FINAL EXAM (TOTAL OF 83 POINTS)
Deadline:Tuesday, December 15, 2020

Instructions:

- Do the questions individually.
- Make one PDF format file for writing your analysis/results in the format <RollNo>_final.pdf
- Do not zip your submissions.
- If the solution requires you to use paper, paste a good quality image of the solution in the document that you are submitting.
- Queries, if any can be posted on google classroom.
- Note: Answer the questions in bullet points. Keep your responses crisp and to the point.

PART - I

1. What are Westin's four states of privacy? How is "Reserve" property preserved on Twitter? Who among fundamentalist, pragmatist and unconcerned would be concerned about "Reserve" property? Explain.

   [**2 + 1 + 1 = 4 marks**]

2. Android app permission mechanism has moved from opt-out to opt-in. But, when we sign-up for Facebook there is a single Terms and Conditions page. To tweak any of the default settings we should visit the settings page. In FCS we studied how effective embedded training could be. Design an opt-in mechanism to manage privacy on Facebook. Mention at least 4 prompts that you would want Facebook to display.

   [**8 marks**]

3. A lot of discussion in the course is around "usable security". While eXpandable grid is a step towards making security more accessible, it is not perfect for a scenario with less number of permissions. Given a scenario where there are only 3 permissions [read, write, delete] and 2

levels [yes or no] can you think of a better way of representing the eXpandable grid?

[**5 marks**]

4. What is federated identity management? How is it achieved by google accounts? Does “sign in with google” on a third party website qualify as federated identity?

[**5 marks**]

5. Differentiate between the utility of memory forensics and server logs?

[**5 marks**]

6. You are the founder of a startup “amazeon.in” an online shopping website competing with the popular “flipkart.com”, amazeon is doing great and you are looking for expansion. What parties in the security business are liable to you? Customers and the Govt. of India expect some primary responsibilities with the data, list few responsibilities, and how are you liable to your customers?

[**5 marks**]

7. Personally identifiable information is data using which one can identify someone uniquely. Few examples of personally identifiable information are Aadhar Card and passport number. On a scale of 1 to 10, one being least sensitive and 10 being personally identifiable information rank each of the following, and give a reason why?
    A. Facebook username
    B. Gmail ID
    C. College ID card number
    D. Information about the bus number you take
    E. Your percentile in the last semester

[**5 marks**]

8. “Do not sell my personal information” is often overlooked by users as there is no icon associated with it. The State of California has now

proposed an official icon to include next to that new opt-out text. Read about the proposal here.

a. From what you have learned in FCS class. Comment on “privacy is not easy to visualize”. Why?
b. Give 2 reasons why this privacy icon initiative will work and 2 reasons why this will not work. [Note: Do not restrict your reasons to a single concept like usability.]

[4 + 4 = 8 marks]

PART - II

1. Consider the following cryptography library's API:

[6 * 4 = 24 marks]

Variable name	**Meaning**
m	Message in plain text
private_alice	Alice's private key. Only available with Alice.
public_alice	Alice's public key. Everyone knows Alice's public key.
private_bob	Bob's private key. Only available with Bob.
public_bob	Bob's public key. Everyone knows Bob's public key.
sym	A symmetric key
encrypt(m, k)	A function that encrypts 'm' using the key 'k' and returns a ciphertext 'c'. Ex: DSA, AES
concat(a, b)	Concatenates a and b. *Assume* that the receiving party has access to a function that splits a concatenated message perfectly, hence they know how to unambiguously identify a and b.
hash(m)	A generic hash function that takes 'm' as input and gives the hash 'h' as output. Ex: SHA-256 A hash is used to verify if the

	received message is same as the one sent to them.
sign(m, k)	A signature function that takes message ‘m’ and key ‘k’ and returns a signed message ‘m’. Signatures are signed by private keys, and a public key is used to verify the signature.

Alice is sending the following messages to Bob in the specified order. Is it possible for Bob to decrypt the message? If Bob can successfully decrypt a message comment about: 1) confidentiality 2) non-repudiability 3) steps to decrypt the message

a. encrypt(concat(m, hash(m)), public_alice)
b. encrypt(concat(m, hash(m)), public_bob)
c. encrypt(m, public_bob)
   sign(hash(m), private_alice)
d. encrypt(m, public_bob) ; sign(hash(m), private_bob)
e. encrypt(sym, public_alice) ; encrypt(sym, public_bob) ; encrypt(m,sym)
f. encrypt(sym_1, public_alice)
   encrypt(sym_1, public_bob)
   encrypt(sym_2, public_alice)
   encrypt(sym_2, public_bob)
   encrypt(encrypt(m, sym_2), sym_1)
   sign(sym_1, private_alice)
   sign(sym_2, private_alice)

PART - III

Answer the following in one line:

[7 * 2 = 14 marks]

1. Among signature based malware detection and anomaly based malware detection which technique can handle novel attacks? Why?
2. When using a system like Tor, to ensure privacy you must route your DNS traffic through the system. Why?
3. Should a company notify security breach if the stolen data is encrypted? Why?
4. How do computer viruses use encryption to their advantage?
5. You lost your locked mobile phone, what are the privacy concerns from the loss if your phone is password protected?
6. Can a malware cause hardware damage? How?
7. What is a fail-safe default? Among opt-in and opt-out which mechanism qualifies as fail-safe default?