This is CS50x

OpenCourseWare

Donate (https://cs50.harvard.edu/donate)

David J. Malan (https://cs.harvard.edu/malan/)
malan@harvard.edu
(https://www.facebook.com/dmalan) (https://github.com/dmalan)
(https://www.instagram.com/davidjmalan/) (https://www.linkedin.com/in/malan/)
(https://orcid.org/0000-0001-5338-2522)
(https://www.quora.com/profile/David-J-Malan)
(https://www.reddit.com/user/davidjmalan) (https://twitter.com/davidjmalan)

How to Keep Your Computer and Phone Secure

Introduction

- As users of technology, we're all familiar with the need for security, even if we aren't familiar with the technical details.
- In the real world, we encounter different levels of security. For example, a building might have bars on the windows of the first level, but not the second or third levels. While it would still be possible for an adversary to break in, it would require much more effort, with a ladder or the like, so the probability or likelihood would be greatly reduced.
- Digitally, our devices are secure to some extent, but can never be perfectly secured. With enough resources, an adversary will be able to break in, so what we need to do is raise the bar so that there is high effort to do so.

Passcodes

- One way to define “being secure” is the ability to keep someone out of our resources and data by requiring a lot of time to hack in.
- On our laptops or phones, we may or may not have set a password required for access. Without one, anyone with the device can get access to our data.
- The top passwords in the world, unfortunately, are easy to guess:
  1. `123456`
  2. `123456789`
  3. `qwerty`
  4. `password`
  5. `1234567`
  6. `12345678`
  7. `12345`
  8. `iloveyou`
  9. `111111`
  10. `123123`

- For some accounts, like an online game we don’t care much about, these passwords might be sufficient. But for other accounts, we probably want a stronger password.
- A **brute-force attack** refers to the technique of trying all possible passwords until the correct one is found. This might be done with software, as with connecting a phone to a computer via a USB cable, but an adversary can even build a robot to tap all possible passcodes on a phone screen directly.
- With a 4-digit passcode, we have 10,000 possible passcodes, since each digit can have one of 10 values. But a computer can generate all of them quickly.
- We can demonstrate this by writing a program that prints out all possible products of 4-digit passcodes, in a programming language called Python:

```
from string import digits
from itertools import product

for passcode in product(digits, repeat=4):
    print("".join(passcode))
```

  - This program takes less than a second to run.
- With a 4-letter passcode, with 26 different letters possible for each place, both uppercase and lowercase, we would have `52 x 52 x 52 x 52` possibilities, or more than 7 million possible passcodes.
- We can change our program to use letters instead of digits:

```
from string import ascii_letters
from itertools import product
```

```
for passcode in product(ascii_letters, repeat=4):
    print("".join(passcode))
```

    - Now this program takes around ten seconds to run.
- We can expand our passcode to use any combination of characters, like letters, numbers, and symbols like `!` or `#`.
- On a typical keyboard, we'll have 32 symbols, in addition to 26 uppercase letters, 26 lowercase letters, and 10 numbers, for a total of 94 different symbols. So our passcode can be one of `94 x 94 x 94 x 94` possibilities, which ends up being one in over 78 million.
- We'll change our program to use every character:

```
from string import ascii_letters, digits, punctuation
from itertools import product

for passcode in product(ascii_letters + digits + punctuation, repeat=4):
    print("".join(passcode))
```

    - Now, our program takes much longer, though we can see its progress and it eventually finishes in a few minutes.
- With 8 characters, we have quadrillions of possibilities, or millions of billions, and with 2 additional characters, we'll end up with quintillions, or billions of billions.
- We can see the theme of tradeoffs, where a longer passcode might increase the difficulty of our passcode being guessed, giving us the benefit of increased security, but comes at the cost of greater difficulty for us humans to remember and type it in.
    - We might even be tempted to write it down on a piece of paper somewhere, leaving us open to other types of attacks.
    - Or, we might be tempted to use the same password on different sites, and if any one of those sites are compromised, an adversary could use our passwords on those other sites as well.
- On many devices, like an iPhone or Android, trying to log in incorrectly too many times in a row will lock us out from further attempts, telling us to try again in a minute or more. And it turns out this is a security feature, slowing down our adversaries who might be trying to guess our passcode. Now, even with 10,000 possibilities for a 4-digit passcode, this might take 10,000 minutes or more.
    - But now we might be preventing ourselves from getting in, if we accidentally make a mistake when we try to log in.
- With biometric technologies like face scanning or fingerprint reading, we might accept more convenience for "enough" security, even if a twin might be able to log in as well.
- **Two-factor authentication** refers to the use of an additional format of information to log in, such as a fingerprint or temporary code from a message or app. Since this tends to be

something we *have*, in addition to what we *know* (our username and password), it's even more difficult for adversaries to log into our account.

- **Password managers** are applications that store login information for us, so instead of remembering many different, complex passwords, we only need to remember a single master password. The downside might be a greater risk to us, if our master password is discovered somehow.

Encryption

- **Encryption** is the scrambling of information so that it can't be read without a **key** to decrypt it.
- Password managers, for example, encrypt your passwords so even if someone tries to open the file containing them, it won't be readable to them.
- `https://` is a secure way for browsers to open web pages, without anyone in between able to read the contents as well.
- **End-to-end encryption** means that our messages are encrypted between us and who we are talking to, so even if we are using a third-party chat or video service, the companies running them are not able to decrypt or read the contents of our communications.
- Zoom, for example, had previously advertised end-to-end encryption, but only implemented it as encryption between us and Zoom. Only recently have they rolled out true end-to-end encryption between the participants in a meeting, but some features won't work as a result.
- One might argue that Zoom is secure due to the end-to-end encryption, but it would have to be implemented correctly, and we would have to be sure our personal computer doesn't have any malicious software listening in once we're connected.
- To log into a meeting, too, we might go to a link like `https://zoom.us/j/5551112222`. But that was easy to guess and be shared by any of the participants, so newer meetings might require a password with a link like `https://zoom.us/j/5551112222?pwd=######`. Again, there's a tradeoff of less convenience and usability, for greater security.

Q&A

- When phones limit the number of guesses for passcodes before requiring you to wait before trying again, does that apply to software as well?
    - Depending on the device, lockouts might still apply even if the phone is connected via a USB cable to a computer making attempts via software.
- Are hardware two-factor authentication devices, like the ones that you plug in via USB, a good idea?
    - Yes, since they are a second factor protecting our accounts, but they come at the downside of being a physical device we have to keep with us, and not accidentally lose or break. A software-based second factor might be better since we might

notice our phone missing sooner, though we should avoid SMS, or ordinary text messages, since they can be intercepted or forged.

- Are there security concerns around cookies?
    - A cookie is a piece of data that a web server tells our browser to store, so when we visit that website again later, we don't need to log in, like a virtual version of a handstamp from an amusement park. But this also enables third-party companies like Facebook and Google to track us for marketing, since they place advertisements on many thousands or millions of sites across the web, and can see the same cookie from us as we visit each of them. Our browsers can prevent this with a settings to disable "third-party cookies," though this might have long-term effects if websites can no longer advertise to us effectively and need to charge us directly as the user.
- Can someone unlock your phone with a picture of you?
    - Typically, phones use infrared or other sensors to prevent this problem, but given enough time and resources, it might be possible to create a mask or puppet that's accurate enough.
- Is it possible to clear cookies so we're not tracked?
    - Yes, modern browsers also have an "incognito" or "private" mode, where those windows have no cookies or history kept. Browsers can also be configured to delete cookies regularly, but we would have to log in to our sites more often as well.
- Is it a bad idea to use our email credentials to log into other websites?
    - Sites that ask us for our login information directly are a bad idea to use. But the sites that properly redirect us to a page from our email provider, like Google, are secure. This relies on a technology called OAuth, where *Google* checks our credentials and only sends back a secure piece of information to the site about who we are, but not our passwords. We should always be sure that we type our credentials into the official URLs (like from `google.com`).
- What are VPNs?
    - VPNs are virtual private networks, which allows us to connect securely to a school campus' or company's network using encryption. So the internet traffic from our computers go to the other network first, and then elsewhere on the internet. This can be used to access printers or file shares at a physical location, or for video streaming websites from countries that aren't supported, since the VPN makes us *appear* to be connecting from that network. VPNs also help people in geographies or networks that might otherwise be insecure, since they encrypt all traffic. And the downside is that they typically slow down our traffic as well, since there's more distance for the information to travel.
- How do you connect to a device you're trying to break into?
    - This likely requires specialized software, in addition to a normal USB cable, since the manufacturers of the device want to make this difficult by design.

- Are lock patterns secure?
    - It depends on how long and complicated the pattern is as well, since a simple line is probably easily guessed. And others nearby can also easily watch you unlock with a pattern.
- What software should we use to communicate securely?
    - Apple's iMessage and Facebook's WhatsApp both use end-to-end encryption, but we have to accept that those companies actually implement it correctly, without allowing anyone else access. There are other open-source messaging apps with end-to-end encryption, like Signal and Telegram, where anyone can review the source code for them, reducing the probability that they are compromised.
- Are there other types of attacks on passwords?
    - Brute-force attacks are the simplest, but given information about a person, an attacker might use a program that guesses passwords with that information, like a birthday, dog's name, or even all words in the dictionary, since that might be a much quicker way.
- How safe is saving our passwords in Chrome?
    - Many browsers have built-in password managers now as well, though it might be unclear whether your other passwords are encrypted securely with only something you know.
- Are newer types of fingerprint sensors, like the ones under the glass display, as secure?
    - These might not be vetted or reviewed by the academic community yet, but they would likely have some tolerance level for similar enough fingerprints. A manufacturer's car keys, for example, might only use one of a thousand or ten thousand different codes, so you might be able to unlock someone else's car in a large parking lot.
- Does Harvard have a cybersecurity course?
    - Harvard doesn't have one available online, but many other institutions do.