Computer and Network Security: Motivation

Kameswari Chebrolu

Outline

- What is Computer and network security?
- Why is security important?
- Why is security hard?
- What does all this mean to me?

Outline

- What is Computer and network security?
- Why is security important?
- Why is security hard?
- What does all this mean to me?

What is Computer Security?

*“**Computer Security** is the process of preventing and detecting unauthorized use of your computer. It involves the process of safeguarding against intruders from using your computer resources for malicious intents or for their own gains ”*

(From www.cert.org)

What is Network Security?

“**Network security** consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer **network** and **network**-accessible **resources**. ”

(From wikipedia.org)

Terms from Definition

- Resource
- Un-authorized use
- Intruders/Attackers
- Safeguard/Defense

Resources

- Computer could be replaced by laptops, desktops, cellphones, medical devices, ATMs, cars etc
- Resources(**Digital assets)** have value
  - CPU
  - Disk Space
  - Network Connection
  - Data: Passwords, Contact List, Credit Card #s, Secret Files, Trade/Military secrets
  - Entire System or Network

Unauthorized Use

- Steal Identity/Information
  - Credit card, social security numbers, Intellectual property
- Cause Inconvenience
  - Reboots, pop-ups, corrupt files
- Disruption of service
  - Launch denial-of-service (DOS) attacks; deface website
- Warfare (spying, sabotage)

Terms from Definition

- ~~Resource~~
- ~~Un-authorized use~~
- Intruders/Attackers
- Safeguard/Defense

Intruder/Attacker Profile

- Can be anyone: insider, outsider, vendor, service-provider etc
- Assumed very powerful
  - Has access to large computational power
  - Can intercept and modify messages
  - Can buy people off
  - Knows implementation details

Incentives for Attacks

- Glory/Bragging Rights
- Malice
- Competition
- **Money (e.g. bug bounty)**
- Political/ Private Activism (e.g. stuxnet worm , Anonymous Group,)

Upto $20k per bug

Underground Economy

Service	Price
Hack a normal website	$9.99
Hack a high profile site	$9.99 +
Govt. Database of Names, addresses, Phone etc	$20 per 1KB
Fresh emails for spam	$10 per 1MB
http://xxx.yyy.mil full site admin control	$499
http://www.xxx.edu full site admin control	$88
Zero day against iOS	$500,000
50,000 botnets for rent for two weeks	$4000
DDOS for one week/hour	$150/$10

- Several companies specialize in finding and selling exploits
  - ReVuln, Vupen, Netragard, Exodus Intelligence
  - The average flaw sells for $35 - 160K
- Nation/State buyers
  - Israel, Britain, Russia, India and Brazil are some of the biggest spenders

Terms from Definition

- ~~Resource~~
- ~~Un-authorized use~~
- ~~Intruders/Attackers~~
- Safeguard/Defense

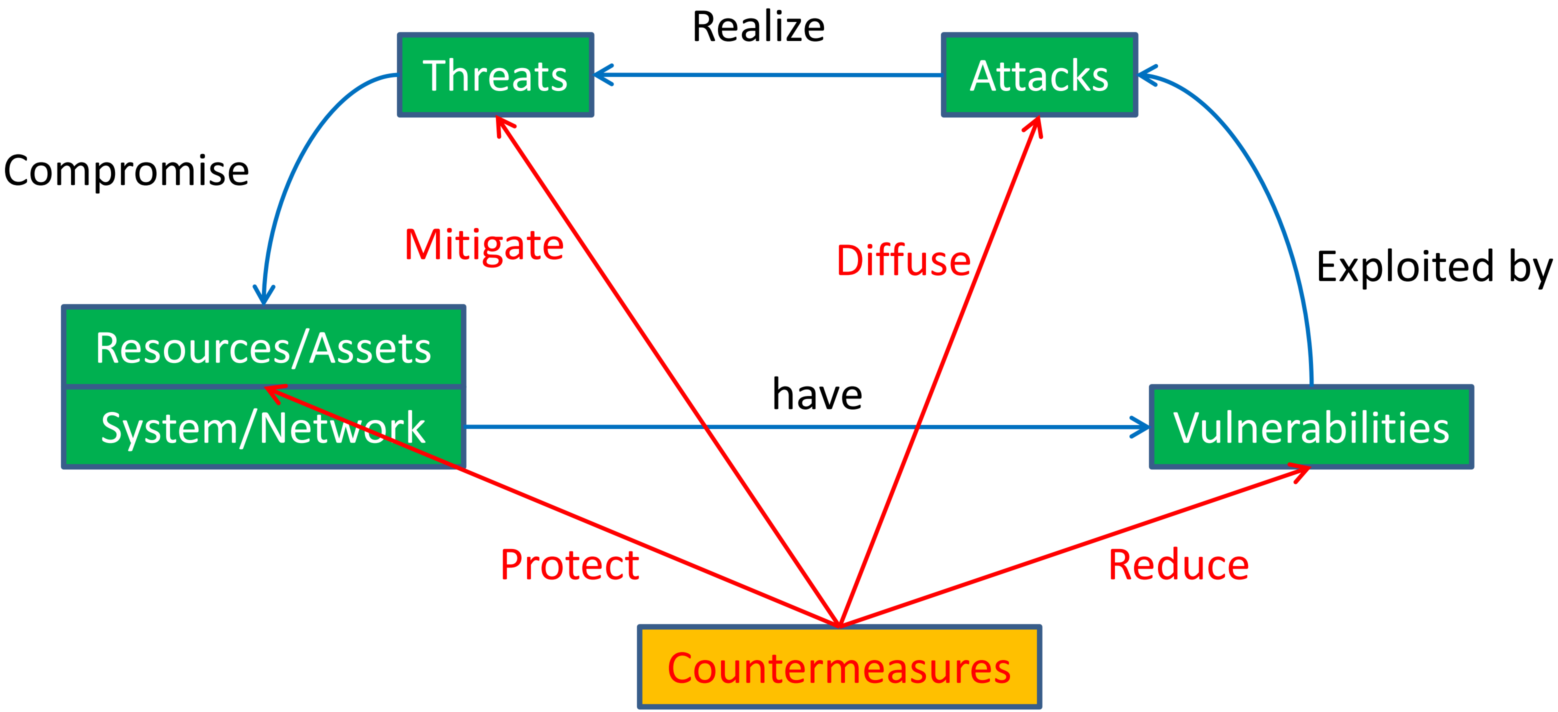
Safeguards/Defense

- Individually, Organization level
- Security achieved via a “policy”. Specifies
  - What **action principals** can take on an **object**
  - E.g. Only Bob may use this machine
  - E.g. Only Bob may view the contents of this message
- Security mechanism: method or component to enforce a policy
  - E.g. Biometric locked room for Bob’s machine
  - E.g. Encryption to hide message content

Safeguards/Defense

- Many techniques, products, companies
  - Encryption methods, Digital signatures, Hashes etc
  - Anti-virus, firewalls, IDS, Vulnerability scanners
  - Cloud security, Consultancy (threat detection, risk assessment, management etc)

Behold the Security Arena!



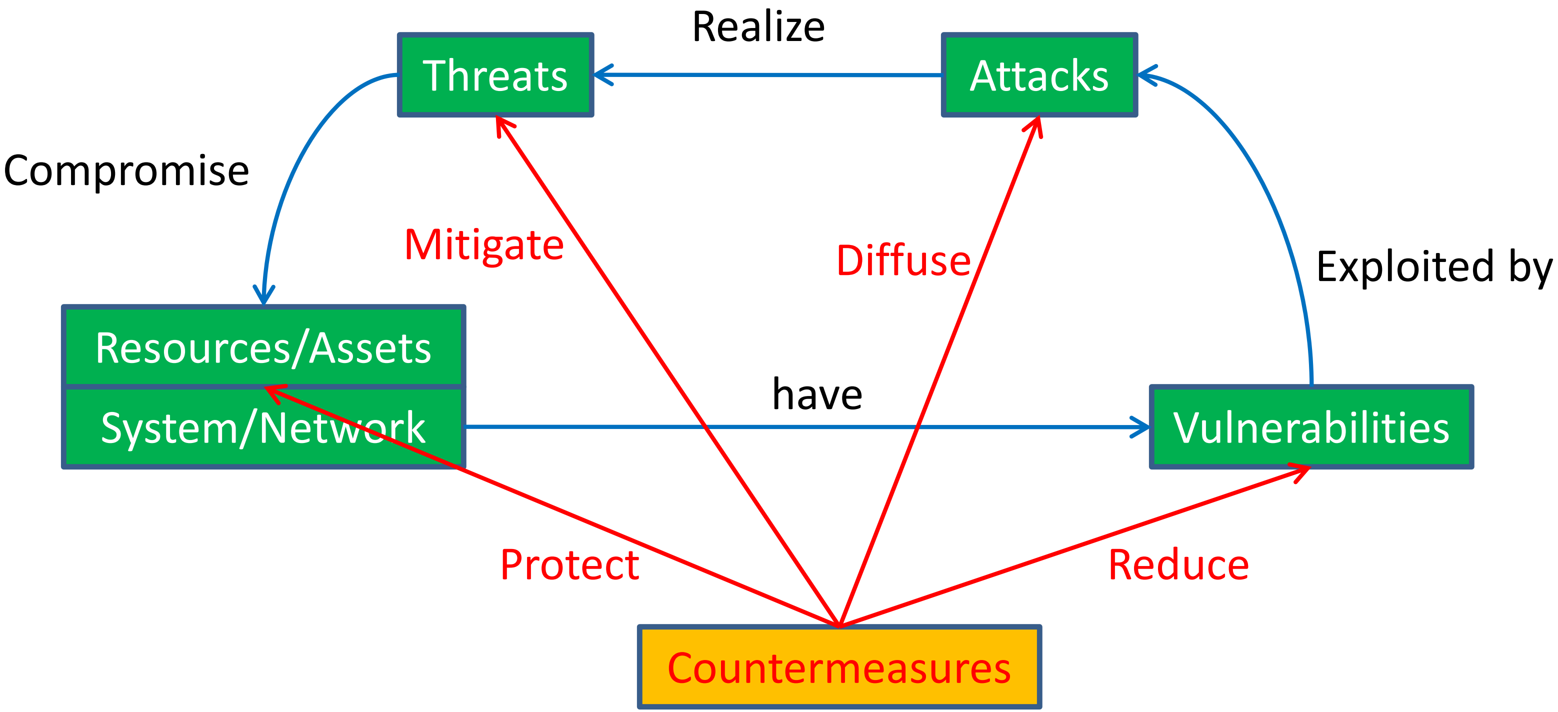
Example

- Asset: Student marks-sheet
- System: Residing on Instructor’s computer
- Threat: Student changing marks in the sheet
- Attack: Crack password
- Vulnerability: Weak password
- Countermeasures: Strong authentication; Strict punishment

Another Example

- Asset: Webpage
- System: Hosted on a web server
- Threat: Deface the webpage
- Attack: SQL injection + Crack Password
- Vulnerability: Application software; Weak Password
- Countermeasures: Validate input, Least privilege, Strong authentication

Behold the Security Circus!



Tussle between Defenders and Attackers

Outline

- ~~What is Computer and network security?~~
- Why is security important?
- Why is security hard?
- What does all this mean to me?

Why is Security Important?

- At a personal level:
  - Preserve privacy (e.g. what I browse)
  - Prevent access to confidential information (passwords, bank/property details)
  - Misuse of your resources for illegal activities
  - Avoid inconvenience (reboots, pop-ups, corruption of files due to virus)

- At business level:

“There are only **two types of companies**: those that have been hacked, and those that will be.”
-- Robert Mueller, **FBI Director**, 2012

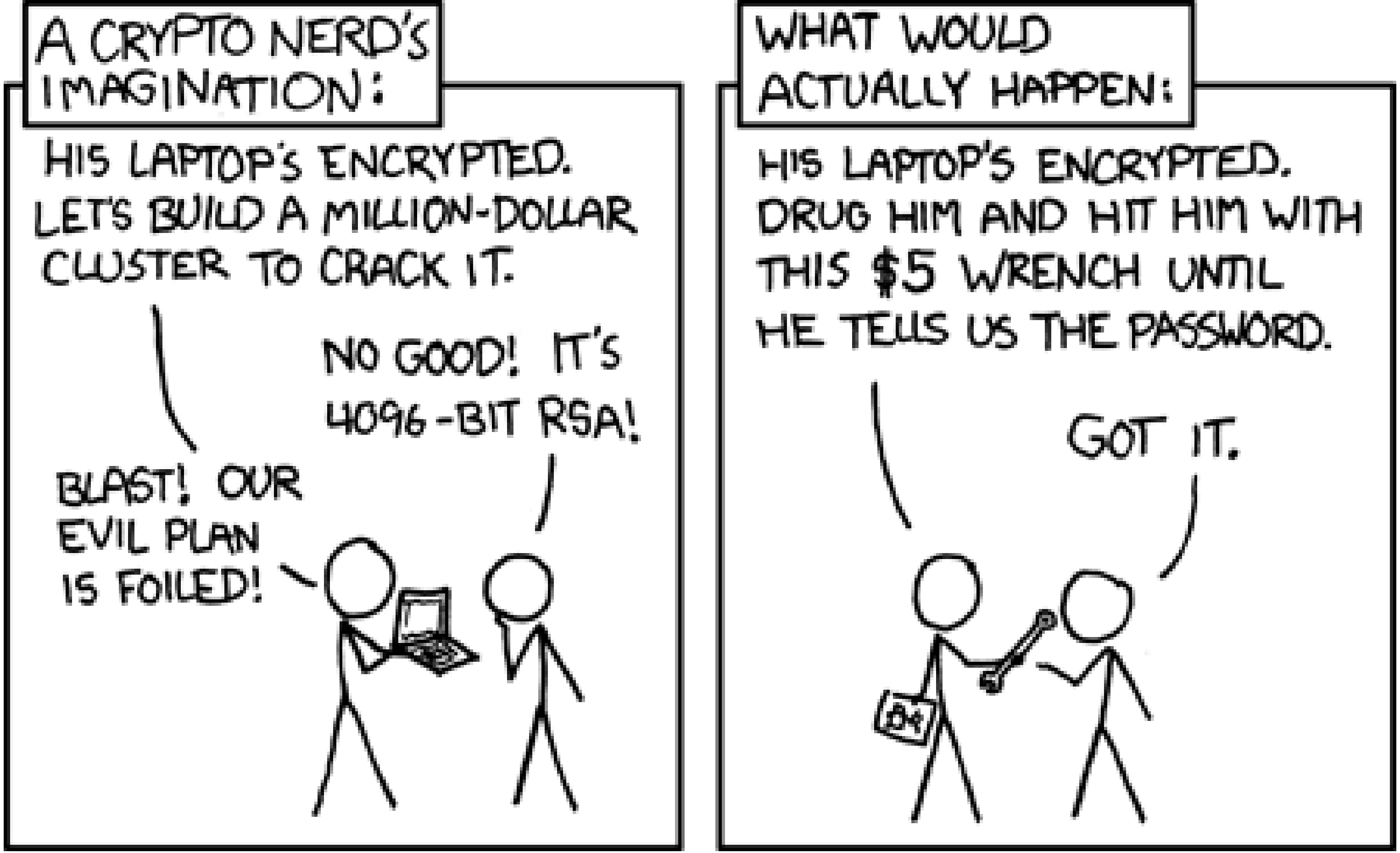
- At business level:
  - Prevent access to confidential data like credit/debit card, passwords, DOB etc (ebay, 2014, 145 million records stolen)
  - Avoid financial loss (Morris worm, 1988, estimated damage $100,000–10,000,000)
  - Prevent access to intellectual property (many companies, operation Aurora, 2009)
- Nation level: Cyber warfare
  - Protection from enemies/terrorist groups; (Stuxnet worm, 2010, Iran’s nuclear enrichment facility)

Statistics

- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Why is Security Hard?

- Complex System: Hardware, Software, Storage, Network, Data, Peripheral devices, People
  - Only as Strong as the Weakest Link in the Chain
  - “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”-- *Bruce Schneier*


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

- Tough environment:
  - Defender: Find/Eliminate all vulnerabilities
  - Attacker: Find only one vulnerability
  - “A good attack is one that the engineers never thought of.” -- *Bruce Schneier*

- Ease of attacks
  - Cheap
  - Distributed, automated
  - Anonymous
  - Insider threats
- Usability vs Security
  - More focus on usability and performance; Security often an after though
  - Security mechanisms often viewed as nuisance

Takeaway

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.“ -- Gene Spafford

- Perfect Security is impossible
- Tradeoff security with other goals (Usability/Cost)
- High level goal: Risk management not complete protection

Outline

- ~~What is Computer and network security?~~
- ~~Why is security important?~~
- ~~Why is security hard?~~
- What does all this mean to me?

What does all this mean to me?

- Can protect yourself
  - Install anti-virus, understand risks of downloads, sharing info in websites etc
- Ethical hacking (help the community)
- Research
- Jobs

You will *not* be a security expert after this class

Goals of the Course

1. Appreciate the challenges posed by security
2. Understand common exploits and how to defend/avoid them
3. In the process, explore/familiarize with a few popular standards/protocols
4. Implement/experiment some of the ideas (in the form of projects)
5. Get a high level overview of ongoing research/hot topics in this space

Summary

- Definition of computer/network security
- Security Arena
  - Acquainted with some terminology
- Why security is hard/important?
- What will you get out of this course