EECS 565 Introduction to Computer and Information Security

Homework III

1.1. The code segment below is known to be vulnerable. Please examine the code and explain the vulnerability. (15 points)

This code segment is vulnerable to buffer overflow attacks.

The second line of `func()` function attempts to copy 517 bytes of data (read from `myfile` in the `main()` function) into a 12-byte string. This will cause buffer overflow.

```
/* vulnerable.c */
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int func (char *str){
  char buffer[12];
  strcpy(buffer, str);

  //More code here

  return 1;
}

int main(int argc, char ** argv){
  char str[517];
  FILE * myfile;
  badfile = fopen("myfile", "r");
  fread(str, sizeof(char), 517, myfile);
  func(str);
  return 1;
}
```

1.2. Bob proposed a solution, as shown below. Does it really solve the problem? Please explain. (15 points)

No! This does not solve the problem.

The `canaryWord` and the `secret` variables are both stored in the stack. They are adjacent to each other. The attacker could overwrite both variables with identical value. In this case, the if- statement will return "true".

```
/* vulnerable.c */
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int func (char *str){
  int secret;
//getRandomNumber returns a random number
  secret = getRandomNumber();
  int canaryWord = secret;
  char buffer[12];
  strcpy(buffer, str);

  //More code here

  if (canaryWord == secret)
    return 1;
  else
    { ... error handling ...  }
}


int main(int argc, char **argv){
  char str[517];
  FILE * myfile;
  myfile = fopen("myfile", "r");
  fread(str, sizeof(char), 517, myfile);
  func (str);
  printf("Returned Properly\n");
  return 1;
}
```

2. Spam (30 points) 垃圾邮件过滤

Simple spam filters implement either a whitelist or a blacklist. The whitelist mode is similar to the "default deny" mode of a firewall, while the blacklist mode is like the "default allow" mode of a firewall.

2.1 identify the primary advantage of the whitelist mode.

This is very secure, since only emails from known senders could pass the filter.

2.2 identify the primary disadvantage of the whitelist mode.

The filter rules are too restrictive.

Or: many legitimate emails (e.g., emails from new senders) will be blocked.

3. Trojan horse and covert channel (40 points)

3.1 In an intelligence agency, a desktop computer is infected by a Trojan horse, which records key strokes and sends them to an overseas server via an encrypted TCP connection. In the security settings, IT administrators are not authorized to login to the infected computer. Is it possible for them to detect the anomaly? How?

异常

Yes, it is still possible for IDS to detect the anomaly. For example, abnormal (persistent) connection to an unknown server. Or, the server may be on a blacklist.

3.2 After the Trojan horse was discovered, the IT team starts to evaluate the damage. An administrator commented: "our firewall was manufactured and configured before the implementation of the Trojan horse; therefore, it was not possible for the firewall to block the covert channel set by the Trojan horse." Is he/she correct? Why?

No, he is wrong. Any of the following (or other reasonable explanation) is acceptable.

1. The firewall may be running in a whitelist mode that only allows connections to/from known IPs.
2. The firewall may only open ports to a few known services, hence, the port may be blocked.
3. The overseas server may be on a blacklist.

There could be other reasonable explanations.