Transport Layer Security Report

- Question 2:
    - When it came to the TLS reports from the different websites there were a lot of similarities observed. For example every website I got a report on preferred AES as its Symmetric Encryption Algorithm, with ChaCha20 support as well. A streak of the most interesting similarities though were in the final three websites. These three reports seemed nearly identical including their certificate chains, the last two even have validation dates just hours apart. This leads me to believe that the way these three are set up is common for either most websites that are not large commercially or academic, or that this is how many gaming websites are set up as all 3 are websites in which you play a game on them. When it came to some key differences almost all of the websites had HSTS enabled with the exception of those 3 gaming websites and espn. The wiki fandom website did have it enabled but it was flagged as being too short.
- Question 3:
    - I would like to know more about innate patterns seen within TLS reports, I believe I saw a pattern in my last 3 websites but I am interested if there are more patterns that could be picked up on for government or academic websites as well.
    - How beneficial is it to have both EC and RSA certs, is the added security worth it?
    - Which of the two is better to use? I saw the appliedcrypto site just uses EC which is the only of its kind I saw. Every other site uses either both or just RSA, what is the reasoning behind this?
    - What does a website that does not use AES with ChaCha20 look like? Are those websites generally less secure or is the opposite the case?

Reviewed by: Plez Ownby