Individual Project (CS3IP16)

Department of Computer Science

University of Reading

Project Initiation Document

## PID Sign-Off

|  |  |
| --- | --- |
| **Student No.** | **27016005** |
| **Student Name** | **Daniel Broomhead** |
| **Email** | **D.L.Broomhead@student.reading.ac.uk** |
| **Degree programme** (BSc CS/BSc CSwIY) | **BSc CS** |
|  |  |
| **Supervisor Name**  *(Consultation with supervisor is mandatory)* | **Mohammed Al-Khafajiy** |
|  | Supervisor to sign PID form on Bb (grade centre) |
| **Date** | **08/10/2020** |

# SECTION 1 – General Information

## Project Identification

|  |  |
| --- | --- |
| **1.1** | **Project Title** |
|  | **Investigating the parallels between using a RAT-style software for malicious intent and virtuous purposes.** |
| **1.2** | **Please describe the project with key-phrases (max 5)** |
|  | RAT, Security, Support, Malware, Trojan, Investigating the use of RAT for malicious and good |
| **1.3** | **E-logbook maintenance agreed with supervisor**  *Use Google doc, OneDrive, or any mobile App whereby you will be able to generate a PDF copy* |
| **OneDrive** |
| **1.4** | **GitLab link for maintain source code and research data**  *Any change in GitLab link and Source code repository MUST be explicitly mention in final report* |
| https://csgitlab.reading.ac.uk/br016005/final-year-project |

# SECTION 2 – Project Description

|  |  |
| --- | --- |
| **2.1** | **Summarise the project’s background in terms of research field /application domain (max 100 words).** |
|  | RAT = Remote Administration(/access) Tool(/Trojan)  The background of this software breaches across many different fields of computer science, for example, the design and implementation demonstrates the key fundamentals of software engineering, while the actual implications of the software lie heavily in the cyber security field - representing both offensive security, defensive security and malware. The project delves into the applications of a remote administration/access tool, the social, ethical, and legal ramifications of implementing one, and the possible dangers that may be associated with one.  The Development, Production, Delivery, Deployment, and implementation of a RAT style software. Demonstrating how the same style of software can be used as a malicious weapon but also a very useful admin and support tool. I am to show the parallels between software which can be used for the greater good, and the greater evil. |
| **2.2** | **Summarise the project aims, objectives and outputs (max 250 words).** These aims, objectives, and outputs should appear as the tasks, milestones, and deliverables in your project plan (fill out Section 3). |
|  | The project aims to demonstrate to the reader the effectiveness of a RAT-style piece of software, and the various uses of one.  Aims:  To create a fully working RAT-style Application which can demonstrate the differences and parallels between piece of software developed solely for good intentions and one developed with malicious objectives.  The objectives:  Research into RAT-style software  Create a basic RAT-Style Prototype  admin privileges.  Test on a compromised system.  Basic UI  access to target via file system  access to target via full control  hooking to target  passive monitoring of target  capture of keyboard  capture of mouse  capture of clipboard  Advance to a hidden Malicious style RAT prototype. **creepware**  Invisible  bypass security and firewalls  undetected installation  Advance to a support utility style RAT prototype.  Clear prompts  user disconnect option  visual aids  logs for client  Show the differences between the two    Delivery methods:  investigate the different methods used to obtain access to a system and install the RAT software  show how these differ between legal uses of the software and illegally intended uses.  Social, Legal, Ethical Aspects:  Investigate the SLE aspects of a legal RAT and a Malicious RAT.  Investigate scamware    Outputs:  Successfully design and develop a fully working Remote access tool.  Demonstrate the differences between a RAT designed for Assistance / Aid and one designed for malicious intent.  Demonstrate the various delivery methods possible to get a RAT onto the target device.  This project should discuss the vulnerabilities to a malicious RAT and how to attempt to protect yourself from this sort of attack. |
| **2.3** | **Initial project specification – roughly indicate key features and functions of your finished program/application. Indicate possible method, data source, technology etc. (max 400 words)** (Sensible and relevant Charts, Table, and Figures can be used) SIPOC |
|  | A working remote access tool which has the potential to be used for good purposes and evil purposes.  Must be able to see the target computer: the program cannot connect to a device it cannot recognise, therefore must be able to see it.  Must be able to connect to the target computer: must be able to successfully connect to the target device via internet or across a local connection.  Must allow application user to monitor target’s activity, manage files, install additional software, control entire system, including any present application or hardware device, modify main system settings, turn off or restart computer. Ideally would allow monitoring behaviours through keylogging etc, accessing confidential information and passwords. The ability to take screenshot, manage peripherals such as activating a system’s webcam and recording the video, formatting drives, deleting, downloading, and altering files/file systems, as well as distributing files.  Should give full control over the target computer. This should range from controlling the filesystem, to capturing the mouse, keyboard and even clipboard contents,  Does not need to be able to turn on computer! Just hook to a computer once it is turned on.  Either two separate RATs, one malicious and one for software aid – or if possible, one RAT with a switch between sinister mode and legitimate mode. There are many ideas that could be implanted into the switch, such as making the program look like it has crashed and exited while still maintaining full functionality.  For the sinister mode, inconspicuousness is key, there should be minimal to no indication that the system has been compromised, there should be as few visual clues possible, while maintain maximum performance, ideally the program should be running completely invisibly in the background, like a daemon, may have features to bypass security.  For the legitimate version, almost the complete opposite is true, visual clues are absolutely essential, the target computer should be able to disconnect at any point if the user feels that something is not right, the system should time out after idling for too long, and most definitely should not be running in the background without the users permissions.  Must have multiple delivery methods, such as via USB RubberDucky, Cloning via a git repo, sideloading, malicious email links, and giving permission to install (legitimate version).  I also intend to discuss the security side of things throughout the project, ranging to protecting yourself from them, to the implication of how the exact same software at the most basic level can be extremely dangerous but also significantly helpful based on way it is used. |
| **2.4** | **Describe the social, legal, and ethical issues that apply to your project. Does your project require ethical approval? (If your project requires a questionnaire/interview for conducting research and/or collecting data, you will need to apply for an ethical approval)** |
|  | All of the issues that apply with the project are only prominent in the case of using this software on devices that I do not own, or devices not being used for testing and demonstration purposes only. In these cases there are no legal, social, ethical, or moral implications.  In the event that this project gets extended to be tested on other devices, and  For the demonstration of the possible malicious applications of this program, there are many SLE issues, therefore I will need consent from the system owner or to test it on a local system .  GDPR issues. Personal issues. Mental issues.  Computer Misuse Act.  Data Protection Act. |
| **2.5** | **Identify the items you may need to purchase for your project. A cost up to £200 can be applied (include VAT and shipping if known). You need to have consent of your supervisor. Your request will be assessed by the department.** |
|  | Various delivery formats,  USB rubber Ducky, etc ≈ $50 <https://shop.hak5.org/products/usb-rubber-ducky-deluxe?variant=353378649>  Or Bash Bunny = https://www.amazon.co.uk/Hak5-BASH-BUNNY-HAK5/dp/B0725Q36NJ  or ≈$199 <https://shop.hak5.org/products/usb-rubber-ducky-deluxe?variant=31762628378737>    [Debugging Rubber Duck (little yellow one preferably)](https://www.amazon.co.uk/Munchkin-Rubber-Safety-White-Reveals/dp/B000GUZC2A/ref=sxin_9_ac_d_rm?ac_md=0-0-cnViYmVyIGR1Y2s%3D-ac_d_rm&cv_ct_cx=rubber+duck&dchild=1&keywords=rubber+duck&pd_rd_i=B000GUZC2A&pd_rd_r=8a669fdc-f652-4867-a97e-2982fd3e85ab&pd_rd_w=WDLZm&pd_rd_wg=OMM35&pf_rd_p=0c799c14-fd2d-4652-a647-3581649b0ff7&pf_rd_r=QYKNDYMH46HRX64YX1C1&psc=1&qid=1602066390&sr=1-1-fe323411-17bb-433b-b2f8-c44f2e1370d4) £2.79 |
| **2.6** | **State whether you need access to specific resources within the department or the University e.g. special devices and workshop** |
|  | An internet connected device which I can test the software’s functionality and various delivery methods on. Admin privileges on a system. permission to boot from external drive. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **llSECTION 3 - Project Plan** | | | | | | | | | | | | | |
| Please provide your project plan.  Below is an example project plan, you can use any tool or software to generate yours. | | | | | | | | | | | | | |
| **Project stage** | **START DATE: ../../…. <enter the project start date here>****Project Weeks** | | | | | | | | | | | | |
| 0-3 | 3-6 | 6-9 | 9-12 | 12-15 | 15-18 | 18-21 | 21-24 | 24-27 | 27-30 | 30-33 | 33-36 | 36-39 |
| 1 Background Research |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 Analysis/Design |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 Develop prototype |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 Testing/evaluation/validation |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 Assessments |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |