Executive Summary

Business Domain	Type of testing required	Mobile Platform	Total Duration	Region
Communications	Security Testing	Android & iOS	15 days	Bangkok, Thailand

Client

Our client, based out of Thailand, builds tools that unlock the full potential of mobile messaging in the workplace. They develop powerful and customizable mobile communication platform for large companies.

Our client aspires to unlock the true potential of cloud and mobile and revolutionize the way people work that would result in enhanced efficiency and productivity of the workforce. The app has the potential to transform the workplace in term of seamless communications, faster decision making, streamlined escalation, instant problem solving amongst staff, timely status updates, share files, send and receive e-Forms and e-Reports, etc.

The app is capable of building customised forms, tracking and approving tasks in real-time, setting performance goals and sharing knowledge.

Business Context

As the mobile app is an enterprise business communication tool, security was of paramount importance. The priority areas were to test the authentication bypass (username/password) and injection flaws which generally indicate how efficiently the app responds to the user query. Hence, all the messages and files had to be encrypted, both in-transit and at-rest via military-grade encryption. Simply put, the data had to be secure with integrity maintained all through.

TestOnDemand Solution

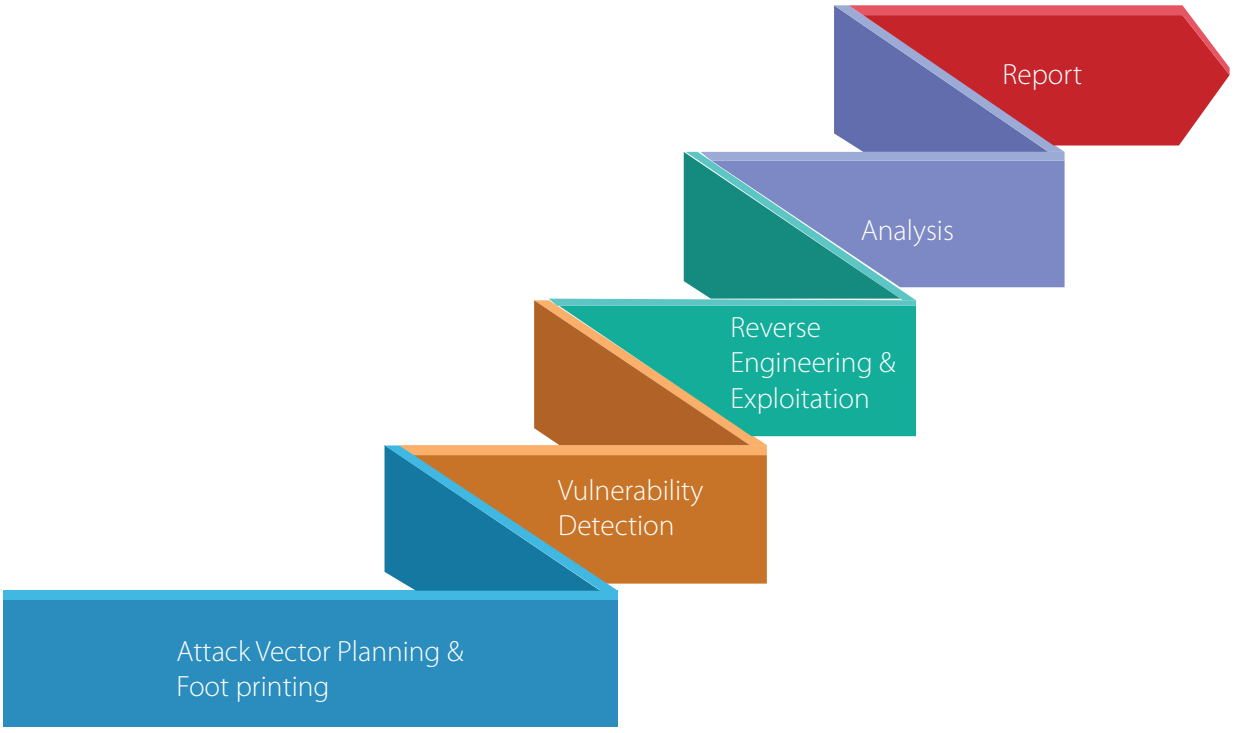
TestOnDemand team identified critical vulnerabilities in the application through custom security frameworks and in-house developed tools that could have otherwise led to data leakage and compromised integrity. Using TestOnDemand 5-step approach, the team performed a complete assessment of the mobile application using checklists that incorporated guidelines from standards such as OWASP Top 10, NIST, etc., as well as published zero day vulnerabilities.

The high-level sequence of activities included the following tests:

Fundamental tests like Authentication, Session management, Input validation, Error handling, etc. **Technology tests** like Analyzing the log files, Local data storage, Reverse engineering the app code; **Business login tests** like Privilege escalation, analyzing application components, etc. were performed on the application.

The team also executed the tests keeping in mind the hacker's perspective, which gave it a unique proposition of both the structured testing methodology and the hacker's view.

A Daily summary of progress along with a detailed Weekly Report kept the client informed of TestOnDemand team's activities and results. A Summary report was shared after the vulnerabilities were identified. A Final report was also generated with comprehensive information on the security issues found.



Engagement Metrics

- Number of Days – 15 days
- Location (work location) – TestOnDemand Office
- Test Areas – Mobile application
- Number of rounds – 2

Findings/Error Matrix

- 17 Vulnerabilities were identified
- 12 Vulnerabilities had a CVSS score of 8 and above (on a scale of 1-10)

Key Outcomes

- On testing the app, the Overall Security Threat profile was designated as "High risk" meaning there was a high probability of security issues in the application
- A detailed list of recommendations was shared that could help patch each Vulnerability type
- The Client was able to remediate the critical vulnerabilities which could have otherwise helped an attacker to trick the victim by making calls to the defined numbers as well as bypass the authentication process
- The Client also fixed the local storage issues in the app, which could have revealed sensitive user informa tion to hackers