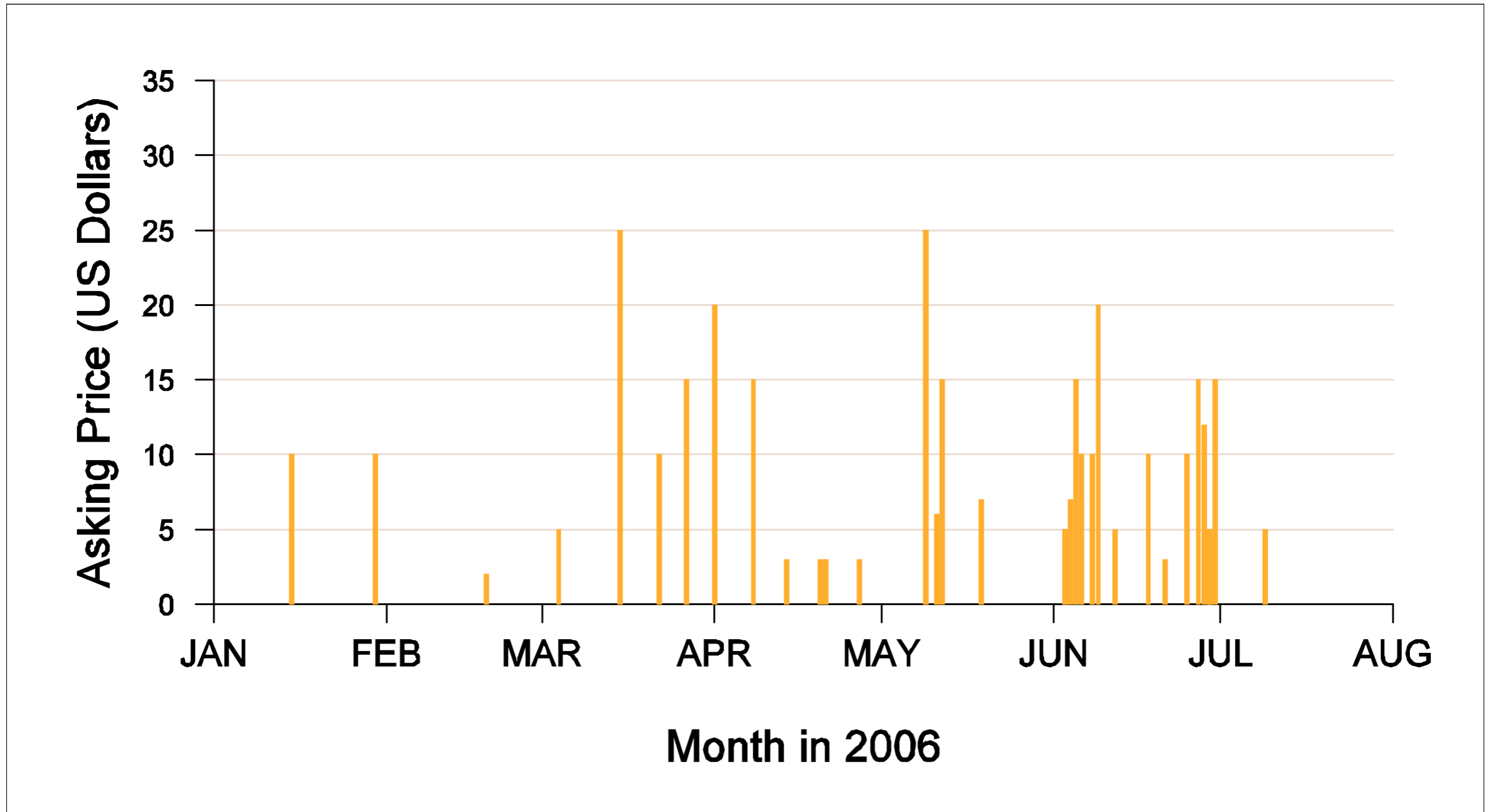




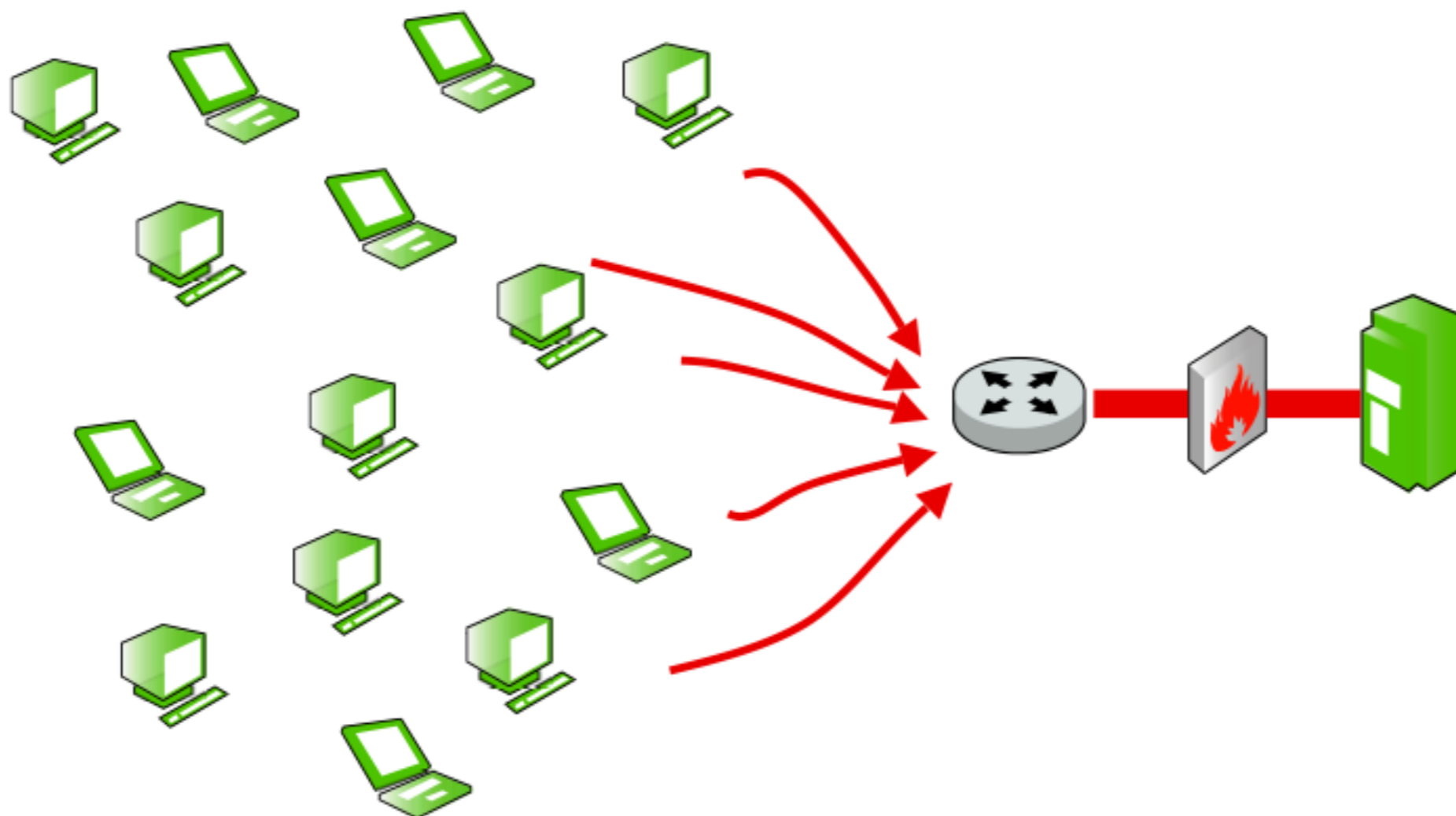
(DDoS) Distributed Denial of Service

- Attack on availability
- Overload the victim with traffic
- Most current attacks use “bots”
 - “bots” are machines under control of the attacker
 - major usage: spamming, DDoS
 - How?
 - Use “come and get it” with infected “free” software
 - Use exploits to penetrate machines, possibly via worms
 - Buy or rent them
 - Steal them!

Asking Prices for Compromised Hosts



DDoS Example





DDoS (con't)

- Largest DDoS recorded —> 1tbps
 - using insecure IoT devices

Details on the Course



Administrivia

- Website:
 - sharif.edu/~kharrazi/courses/40441-981/ (will be up soon)
 - You are expected to check the website regularly
- Prerequisites: 40-443 Computer Networks and 40-424 Operating Systems



Administrivia

- TAs
 - Kavian AmirMozaffari
 - Farid Zandi
- Grading (tentative)
 - 10% quiz
 - 40% homework
 - 20% midterm
 - 30% final



Policies

- Late Homework
 - One day late will cost you 25%, two days 50%, and three days 75%.
 - No homework will be accepted after the third day.
- Cell phones
 - Please turn them off before entering class.
- Cheating and Copying
 - First time you are caught you will get a zero for the task at hand.
 - Second time you are caught you will fail the course.
 - Providing your assignment to someone else is considered cheating on your behalf.



Acknowledgments/References

- Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.
- [Nazario08] Jose Nazario, Arbor Network, USENIX Security, 2008.
- [Cappos06] CS3923 / 6813: Computer Security, New York University, Fall 2016.
- [Bellovin06] COMS W4180 — Network Security Class Columbia University, Steven Bellovin, 2006.
- [Schneier] Attack Trees, Bruce Schneier, Dr. Dobb's journal.
-