Cardiff University

School of Computer Science and Informatics

CM3203 - One Semester Individual Project - 40 Credits

Initial Plan

creating a machine learning model based on network activity to detect attacks from malicious web server

Author – Balqees Ali Al-Ajmi

Supervisor – Amir Javed

Moderator – Martin J Chorley

Table of Contents

Project Description

Background information

The Online social networks such as Twitter, Facebook, Tumblr are potentially vulnerable to the danger of collective contagion and propagation of malicious viral material such as spreading rumour [18] and detrimental content following emotional events widely published (Burnap, P et al, 2014). The dissemination of malicious software (malware) through URLs is considers as one of the misuse cases though the online social networks. The URL is the Uniform Resource Locator abbreviation, which is the global worldwide web address of documents and other resources. The compromised URLs for cyber-attacks are known as malicious URLs, where hackers can inject malware on web pages (e.g. Trojans or Worms, etc) to steal user data and to acquire money on illegal way. Moreover, malicious URLs considered as one of the major cyber-crime's mechanisms. These hackers host unrequested content and target unsuspected users, who make them victims (theft of money, identity theft, malware installation, etc.) and this has contributed to losses of billions of dollars annually (Hong, J., 2012). In point of fact, nearly one-third of all websites have been classified as potentially malicious in nature, which illustrates that the number of malicious URLs is being used to commit cyber-crimes increasing rapidly (Liang, B et al, 2009). AVTEST estimates that the malware compromised websites rate raised significantly into 95 millions in 2017.

It is extremely essential to detect and act on such certain threats in a timely manner. Therefore, to address Web-based attacks, there is a great effort has been directed towards detection of malicious URLs and to protect the users from the treat of the malicious. In the last few years, with the advancement of Machine Learning, several activities are executed using machine learning algorithms. Unfortunately, there has been little work has been performed on security and protection with machine learning algorithms.

Brief Description

This project will investigate the clear URLs and the malicious URLs and Identify those URL that are pointing to malicious web servers depending on virus Total and implementing two machine learning models and techniques to detects the attacks from malicious web servers. To compare between the two Machine Learning models will be reviewed on sandboxed environments using two VirtualBox running two different Win OS will be understood to aid in the implementation phase. All the implementation of the project will use python as programming language and will be implemented on a Mac device and a documentation and reflective exercises on the achievements will be included. The overall aim of this project is detecting malicious content based on online social network and URLs depending on two machine learning models techniques.

Project Aims and Objectives

This section will present a list of more detailed aims and objectives of the proposed project.

- **Aim:** To build a machine leaning model that can detect a drive-by download attack based on network traffic.

- Objectives:

1. To setup a sandboxed environment such as cyber range that could be visit malicious web servers and capture network traffic.
2. To pre-process the data in machine readable format, so that it can be used for building machine learning model.
3. Using python-based libraries and modules to implement Machine Learning models.

4. Do background study to identify popular model and build machine learning model that can distinguish malicious traffic from benign.

Supervisor roles – Amir Javed

There will be a meeting each week on Tuesday and Thursday for a short duration of 20-30 minutes with the supervisor Amir Javed where advice, guidance and feedback will be provided.

Ethics

The project as discussed with the supervisor is likely to require an ethical approval. This is because of gathering data from online social network such as data that are contains URL and this will not include any personal data. Moreover, creating the two machine learnings will be based on handing network traffic in the project. However, I believe there are no personal data will be stored in the network traffic or it is accessible to any user and data was gathered from specific online social media. Therefore, there is no need to ethical approval. However, there will be ethical consideration during the entire major and in the final report. And also, I will make sure that all laws and guidelines are adhered to, especially in regard to data during doing the project.

Work plan

A work strategy has been designed to manage the report efficiently and produce a successful project. The task schedule splits the project work duration weekly, which results into fifteen weeks. There will be two regular meetings per week with the supervisor for 30 minutes each Tuesday and Thursday excluding the Easter recess, therefore, it is not included in the work plan. Additionally, all necessary activities to complete the project were included with the deliverables, milestones and progress review meetings has been included in the work plan schedule. The work plan is presented in the next page.

Weeks	**Tasks**	**Deliverables/ Milestones**
Week 1 1st Feb - 5th Feb	-Supervisor meeting - Prepare Initial plan report draft. - Finish Initial plan report after getting feedback from supervisor.	- Initial plan draft
Week 2 8th Feb - 14th Feb	- Submit Initial plan report. -prepare Final report structure. - Start background research on: • Gathering data. • URL checking process. • Create sandboxed environments. • Machine learning process. • Machine learning algorithms for detect attacks from malicious web server. • Python machine learning libraries and modules. • machine learning algorithms that are suitable for detecting URL malicious.	- Initial plan report: project description, aims and objectives and work plan. - Written background research (Background section). **- Milestones:** • Initial plan report submitted by 8th of February

Week 3 15th Feb – 21st Feb	- Start the Approach section (Specification and Design): • Describe current approaches of designs for the chosen machine learning algorithms. • Describe the chosen approaches with Justification. - List requirements and specification of the software that will be developed. - Decide upon python libraries for implementation the learning model. - Evaluate the design and libraries chosen for the implementation.	- Approach section (Specification and design)

Week 4 22nd Feb – 28th Feb	-Start implementing two different machine learning models (two different algorithms) using python.	
Week 5 1st Mar – 7th Mar	**- Progress review (Special Meeting)** - Collect data (that contains URLs) - publicly available source of URL's classified as malicious [pointing to malicious web servers]. - Identify and analyse data related to malicious URL checking. - Implementation: • Continue implementing two different machine learning models (two different algorithms) using python.	**Progress review (Special Meeting)**
Week 6 8th Mar – 14th Mar	- Implementation: • Continue implementing the two different machine learning models using python. • Finish ML models	- Two machine learning models code in python. **- Milestones:**

		• The machine learning models works and functions correctly as the chosen algorithms.
Week 7 15th Mar – 21st Mar	**-** Implementation	**----------------**
Week 8 22ndMar – 28th Mar	**-** Implementation	**----------------**
Easter Recess **Week 9/** 29th Mar – 4th Apr **Week 10/** 5th Apr – 11th Apr **Week 11/**12thApr – 18th Apr	**-** Implementation: • Continue implementing. **-** No meetings will be scheduled for these weeks.	- Results and Evaluation section. **- Milestones:** • Software has been evaluated.

	• Test the implemented machine learning models. - Fix any errors and bugs that arise from testing. - Evaluate the implementation.	• Results has been captured and written.
Week 12 19th Apr – 25th Apr	**- Progress review (Special Meeting)** **-** Write Future work section: • Future improvements. • Social engineering method to detect attacks from web servers. • How the project could be taken further	- Future work section.
Week 13 26th Apr – 2nd May	- Write abstract, introduction, acknowledgements and conclusion sections. _Restructure and organise all final report sections	- Abstract, introduction, acknowledgements and conclusion sections. - Final report first draft **- Milestones:**

		• Final report first draft completed.
Week 14 3rd May – 9th May	**- Progress review (Special Meeting)** **-** Compile and update table of contents, table of figures, glossary, table of abbreviations, appendices and references after combining all sections. - Review the report and fix any errors	**- Progress review (Special Meeting)** **-** Table of contents, table of figures, glossary, table of abbreviations, appendices and references.
Week 15 10th May – 16th May	**-** Proof read all the Final report. - Submit the Final report and the source code.	-Final Report with all sections. **- Milestones:** • Submission of Final Report and the source code by 14th May 2021

Milestones and deliverables

As it can be seen in the work plan, there will be several milestones and deliverables during the project duration. The following list illustrates the most significant milestones and deliverables for this project:

- **Initial plan report (Complete version) – submitted by 8th February**
    - The completed version of the report including project description, project aims and objectives and a complete work plan.
- **First draft of the following sections**
    - Background research, approach (design and specification), implementation, results and evaluation and future work that will be delivered in different weeks according to the work plan
- **Implementation**
    - Python code on the implementation of two machine learning models
    - Python code to captures network traffic and pre-process the data.

- **Final report draft (Continuing the previous sections in the first draft)**
  - Final report with complete main body sections and supporting sections (Title page, abstract, acknowledgements, table of contents, table of figures, glossary, table of abbreviations, appendices and references)
- **Final report (Complete version) – submitted by 14th May**
  - The complete version of the final report with all the sections included and proof read.

Conclusion

In conclusion, this report presented the proposed project description, aims and objectives and a clear work plan that will be followed in the next phase of the project with the deliverables and milestones.

References

Liang, B et al, 2009. *Malicious Web Pages Detection Based on Abnormal Visibility Recognition*. [online]. Available at: https://ieeexplore.ieee.org/document/5138008 [Accessed at:01/February/2021].

Hong, J., 2012. *The state of phishing attacks | Communications of the ACM*. [online]. Available at: https://dl.acm.org/doi/abs/10.1145/2063176.2063197 [Accessed at: 01/February/2021].

AVTEST. *Security Report 2017/18: The Independent IT-Security Institute*; AV-TEST: Magdeburg, Germany, 2018.

Burnap, P et al, 2014. *Tweeting the terror: modelling the social media reaction to the Woolwich terrorist attack*. [online]. Available at: https://link.springer.com/article/10.1007/s13278-014-0206-4 [Accessed at:03/ February /2021].