CS458

Bo Liu
b69liu
20521697

September 2017

1 Written Part

1. (a) Integrity
The photo sent is replaced. So the one receiver gets is not the right data.

   (b) Confidentiality
My information(username and password) should not be know to others. But now the attacker knows it, and they can access my secured account and see all my private baby photos.

   (c) Privacy
Some of my personal information are told to others without my agreement. It violate the pravity policy.

   (d) Integrity
The worm locks users' data so that they cannot access it.

2. (a) Integrity
Fabrication
Mallory fabricate her letter as Alice's letter to Bob.

   (b) Confidentiality
Interception
Mallory accessed the letter without permission.

   (c) Integrity
Modification
Mallory modified the content of the letter.

   (d) Availability
Interruption

The letter was blocked, so Bob could not receive it.

Belkin wireless network router in 2003 is a case similar to scenario C. It blocked the request sent from router and reply the sender a commercial. The real server cannot received the request and reply.

3. (a) Preventing
   The fire will not destroy it.
   (b) Detecting
   The sensor will notify me if the water entering. So I can do something to save it before it is too late.
   (c) Recovering
   If one server is broken, the lost data can still be restored.
   (d) Detering
   The purpose is to find the potential vulnerabilities and fix it. Therefor, it makes the server harder to attack.

4. If the user were to forget the password, the server would have not been able to find it back.

2 Coding Part

(a) sploit3
Victim: Carol
This exploit also use buffer overflow, but we write a file to break that 2048 buffer. It creates a huge file, to ask the Backup to backup. In copyFile function, the area of RA seems protected, but I observed the exceeded data went to stack of main function. So I slightly increased the length to edit main's RA.
Fix: use dynamic array, or check the length of input.

(b) sploit4
Victim: Eve
This exploit is to attack the sprint in Usage. As explained in the reading material, there are two sprint function in Usage function. Alought the first snprint check the lenth, we can hide the placeholder in string, so that only the second sprint can translate it. After the translation, the buffer overflow will occur.
Fix: never user sprint, or always remember to limit the length of string.

3 table

user	sploit	type	flag
david	1	buffer overflow	
bob	2	fake ls	
carol	3	buffer overflow	
eve	4	format string	

e9d40726899bcdb3e306c363fb14bb267ebbac581edb12f699053c6eb5e6e65f -
c0a489ca50ecfe0196056b4128acde3a872f110d82eb1dbb35c3a8851d04d3cb -
363fd36274c5cee423b330dc9663ad7592138e4363d8f3a17702d9001b709cc9 -
630cca206c7d290199db41f6a4d76c8b03e4b7f1ebe6b38eead170427c0e8653 -