Coursework 1 - Exercise 8

November 9, 2023

Consider the following two-step method for Alice logging into a server S

1. **Setup**: Alice picks a password P and a number N and then computes the following sequence:

$$x_1 = f(P, 1), x_2 = f(x_1, 2), x_3 = f(x_2, 3), ..., x_N = f(x_N - 1, N)$$

, where $f()$ is some easy to compute function but hard to invert. She then stores the pair (x_N, N) with the server to whom she wishes to login later. Similarly, the server maintains for each user the (different) value x_N and the index N.

2. **Authentication**: When Alice wants to have access to the host, she types her username and the host looks up her entry and sends $N - 1$ to her. She then responds back with the value $x_N - 1$, which the host verifies by computing $f(x_N - 1, N)$ and comparing against the stored value x_N. If the two values match, the server gives Alice access to her account and replaces the values (x_N, N) with the values $(x_N - 1, N - 1)$.

---

a) What are the advantages (if any) of this scheme over ordinary passwords?

1. While the hash function just needs one inversion to recover the original value, the larger the N value is and the more times the user logs in, the more inversions are needed to recover the original values
2. Given that the function is hard to invert, if the value x_N was breached the function f would still be needed to inversed, that would be comparable to reversing a hashed password, but the attacker would still need to find out the N value
3. If the $x_N - 1, N$ was discovered by an attacker while the user is authenticating, the attacker would still have to inverse f function, beacuse x_i values change every time the user logs in

b) What are some attacks (if any) that can be applied to this scheme?

1. If an attacker finds out the $x_N - 1$ and the session is still active, the attacker can log in
2. If the original P value is discovered, the attacker would just need the N value and the security will be the same as a normal password
3. If the attacker attempts to brute force the x_i value, the security is the same as any other method of security with a password with the same lenght