**Threat Model Report**

Threat Model Report

In your introduction describe the reason for this report such as the following: You are a cyber threat analyst for a mobile applications company. You have been assigned lead of a mobile application security project and have been tasked to prepare a report of threat models for this technology. This threat model report will discuss mobile application architecture, mobile data, threat agent identification, methods of attack, and possible controls. It is intended to provide senior management a greater understanding of mobile application security and its implementation.

Mobile Application Architecture

Architecture Considerations

Discuss architecture considerations for mobile applications and architecture. What is the design of the architecture (network infrastructure, web services, trust boundaries, third-party APIs, etc.)?

Mobile Application

Select and describe a mobile application. What are the common hardware components? What are the authentication specifics? Which architecture considerations are relevant to your mobile application you chose?

What should or shouldn't the app do? Describe device-specific features used by the application, wireless transmission protocols, data transmission mediums, interaction with hardware components, and other applications.

Mobile Application Security

Identify the needs and requirements for application security, computing security, and device management and security. Describe the operational environment and use cases, and identify the operating system security and enclave/computing environment security concerns, if there are any. This can be fictional or modeled after a real-world application.

Mobile Data

Business Requirements

Define what purpose the mobile app serves from a business perspective. In LEO Step 2, you will find a lengthy list of questions – consider them as you define this area as well as your data requirements below.

Data

Define what data the app will store, transmit, and receive. Include a data flow diagram to determine exactly how data is handled and managed by the application. You can use fictional information or model it after a real-world application. Please put your Figures at the bottom of this report in the “Figures” section. Refer to Figure X (assign a number) and discuss the data flow.

Threat Agent Identification

Discuss common security threats to the mobile application. Also identify the threat agents. Examples provided in LEO Step 3 include reverse engineering, weak passwords, outdated encryption algorithms, and lack of multifactor authentication. Please be sure to research others that may be more significant and relevant to the mobile application you choose.

In a separate paragraph discuss the process for defining what threats apply to your mobile application. Your LEO tutorials talks about Open Web Application Security Project (OWASP) as a resource, but again please be sure to research others – the idea here is to not just discuss threat but the process behind determining what those threats are.

**Methods of Attack**

Identify and discuss different methods an attacker can use to reach the data. This data can be sensitive information to the device or something sensitive to the app itself. Provide senior management with an understanding of the possible methods of attack of your selected mobile application.

**Possible Controls**

Discuss the controls to prevent attacks. In LEO Step 6, you will find a lengthy list of questions – consider them as you define this area.

Conclusion

This threat model report covered mobile application architecture, mobile data, threat agent identification, methods of attack, and possible controls. From here discuss your overall conclusions and recommendations…

References

Aleisa, N. (2015). A comparison of the 3DES and AES encryption standards. *International Journal of Security and Its Applications* 9(7). doi: 10.14257/ijsia.2015.9.7.21

Defense Human Resource Activity. (n.d.). *Common Access Card (CAC) Security*. Retrieved from http://cac.mil/common-access-card/cac-security

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Computer Security: Guide to integrating forensic techniques into incident response: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-86). Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12. Retrieved from http://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital\_forensic.pdf

Tables

Table 1

*Demographic Data on All 178 Respondents*

|  |  |  |  |
| --- | --- | --- | --- |
| Population Description | Male | Female | Total |
| Age ≤ 29 Years  | (*N* = 23) 20.7% | (*N* = 10) 14.9% | (*N* = 33) 18.5% |
| Age 30-45 Years  | (*N* = 34) 30.6% | (*N* = 29) 43.3% | (*N* = 63) 35.3% |
| Age 46-59 Years  | (*N* = 44) 39.6% | (*N* = 24) 35.8% | (*N* = 68) 38.2% |
| Age 60 Years or older  | (*N* = 10) 09.0% | (*N* = 04) 06.0% | (*N* = 14) 07.9% |
| Experience 05 Years Exact  | (*N* = 15) 13.5% | (*N* = 10) 14.9% | (*N* = 25) 14.0% |
| Experience 06-10 Years  | (*N* = 30) 27.0% | (*N* = 21) 31.3% | (*N* = 51) 28.6% |
| Experience 11-19 Years  | (*N* = 38) 34.2% | (*N* = 26) 38.8% | (*N* = 64) 35.9% |
| Experience ≥ 20 Years  | (*N* = 28) 25.2% | (*N* = 10) 14.9% | (*N* = 38) 21.3% |

Table 2

*Measures of Central Tendency and Variation*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | *N*Statistic | *R*Statistic | *M*Statistic | *SD*Statistic | VarianceStatistic | SkewnessStatistic | SkewnessStd. Error |
| Gender  | 178 | 1 | 1.38 | .486 | .236 | .515 | .182 |
| Age | 178 | 3 | 2.35 | .872 | .761 | -.034 | .182 |
| Experience  | 178 | 3 | 2.65 | .970 | .942 | -.176 | .182 |
| Valid *N*  | 178 |  |  |  |  |  |  |

Figures



*Figure 1.* Hospital Information Support System.