SNOW CRASH

Using QR codes as a means of cyber attack

Final Report

2020-04-30

Brendan D. Burke

C00232110@itcarlow.ie

Contents

Introduction 2

Objectives 2

Section 1, Snow Crash Tool 2

Section 2, Phishing Attack 2

Section 2, WiFi Access Point Attack 3

Section 2, MMI code Attack 3

Section 3, QR code malware 3

Problems Encountered 4

Time 4

New technologies 4

Documentation 4

Android 4

Learning Outcomes 4

Shell 4

Wireless Hacking 5

QR codes 5

Videos 5

What would be Done Differently 5

Research 5

MMI Codes 5

Phishing 5

Conclusion 6

Acknowledgements 6

Plagiarism Declaration 6

Introduction

The Snow Crash project consists of a collection of attacks utilising QR code technology. This document is the final report of how well the project fared and how many of the project goals were realised.

Objectives

Section 1, Snow Crash Tool

Create malicious QR codes and place them in appropriate folders.	Achieved
Successfully use custom wordlists used for QR creation.	Achieved
Provide a comprehensive set of inbuilt wordlists.	Achieved
Create QR files from binary executables.	Achieved
Provide a means for a slideshow of QR codes for hardware cameras.	Achieved
Run tests against ZBar QR reading library and log the output.	Achieved
Create logfiles and provide feedback and debug information on how the parser handled the malicious QR code.	Achieved
Provide the option for incorporating other libraries like ZXing or custom user libraries.	Not Achieved
Provide a means for creating other types of 2D barcodes e.g. Aztec codes.	Not Achieved
Provide a means of placing 2D barcodes inside one another for barcode inception style attacks described by (Dabrowski, et al., 2014).	Not Achieved
Provide a means of creating artistic/stylish QR codes and accompanying posters with text.	Not Achieved

Section 2, Phishing Attack

QR code works as intended and directs victim to phishing site.	Achieved
URL loads with minimal or no warnings.	Achieved
URL is not blocked by Google Safe Browsing API.	Achieved
Sensitive data can be retrieved by an attacker.	Achieved
Comparison of different QR scanners and see how they behave.	Achieved
Conduct a real phishing campaign and collect data on QR usage and effectiveness as a means of phishing. Compare data against a mass phishing	Not Achieved

campaign sent via email and against a more targeted spear-phishing campaign.	
Create multiple posters and see which is most effective in drawing potential victims.	Not Achieved
Test URL forwarding capabilities on a custom domain to evade Google Safe Browsing and similar APIs.	Not Achieved

Section 2, WiFi Access Point Attack

Create a QR code that logs a user into a network automatically.	Achieved
Set up an AP with Kali to sniff user traffic.	Achieved
Create and present a fake captive portal to the user.	Achieved
Harvest credentials from the portal.	Achieved
Compare different QR scanners and see how they behave.	Achieved
Demonstrate packet-injection or other advanced MITM techniques.	Not Achieved

Section 2, MMI code Attack

Get any MMI code to execute on a phone via QR code.	Not Achieved
Get any UUSD code to execute on a phone via QR code.	Not Achieved
Create a custom wordlist of various UUSD and MMI codes.	Achieved
Create a corresponding gallery of UUSD and MMI QR codes.	Achieved
Get a dangerous UUSD or MMI code to execute e.g. change PIN code, factory reset data, call premium number, etc.	Not Achieved

Section 3, QR code malware

Keep any apk or exe used under the upper size limit of 2,953 bytes.	Achieved
Sideload an apk onto a device using only the QR scanner.	Not Achieved
In the case of Windows, load and execute the exe without being blocked by an anti-virus or Windows Defender.	Achieved
Add features to the initially benign apk or exe.	Achieved
Get the apk onto the device without “install unknown apps” setting turned on i.e. exploit a vulnerability in the camera or QR code reader.	Not Achieved
Add ransomware capability to the apk or exe.	Achieved
Add the ability to communicate with a remote C2 server.	Not Achieved

Problems Encountered

Time

For a long period of the project I felt behind and under pressure. At around Easter time I did manage to make some headway and catch up. I definitely feel like the project could use an extra month of polish but at a certain point I will just have to submit it irrespective of the state it is in. We all wish we had 25 hours in a day, but we simply do not. Good time management is a skill, and it is one I can certainly improve at.

New technologies

There were some new technologies that I had never worked with before. Wifipumpkin was one that took me a very long weekend to crack. I am very thankful for the developer's Discord channel where I managed to work out most of the issues I had. I realised that I need to learn a lot more about shells and shell scripting. While my script runs and does what it is supposed to, I feel that a lot of the codebase can be tidied up. In the future I will take some time and do a better implementation. The MMI code attack was frustrating when it would not work but I felt compelled to document and outline my failure.

Documentation

I definitely was not well prepared for the project documentation. The limited amount of UML and project planning we did in our Software Engineering module last year was in no way preparatory for what was asked of us this year. Overall, the documentation took up a lot more time than I anticipated. This was my first time doing a project of this scale and I will certainly be aware of what is required document-wise in the future.

Android

I naively believed that all the Java programming I had done would be enough to code a malicious apk and sideload it onto a device using a QR code scanner. While perhaps a good idea it was far beyond the scope of my skills. I lost a number of hours getting a hello world apk sideloaded onto a device via the QR code scanner. Since I could not really control any parameters of the scanners I tried I swapped to Windows where I had some control over how ZBar would handle input which made the world of difference. This was the only real major set back to the project but I luckily had a fallback.

Learning Outcomes

To say the project was educational would be an understatement. I learned a collage of new skills that will greatly benefit me moving forward.

Shell

I intend to spend a lot more time getting comfortable with the terminal and leaving GUIs behind except for when absolutely necessary. There were many little tricks like Bash's native string replacement that were very enlightening. Learning the differences between POSIX and non-POSIX shells and how they all have their own little quirks was a lot of fun and an area I definitely will expand my knowledge in.

Wireless Hacking

Earlier this year we were given a Kali Wireless Hacking project for our networking module which set me down the path of examining different wireless attacks. I began to look at how I could incorporate one into my own project and etched out a plan to create an access point with a convenient QR code login. I think my choice to utilise wifipumpkin for the project was a good one and it is a nice tool to have some experience with.

QR codes

QR codes were central to my whole project. I can safely say that I will never view them in the same light ever again. It was interesting learning about the variety of ways they have been applied and problems they've been utilised to solve. Given how QR codes are now used for checking into a location with a COVID tracker app or making crypto payments I will be considering the security ramifications of such a system in the back of my mind.

Videos

While I am happy with the videos I made for demoing and documentation purposes they took an awful lot of time to put together. Capturing footage from mobile devices was new and a lot of fun.

What would be Done Differently

Research

There were two books on shell scripting that I feel would have helped me write a much better program but between juggling everything else for 4th year I'm not sure it would have been possible. With regards to the Android situation, I should have spent more time researching if what I was proposing was really feasible. Or perhaps whether it was actually within my skill set. Ideally I would have started this project way back during work experience of third year but hindsight is 20/20.

MMI Codes

I should not have spent as much time as I did on a dated attack vector. I would have been better off focusing on cleaning up other parts of my project or documentation. I can be hard to know when to cut your losses and not sink any more time into dead end ideas or projects.

Phishing

The attacks that I conducted were theoretical, but I would love to conduct a real phishing campaign with QR codes and see their effectiveness. There seems to be a misplaced trust in QR codes or perhaps a lack of suspicion surrounding their contents. All the attacks that I performed were conducted on my own machines. Trying to gauge the effectiveness of such attacks is difficult and as it stands, I can only guess as to how they would fare in the real world.

Conclusion

I consider the project to be a success overall. While I did not achieve everything I wanted I did hit upon all the main markers. The core question that started this project was whether you could squeeze a malicious executable into a QR code, and I feel that was definitely answered. I thought that at the end I would never want to write another shell script or look at a QR code again but I intend to go back and do a much better implementation down the line. Overall, it was a very good experience.

Acknowledgements

I would like to thank Joseph Kehoe for being a fantastic project supervisor. Many thanks to Richard Butler for all his hard work and sympathetic ear. A big thank you to Keara Barrett for setting us that wireless assignment as it really gave me some inspiration. Quick thanks to the folks in the wifipumkin and LHC Discord servers who always helped but never spoon fed.

Plagiarism Declaration

- I declare that all material in this submission is entirely my own work except where duly acknowledged.
- I have cited the sources of all quotations, paraphrases, summaries of information, tables, diagrams, or other material; including software and other electronic media in which intellectual property rights may reside.
- I have provided a complete bibliography of all works and sources used in the preparation of this submission.
- I understand that failure to comply with the Institute's regulations governing plagiarism constitute a serious offence.

Student Name: Brendan Burke
Student Number: C00232110

Signature:
_____________Brendan Burke_____________________

Date:

_____________30/04/2021________________________