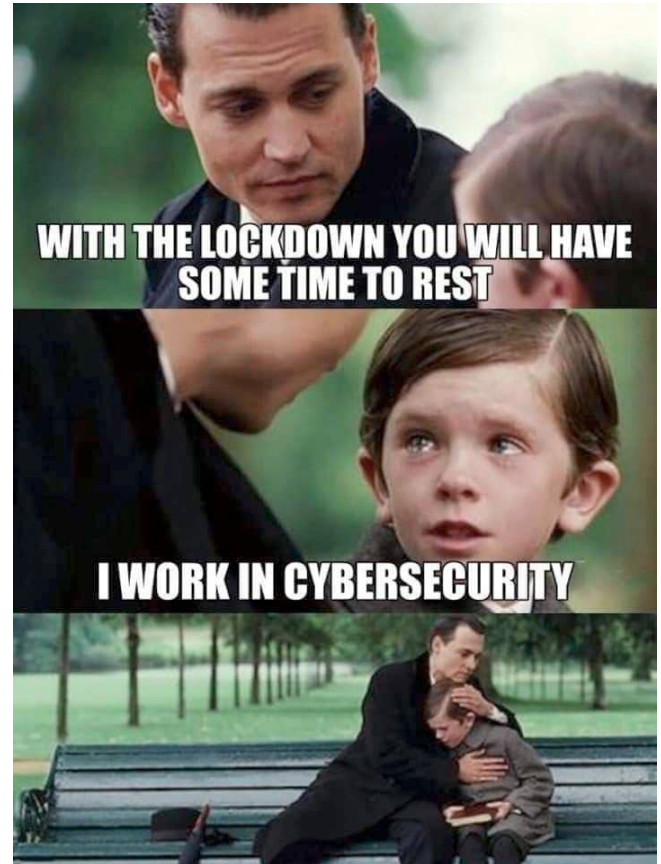


Web Security

Kameswari Chebrolu

Department of CSE, IIT
Bombay



<https://blog.internxt.com/cybersecurity-meme/>

Outline

- What is Computer security?
- What is Web security?
 - Why is it important?
 - Why is it 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)

Terms from Definition

- Resource
- Unauthorized 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 (bug bounty/Ransomware/Black Market)**
- 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
- At organization level, security achieved via a “policy”
 - What **action principals** can take on an **object**
 - E.g. Only Bob can access the webpage
 - E.g. Only Bob may view the contents of a webpage
- Security mechanism: method or component to enforce a policy
 - E.g. Authentication via Login page
 - E.g. Encryption to hide message content (https)

- Many techniques, protocols, products, companies
 - Encryption algorithms, Digital signatures, Hashes, CSRF tokens, Input sanitization etc
 - HTTPs, HTTP header options
 - Anti-virus, firewalls, IDS, Vulnerability scanners
 - Consultancy, Pen-testing companies (threat detection, risk assessment, management etc)

- “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.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



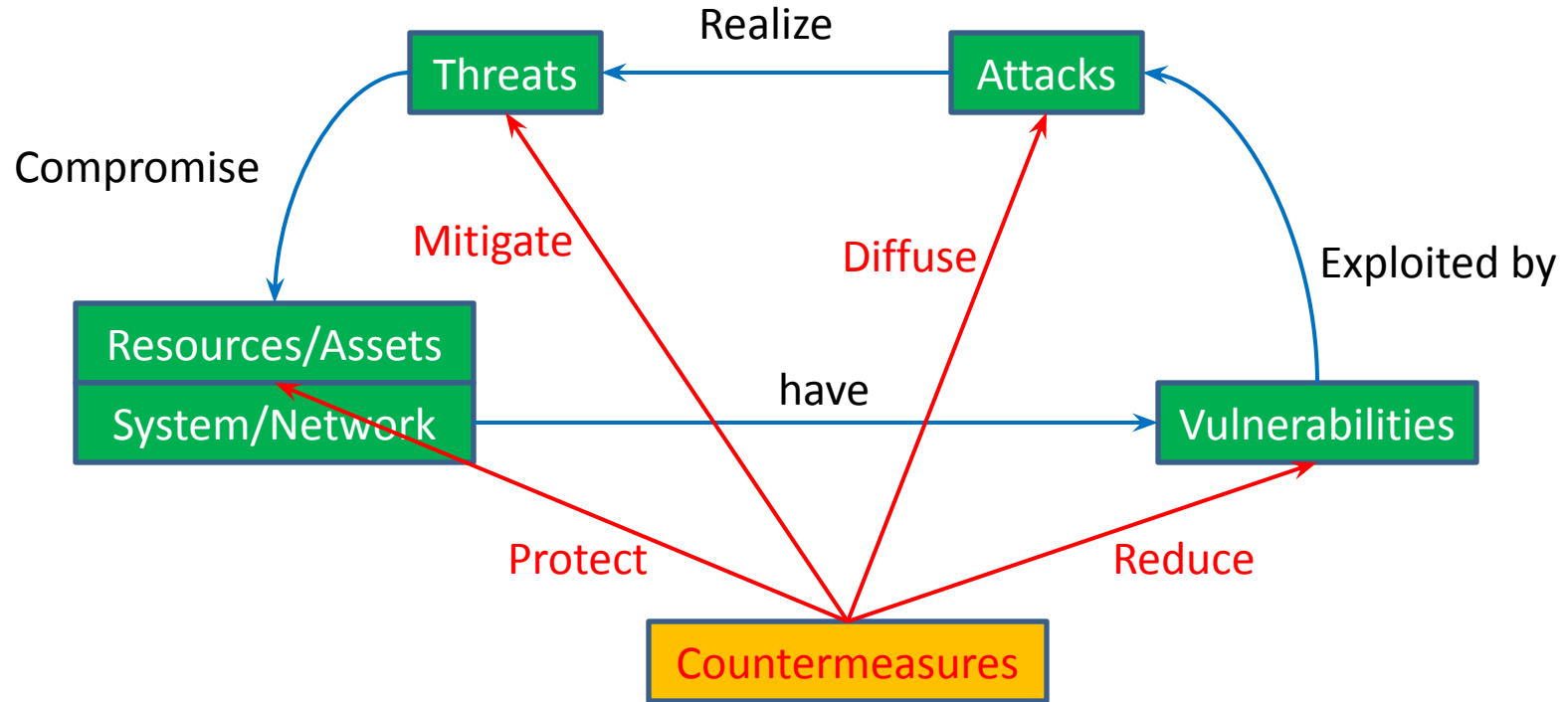
WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



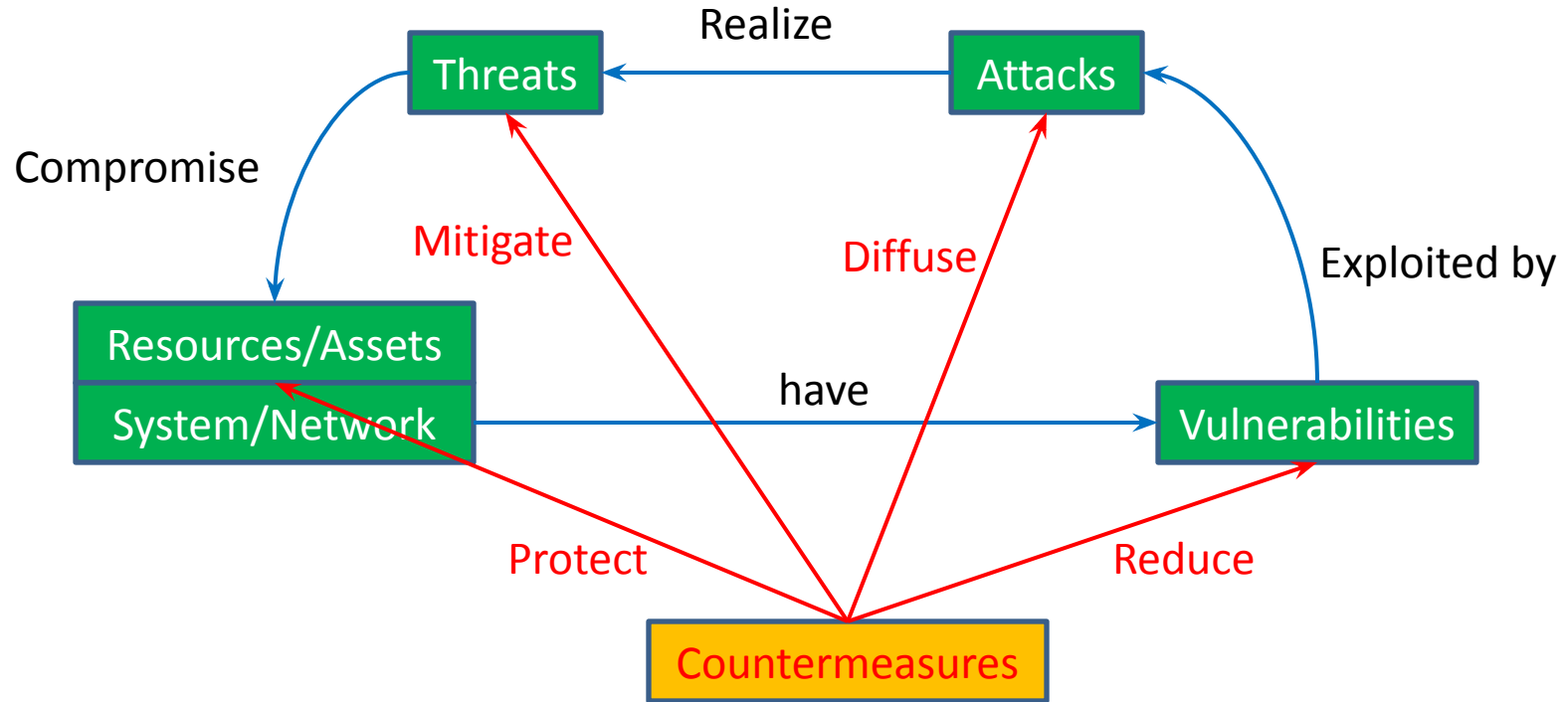
Behold the Security Arena!



Example

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

Behold the Security Circus!



Tussle between Defenders and Attackers

Outline

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


Web Security

- Replace computer with website/web-application!
- Encompasses measures and practices designed to protect websites/web-applications
- **Goal:** ensure CIA (**Confidentiality, Integrity, and Availability**) of data and services hosted on the web
 - Confidentiality: information is accessible only to those authorized!
 - Integrity: Information is not altered or tampered with
 - Availability: Information and resources are available when needed

Why is Web Security Important?

CoWIN Data leak! Aadhaar, PAN Card info, shared on Covid vaccination portal, made public by Telegram: Report

3 min read • 12 Jun 2023, 05:17 PM IST

Join us 

Livemint

Personal information of Indian citizens, including Aadhaar and PAN card details, are reportedly available on Telegram due to a data breach caused by the CoWIN portal



CoWIN data leak: Screenshot of leaked details of Congress leader P Chidambaram by Telegram bot (Saket Gokhale)

5 AIIMS Servers Hacked, 1.3 TB Data Encrypted in Recent Cyberattack, Govt Tells RS

Media reports citing investigators had earlier revealed that records of nearly 3-4 crore patients, including high-profile politicians, were compromised.



Air India claims 4.5 million passengers affected by February data breach

SITA, which serves the Star Alliance of airlines including Singapore Airlines, Lufthansa and United, had in March said it had faced a "highly sophisticated" cyber-attack after which it initiated containment measures.

By: **REUTERS** | Updated on: Aug 21 2022, 17:33 IST

Follow us 

Share via:



At personal level

- Web is an integral part of our everyday life
 - Used for communication, business transactions, social interactions, and more
- Web Security helps in
 - Preserving privacy (e.g. what I browse)
 - Preventing access to confidential information
 - Passwords, bank/health records



- Misusing your resources for illegal activities
 - Downloaded malware during browser can cause this
- Avoiding inconvenience such as reboots, pop-ups, corruption of files
 - Again downloaded malware during browsing can cause this

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

- Web security crucial to
 - Safeguard customer data
 - Protect the integrity of transactions
 - Business Continuity and Productivity
 - DDOS attacks can disrupt service
 - Prevent Intellectual Property theft
 - Many industries are subject to regulatory/compliance requirements

- Check out:

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

Outline

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

Why is Web Security Hard?

- 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*
 - Cat and Mouse game
 - Landscape is dynamic
 - Constantly evolving new techniques and strategies to exploit vulnerabilities
 - Need continuous learning and adaptation.

- Complexity of Web Technologies:
 - Mix of complex technologies, frameworks, and components; lot of third-party stuff
 - Easy to introduce vulnerabilities
 - Defense requires deep technical understanding
- Diverse Ecosystems: range of browsers, devices, and operating systems!
 - Vulnerabilities may manifest differently on different entities!

- Scale of Web Services:
 - Many web services are large-scale and/or cloud-based
 - Security of data in transit and at rest, configurations in cloud are complex!.
- Rapid Development Cycles to release new features
 - Pace of development leads to security oversights

- Ease of attacks

- Automation

- Many automated tools to scan websites and launch attacks
 - Easy to obtain exploit kits on the dark web or other illicit channels
 - Allow attackers with minimal technical skills to launch attacks

- Cheap

- Plenty things sold cheap in blackmarket!

- Distributed and Anonymous

- Internet supports anonymity and distributed attacks easily

- Insider threats

- Usability vs Security

- More focus on usability and performance; Security often an after thought
 - Security mechanisms often viewed as nuisance

- Human Factors:

- Human errors, both in development and use
 - Misconfigurations, poor coding practices, and lack of security awareness
 - “The user’s going to pick dancing pigs over security every time.” – Bruce Schneier

- Submit password details at fake look-alike site in response to email (**Phishing**)
- Download malware app that boasts new features (whatsapp gold **malware; trojans**)
- Trust pop-up ads that warn of computer infection and buy fake and potentially dangerous anti-virus protection (**scareware**)
- The list goes on.....

Dear Wells Fargo customer

We regret to inform you that your Wells Fargo account could be suspended if you don't re-update your account information. To resolve this problems please [click here](#) and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 72 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using Wells Fargo in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to Wells Fargo.

Regards, Safe harbor Department Wells Fargo, Inc
The Wells Fargo team.
This is an automatic message. Please do not reply.

(Interesting capitalization here. Why not capitalize Harbor and Team? Because this is a phishing scheme!)



WARNING!

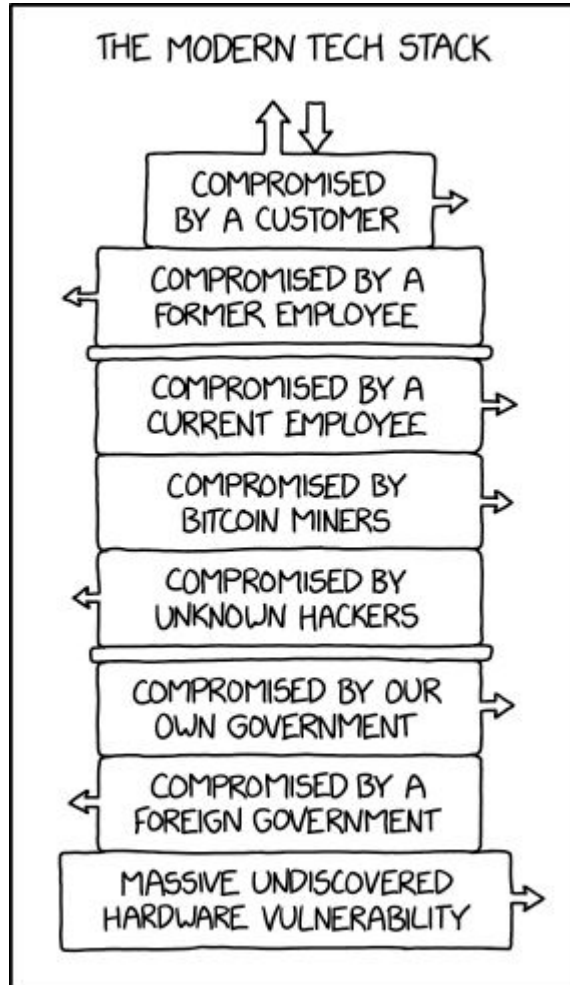
5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✗ System crashing
- ✗ Files deleted
- ✗ Personal info stealing
- ✗ Loss of Wi-Fi
- ✗ Infecting your other devices

Remove viruses now

I don't want to be safe



https://www.explainxkcd.com/wiki/index.php/2166:_Stack

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?

- Cybercriminals are always on lookout to exploit vulnerabilities in web applications
 - To compromise your system, steal your data, or disrupt services
- Study web security → proactively defend against these exploits.
 - Understand common threats and defense mechanisms
- Ethical hacking (help the community)

- Research
 - Aim to identify vulnerabilities, understand emerging threats, and develop effective countermeasures
 - Vulnerability Analysis, Security Protocols/Mechanisms and Standards, Malware Analysis, Privacy issues, User-centric security practices
- Jobs
 - A rapidly growing field with high demand for security professionals
 - Plenty jobs in web development
 - Understanding web security is crucial to building secure applications

Goals of the Course

1. Understand Web background
2. Appreciate the challenges posed by Web Security
3. Understand common exploits and how to defend/avoid them
4. In the process, explore/familiarize with a few popular standards/protocols
5. Implement/experiment the ideas (in the form of labs)

“"The value of a education is not the learning of many facts but the training of the mind to think." – Einstein???

Summary

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