Practice Exam Discussion COMP6[48]41

Q A.1.	Question	Discussion/Explanation
a)	*not really relevant*	
The largest of the Yahoo data breaches occurred in late 2013. According to the latest information which we know about it (based on a public announcement by Yahoo in late 2017) **how many user accounts were potentially affected by the breach?**		I am not sure why it choose A(Yuchen) https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804
A. 3 billion B. 1 billion C. 100 million D. 10 million E. 23		
Solution (highlight text)		AAAAAAAAAAAAAAAA
b)		
For this data breach Yahoo reported: "...the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include passwords in clear text" However, hackers were able to find many plain text passwords. A newspaper reporter is interested in how hackers could have found the plaintext passwords if Yahoo only stored hashed passwords and asks you if using MD5 was the problem. **What would have the impact on the ability of hackers to find plaintext passwords if Yahoo had used a more recent hash algorithm, SHA256, rather than MD5?** **Justify answer**		
Answers		
A. It would completely solve the problem		
B. It would largely, but not entirely, solve the problem		Id argue this, since SHA256 is unbroken, so it would be super difficult to use a rainbow table with SHA256, but not impossible - you can still create a rainbow table Assuming no salt used - wouldn't it be ezpz to figure out common passwords by using a rainbow table to precompute their hashes?

C. It would have a small impact, but the problem would remain largely unsolved	It would still be vulnerable to rainbow table attacks as it is still unsalted. However using a collision resistant algorithm rather than MD5 would add more work for the attacker. - correct me if Im wrong, but SHA256 is unbroken and therefore collision resistant, just not collision-proof
D. It would not be of any help whatsoever	

Q A.2.	Question	Discussion/Explanation
After the breach Yahoo considered transitioned to using the following password hashing scheme, rather than MD5, to hash its users' passwords. The proposed scheme involved giving each user a public "salt", and then encrypting a standard and publicly known IV using the user's password, and then encrypting that state using the user's salt, and then repeating those two steps over and over again, repeatedly re-encrypting the output of the previous encryption using the same password and the same salt over and over again, 2^n times. The salt, n, and the final hash output are stored. The password is not stored. When users supply a password to be validated the process is repeated for the supplied password and the output of the process is compared with the stored final hash output to see if they match. **Explain the likely purpose of the salt and the large number of repetitions.**		
Solution (highlight text)		
Salt		Prevent rainbow table attacks where the attacker compares the hash of a known string and the hashed password by making the hashed passwords unique.
Large number of repetitions		I guess it may extend the length of code to protect the collision attack?(Yuchen)
		Make an infeasible amount of work for the attacker, large number of repetitions are a form of key strengthening, which would increase the time it takes for the system to compute a single hash

Q A.3.	Question	Discussion/Explanation
In this question there are no marks for selecting a concept - marks are for the explanation you provide. The film The Usual Suspects provides an effective demonstration of which of the following security concepts: A Defence in depth B Dual Control systems C Man in The Middle D Type I / Type II error trade-off E Zero-Knowledge Protocols **Explain how it effectively demonstrates this concept.**		Did we watch this film? (The Usual Suspects) - no but the question should be similar for War Games Intro.
		War Games: - Defence in Depth - Dual Contrl Systems - Type 1/ Type 2 error trade-off

Q A.4.	Question	Discussion/Explanation
Recently there have been many widely publicised data breaches for example CBA, Equifax, and Ticketfly. Who else will be breached? Make a prediction: **Who do you predict is most likely to be in the news over the remainder of this year with a major and "unexpected" data breach?** *Who* *Justify your prediction* No marks for who, all marks for justify EXCEPT* a bonus 10 exam marks if your prediction comes true between after the exam and before the day that results are submitted. If it comes true this year but after marks are submitted then an ice cream for you! * Offer does not apply to employees or their families, or if you are involved in the breach. Accessories not included.		Focus on the recent attack for uni?(Yuchen) Some company's password breach/leak Justification: Most likely to make it onto the news because it is so big. Also may be a result of a phishing attack or some other form of social engineering. Once you gain access to one account, you basically have access to the whole company (depending on their security)

Q A.5.	Question	Discussion/Explanation
Give an example of recent widely reported news story		Did anyone find recent type 1

which has involved Type I and Type II errors, where the reportage predominantly focussed on one of the types of error and tended to overlook the other. *What was the news story?* *When was the news story?* If the news story was not so well known give some keywords so we can search for it on Google for partial marks: *Fall-back keywords (partial marks only if the story is on the first page of search results returned)* *Explain the error that was predominantly reported* *Explain the error that was not so predominantly reported*	and type 2 error news?

Q A.6.	Question	Discussion/Explanation
a)		
You are contacted by a reporter who writes for an education news blog, who is confused by the 2018 Dimension Data report. She asks you to simply and clearly explain: **What is supply chain risk and how can companies defend against it?**		
b)		
She also asks you to comment on how significant and accurate each of the following two claims quoted from the report is likely to be, and how significant they are for her readers: b) {{{ While Australia is a frequent target, it's also a major source of attacks. In the last year, 57% of cyberattacks in the Asia Pacific (APAC) region originated from Australia, the USA, and China. A staggering 66% of attacks on the financial sector in APAC originate from Australia. }}} Is this statistic important for me to tell my readers about? Highly Maybe Probably not		

How accurate is this claim likely to be? Likely Possible Unlikely **Justify these opinions** (all marks are for the justification)		
c)		
{{{ Figure 2: Types of attacks most commonly perpetrated in Australia ... Baiting / social engineering 0% }}} Is this statistic important for me to tell my readers about? Highly Maybe Probably not How accurate is this claim likely to be? Likely Possible Unlikely **Justify these opinions** (all marks are for the justification)		

Q A.7.	Question	Discussion/Explanation
a)		
You are a security engineer consulting to the government, who is alarmed by the 2018 Dimension Data report. The Office of the Minister for Education tells you that the minister wants to call you in an hour and ask you how seriously she should take the claims in the report that educational institutions are the top targets for cyber-attacks in Australia, why would criminals want to attack educational institutions, and what is the appropriate response for the government to make? What would you say? You'll only have 5 minutes on the phone with the minister to respond - so keep it short and clear, and make sure you justify your conclusions and recommendations. **How seriously should she should take the claims in the report that educational institutions are the top targets for**		

cyber-attacks in Australia?		
b)		
b) Why would attackers want to attack educational institutions?		
c)		
c) What is the appropriate response from the government?		

Q A.8.	Question	Discussion/Explanation
a)		
Attached are some pictures of the inside of a cheap 3-disc combination padlock. Suppose an attacker has a disassembled lock in their possession to study. They want to manipulate open another (non-disassembled) lock of identical make but with a different 3-digit combination - but they don't know the combination. Suppose that, like for Master combination padlocks, by putting tension on the shackle you can discover the first number of the combination, and further suppose that the lock automatically makes a sound when all 3 notches line up correctly (i.e. when the combination is correct.) If turning the wheel in one smooth motion up to one full revolution is 1 unit of work, **estimate how many bits of security the padlock provides.**		Assuming 10 digits per disc, We can get 10^2 possible permutations from the last two discs. Because you get the indication that it is unlocked automatically, it might be 10^1 on average since you get feedback. Logically you don't have to go through all the combinations so assuming it is asking on average how many bits you only need to try 5 numbers in the second and 5 in the third.
Solution		
Bits of security Briefly explain your reasoning		
b)		
The following sub-questions relate to a Yale style pin tumbler cylindrical lock of the quality and sort typical in residential house front door locks. Suppose an attacker was going to try to brute force over all possible keys by trying one key at a time, and suppose trying a key is one unit of work.		Depends how many pins

How many bits of security would the lock provide against this attack on <u>average</u>? Briefly explain your reasoning Bits of security	
Solution	
Bits of security Briefly explain your reasoning	
c)	
Suppose the lock could be bumped, and suppose each striking of the bump key is one unit of work. **How many bits of security would the lock provide against this attack on average?**	
Solution	
Bits of security Briefly explain your reasoning	
d) (2 Marks) Suppose the lock can be picked, and suppose lifting a pin smoothly up and down is one unit of work. **How many bits of security would the lock provide against this attack on average?**	
Solution	
Bits of security Briefly explain your reasoning	

Q A.9.	Question	Discussion/Explanation
This question involves devising a way to effectively and realistically perform social engineering on the UNSW Deputy Vice-Chancellor (Academic). You must not do anything illegal rude disrespectful or invasive in the real world in preparing for this question, or inconvenience or annoy or alarm him or anyone who works for or with him or knows him. Most importantly you are not to invade the privacy of his family or personal life in any way. You are restricted to looking at publicly available information and entirely passive methods.		

The exam question: **What is the name of the UNSW Deputy Vice Chancellor (Academic)?** In the DVC(A)'s office there is a displayed a framed photograph of a group of UNSW students. **Clearly explain a simple and safe social engineering strategy you yourself could follow to find out who is in that photo.** You'll be assessed on how realistic, simple, effective, non-risky, time consuming (sooner is better than later!) your method is and how you are likely to be able to learn the required information.	
Solutions	
VC(A): Merlin Crossley	

Q B.1.	Context	Discussion/Explanation
The union and the university have asked you as an independent expert to comment on the security of the online election process they follow for union votes. A vote (called a Protected Ballot) is called whenever the union is contemplating a strike - it is the first step needed under law before the union can eventually strike. In general, the university does not want the union to strike and would always welcome the No votes winning, and the union organisation is keen to be permitted to strike and would always welcome the Yes votes winning. The software vendor (who also runs the election) explains that their electronic voting system is secret valuable intellectual property and the they will only let you view the source code and/or operation of the system if you sign an extremely restrictive Non-Disclosure Agreement (NDA) which would then require you to show them in advance anything you might write or say about the system and means that you would require their explicit written consent before you can discuss or publish anything about the system. There is nothing in the contracts that the union and the university have with the vendor which prevents the vendor from imposing this secrecy requirement on you.		

The only public data about the system you can obtain is an email (reproduced below) sent to a member of the union for the previous protected ballot - advising them of the need to vote and giving instructions on how they do that. {{ PROTECTED ACTION BALLOT OF MEMBERS OF THE NATIONAL TERTIARY EDUCATION UNION WHO ARE EMPLOYEES OF THE UNIVERSITY OF NEW SOUTH WALES DESCRIBED IN ORDER (B2018/334) PROTECTED ACTION BALLOT - VOTING INSTRUCTIONS Online internet voting in this Protected Action Ballot OPENS at 9:00am AEST on Wednesday 16 May, 2018 and CLOSES at 10:00am AEST on Thursday 24 May, 2018. To cast your vote using the Internet: Go to the URL: https://evote.electionz.com/e/NTEU by either clicking the link or copying the link into your internet browser's address area (usually top left of screen). You will then be presented with a screen that allows you to "Login" by entering your NTEU Membership Number and a four (4) digit random personal Password. If your membership number has any zeros at the beginning, these will need to be omitted. Your Password is 1337 You will then be asked to cast your vote. You may indicate your preference by marking one (1) of the following options: "YES" - (I approve of this action) "NO" - (I do not approve of this action) To vote "YES", click in the "YES" box; or To vote "NO", click in the "NO" box. Click the "Next" button. You will then be asked to confirm your vote. To confirm your vote selection(s), click the "Submit" button; or To amend your vote selection(s), click the "Back" button and then change your vote.	

Click the Ãcâ‚¬Å"Close" button to end your voting session and return to the "Welcome" screen. Once you have confirmed your vote selection(s), your Password will be "consumed" and you will not be able to vote again. Your vote selections will be electronically detached from your record immediately upon confirmation so your vote is guaranteed to be completely secret and confidential. Australian Election Company Ballot Agent Email: help@austelection.com or jkidz@austelection.com Phone: 1800 124 421 }}} Write brief responses to the questions below based on the email above from the previous ballot, and making any other reasonable assumptions needed.	
Question	
Would you sign the Non-Disclosure Agreement? **Briefly justify your answer**	
Answers	
What are your four main concerns about this electronic voting system? Rank them with the main concern first down to the least main concern last.	
Answers	
What are the three most significant ways it could be attacked or fail?	
Answers	

Q B.2.	Context	Discussion/Explanation
The following question refers to the film "The Towering Inferno" and the city and the time and the situations depicted in the film.		

The Towering Inferno was made in 68 (4.1 stars on Amazon). However it demonstrates vulnerabilities still relevant today. At the end of the film the Fireman has the following conversation with the Architect: {{{ Fireman: And I'll keep eating smoke and bringing out bodies... ...until somebody asks us... ...how to build them. Architect: Okay. I'm asking. Fireman: You know where to reach me. So long, Architect. }}}	
Question	
Suppose you are the Fireman. The Architect comes to you asking for your advice. **List and briefly justify the main four weaknesses in the design of the tower** revealed by the events in the film and make recommendations for how to design safer towers in the future.	
Answers	
The Mayor comes to you asking for your advice. **List the main four actions he should take to ensure that citizens in the city are safer from tower fires.**	
Answers	

Q B.3.2	Context	Discussion/Explanation

On the Python mailing list Paul Rubin shared code for a general purpose cyptographic library he had written. It generated some discussion. Draft brief responses to the two questions asked below (Edited extract from http://mail.python.org/pipermail/python-list/2002-April/100319.html): {{{ Richard Parker <richard@electrophobia.com> writes: > I just took a quick look at your Python code. I'd encourage you to not use > the secret prefix method to construct a MAC from a hash function, i.e. > MAC(x) = H(K || x). This method is generally considered to be insecure. > Use the HMAC construction instead. }}}	
Question	
Could you explain the problem here and how it is solved by HMAC?	
Answers	
Do you think [this insecurity] matters in practice, given that this is running in an interpreted language on a general purpose PC? Practical attacks probably involve computer viruses peeking at memory rather than cryptanalysing SHA.	
Answers	