Spring 2016 Computer Science and Information Technology II

Computer and Network Security Homework

Release Date: 5/6/2016, 14:20

Due Date: 5/20/2016, 14:20

Instruction

- **Submission Guide:** Please submit your homework report to CEIBA.
- You may encounter new concepts that haven't been taught in class, and thus you're encouraged to discuss with your classmates, search online, ask TAs, etc. However, you must write your own answer. Violation of this policy leads to serious consequence.
- TA's mail: r04922156@ntu.edu.tw

Problem 1: the CIA triad (20%)

Information security is the practice of defending information from unauthorized access, modification or disclosure. The CIA triad, Confidentiality, Integrity and Availability, is at the heart of information security. These three principles are applicable across the whole subject of security analysis.

Please explain these three major security principles and give each an example in the real world if it gets violated. Can you think about one more important security principle outside the CIA triad? What will happen in the real world if it cannot be fulfilled?

Problem 2: Authentication (30%)

Have you already watched the movie Captain America: Civil War (2016)? After falling asleep for nearly 70 years, captain has lost contact with agent Peggy. The only thing he wants to do is staying in touch with her again. However, everyone knows now captain is a charming guy and many girls pretend to be the real Peggy, which confuses him a lot. Thus, Captain America is here to ask for your assistance. You need to help him choose the best way to authenticate the real agent Peggy.

Recall that there are three common factors of entity authentication:

- **Something you have**: love ring, key of your house
- **Something you know**: birth date, the place you met each other
- **Something you are**: birthmark, voice

In this problem, you need to write down the pros and cons of each category to help captain decide.

Problem 3: Cryptographic Hash functions (30%)

Recall that a secure hash function H should satisfy three properties:

- **Onewayness**: Given $y = H(x)$, hard to find x' such that $H(x') = y$
- **Weak collision resistance**: Given x, hard to find $x' \neq x$ such that $H(x) = H(x')$
- **Strong collision resistance**: Hard to find $x' \neq x$ such that $H(x) = H(x')$

1. The third version of online rock-paper-scissors is conducted as following:

$$\begin{aligned} &Alice \rightarrow Bob : H(x_1, r) \\ &Bob \rightarrow Alice : x_2 \\ &Alice \rightarrow Bob : x_1, r \end{aligned}$$

   $x_1, x_2 \in \{rock, paper, scissor\}$ and r is a random number used as salting. To prevent Bob from cheating, which means Bob cannot know Alice's choice, please identify at least one main hash property being used here. To avoid Alice to regret, which means Alice cannot change her choice, please also identify one main hash property being used here. You should also justify your answers.

2. If both Alice and Bob are lazy and they don't want to spell and compute large numbers, they use 3 bits to represent x_1, x_2 and r, respectively. The representation of x_1, x_2 is listed below.

x	meaning
100	rock
010	paper
001	scissor

   Can Bob deceive Alice by knowing her choice? You should give short explanation about your answer.

3. Alice and Bob learn a lesson at this moment. They choose to use 1024 bits to represent x_1, x_2 and r, respectively, and design a new hash function as below.

$$H(x, r) = x \oplus r$$

   and $\oplus$ is a bitwise xor operator. Can Alice fool Bob by changing her choice? You should give clear explanation to justify your answer.

Problem 4: the FUN of games (20%)

CTF, the acronym of Capture the Flag, is a traditional outdoor game where two teams each have a flag and the objective is to find other team's flag, located at the team's base, and bring it safely back to their own base. In computer security, CTF is a computer security competition, usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world. This kind of competitions usually challenges the competitors their knowledge and ability on the design of systems, algorithms, binary analysis, reverse engineering, cryptography, mobile security and others. You can find much more information in the CTFtime website or by googling.

In this problem, we want to take you to experience a little fun of the CTF games. You are asked to solve the problems from level 1 to level 12 in the Natas section of the overthewire website. The direct entrance is `http://overthewire.org/wargames/natas/`. For each level, you should give short explanations about how you win the games to get the points. We also list some hints below for you if you get stuck too long. Enjoy it!

Bonus (32%): We encourage you to challenge yourself and finish more levels as much as you can. The more levels you complete, the more points you will get besides the basic scores. Don't forget to write down how you achieve your excellent work.

- Level 1: developer tools
- Level 2: google is your friend
- Level 3: robots.txt
- Level 4: HTTP header referer
- Level 5: HTTP cookies
- Level 6: secret location
- Level 7: remote file inclusion
- Level 8: $bin2hex(strrev(base64encode(\$input))) = encodedSecret$
- Level 9: shell injection
- Level 10: grep is your friend
- Level 11: $x \oplus y \oplus y = x$
- Level 12: file upload vulnerability and hidden form input value
- Level 13: exif_imagetype only checks first byte
- Level 14: sql injection
- Level 15: blind sql injection
- Level 16: command substitution
- Level 17: time-based blind sql injection
- Level 18: session hijacking
- Level 19: hex
- Level 20: customized format
- Level 21: session sharing
- Level 22: browser is not your friend
- Level 23: loosely typed language
- Level 24: http_build_query
- Level 25: ..././ and HTTP_USER_AGENT
- Level 26: PHP object injection
- Level 27: SQL truncation
- Useful tools: curl, sqlmap