CS396: Security, Privacy and Society (Fall 2022)
Homework #3, December 7, 2022

Instructor: Abrar Alrumayh

Instructions

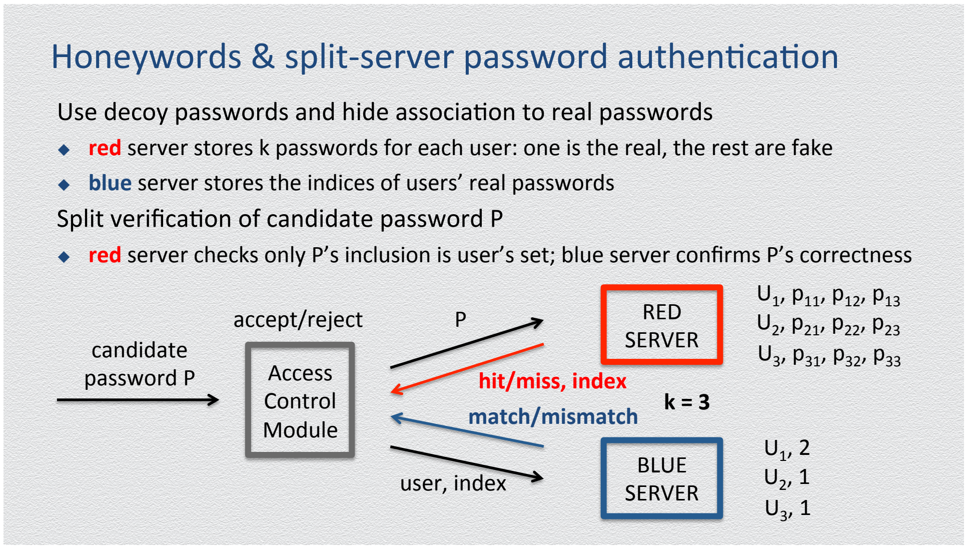
Please carefully read the following guidelines on how to complete and submit your solutions.

1. The homework is **due on Wednesday, December 14, 2022, at 11:59pm**. Starting early always helps!
2. Solutions are accepted only via Canvas, where all relevant files should be submitted **as a single .zip archive**. This should include your typed answers **as a .pdf file** and **the source code** of any programming possibly used in your solutions.
3. If asked, you should be able to explain details in your source code (e.g., related to the design of your program and its implementation).
4. You are bound by the Stevens Honor System. For Homework #3, you may work either **by yourself or in pairs**—in this case, your team **names should appear clearly** on your hand-in, and **2 same hand-ins are required**. Any collaboration beyond this is not allowed. You may use any sources related to course materials, but information from external sources must be properly cited. Your submission acknowledges that you have abided by this policy.

Problem 1: Understanding NSEC5 (40%)

Introduced by Goldberg *et al.* and currently under IETF's consideration for standardization, *NSEC5* comprises a replacement of the NSEC3 protocol for removing an identified vulnerability. Read the Introduction section from the original paper, and answer the following questions.

1. What *type of leakage* does NSEC3 allow for and what is the *technical reason* behind such vulnerability? (10%)
2. What are the core *technical features* of the new cryptographic hash function used by NSEC5 that allows for correct verification of non-existing domain names, yet preventing the type of leakage NSEC3 allows? (10%)
3. NSEC5 requires distributing a *signing key* to any secondary DNS resolver, who by definition is assumed to be *untrusted* with respect to validity of the provided answers for non-existing domain names. How is this technical choice justified? (10%)
4. In terms of secure system design, what is the lesson learnt in view what justified the development of protocols DNSSEC, NSEC, NSEC3 and NSEC5? (10%)



Honeywords & split-server password authentication

Use decoy passwords and hide association to real passwords

- red server stores k passwords for each user: one is the real, the rest are fake
- blue server stores the indices of users' real passwords

Split verification of candidate password P

- red server checks only P's inclusion is user's set; blue server confirms P's correctness

Figure 1: Hardening password security by employing decoy passwords in a split-server architecture.

Problem 2: Intrusion detection (40%)

Introduced by Juels and Rivest, *Honeywords* comprise a non-cryptographic method for hardening password security against stolen password files after successful breaches into authentication servers. The idea is to employ *decoy* passwords so that any user's account is associated with not only one (the real) password, but also with many fake ones, and then distribute password verification *across two servers*, say one red and one blue, each storing and verifying "half" of the credentials needed to be verified in order to successfully authenticate a user (see also Figure **??**). Read about the Honeywords authentication system from the original paper, and answer the following questions.

(1) How does this split architecture improve security? Consider the two cases where an attacker compromises only one of the servers. (10%)

(2) How does this system make password cracking detectable. (10%)

(3) What constitutes a good honeyword for a user whose real password is `Bo$tonRedSox76`, if honeywords are generated by tweaking real passwords? Provide a few examples. (10%)

(4) Stevens employs the Honeywords authentication system, and you just stole the passwords list, `000000000000000000000000000`, `itWb!%s45_3gMoI00286!*mooewTi409##21jUi`, `Blink-123`, and `Blink-182`, of an employee in the Office of the Registrar. If you have only one chance to impersonate him/her (and try to increase your GPA), which password will you choose and why? (10%)

Essay 3: Are smart speakers invading privacy? (30%)

The adoption of *smart speakers* is rapidly increasing: More than half of the US population own a smart speaker (e.g., Amazon Echo, Google Home, Apple HomePod, etc.) and ownership trends are predicted to keep rising. Smart speakers make Web search easier and daily routines more convenient, by allowing users to complete tasks quickly and efficiently using natural language. Yet, as such systems become more prevalent, new *security and privacy concerns* need be addressed:

- First, in order to respond quickly to service the user's command, smart speaker devices are permanently on and continuously listen in the background. This requirement has alone led to major concerns over user privacy.
- Second, the convenience of these devices is tempered by the possibility of performing also unintended actions due to the complex situation at the home. Anyone, such a guest in your home or a stranger shouting through an open window, might be able to get access to the smart speaker and any tasks controlled by it.
- Third, the use of third-party apps on smart speaker platforms introduces arguably even more serious privacy risks due to the open nature of the app marketplaces. Unlike the built-in apps, which are developed and maintained by the smart speaker provider, anyone can host and operate such third-party app.

Read more about such issues here, here, and here, and answer the following questions.

- Identify the main stakeholders and describe any security-related impacts of this new technology to these stakeholders. (10%)
- Describe the privacy concerns of the smart speaker devices that carry social and/or ethical implications that can affect individuals or the entire society. (10%)
- Provide some standard professional codes of ethics that you would like to take, and explain how these codes apply to mitigate the threat involved in each issue. (10%)