Julian Garcia

CSE 489

August 24, 2021

Two articles on Cybersecurity

1. *The new normal of cybersecurity: Ransomware, phishing and zero trust*

Article Link:

https://securitybrief.co.nz/story/the-new-normal-of-cybersecurity-ransomware-phishing-and-zero-trust

How this article relates to me:

In my current internship, I'm helping to develop software which could easily come under the attacks detailed in this article, and might be especially targeted for attack considering it contains some sensitive data. Moving to a zero-trust policy would help assure that this data would at least be difficult to ascertain.

Exam Questions:

1. What is zero trust?

   Answer: The notion that we should trust anything or anyone, whether it be inside a local trusted network, such as an office connection, or outside of it. No user or device is granted any trust, and as such constant checks are run for constant reassurance that the user or device isn't malicious.

2. What is perimeter security, and what may be the flaw in implementing only perimeter security?

   Perimeter security is the concept of ensuring external attacks cannot penetrate what you're securing. The flaw in this kind of security is that it does not check for any possible attacks from the inside.

2. ***Facial Recognition Technology: Current and Planned Uses by Federal Agencies***

   Article Link: https://www.gao.gov/assets/gao-21-526.pdf

   How this article relates to me:

   The full piece was 90 pages long, with a one page summary, so I mainly skimmed the sections related to the actual technology involved in facial recognition, and the possible uses of the technology. I feel as though facial recognition will end up being more prevalent in most of our lives as the technology moves forward, and the listed uses of the technology can serve as some assurance of that. As the technology improves we may see critical identification standards move to facial recognition and it could pose some ethical concerns I've been curious about.

   Exam Question:

   1. Name two ways that federal agencies currently use facial recognition.

      Answer:

      Possible choices are:

      - Digital access/Cybersecurity
      - Domestic law enforcement
      - Physical Security/Access to physical spaces
      - Border and transportation security
      - National Security and Defense