# CS306: Introduction to IT Security (Fall 2018)
# Homework #3

Instructor: Nikos Triandopoulos

November 28, 2018

## Instructions

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

1. The homework is due on **Wednesday, December 4, 2018, at 11:59pm**. Late submissions are accepted subject to the policy specified in the course syllabus. Starting early always helps!
2. Solutions are accepted only via Canvas, where your answers should be typed and submitted as a .pdf file.
3. You are bound by the Stevens Honor System. Collaboration is **not** allowed for this homework. 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.
4. This assignment provides a 20% **extra credit** opportunity!

## Problem 1: Can you crack a password? (24%)

Stevens IT requires users to choose passwords that consist of exactly 10 capitalized letters, which are stored in hashed form using either SHA-1 or SHA-256. Eve compromised Stevens' authentication server, long enough to learn the password hash of Alice, the TA for CS306.

**(1)** Describe and name an attack with which Eve can compute Alice's password.

**(2)** Describe how the above attack is affected, if at all, and why, when the server hashes passwords using user-specific salts, stored in plaintext, that consist of 10 alphanumeric characters.

**(3)** Describe how the above attack is affected, if at all, and why, when Eve has previously taken CS306 and knows and understands the birthday paradox.

## Problem 2: A password, but which password? (24%)

To hardened password security, Stevens adopted the honeywords password model, shown in Figure 1, where plaintext decoy passwords are used for user authentication in a split-server architecture.

**(1)** Explain the ways with which honeywords improve password security.

**(2)** Assuming that the server generates honeywords by "tweaking" real passwords, i.e., by keeping the main structure of a user's password but changing special symbols and numbers, list 10 passwords that would constitute good decoy passwords for a new user, Alice, who uses password `pa$$w0rd5`.

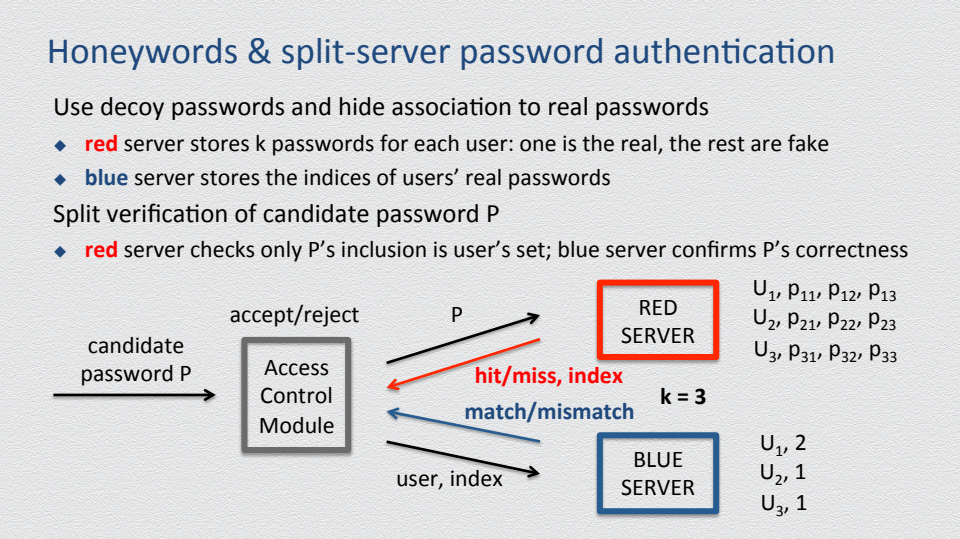


Figure 1: Password verification using "honeywords."

**(3)** You successfully broke into Steven's red server, long enough to steal the honeywords list of Bob, a senior administrative assistant in the Office of the Registrar, which consists of six passwords:

`Blink!@*)123`, `Blink-182`, `Blink-000`, `Blink-42379242235`, `B_17_l_34_i_15_n_80_k_27`, and `itWb!%s45_3gMoI00286!*mooewTi409##21jUi`.

Which one password will you choose, and why, to impersonate Bob and increase your GPA?

## Problem 3: Sir, is this your public key? (24%)

CS306 makes use of public-key encryption for any course-related communication. Enrolled students and staff members have their public keys registered with a trusted certification authority (CA) (e.g., Symantec). For efficiency reasons, public keys become available to interested users through an online service that is administered by Mallory, a new cheap cloud provider, where users can verify the validity of provided public keys via Merkle-tree hash proofs, as shown in Figure 2. Specifically:

- The CA provides Mallory with the public-key directory $D$ along with a special certificate $C$ that is the Merkle-tree digest of the directory, signed by the CA.
- To send a confidential message to Bob, Alice asks Mallory for his public key $pk_B$—even if she had previously used $pk_B$, since public-key pairs can be occasionally refreshed or revoked.
- Along with Bob's public-key record $(i_B, \text{Bob}, pk_B)$ in $D$, Mallory also provides Alice with the signed certificate $C$ and a corresponding Merkle-tree hash proof.
- After any change in the class enrollment (e.g., a student drops it or enrolls in it with delay) or whenever any public-key pair is updated, the CA provides Mallory with the new (that is, updated) directory $D'$ and the new (that is, corresponding to $D'$) certificate $C'$.

**(1)** Eve manages to get access to Bob's laptop and steal its secret key $sk_B$. When Bob becomes suspicious of this, he registers a new public-key pair with the CA. Describe and name an attack that allows Eve to collaborate with Mallory in order to learn all subsequent messages sent to Bob.

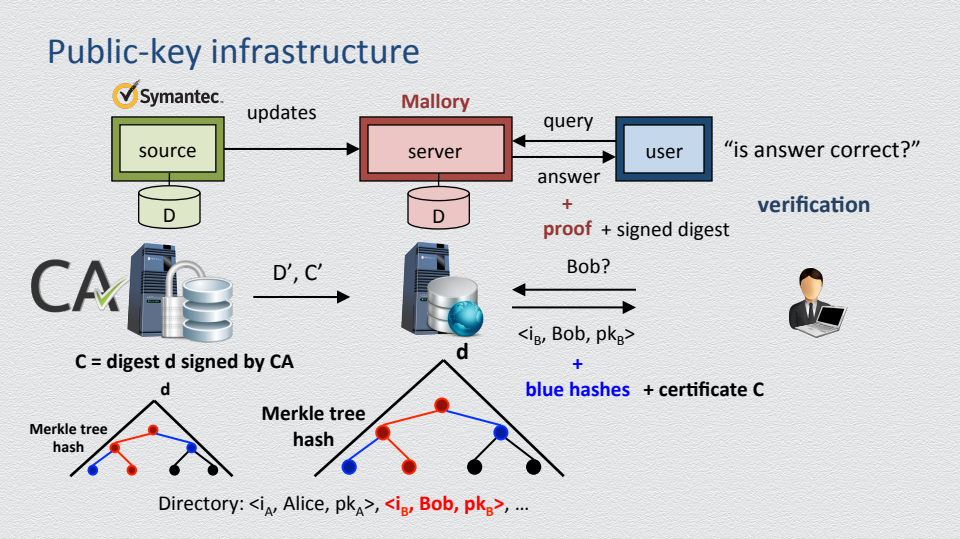


Figure 2: The public-key dictionary-as-a-service model for verifying public keys.

**(2)** Describe how timestamped signatures (i.e., signatures on timestamped messages) can be periodically employed by the CA, so that the users can detect the above attack. You can assume that no public key will be updated twice within the same day, and consider a 1-day signing period.

**(3)** Explain whether the above detection mechanism can be applied to DNSSEC and, if this is the case, what the impact of a 1-minute signing period would be on DNS.

## Problem 4: Can cryptography fail? (24%)

Alice, CS306's instructor, and Bob, CS306's TA, are communicating via terse cryptographically-protected messages to finalize the last homework assignment and the final exam for CS306. They do so by communicating via terse message exchanges which are cryptographically protected.

**(1)** Eve has previously intercepted the following MAC-tagged messages:

> Bob: status update please; are we done with assignments?
> Alice: hmmm... no no; more homework assignments will come!

Describe how Eve can undetectably affect the remaining CS306 assignments (without explicitly knowing the shared secret key) by manipulating the following MAC-tagged messages:

> Bob: is there time for a forth homework?; please advise
> Alice: yes, thanks for the reminder!; post HW4 with a 2-day deadline...

in the case where Alice and Bob use custom-made tags for messages of the form $m_1; m_2$ (i.e., consisting of two arbitrary-long parts $m_1$, $m_2$), by applying a secure MAC on their concatenation $m_1 \| m_2$.

**(2)** Eve knows that the final exam's three problems will be chosen from a predefined list of 10 known topics via asymmetrically encrypted messages of the following form:

> Bob: Which topic will problem #1 cover?
> Alice: Topic 7.

Bob: Which topic will problem #2 cover?
Alice: Topic 2.
Bob: Which topic will problem #3 cover?
Alice: Topic 8.

Describe how Eve can learn the final-exam topics (without explicitly knowing Alice's or Bob's secret key), in the case where Alice and Bob encrypt their messages using plain RSA encryption.

**(3)** Due to high student enrollment in CS306, Alice decides to use extra help with the exam monitoring and grading, and asks Bob to urgently hire a qualified student as proctor and grader. A day before the final exam, Bob posts an announcement of the available position at a university forum, and within minutes he receives an email from Gmail account CharlesSuperPower1999@gmail.com, sent by Charles, who claims to be a former CyS graduate student. The email contains Charles' resume and Charles' RSA public key $PK_C$, asks Bob to reply with the exam solutions, should he gets the position, in order to appropriately prepare for the job at hand, and is digitally signed using RSA. Bob likes the candidate's resume and is able to verify the email signature.

Describe why, or why not, Bob should go ahead with the request and send Charles the exam solutions, encrypted under $PK_C$ using RSA.

## Problem 5: Are cloud-based solutions cloudy? (24%)

CS306 makes use of a designated cloud-storage space at BestCloudStore, a cloud-storage provider that makes use of deduplication for cost-reduction purposes. By design, the client BestCloudStore application notifies the user who requests to upload a file $F$, whether $F$ was uploaded "virtually" or "physically," depending on whether $h(F)$ in a new or already known digest.

**(1)** To hand-in the take-home quiz for CS306, students are asked to upload their answers to the course BestCloudStore space, where new uploads are allowed, overwriting existing ones. The exam consists of 10 true-false questions and the submission file is a `.txt` file that should have student-specific name (to allow grading) but the following fixed format (to allow fast statistics):

```
Stevens-CS306---1:T; 2:F; 3:T; 4:T; 5:F; 6:T; 7:F; 8:F; 9:T; 10:F;
```

Describe a strategy that allows Eve, the only student who has not studied for the quiz, to submit an answer that is better than an answer based on random guessing.

**(2)** Bob is the Chief Scientist at BestCloudStore. To harden the security of the provided services with respect to the confidentiality of customer data "at rest," Bob proposes to Alice, the Executive Product Manager at BestCloudStore, the following update: The client BestCloudStore application comes embedded with the public key $PK_{BCS}$ of BestCloudStore, and any new file $F$ is uploaded as $RSA\_Enc_{PK_{BCS}}(F)$, that is, encrypted under $PK_{BCS}$ using plain RSA.

Explain the effect that this proposal will have on the cost-reduction benefits due to deduplication.

**(3)** In a long meeting, Bob and Alice decide to move forward with the above proposal but with one difference: Files will be uploaded encrypted using ElGamal rather than plain RSA encryption.

Explain the effect that this revision will have on the cost-reduction benefits due to deduplication.