ECE 568: Assignment 3

Introduction

Please answer the following questions. Your answers should be written in full sentences, and any quantitative claims about security should be justified (*i.e.*, more than just ”yes” or ”it’s much more secure”). The completed assignments should be submitted in **hard copy during class** on the week of March 28, 2016, and work must be done *individually*.

SSL

The transport phase of SSL performs the following operations to prepare data for transmission:

Step	Description
i	Messages are broken into 4kB fragments
ii	Each fragment is compressed
iii	A sequence number is appended to each chunk
iv	A MAC of each chunk is computed
v	Each chunk and MAC is encrypted

Indicate what the consequences would be if each of the following changes is made to the SSL transport phase protocol.

1. Omitting step I **[1 mark]**
2. Omitting step ii **[1 mark]**
3. Omitting step iii **[1 mark]**
4. Omitting step iv **[1 mark]**

Hash Functions

An attacker tries to attack a hash function *H* by brute force. For any string *s*, *H(s)* is *n* bits long and, it’s a well-implemented hash function, so all n-bit strings are equally probable as the output for any randomly-chosen input. Let *h* be a given n-bit string. The attacker wants to find an input (pre-image) *m* such that *H(m) = h*. To this end, the attacker tries random input strings every time.

ECE 568: Assignment 3

1. Is the attacker trying to commit a selective forgery or an existential forgery? **[1 mark]**

2. What is the probability that the attacker will succeed on its first attempt? **[2 marks]**

3. What is the probability that the attacker will succeed on the *k*'th random try? **[2 marks]**

4. What is the expected number of attempts before success? **[2 marks]**

Web Security

The article "*Evaluation of TFTP DDoS amplification attack*" is available from the course website. It provides an overview of a class of DDoS attack tools, referred to as "amplification attacks", and introduces a particular amplification attack utilizing TFTP services.

1. Briefly describe what an amplification attack is and how it increases the impact of DDoS. **[1 marks]**

2. Briefly describe two mitigation approaches for DDoS attacks. **[4 marks]**

3. Briefly describe the format of the new amplification attack proposed this article. **[4 marks]**

Total: 20 marks.