Initial Plan - Security Analysis in SMS-based Applications

Author: Finn Milliner - 1814916
Project Supervisor: Neetesh Saxena

CM2303
One Semester Individual Project
40 credits

Project Description

With growing reliance on digital devices in our society, especially smartphones, it is more important than ever to be aware of how secure our data and our devices are.

SMS is a critical component of the security infrastructure for many applications and the usage stats for the service are extremely high; recent research found that mobile subscribers in the UK alone sent over 65 billion SMS and MMS messages in 2019 [1] and over 350 billion text messages are sent each month globally as of 2014 [2].

With its popularity, attention is drawn to exploiting the wide number of users the service can reach for scammers, hackers and more who can use the service in a few different ways to gain data, access or money from unsuspecting victims. “Because the messages are stored on these systems longer than necessary, it increases the window of vulnerability through which the hacker can attack. Rather than having to defend a system for a few seconds to prevent a hacker from stealing a message, it needs to be protected for days, weeks, months.” [3] says Wickr CTO Cristopher Howell in reference to the virtual path our SMS messages take between sender and receiver, highlighting the potential weak points in a system that is used by so many but understood by very few.

Analysing just how secure it is to use and finding potential alternatives or countermeasures to exploits could potentially save many companies and individuals from having data stolen or compromised, or even just raise awareness to everyday users who are unaware of the associated risks.

This project aims to analyse the security level of the applications and services that are either based on Short Message Service (SMS) (such as SMS-based mobile-banking) or do use SMS to provide some sort of service, such as in One-time Password (OTP).

Said analysis includes researching how the applications function and how the structure of SMS could be exploited as well as identifying any known security flaws that exist.

The outcome will reflect research-based advantages and limitations with quantitative information about the security level of the application and services used. The work will also recommend countermeasures to address the existing/found security issues. Another outcome could be the proposal of potential ideas to provide better alternatives to SMS or fixes to the identified issues through the research completed during the analysis.

Aims and Objectives

1. *Outline key security flaws or exploits in SMS-based applications or services which use SMS.*
    a. *Identify and detail a selection of SMS-based applications or services.*
    b. *Analyse their use and structure.*
    c. *Research into any large-scale events of security compromise relating to SMS*
    d. *Outline related security flaws and exploits.*

2. *Identify and explain both the advantages and limitations of using SMS in providing a service, providing quantitative data on the level of security.*
    a. *Research limitations and advantages of SMS as a service with relation to why it is so popular.*
    b. *Provide quantitative data on the security of SMS.*
    c. *Analyse and document the provided data and how it is applied to real world context.*

3. *Recommend countermeasures or alternatives to address the issues found.*
    a. *Reflect on whether SMS is indeed secure enough for use or if an alternative must be found with justification.*
    b. *Find existing alternative solutions which are similar enough to replace SMS and explain how they are appropriate.*
    c. *Hypothesise potential ideas for non-existing solutions which may be possible.*
    d. *Suggest how these possible solutions could be developed and provide an analysis on why they are beneficial.*

Ethics

I do not need to apply for any ethics assessments as the data I will be using throughout the project's lifetime will be gathered from online repositories and gateways and I will not be collecting PII from any humans/users.

Work Plan

Throughout the whole of my project I intend to meet with my supervisor every week to discuss the progress of the project and review the work I have completed and what I have to aim for next. I plan to regularly update and check off each step week by week to ensure I am keeping up with my planned schedule and allowing for any unforeseen changes in the project as time goes on. As I am completing a research based project and providing an analysis, writing my report will be something I also continue week to week as it will happen intrinsically as I complete my various researches and documentation.

Attached as a supporting document is my Gantt Chart which is labelled with numbered tasks, each task description is shown in the week-by-week breakdown listed below.

Major Milestones

1. Select an appropriate number of SMS based applications to analyse so there is sufficient information to work with.

2. Provide a detailed discussion on all of the selected applications security flaws.
3. Find a source for the quantitative data on SMS security.
4. Find existing alternatives or solutions for SMS weaknesses.
5. Hypothesise one or more potential non-existing solutions/alternatives for SMS.
6. Finish first draft of write-up.

Week 1 - 7/02/22

- Task 1 - Hand in initial report.
- Task 2 - Read more about the background of SMS research and related papers.

Week 2 - 14/02/22

- Task 3 - Research the most popular or widely used SMS applications.

Week 3 - 21/02/22

- Task 4 - Research how much information is available for each SMS service.
- Task 5 - Provide concrete selection of chosen SMS services for a deeper analysis.

Week 4 - 28/02/22

- Task 6 - Read up and make notes on any large scale or well known events of SMS security being breached or abused.
- Task 7 - Analyse and document the security flaws and exploits found relating to my chosen SMS services.

Week 5 - 7/03/22

- Task 8 - Research limitations and advantages of SMS.

Week 6 - 14/03/22

- Task 9 - Research and document why SMS is so widely used, considering socioeconomic factors.

Week 7 - 21/03/22

- Task 10 - Search for a source to provide data which gives quantitative context to the security of SMS.

Week 8 - 28/03/22

- Task 11 - Analyse the data acquired from the source in order to associate with real world context and the meaning behind the data itself.

Week 9 - 4/04/22

- Task 12 - Reflect on how SMS is used and provide write up on if it is appropriate for use or if it is more suitable to be replaced and why.

Week 10 - 11/04/22

- Task 13 - Find existing alternative solutions which are similar enough to replace SMS and explain how they are appropriate, providing a full analysis into how suitable they are.

Week 11 - 18/04/22

- Task 14 - Hypothesise potential ideas for non-existing solutions which may be possible.
- Task 15 - Research into the future of mobile communications; protocols, applications, methods etc.

Week 12 - 25/04/22

- Task 16 - Suggest how these possible solutions could be developed and provide an analysis on why they are beneficial.
- Task 17 - Ensure all research which was used is cited and included in my final analysis on SMS security.
- Task 18 - Create the first full draft of the report.

Week 13 - 02/05/22

- Task 19 - Compare documentation and write up as well as research conducted throughout the whole project to verify all aims and goals have been achieved.
- Task 20 - Penultimate meeting with supervisor.
- Task 21 - Create second draft of the report

Week 14 - 09/05/22

- Task 22 - Final meeting with supervisor before hand-in.
- Task 23 - Spelling and grammar checking for the final iteration of the report, checking all references are cited correctly.

Final Report Due - 13/05/22

- Final hand in by 23:00.

References

[1] Aaryaman Aashind, Jan 2022. *Texting Statistics UK [2022 Edition]*. Available: https://cybercrew.uk/blog/texting-statistics-uk/ [accessed 03/02/22]

[2] The Open University, 2014. *Text Messaging Usage Statistics*. Available: https://www.openuniversity.edu/news/news/2014-text-messaging-usage-statistics [accessed 03/02/22]

[3] Wickr CTO Cristopher Howell, Nov 2019. *How SMS Works and Why You Shouldn't Use It Anymore*. Available: https://www.popularmechanics.com/technology/security/a29789903/what-is-sms/ [accessed 03/02/22]