CSCI 245 Life, Computers, and Everything

Security and The Lack Thereof

Image source

How can the security of a system be compromised?

What is cyber security?

What are the properties of a secure system?

- □ Confidentiality
- □ Authenticity
- □ Integrity
- □ Scalability
- □ Availability
- □ Accessibility
- □ Non-repudiation
- □ Flexibility

What are the properties of a secure networked system?

- ☑ Confidentiality
- ☑ Authenticity
- ☑ Integrity
- ☑ Freshness
- ☑ Scalability
- ☑ Availability
- ☑ Accessibility
- ☑ Non-repudiation
- ☑ Flexibility

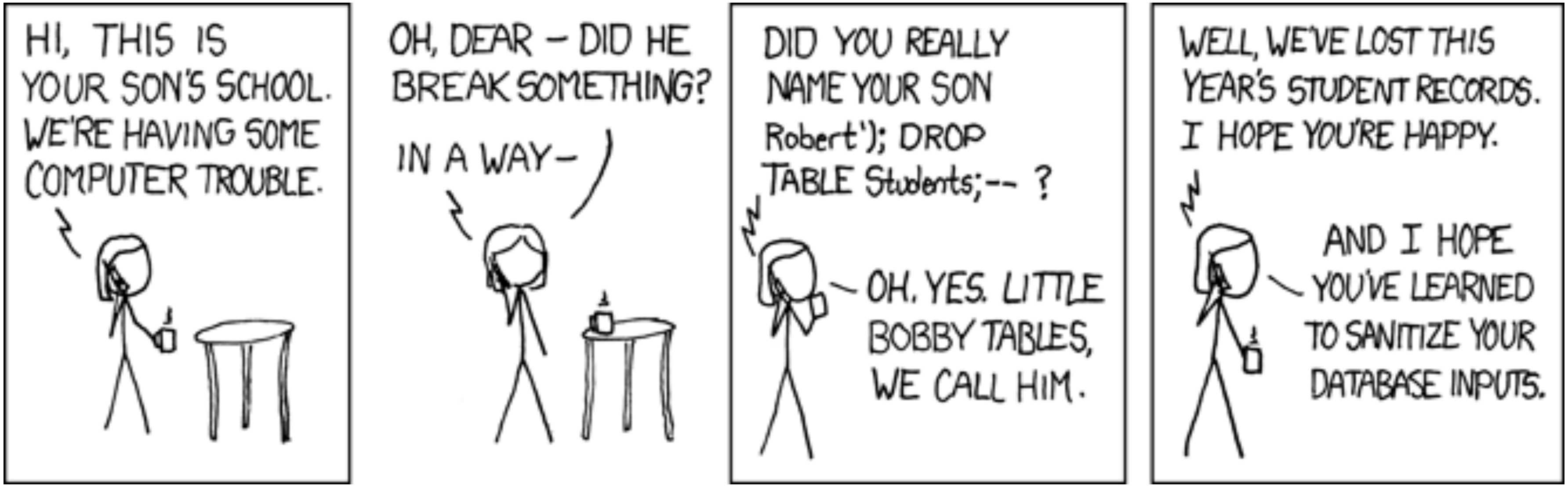
Motivations

Why do people break into systems?

Kinds of Attacks

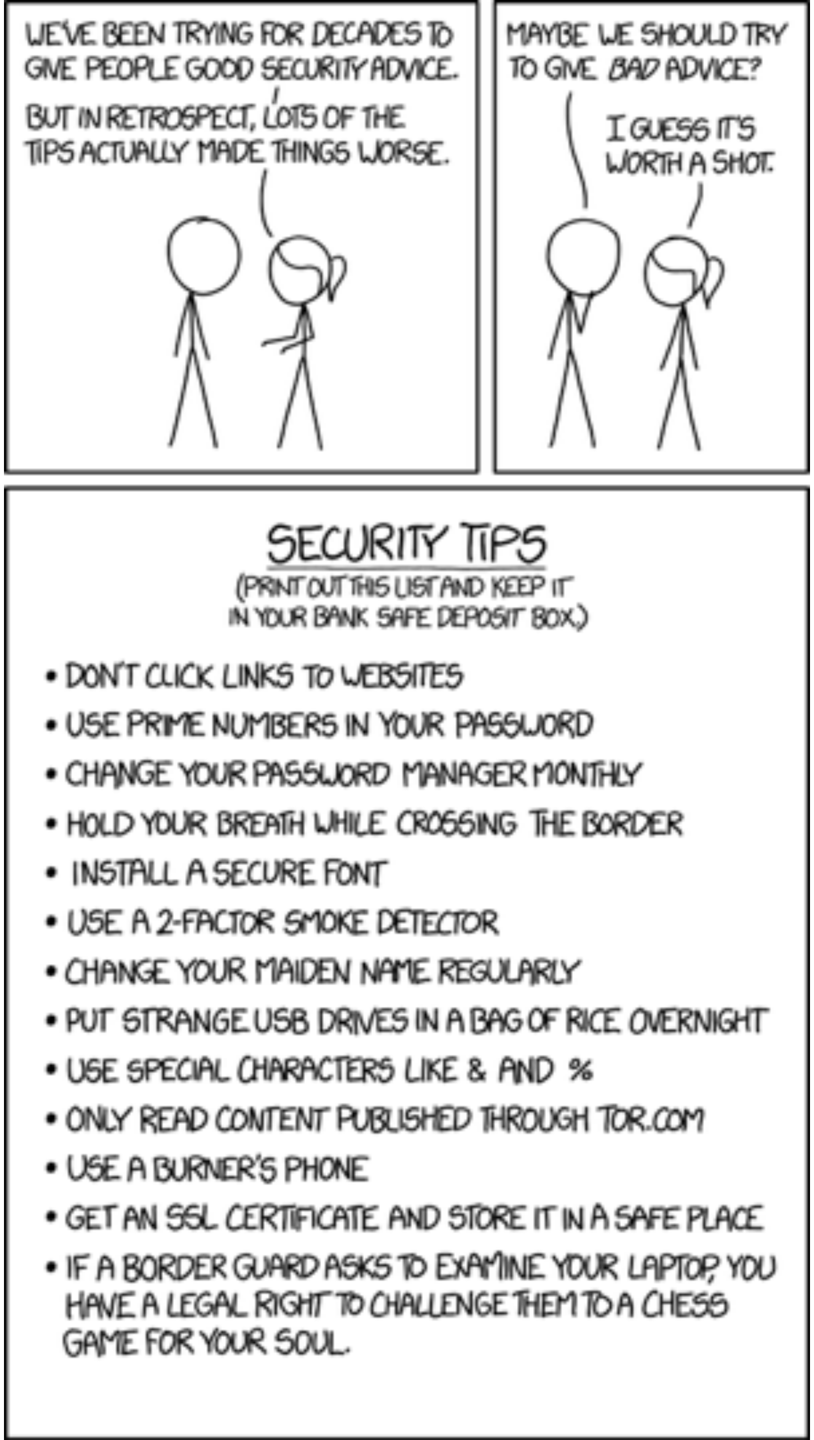
How can the security of a system be compromised?

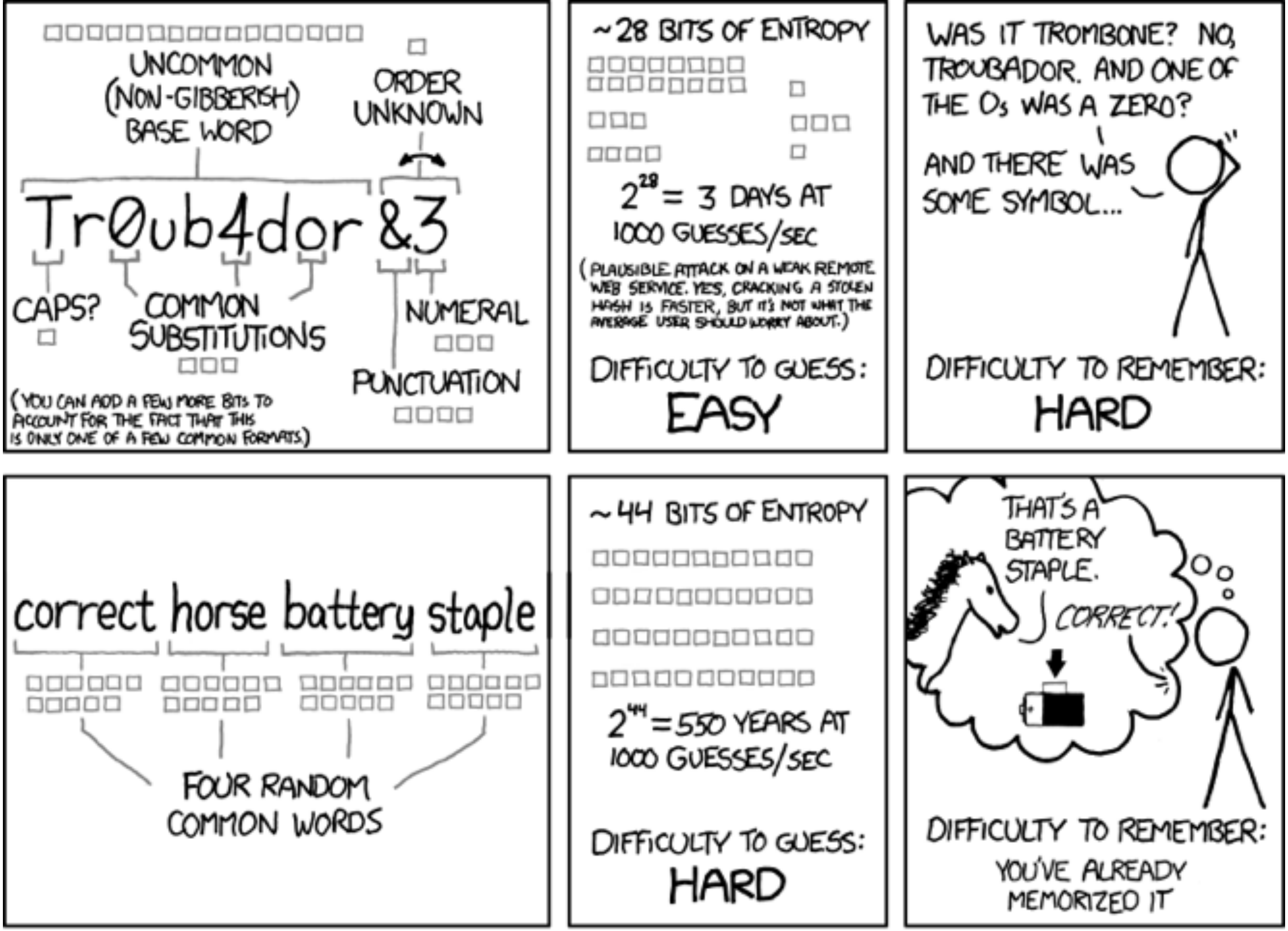
- Passwords
- SQL injection
- Cross-site scripting (XSS)
- DoS
- MitM
- Packet sniffing
- Malware: worm, virus, trojan, rootkit, adware, spyware, …
- Phishing
- Ransomware
- Botnets
- …


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Avoiding Attacks

What kinds of defenses can be used against cyberattacks?


WE'VE BEEN TRYING FOR DECADES TO GIVE PEOPLE GOOD SECURITY ADVICE.
BUT IN RETROSPECT, LOTS OF THE TIPS ACTUALLY MADE THINGS WORSE.
MAYBE WE SHOULD TRY TO GIVE *BAD* ADVICE?
I GUESS IT'S WORTH A SHOT.
SECURITY TIPS
(PRINT OUT THIS LIST AND KEEP IT IN YOUR BANK SAFE DEPOSIT BOX.)
• DON'T CLICK LINKS TO WEBSITES
• USE PRIME NUMBERS IN YOUR PASSWORD
• CHANGE YOUR PASSWORD MANAGER MONTHLY
• HOLD YOUR BREATH WHILE CROSSING THE BORDER
• INSTALL A SECURE FONT
• USE A 2-FACTOR SMOKE DETECTOR
• CHANGE YOUR MAIDEN NAME REGULARLY
• PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
• USE SPECIAL CHARACTERS LIKE & AND %
• ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
• USE A BURNER'S PHONE
• GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
• IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Liability

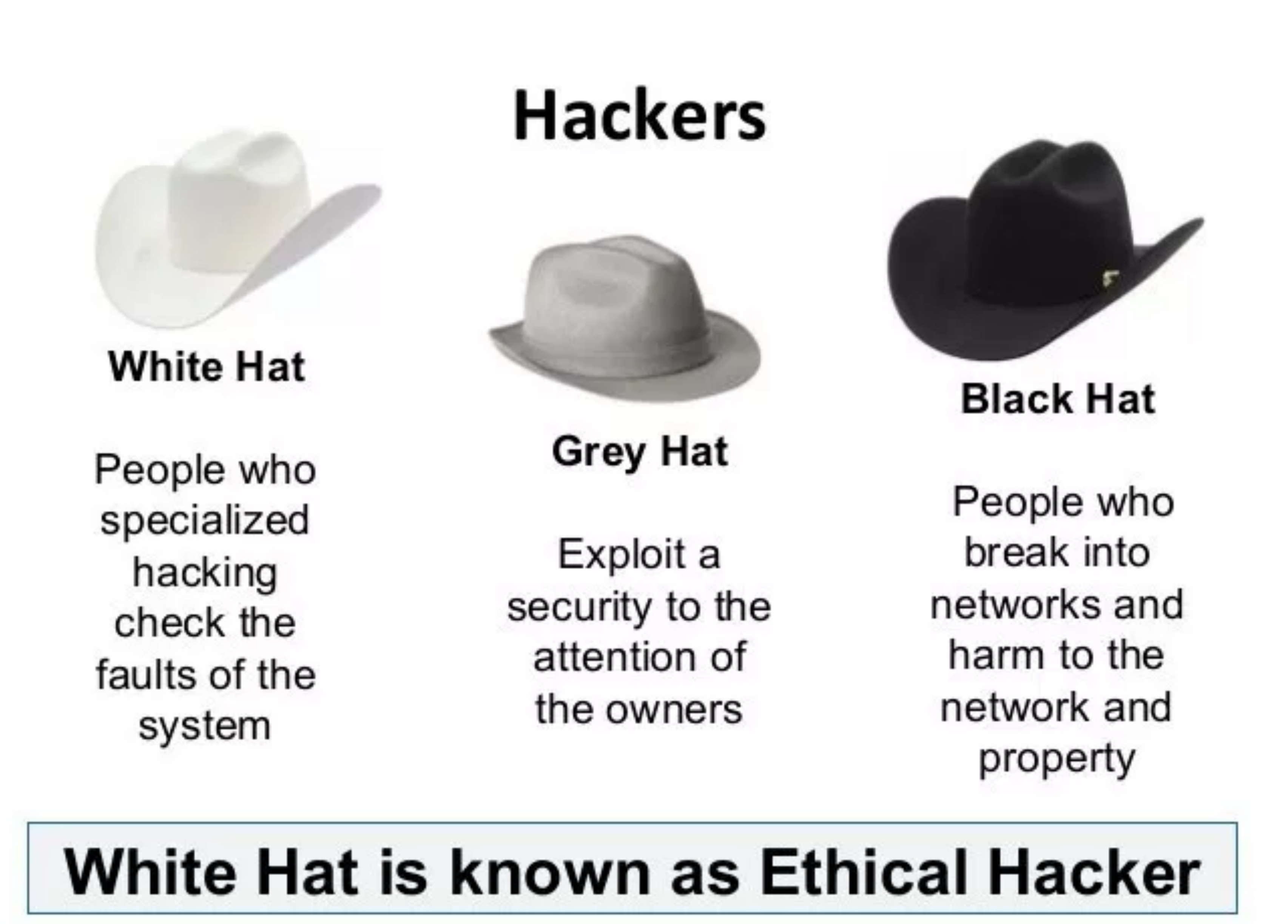
Are businesses liable for damages to individuals if their information is stolen from a computer system?

Black Hat Hacking

What are the penalties for cybersecurity attacks?

Gray Hat Hacking

White Hat Hacking



Hackers

White Hat

People who specialized hacking check the faults of the system

Grey Hat

Exploit a security to the attention of the owners

Black Hat

People who break into networks and harm to the network and property

White Hat is known as Ethical Hacker

https://www.prophethacker.com/2016/11/white-hat-gray-hat-black-hat-hackers.html

Penalties for Hacking

The U.S. Computer Fraud and Abuse Act covers:

- Transmitting code that causes damage to a computer system
- Accessing without authorization any computer connected to the Internet
- Transmitting classified government information
- Trafficking in computer passwords
- Computer fraud
- Computer extortion

The Firesheep Incident

A programmer releases **Firesheep**, a Firefox browser extension that makes it easy to sidejack open Web sessions.

You install Firesheep. When someone in your WiFi network visits an insecure web site, information about that user is shown in a sidebar. By double-clicking on the user's photo, you can "become" that user.

Websites have the responsibility to protect their users. If they do not, you can "teach them a lesson" with Firesheep. The author of the browser extension states that this does not turn good people into evil: it just forces websites to step up their security.

The Firesheep Incident

The author of Firesheep claimed that by releasing the browser extension, he helped to make web sites for secure for their business and their users.

Was this the right thing to do?

Kantian Analysis

Utilitarian Analysis

Virtue Ethics Analysis

The nice guy's dilemma

Greg is a bona-fide good person and a first-year computer science student. He reads news about security exploits every day.

This morning, he reads about a big bug in a Linux package. He downloads an exploit script to test it out on a lab machine.

Greg could run the script and see if he can become super user in the Linux system of his university.

The nice guy's dilemma

Kantian Analysis

Utilitarian Analysis

Virtue Ethics Analysis

The university has an appropriate computer usage code that states that one should not attack the system.

Greg could try the exploit and see if it works. If it works: (1) he would learn something about security; (2) he could tell the sysadmin which would help her know of the vulnerability.

What should he do?

What else?