Rubric for Final Project

Course: Network Security (E21.285202U003.A)

Criteria	**Minimum effort**	**Low effort**	**Medium effort**	**Complete task**
Foundations	Justify the selection of the application	Define the expected security properties	Document the attack surface in which the analysis is performed	Complete the threat model by documenting adversarial capabilities
Software Security	Attempt to decompile the application using relevant tools: APK-Tool, dex2jar, JG-GUI, JDAX.	Document presence of obfuscation and general readability of decompiled code.	Perform manual analysis of the decompile code by searching keywords or security hot-spots	Perform dynamic/static analysis of the decompiled code using tools like MobSF and document the results
Network Security	Sniff traffic to find hostnames and document the server-side TLS configuration using Qualis SSL Labs	Perform MITM attacks using the relevant tools: mitmprox, sslsplit or BurpSuite.	Perform MITM attacks with a malicious root certificate installed. The tool apk-mitm helps with recent Android versions	If MITM is successful, analyze the nature of captured traffic. Otherwise, document why MITM failed (pinning or CT support).
Authentication	Describe the need for authentication in the application.	Describe what authentication mechanisms are in place (both user and device-oriented)	Analyze the security of the implemented authentication mechanisms and workflows (password resuse/reset)	Suggest improvements to the deployed authentication mechanisms.

Criteria	Minimum effort	Low effort	Medium effort	Complete task
Privacy	Describe the nature of the data collected by the application	Describe the Android permissions requested by the application	Characterize integration with external services, such as social networks, and potential privacy impact	Describe relevant trackers embedded in the application and their role, or privacy features if they exist

Overall Score

Level 1	Level 2	Level 3	Level 4