EECS 398 Fall 2012

Introduction to Computer Security

Final Exam
December 4, 2012

This is a take home exam. The exam consists of 7 questions. The maximum possible score is 100 points. This is an individual exam. You are not allowed to discuss the questions on this exam with anyone else. Exam is due 5 PM EST, Friday December 14th, 2012 to Professor Bailey's office, 4611 BBB.

Name: _____.

Unique Name: _____.

1:	**/18**
2:	**/18**
3:	**/12**
4:	**/12**
5:	**/12**
6:	**/12**
7:	**/16**
Total:	**/100**

BE SURE TO READ AND UNDERSTAND ALL THE QUESTIONS ON THIS EXAM IMMEDIATELY

Problem #1: (18 points) Introduction to Security

Part (a). List and define the three primary security goals (9 points)

1. _____

2. _____

3. _____

Part (b). For each goals listed above, provide one attack whose purpose is to foil that property. (9 points)

1. _____

2. _____

3. _____

Problem #2: (18 points) Physical Security

Part (a). Provide two ways in which we physically authenticate. (6 points)

1. _____

2. _____

Part (b). For each of the two above, provide a SIMPLE example of what this physical authentication is designed to protect and from whom. (6 points)

1. _____

2. _____

Part (c). Describe a SIMPLE way in which each of these two authentication methods can be forged. (6 points)

1. _____

2. _____

Problem #3: (12 points) Operating Systems Security

Provide a brief (one or two sentence) justification for each response (4 points each).

Part (a). Mandatory access control is more flexible for the user and provides worse overall enterprise security.

TRUE or FALSE

Part (b). An attacker getting a copy of the HASH of your (unsalted) password posses little security risk.

TRUE or FALSE

Part (c). When considering buffer overflow attacks, the use of the C function strncpy() provides some additional protection over the use of strcpy().

TRUE or FALSE

Problem #4. (12 points) Malware

Provide a brief (one or two sentence) justification for each response (4 points each).

Part (a). While static signatures for malware detection are often faster than other detection methods, they are easily avoided.

TRUE or FALSE

Part (b). Viruses are identical to worms.

TRUE or FALSE

Part (c). In static code analysis, the reverse engineer dissembles the target program to examine its structure. Such methods are impervious to obfuscation by the attacker.

TRUE or FALSE

Problem #5: (12 points) Network Security

Part (a). Briefly describe what confidentiality, integrity, and authentication guarantees IP, TCP, and UDP provide. (4 points)

Part (b). Why is an eavesdropping attack harder in a switched environment than in a broadcast environment? (4 points)

Part (c). Describe a two forms of denial of service attacks. (4 points)

1. _____

2. _____

Problem #6: (12 points) Web Security

Part (a). Briefly describe WHY an SQL injection attack works. (6 points)

Part (b). How are a Cross-site scripting (XSS) and a Cross-site request forgery (CSRF/XSRF) attacks different? Specifically focus on what trust is being exploited. (6 points)

Problem #7: (16 points) Cryptography

Provide a brief (one or two sentence) justification for each response (4 points each).

Part (a). Good entropy sources are plentiful.

TRUE or FALSE

Part (b). Factoring the product of two primes has been PROVEN difficult.

TRUE or FALSE

Part (c). Encrypting a message provides both confidentiality and integrity.

TRUE or FALSE

Part (d). Writing your own version of RSA is a good idea.

TRUE or FALSE

Ae yvv nf dpv eibak eifm jsunmess dw sqixo kgic mozm dw Szivmp hn 4611 LJS so bmtdifm rm ehid vasdvq