UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR10058 COMPUTER SECURITY

Monday 15 th August 2016

14:30 to 16:30

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION

Year 3 Courses

Convener: C. Stirling
External Examiners: A. Cohn, T. Field

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. **Hash functions**

Let $\mathcal{M} = \{0,1\}^*$ and $\mathcal{T} = \{0,1\}^n$ for some integer n.

(a) Explain what does it mean for a hash function $h : \mathcal{M} \to \mathcal{T}$ to be one-way. [*3 marks*]

(b) Explain what does it mean for a hash function $h : \mathcal{M} \to \mathcal{T}$ to be collision resistant. [*3 marks*]

(c) Suppose $h : \mathcal{M} \to \mathcal{T}$ is collision resistant. Is h also one-way? If so, explain why. If not, give an example of a (presumed) collision resistant function that is not one-way. [*4 marks*]

(d) Suppose $h : \mathcal{M} \to \mathcal{T}$ is one-way. Is h also collision resistant? If so, explain why. If not, give an example of a (presumed) one-way function that is not collision resistant. [*4 marks*]

(e) Let p be a prime number and g a generator of $\mathbb{Z}_p^*$. Consider the function $h : \mathbb{Z} \to \mathbb{Z}_p^*$ where $h(m) = g^m \bmod p$.

i. Is h collision resistant? Explain your answer. [*3 marks*]

ii. If we assume the difficulty of the discrete logarithm problem in $\mathbb{Z}_p^*$, can you explain why this function is one way? [*3 marks*]

(f) Bob is on an under cover mission for a week and wants to prove to Alice that he is alive each day of that week. He has chosen a secret random number, s, which he told to no one (not even Alice). But he did tell her the value $H = h(h(h(h(h(h(h(s)))))))$, where h is a cryptographic hash function. During that week Bob will have access to a broadcast channel, so he knows any message he sends to Alice will be received by Alice. Unfortunately Bob knows that Eve was able to intercept message H. Explain how Bob can broadcast a single message everyday that will prove to Alice that he is still alive. Note that your solution should not allow anyone (and in particular Eve) to replay any previous message from Bob as a (false) proof that he still is alive. [*5 marks*]

2. **Memory safety**

Consider the following C code.

```
void vuln(int a[], int b[], size_t m, size_t n) {
     for (size_t i = 0; i < m; i++) {
         int tmp = a[i];
         a[i] = b[n-i];
         b[n-i] = tmp;
     }
}
```

(a) Depict the stack frame of a call to `vuln` before the execution of the `for` loop. You will assume that the code is executed on a 32-bit machine, with the size of the int data type being 4 bytes, and the size of the `size_t` data type being 4 bytes. `size_t` is defined by the C standard to be the **unsigned integer** return type of the `sizeof` operator. [*5 marks*]

(b) This code is not memory-safe. Explain why and show how an attacker could exploit it. [*4 marks*]

(c) Which of the following conditions on `a`, `b`, `m`, and `n` would ensure that `vuln()` be memory safe? If it is sufficient explain why. If not give an example of an input that would satisfy that condition but would be unsafe.

i. `a != NULL && b != NULL` [*3 marks*]

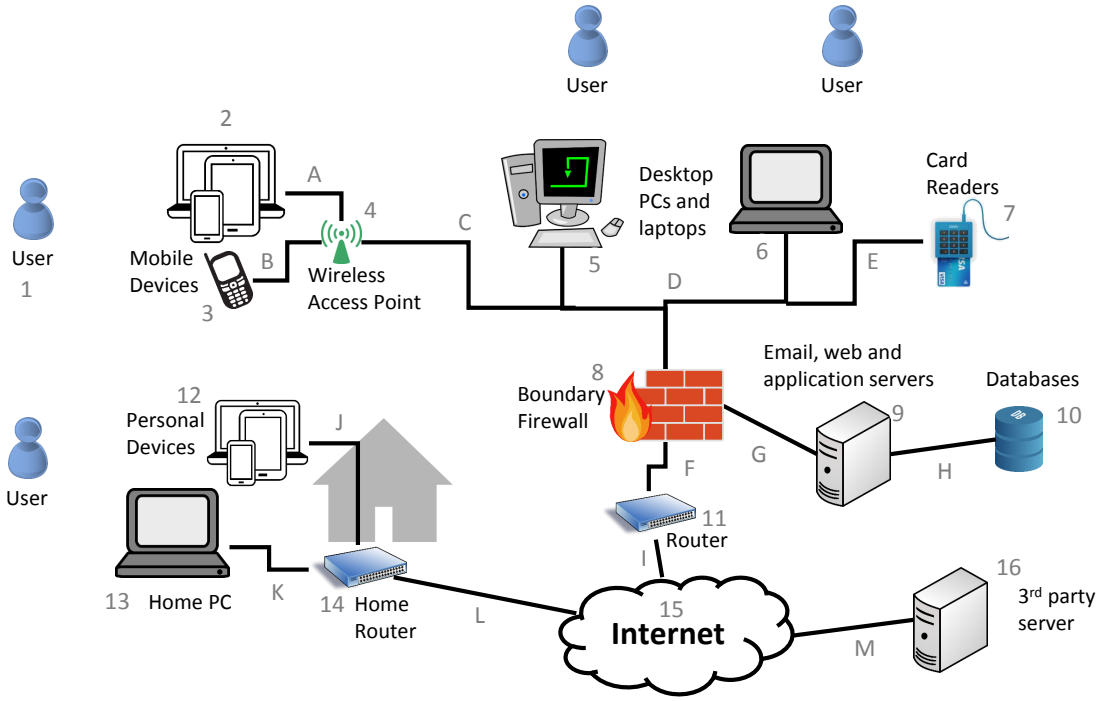
ii. `a != NULL && b != NULL && m == 0 && n == 0` [*3 marks*]

iii. `a != NULL && b != NULL && m == n` [*3 marks*]

iv. `a != NULL && b != NULL && m < size(a) && n < size(b)` [*3 marks*]

(d) Suggest a better condition than those shown in Part (c) above. Your solution should ensure that `vuln` is safe, and be as general as possible. Explain your solution. [*4 marks*]

3. The CEO of AcmeCo has been reading about how other companies have been compromised and is now nervous that his company may not be as secure as he would like. He has hired you as a security consultant to review AcmeCo's network setup. The following diagram shows the current network. Nodes have been labeled with numbers and edges on the graphic have been labeled with letters, please use these in your answers to refer to specific sections of the network.



(a) List three nodes (numbers) on the network that are beyond the control of AcmeCo's network administrator. [*1 mark*]

(b) The CEO is worried about ransomware causing damage to the network. Ransomware is a type of malicious software that infects computers typically through email attachments. It waits a bit and then encrypts all of the files that a computer account has access to, including network resources like databases. The malicious actors then ask for money to decrypt the files. If you installed a malware scanner on the boundary firewall (8) would it protect nodes 5-10 from ransomware? Explain. (You can assume that the malware scanner is 100% accurate.) [*4 marks*]

(c) Cyber Essentials has 5 requirements a company must follow in order to obtain the certification. One requirement is Malware Protection. Name one other requirement and give an example of how following that requirement would limit the damage caused by ransomware. [*3 marks*]

QUESTION CONTINUES ON NEXT PAGE

(d) The CEO tells you that they have budget to add one more firewall to the network. On what edge (letter) would you add the firewall? Explain why you would place it there. [*5 marks*]

(e) At what OSI network level should this new firewall operate? Explain your answer. [*3 marks*]

(f) When examining the network you find that the wireless access point (4) does not authenticate devices and you cannot tell which employee mobile devices 2 and 3 belong to. How might this impact the security property of Availability? [*3 marks*]

(g) The CEO would like you to add authentication to the wireless access point (4) so that only employees can connect to the WIFI. When you look on the access point you see that it is currently being used by all types of devices including: mobile phones, laptops, printers, and a Smart TV. Describe an authentication system that would work for all these devices and ensure the property of Accountability on the network. [*3 marks*]

(h) You inspect the boundary firewall and discover that the following commands were used to set it up:

```
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j ACCEPT
```

One of these commands is a very bad idea to run on a boundary firewall. Which line and why? [*3 marks*]