human renAIssance

@p0wnyb0y

>whoami

- 12 years old and enjoy messing with tech
- I’ve been going to DEF CON + r00tz since 2014.
- I mostly dabble in computer security (InfoSec)

I also enjoy (non-tech related)…

- Trumpet player
- Star Scout
- Writing/journalism

If we could clone…

We could get more accomplished using human clones. 4-5 carbon copies of yourself could run around and carry out whatever task you need them to.

Your clone could:

- Complete your mundane chores
- Work your 9-5 job while you sleep in
- Talk to other people for you
- Do everything that you could do, but with greater efficiency and power

This concept sounds fantastic, but also fantastical. Could cloning actually happen in the near future?

What would you say if I told you the cloning era has already started?

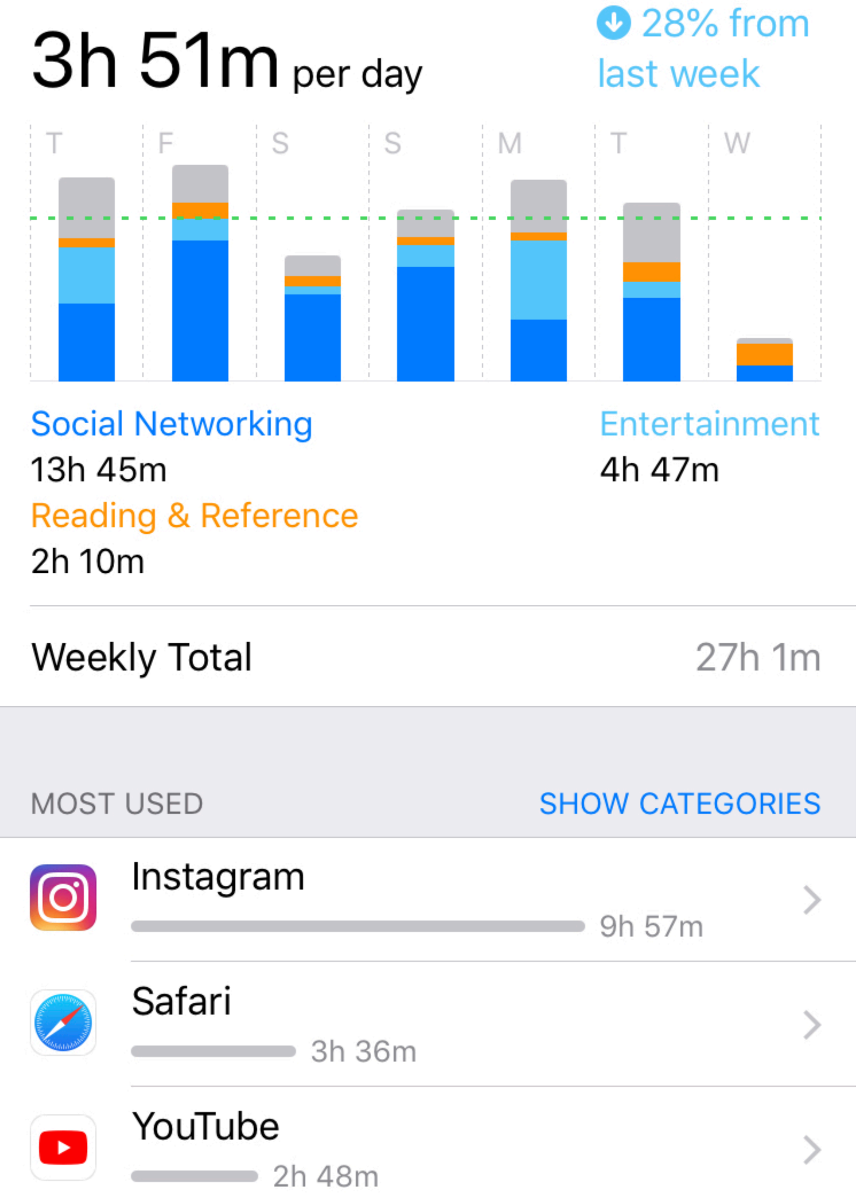
“I’ve been hacked!”

Why do people say they’ve been hacked, when it was only their account that was compromised? After all, wasn’t it just an account?

As a user spends more time with apps and websites, they start to learn more about their user. For example, social networking apps can gather tons of info from a user: hobbies and passions, likes and dislikes, birthdays, parent’s names, where they lived or went to school, etc. (more on next slide…)

With time, the ‘fine’ line between the human user and the program becomes blurry. When the app (or phone) is hacked, the user itself is also hacked.

And, if your account was compromised, how much data could a hacker obtain? How much damage could be done?



3h 51m per day

28% from last week

Social Networking
13h 45m

Entertainment
4h 47m

Reading & Reference
2h 10m

Weekly Total 27h 1m

MOST USED

SHOW CATEGORIES

Instagram 9h 57m

Safari 3h 36m

YouTube 2h 48m

“I’ve been hacked!” cont.

Information apps/websites might have on you:

- Pet names
- Child names/D.O.B.
- Political stance
- Employer
- Relatives
- Current location
- Photo library/camera roll
- Microphone/camera access
- Email/phone number/S.S.N.
- Military experience
- Spouse’s name
- Profile pictures/handles/usernames

“I’ve been hacked!” cont.

Scenario:

Zac had his social media account compromised. A hacker tried to log in to the account using an old password from another site’s leaked database, which worked. The hacker was trying to find as many details about Zac as they could. The reason: identity fraud; the hacker was trying to pull out a loan in Zac’s name.

Zac gave the platform every little detail about him, which gave the hacker an ‘slight’ advantage. The hacker could now see Zac’s birthday, full name, hometown, favorite sports team, first job, first car, current residence, etc. The social media platform also had a marketplace/shop page, where Zac bought from frequently. His credit card details were tied to the account, and were visible to the intruder.

An email was tied to the social media account too. Using information the hacker found from the social media account, such as home addresses and phone numbers, the hacker spoofed customer support and gained access to the email. Important emails, such as banking information and health records, were clearly visible to the perpetrator. Several years’ worth of mail, all from one password and a little bit of social engineering.

“I’ve been hacked!” cont.

Lesson:

As the number of people that use the Internet increase, the number of documents and files on the Internet increase. This also means that there is more important or personal information being put on the Internet. If websites and apps use more and more of these types of information, they need to make sure they use greater security.

For example, if Zac had enabled 2FA, the chances of him being hacked would have been reduced greatly. The perpetrator would have needed to access to Zac’s phone or email to login successfully. 2FA would have prevented the hacker from reaching all of Zac’s sensitive data. The social media platform could have also implemented a 2FA mechanism when accessing more sensitive data, such as birthdays or credit cards.

<future>

At some point in the future a social network will be able to post on your behalf. You provide the network's AI (bot) messages, locations, writings, etc. which can allow it to learn your specific, personal style of posting.

Would close friends and relatives notice the difference? As AI becomes more sophisticated, the answer starts to point toward 'no'. Details as specific as word choice or style of writing can help deceive, even the closest of friends, into believing they're talking to a real human.

This technology could be used maliciously, too. How would you prove that the 'person' at the other end of the line is a real human?

<future> cont.

Everyone grieves for the loss of a loved one. What would you give to be able to speak to that person one more time?

After death, the social network could keep on creating content on their behalf and would appear as if nothing had ever happened to them. AI would use the person's same whit and charm, continuing to post indefinitely, even reflecting on past events.

As an add-on service, perhaps one can purchase the AI option at their loved one's cemetery. Instead of just a hologram that person's entire online identity can be uploaded/accessed so that visitors could have real conversations with the deceased.

<future> cont.

While the concept of AI taking physical form is not new, the advances in cloud based services makes it more probable to happen in the future. Any physical body can access their AI from anywhere in the world(s). A whole new realm of cybersecurity will begin. How will we protect our clones? How will we securely update our new shells? What are the legal ramifications? Where do we argue death penalty cases, when the AI may be stored without international boundaries?

These are questions that my generation will have to figure out.

<future> cont.

Neuralink is a company that develops high bandwidth brain-machine interfaces which connect humans and computers. “This is going to sound pretty weird, but ultimately, we will achieve symbiosis with artificial intelligence,” Neuralink co-founder Elon Musk said at a press conference.

Musk stated that “…even in a benign AI scenario, we will be left behind. Hopefully it is a benign scenario, but I think with a high-bandwidth brain-machine interface, we can hopefully go along for the ride.”

The development and usage of brain-machine interfaces will be the next step in human-AI relationships. Could it also be the next step in human cloning? Artificial intelligence could precisely emulate/clone a human by decoding and learning the patterns of the human’s brain signals. By learning from the source of the human itself, AI could respond to situations to how the human would with better precision. BMI technology, combined with extensive data and artificial intelligence, might create a more ‘realistic’ human clone.

>git merge clones

The cloning era has already begun. People are already freely giving up their valuable information that can be used to seed AI in the near future. We need to start having detailed conversations about the legality, morality and ethics of human cloning.

- Should clones be given extremely dangerous jobs?
- Will clones stay alive forever? Will a clone’s ‘brain’ be uploaded and downloaded to different physical bodies after sufficient damage?
- Does the concept of cloning conflict with certain people’s spiritual views? Are humans meant to live past death?
- Do people that receive the death penalty get a second chance at life, maybe after a certain duration of time?
- Should clones be programmed so that they do not break any laws/go against their government? If not, what is the procedure for dealing with clones that do wrong?

>sudo shutdown

Soon, no matter how you may feel about them, human clones will go out into the real world. Whether these clones will be used on the battlefield or at the office, they will start appearing. Future technology will be capable of creating, storing, and programming these clones- and it’s our goal to manage them and use them only for good.

>whereis p0wnyb0y

Thank you!

You can find me on Twitter at @p0wnyb0y.

This presentation will be put up on my GitHub at github.com/p0wnyb0y.

fin.

Q&A