Dalton Murray

Systems Analysis and Design

INT 6123 – Systems Analysis and Design

Dr. Andrew Makar

October 15, 2023

**IA #6 Spring Breaks R Us**

**Question 1 – For which subsystem(s) is(are) integrity and security controls most important? Why?**

The subsystems we are provided are as follows: resort relations, student booking, accounting and finance, and social networking (Satzinger et al., 2016. p. 182). In an ideal world, all four of these subsystems would be considered the most important as they all have justifications why ensuring integrity exists and security controls are in place are needed. However, in my personal opinion of the order of importance is as follows: Accounting and finance, student booking, social networking, and then resort relations. Ideally, however, all of these systems would have the same levels of integrity and security controls as there is in most cases no realistic explanation to not have them as their system (if made within the last decade) should not have any performance impacts by them. In fact, it is possible that with the right integrity levels, ensuring incorrect data is removed or not inputted in the first place, or otherwise ensuring that the data is inputted correctly could have beneficial effects than not checking it.

Accounting and finance: For the accounting and finance subsystem it is likely to be handling the most sensitive data out of the four listed subsystems. It will be handling and storing people’s credit cards, debit cards, and other bank information which are all higher valued targets. It will also be having to have stored other personally identifiable information (PII) such as their full name, address, their email address, phone number, and maybe even their passport number or their driver’s license number for safety and security purposes. All of these listed should have high levels of integrity ensured and security controls in place in order to limit who can access the data and what can even be viewed as some things should not be able to be clearly (plaintext) viewed.

Student booking: Student booking should be also a highly valued subsystem as it will also handle the student’s personal data which gets sent to the accounting and finance systems, it will likely contain all of the data which will be passed through to the accounting and finance subsystem like their full name, phone number, credit card, debit card, other bank information, email address, phone number, and actual address. However, though the actual banking information is only temporarily stored in student booking before going into accounting and finance their regular profile such as their full name, phone number are still stored here which accounting and finance accesses, thus in the long-term it makes this subsystem less valuable than the accounting and finance subsystem.

Social networking: The social networking subsystem will only be storing photos of locations, posts and comments, and messages between users and in groups. This system should still have a level of integrity and security in it, it is, however, less important than the student booking and accounting and finance subsystems as the information stored is less of a threat or less valuable if it were to be leaked out somehow.

Resort relations: The resort relations subsystem will only be handling contact between the resort and SBRU and the people booking. It will have access to things such as the student booking subsystem in order to gain contact details of the people, however, no data except messages will be stored here.

**Question 2 – What data should be encrypted during transmission through resort wireless networks to SBRU systems? Does your answer change if students interact with SBRU systems using a cell phone (directly, or as a cellular modem)?**

With all four of the subsystems or even other subsystems not listed or other data not listed in an ideal system all of the data should be encrypted while in transmission, at least in some form. Since we are using 3 web apps for 3 of the subsystems and a built-in messaging system for the other there should be at minimum basic levels of security (SSL/TLS certificate). Ideally, all subsystems in transmission will also have other levels of security by encryption or hashing until it reaches the actual subsystem where it can then be unencrypted and unhashed. However, some things, even upon storage should not be unhashed such as people’s passwords. At minimum, passwords should always be hashed, and stored hashed and should not be viewable by anyone at the resort or SBRU in plaintext. The systems and subsystems themselves are the only thing which should be able to compare the person’s login with the stored hash value and determine if it is correct or not. As well, at minimum, payment and banking details should be hashed or encrypted in some way during transmission (on top of SSL/TLS certificates). However, in an even more ideal system SBRU and the resorts will not have any direct contact with payment information and verification and it would all get sent through a third party for processing (Stripe, or PayPal as an example). For the messaging system, it should be at minimum have the users end encrypted to the system, ideally it would be end-to-end encrypted.

I find it difficult to justify not having the most secure possible system in the modern world, as realistically if there is a performance impact it is minimum (unless you are Google or Microsoft, however, they’ll have the processing power anyways to do it) and if you weigh having even in the slowest systems a few second delay versus having someone’s bank account details leaked I would say that I would wait the extra few seconds.

My answer does not change if the people are interacting with SBRU’s system using a cell phone/on a mobile device as I have already listed what I believe to be the minimum necessary requirements, SSL/TLS certifications, password hashing, messaging encryption, bank information encryption. With today’s phones there is not a real impact on performance with this minimum level of security. The only point in which I think my answer changes has to deal with banking and payment information. Today, digital banking is extremely common with phones, and by this, I mean sending payments with a built-in system such as using Apple’s methods to send money or by using Samsung or Google Pay. If the person were using one of these methods to pay, I still believe that it should be encrypted, however, the system is just slightly different than directly inputting a credit card or debit card number.

**References**

Satzinger, J. W., Jackson, R. B., & Burd, S. D. (2016). Systems analysis and design in a Changing World (7e ed.). Cengage Learning.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

*Dalton Murray*