USABLE SECURITY DESIGN

Network Security

Spring 2020

THE MOST POWERFUL SECURITY TOOL

- The Dental Hygienist asked me what was the best home security for her computer.
- Her question was obviously broad
  - Security against worms/vulnerabilities?
  - Security against viruses?
  - Data security?
- Anyone wish to guess my answer?

WHAT IS A WARRIOR'S MOST POWERFUL TOOL?

NO! NO! NO! NO! NO!

- This scene convinced me the Jedi were idiots!
- It isn't the Lightsaber that made the Jedi so dangerous
- Battles aren't won ***during*** the fighting; they are won in the ***thinking*** before hand
- Weapons aren't you most powerful weapon
- YOUR MIND IS YOU GREATEST WEAPON (and tool)
- My answer to my Dental Hygienist?

EDUCATION

YOUR MIND IS YOUR MOST POWERFUL TOOL

- “There is no knowledge that is not power” (Ralph Waldo Emerson)
- Tools serve to amplify, not replace, mental powers
- Some of the most effective attacks simply take advantage of the mentally weak
  - The Nigerian Email Scam – Yes, people do fall for these
- Other attacks take advantage of systems that are too complicated to fully understand
  - Python language sandboxing

NON-THINKING: A DANGER OF TECHNOLOGY

- “The real question is not whether machines think but whether men do” (B.F. Skinner)
- Thousands of years went in to developing our ability to detect physical fraud
- Humanity has not had time to evolve with the technology changes
- The most common attacks are not really about the technology, but the people
  - “Only amateurs attack machines; professionals target people” (Bruce Schneier)

MARKET REALITIES

- Unfortunately, humanity isn't going to evolve much during your life time
- And, equally unfortunately, they aren't going to get much smarter (as a group)
- This is where you come in
  - The most valuable security professional protects ***people*** not systems
  - You want to learn to create tools that helps idiots be safer
  - You need to be the strong mind that protects the weak

A CLIP FROM SID MEIER'S ALPHA CENTAURI

SOCIAL ENGINEERING: *PRETEXTING*

- Pretexting: phoning someone for info while pretending to be someone else
- The goal is to get information that gets you in the system, often a password
- Attacks of this sort are often conducted in stages
  - Attacker starts by getting non-sensitive information
  - Attacker uses non-sensitive information to convince others of his deception
- Your book points out one health institution had 30 such calls a week!

POSSIBLE SOLUTIONS

- Operational Security
  - Limit who has access (AH HA! PRINCIPLE OF LEAST PRIVILEGE!!!)
  - Train absolutely everyone that must have access
  - Periodically test the staff (e.g., by sending them a phishing email)

SOCIAL ENGINEERING: PHISHING

- Phishing: Sending an email that appears to be authentic to get private info
- Easy to create an email that looks authentic.
  - Especially modern emails with HTML and media
  - The resources are often online, so the phishing email simply points to them
  - Email is easily forgible
- Example attacks:
  - Tell user they need to change password (and enter old password first)
  - Tell user they need to update profile including SSN

SPEAR PHISHING

- A targeted email to a specific potential victim
- Aren’t these names clever?

POSSIBLE SOLUTIONS

- Big problem: the target is your customers
  - Can’t really limit them, unless you want to go out of business
  - Can’t really train them
- Psychology
  - Make it hard for them to do the wrong thing
  - Make it easy to do the right thing
  - (Obviously easier said than done…)

LIMITING HUMAN ERROR

- Errors spring from many sources
  - Human automation (drive to the wrong place because its common)
  - Following the wrong rule (information overload)
  - Not understanding the problem/context

UNDERSTANDING HUMAN BIAS

- Humans are not rational
- Humans are designed with a bias toward action
  - If we thought about everything we'd never do anything
  - We're programmed to act without thinking
- Examples of bias:
  - We're more afraid of dying in a plane crash than a car crash

WHEN EMOTION TAKES OVER

- When human logic/thinking reaches the end, emotions take over
- If we don't know explicitly what to do, we respond emotionally
- So, sometimes education has limited value
  - The bad guys will always learn how to exploit the part the users don't know
- One solution is safe defaults (AH HA! FAIL SAFE/FAIL SECURE!)
  - "Our bank will never, ever send email"

ABUSES OF AUTHORITY

- Read carefully the book's examples of how people behave
  - Under someone else's authority
  - When they have authority
- Also, people do not like to admit they make mistakes
  - "Hustlers" take advantage of this
- AGAIN, you cannot design assuming the user is dispassionate and rational

PASSWORDS

- Three ways of authenticating:
  - Something you *have* (token, fob)
  - Something you *are* (biometrics)
  - Something you *know* (password)
- Passwords are the most common because it is the cheapest solution

PASSWORD PSYCHOLOGY: *STRENGTH?*

- It's a good idea to require long complicated passwords, right?
  - Unless the user writes it down (easily compromised)
  - Or has to keep resetting it (easily compromised)
- It's a good idea to require the user to change passwords regularly, right?
  - See the problems above
- KEY POINT:
  - If you make security hard, the user will opt out

PASSWORD SECURITY USABILITY

- Protecting the entry form-factor
  - Bad example: PINs at ATMs
- Protecting the password transmission
  - Passwords sent in the clear are bad. Encrypt or hash!
  - Challenge/Response is a good solution. Simple example:
    - Both sides know password
    - Server sends Nonce
    - Client sends back secure hash of password+Nonce

PASSWORD GUESSING ISSUES

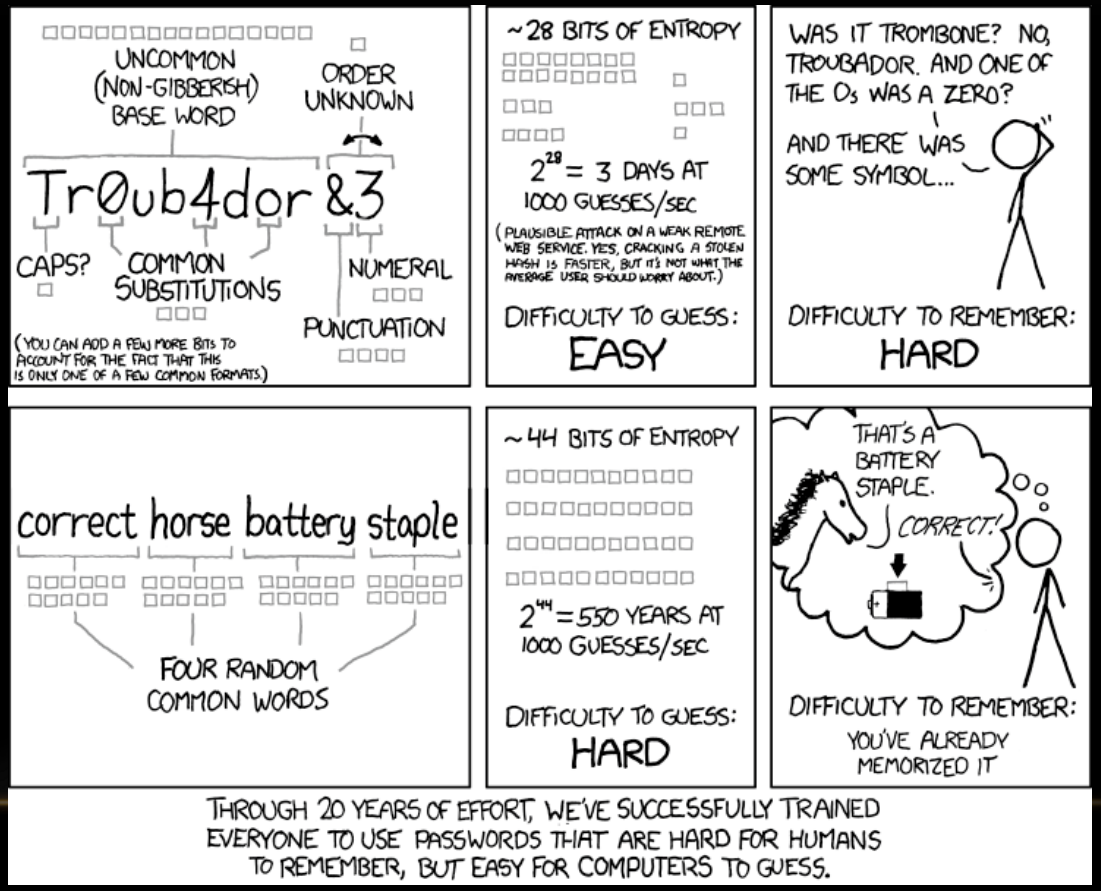
- Common solution is to freeze account or entry after multiple bad attempts
  - This can open up denial of service attacks
  - Can’t use this, for example, in the military
- Better solution is to require good passwords that cannot be guessed
  - However, watch out for “side channel” attacks on password guessing
  - Passwords checked one character at a time are vulnerable to timing attacks
  - Some smart cards passwords compromised by energy consumption

PASSWORD STORAGE

- DON'T STORE THE PASSWORD IN CLEAR TEXT!!!
- No really, I'm serious, don't.
- I'm wagering that one of you will make this mistake this semester in PLAYGROUND
- Better solution: Store the hash of the password (with a salt)
  - You can use this in place of a challenge response
  - This way, the server NEVER knows the password

A WORD ABOUT CHOOSING PASSWORDS

- My favorite method is to choose 4 random words
- XKCD #936:



PASSWORD ENTROPY

- You should understand this
- However, password entropy is beyond the scope of this class
- You might want to look it up on your own
- No really, you should

CAPTCHAS

- Good case study!
  - Combine psychology, usability, and system design nicely
  - Designed around what humans do well that computers do not
  - “Completely Automated Public Turing Test to Tell Computers and Humans Apart”
  - Thanks Alan Turing!