Nicholas Clement

ECEN5032 Homework3: Authentication

1a. A central sign-on facility would increase security by taking normalizing authentication and ensuring that all other university sites do not need to implement their own authentication. It would blanket all university websites and ensure the same security standards across each website, leaving no website any more vulnerable than the next.

1b. This same idea might hurt security by allowing all university websites to be compromised if the central facility is compromised. Similar to the compromising of a Certificate Authority if the central facility is compromised then all tokens it issued cannot be trusted, just like all certificates from a compromised CA cannot be trusted.

1c. If site A is controlled by an attacker the attacker can use the username (u) and Sign(u) to determine the central private key, and thus the Sign(u) for all other sites. This allows the attacker impersonate the user to all other university sites trusting the protocol, without getting authorization from the central facility.

1d. A good way to prevent this security risk would be to ensure that the attacker cannot use sign(u) + the public key to determine the central sign-on private key. One way to accomplish this task is to ensure that all university websites are secure, and sanitized.

1e.

1f.

2a. a-z + A-Z + 0-9 = 26+26+10 possible characters for each character of the password. This comes out to 62 possible characters. The total number of possible combinations for this password are 62^8. This comes out to 2.1834011e+14 possible passwords. Given 4 million attempts per second to ensure cracking the password it would take our adversary 2.1834011e+14/4,000,000 seconds. This comes out to 54585027.5 seconds to ensure cracking of the password. This is equal to 909750 seconds or 15162 hours or 606 days to ensure cracking of the password.

2b. Assuming that cracking the password = exhausting all possible combinations of the hash then it would take 15162 bots working on different combinations of the password to ensure completion in one hour.

2c. Knowing that our 8-character password = 1 byte, we can see that we will need to store 2.1834011e+14 bytes for a comprehensive table.

2d.

2e.

2f.

2g.

2h.

2i.

2j.