DFSC 5325 Organizational System Security

Assignment 2

100 points, due by midnight Sunday, 09/24/2017

1. **What is the definition of Security Accountability? Make sure to briefly explain the security goals and requirements. (7 points)**
2. **Answer the following questions about accountability in an organization. (15 points)**
   a) **What is a basic rule to minimize the potential risk as far as collecting information from consumers is concerned?**
   b) **What is the main responsibility of an Information Security Officer (ISO)?**
   c) **What are some of the challenges that an ISO may be facing in a corporation?**
3. **Which act aims to protect the privacy of consumers' personal financial information? According to this act, are consumers made aware of the privacy policies that financial institutions follow? Are financial institutions allowed to disclose consumer's personal financial information to a nonaffiliated third party? (10 points)**
4. **What is the counterpart of the GLB act in health systems? What is main purpose of this act? (5 points)**
5. **The HIPPA security standard requires four key areas that the entities covered must address. Briefly discuss these four areas and especially discuss how security accountability can be implemented through compliance to the standard. In answering this question, you might want to link these area(s) to the security goals and requirements of Security Accountability. (10 points)**
6. **Suppose you are involved in a project to design the security model for a very large company (e.g. an international investment bank) where there may be frequent changes to the company infrastructure (e.g. through merger or expansion) and users (e.g. due to hiring, firing, transfers, etc.), and you were given the instructions to increase productivity, lower the administrator's workload as well as the administrator to end-user ratio, which security access control model (MAC, DAC, or RBAC) would you use? Justify your answer by discussing the pros and cons of each model, introduce the elements and relationships among elements of the model you prefer, and discuss why it will fit well in the above scenario. You should provide a detailed, thorough answer. (10 points)**
7. **According to Michael Butler, the author of "Extending Role Based Access Control", what is the major drawback of RBAC when it comes down to implementation in operating systems? (8 points)**
8. **Do some research to find out what protection mechanism is implemented by Fedora Linux that disallows executing code stored in the stack? Next, list a security feature implemented by the latest GCC compiler (Gnu C Compiler) and by the `bash` shell to prevent buffer overflow attacks. Why would such protection mechanisms be required? (10 points)**

9. Which statement in the C program "bufferVul.c" below has a buffer overflow vulnerability and why? Can you "patch" this vulnerability? Perhaps, it is a good idea to briefly go through Aleph One's "Smashing The Stack For Fun And Profit" article available http://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf. (10 points)

```
//bufferVul.c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int someFunction(char *str)
{
     char buffer[12];
     strcpy(buffer, str);
     return 1;
}
```

10. Read about the return-to-libc attack and briefly describe how one might use the `return-to-libc` attack to obtain root privileges on a victim machine? (5 points)

11. Almost everybody seems to agree that WEP has been "completely" broken and is consequently insecure. I'd like you to explain in very simple terms the implementation mistakes in the RC4 stream cipher used by WEP that led to this insecurity. What can you tell me about the current state of security for WPA (TKIP) and WPA2 (CCMP/AES)? Which wireless encryption protocol do you use in your home network? (10 points)