EECE 412, Fall 2008

Final Examination

Your Family name: _____

Your Given name: _____

Your student ID: _____

Name of your left neighbor: _____

Name of your right neighbor: _____

#	Points	Out of
1		7
2		5
3		27
4		2
5		12
6		5
7		10
TOTAL		68

Attention: If to answer any of the following questions, you need to make additional assumptions, do so but specify these assumptions explicitly by writing "Additional assumptions: …"

1. **Strength of your password.**
   a. **(1 point) Without revealing password you use for your Campus-wide Login (CWL), indicate below how many low case, capital case, digits, and special characters it has. this is just a sample password**

Number of alpha characters in your password	6
Number of special characters, e.g.,)[!(#@$%^&~;:",.+_-`}{]\/?, in your password	2
Number of numeric characters in your password	1
Total number of characters in your password	9

   b. **(2 points) Compute <u>theoretical</u> entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

Assumptions: 26*2= 52 alpha characters, 26 special characters, 10 numeric characters.

Theoretical entropy of the above password is $\ln_2((52+26+10)^9) = 9\ \ln_2(98) = 9*6.6 = 59.4 \approx 59$ bits

   c. **(2 points) Compute <u>effective</u> entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

Assumptions: 26*2= 52 alpha characters, 26 special characters, 10 numeric characters.

Effective entropy of the above password is $\ln_2(52^6*26^2*10) = 6\ \ln_2(52)+2\ \ln_2(26)+\ \ln_2(10)=6*5.7+2*4.7+3.3 = 46.9 \approx 47$ bits

d. (1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the theoretical entropy of your password. Explain your answer. Assume that your password hash is salted.

(2^59)/(2^21) = 2^38 seconds = 274,877,906,944/3600 = 76,354,974 hours = 3,181,457 days, which is little bit over 8,716 years.

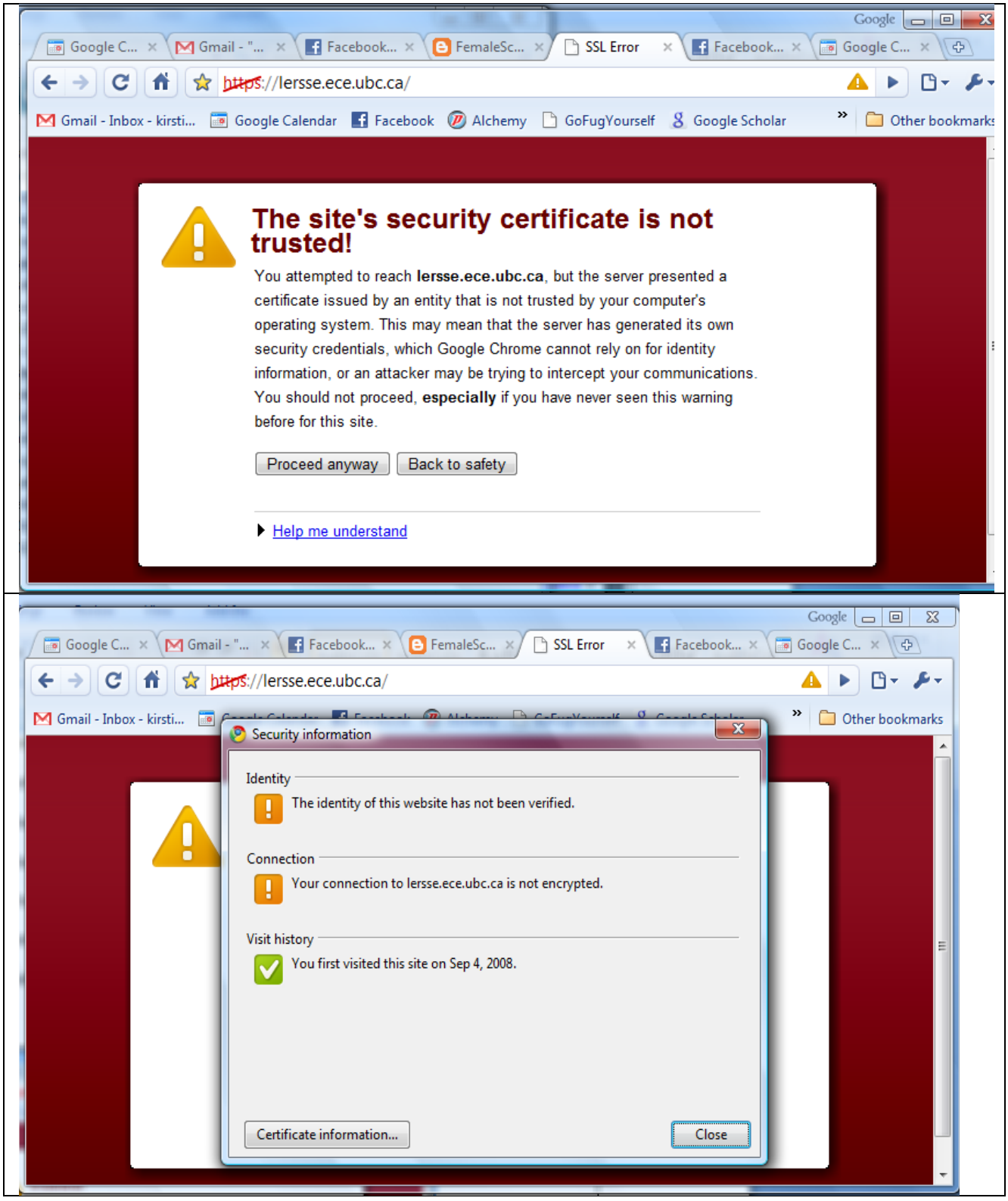
e. (1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the effective entropy of your password. Explain your answer. Assume that your password hash is salted.

(2^47)/(2^21) = 2^26 seconds = 67,108,864/3600 = 18,641 hours = 776 days, which is little bit over 2 years.

2. The Google Chrome browser provides several security cues and warnings to users. The top screenshot on the next page shows the warning if the site's security certificate is not trusted. The bottom screenshot shows the pop-up window if the triangle warning icon at the right side of the URL field is clicked.

   Evaluate the usability of the warning and security cues.

   Reminder: Why is it there? Do users notice it? Do they know what it means? Do they know what they are supposed to do when they see it? Will they actually do it? Will they keep doing it?


Google C...
Gmail - "...
Facebook...
FemaleSc...
SSL Error
Facebook...
Google C...
https://lersse.ece.ubc.ca/
Gmail - Inbox - kirsti...
Google Calendar
Facebook
Alchemy
GoFugYourself
Google Scholar
Other bookmarks
The site's security certificate is not trusted!
You attempted to reach lersse.ece.ubc.ca, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand
Security information
Identity
The identity of this website has not been verified.
Connection
Your connection to lersse.ece.ubc.ca is not encrypted.
Visit history
You first visited this site on Sep 4, 2008.
Certificate information...
Close

3. Handout contains a reproduction of new security-related features in MS Windows Vista.

a. **(7 points)** For each principle for designing secure systems, **put a checkmark** in the following table for those new features that **enable** or **follow** this principle.

Attention: The total number of points for this question will be determine using the following formula: $R - W$, where R is the number of right checkmarks and W is the number of wrong checkmarks.

	User Account Control	Bitlocker Drive Encryption	Windows Firewall	Windows Defender	Preventing exploits	Data Execution Prevention	Application isolation	Windows Service Hardening	Authentication and logon	Network Access Protection	x86-64 -specific features	Other features and changes
Least Privilege												
Fail-Safe Defaults												
Economy of Mechanism												
Complete Mediation												
Open Design												
Separation of Privilege												
Least Common Mechanism												
Psychological Acceptability												
Defense in depth												
Question assumptions												

b. **(10 points)** Write justification for the checkmarks in the above table.

c. **(10 points)** Explain which particular aspects of malware and corresponding protection and detection techniques are used in these new features.

4. For encrypting PIN, which mode of operation would be most appropriate? **Select one**.

   A. Electronic Code Book (ECB)
   B. Cipher Block Chaining (CBC)
   C. Output Feedback (OFB)
   D. Counter Encryption

   Answer: _____

5. Provide examples of measures for each type by writing them in the corresponding cells:

	Deterrent	**Preventive**	**Detective**	**Corrective**	**Recovery**	**Compensating**
Computer/ Technical						
Physical						

6. You are asked to select a hash function for implementing the following authentication scheme:
   1. The server and the client share a 16-byte key K.
   2. The server sends a randomly generated 16-byte challenge N to the client.
   3. The client sends back H = hash(N|K)
   4. Since the server knows N and K, it computes hash(N|K) and compares it with H received from the client.

   Prioritize the properties of hash functions in the order of their importance for the above authentication scheme, from "essential" to "least important". Explain why you ordered the properties in your way.

7. You are hired to advice Royal Bank of Canada on changing their process of developing online banking applications for RBC customers. After examining their process and talking to the developers, you realize that the developers are very experienced with financial and web applications but have next to nothing understanding of software security. Explain what the HSBC software engineering management can do to make the developed software more secure in general as well as specifically for each of the following stages in RBC's software development cycle:

   - Requirements definition

   - Design

- Implementation and testing

- Integration and system testing

- Operation and maintenance