**ECE568: Assignment1**

Name: Chuanrui Li; Student Number: 1000010846

**Security Incidents in 2015**

**Breach of integrity (30 words):**

Volkswagen, automotive manufacturers, installed a software called “defect device” to help cars pass emission tests by using fake data to cheat system. The company paid 6.5 billion for the lawsuits.

Source: http://tinyurl.com/zu2gjr5

**Breach of confidentiality (22 words):**

In 2015, November, the toy firm Vtech had a poor encryption algorithm for users’ password, which caused 4.8 million customers’ personal information stolen.

Source: http://tinyurl.com/hchuznx

**Breach of availability (32 words):**

In 2015, May, A group of hackers hacked the Sony PlayStation Network. All the Sony services including the multiplayer platform, the PlayStation Store and other social feature were unavailable at that time.

Source: http://tinyurl.com/gra7o3u

**Return-Oriented Programming**

**Part1 (100 words):**

The “W (xor) X” protection model makes the memory space that can be either writable or executable, but not for both. For example, hackers can inject the data into the memory space, but the system will throw an exception when the injected data executes.

For the stack-smashing attacks, attackers can successfully write shell code into the memory space and also overwrite the return address in the stack. However, when the program counter starts to execute the shell code during the second step, the system will throw an exception because of “W (xor) X” protection that no memory space can be both writable and executable.

**Part2 (59 words):**

3, Gadgets are organization unit blocks that include both instruction sequence pointers and immediate value. In return-oriented programming, attackers chain those small code snippets that have already written in the program. Each snippet has a return instruction at the end, which helps attacker to control program flow. Because those code are marked executable, it can avoid “W (xor) X” protection.

**Computer virus-Antivirus Coevolution**

**Part1 (75 words):**

Frist, for the traditional encrypted virus, it has a consistent decryption routine and visible sequence of instructions; so antivirus programs can easily detect a virus decryption routine. However, the polymorphic virus uses the mutation engine to generate a new decryption routine each time when it infects a new program. As a consequence, it is hard to find the fixed signature because decryption routines of programs are totally different, which leads to misidentification for antivirus product.

**Part2 (94 words):**

First, ECM only emulates first several lines of instructions in the beginning. If no decrypted-like actions are found in the running program, ECM will stop checking. Based on this, polymorphic virus can add “do-nothing” instructions before the polymorphic decryption routine to hide itself, because ECM may not emulate enough instructions. Second, the CPU emulator in GD cannot detect the polymorphic virus that has different machine language from CPU itself. In addition, it is impossible to simulate all types of CPU in GB, so it will have more viruses for older machine using old machine language.

**Programming Error**

**Part1 (90 words):**

Attacker can use the stdin for string input; the last 8 bytes can overwrite the return address. First 64 bytes in buffer copied from “Arg string”, then buffer copy 80 bytes to the “outbuf” that can cause “outbuf” overflow. Since the last 16 bytes will not be changed in buffer, it can use last 8 bytes to overwrite the return address of foo function.

Stack layout:  
return address 8 chars -> 8 bytes

Fame pointer 8 chars -> 8 bytes

Outbuf -> 64 chars

buf -> 80 chars

**Part2 (26 words):**

In line 17, we can change strcpy (outbuf, buf) to strncpy(outbuf, buf, sizeof(outbuf)), this can prevent the buffer overflow by setting string copy size.