KV6003 Investigation into infrastructure defence in relation to emerging threats

Individual General Computing Project - Terms of Reference

Carl Slatter

24th November 2020

1 Background

The modern technological landscape demands much from innovation. We must find new ways of solving existing and new problems in the world. This is amazing for convenience, and quality of life, but does pose a problem for security. There is Hypponen's law in IOT that states, the more you add in terms of functionality, the more that must be secured. [Hypponen and Nyman, 2017] A concrete cube may be secure, but is not overly functional. I am incredibly interested in the duality between attack and defence. It seems to be a constant cat and mouse game of which defence is paramount. [Genç et al., 2019] I hope that by looking at both sides with a purple team perspective, I can gain a deep understanding of the landscape we have currently and moving forwards.

Cyber-Security is really "Managed insecurity", I intend to discover where cyber attacks are at, and how they have innovated over the years. Cyber threats are growing, how can be detect them? How can we proactively block them? These are questions that must be answered in order to get a good overview. I must be able to show my understanding in a theoretical and practical way to be able to potentially apply it to a real life scenario. I will have to develop my understanding of infrastructure, networking, semi low-level programming and penetration testing.

Developing realistic solutions for smaller businesses is really important. They are arguably more at risk, with less resources for security. [Carías et al., 2020] The is a culture of security snake-oil and scare-ware, and supposed all-in-one solutions rather than defence-in-depth. This is evident in the numerous adverts that claim much and deliver little. [Michener et al., 2010] With the detection work, I hope to show the importance of the human element to security, how it can be the weakest link, or the strongest asset. [Mc Mahon, 2020] I must look at current solutions with a critical eye with care to be realistic about defence.

Malware has evolved over time, what was once an exercise of what was possible, is now a platform for theft and crime. [Love and Love, 2019] Defences catch up over time, it will be eye-opening to see the different methods historically that the two sides try to out-smart each other. [Love and Love, 2019] Malware analysis is something I haven't really touched on before, though I have be interested for a long while now. It will benefit my defence greatly.

2 Proposed Work

I aim to create documentation in the form of my dissertation to describe the Cyber-Security landscape in regards to infrastructure. This will involve talking about infrastructure directly, it's use, implementation and potential pitfalls, but more importantly, how it can be secured. On the other side, I will be looking at the common ways that infrastructure is compromised, in a network setting. I do think that a good comparison is important for this. The dissertation will have the approach of being an overview, as I feel that is the best way to cover the bigger picture. I will go into relative depth where it is nessesary. The experiment will simply just compare a set of attacks to a set of defences, with analysis of the results. Details will come in the synthesis, as it entirely depends on my research to which exact direction I go in.

I will be investigating how threats have evolved as a whole, talking about malware mechanisms, obfuscation and clever exfiltration. I believe it is important to at least touch on how this was done in the past, to understand how the future may follow similar foundations. Naturally an investigation into threats would be pointless without a practical defence, I hope to compare both endpoint and infrastructure defences in relation to both a sample of threats, and to one another. I will then analyse this data and draw sensible conclusions based upon it.

I also hope to create a rudimentary intrusion detection system written in C. This will be a proof of concept to show my understanding, rather than a product. My hopes are that by developing network defence myself, I can gain an even deeper understanding. It will also illustrate the scale that corporate products can run at, including extra methods that are out of scope for me. This is secondary to the main experiment.

3 Aims and Objectives

3.1 Aims

To understand the theory behind defence in relation to common threat vectors. To develop attack and defence skills to aid the theory, in a practical manner.

3.2 Objectives

1. **Analysis of historic threats and malware**
2. **Analyse modern attack:defence landscape**
3. **Analysis of defence technologies**
4. **Explanation of entry vectors and profiling**
5. **Explanation of exploitation**
6. **Explanation of obfuscation**
7. **Explanation of exfiltration**
8. **Investigate IDS/IPS systems w/ comparison**

9. **Illustrate proof of concept IDS**
10. **Investigate antivirus systems w/ comparison**
11. **Discussion of meaningful defence**

3.3 PoC IDS Objectives (It must..)

1. **Detect network interfaces**
2. **Bind to a network interface**
3. **Capture data and output to a file/standard output**
4. **Flag up unusual activity from a few notable attack types**
5. **Control via command switches**
6. **Be well written and meaningful to the idioms of the language**
7. **Have testing/design documentation**

4 Skills

- Programming in C (KF5006)
- Networking Technology 3 (KF6005)
- Advanced Operating Systems II (KF6003)
- Cyber-Security Awareness
- Reverse-Engineering
- Data Analysis

5 Resources

5.1 Hardware

- Dedicated high RAM machine - Already bought
- Lab Machines for possible testing

5.2 Software

- VMware Workstation - To host vulnerable and attacker infrastructure
- VScodium - IDE for IDS development
- Packet Libraries - unsure about specifics at the time of writing, likely scapy and libpcap
- Various Antivirus Licences - Prefer free or monthly subscription
- IDS/IPS/SIEMs Licences - Will have to prefer free or cheap ones (as a small company would)

- Malware Samples - Sourced from Github collections
- Operating System Distributions - Obtained online

6 Structure and Contents of the Report

6.1 Planned Report Structure (Order may change)

Introduction - This chapter sets out the basis of the project, the motivations behind it and what I am looking to investigate. It will summarise the whole project.

Analyse historic & modern defence - This chapter is a broad overview of the cat and mouse game, with a focus on how both sides evolve over time, and how to tip the scales in the defences favour. Analysis of defence technologies directly after (Anomaly Detection, signature matching, whitelisting etc..).

This chapter then covers cases of past incidents, how they happened, why they were effective and what we can learn from them for modern day. I will cover an assortment of notable malware. History and modern may be split into two paragraphs.

Explanation of entry points and profiling - This chapter covers the idea of what a vulnerability is at it's core, how they are found and the commonalities among vulnerabilities. It will include the discussion of common pen-testing tools for the enumeration/scanning phase. Additonally I will look at common attack vectors for malware to get in.

Explanation of malware mechanisms - This chapter covers the common mechanisms of exploitation and stealth that malware makes use of. This includes the use of obfuscation, encryption, exfiltration and the impacts they have. This covers a description of the methods, rather than ouright historic implementation. May be split into their own sections/chapters for the sake of detail.

Investigate antivirus systems w/ comparison - This chapter is to lay out my experiment methodology, why I did what I did, what I'd expect vs what I got and an analysis of the results themselves. A sample of threats/malware may be tested.

Investigate IDS/IPS systems w/ comparison - This chapter is to lay out my experiment methodology, why I did what I did, what I'd expect vs what I got and an analysis of the results themselves. A sample of threats/malware may be tested.

Proof of Concept IDS - I will talk about what can be learned from it, in relation to the scale of commercial products, along with the technologies used.

Discussion of meaningful defence - This chapter encompasses what can be done to aid defence to it's maximum. I will focus on defense in depth and diversification of defence mechanisms. Topics include, proper training, access control, security positive culture, adequate funding, regular security testing, development infrastructure and a wide variety of hardware solutions. Will likely be split into sub paragraphs and sections as it's a vast topic.

6.2 Conclusion

This will summarise all that was found, how it relates to what I set out to discover and what it means for the future of defence.

6.3 List of Appendices

- ToR
- Experiment and PoC Design/Testing
- IDS Source Code
- Experimentation Result Documentation
- Risk Assessment
- Ethics Form (Depending on ethics approval process)

7 Marking Scheme

The marking scheme sets out what criteria we are going to use for the project.

Project Type: General Computing

Project Report

Analysis

- Analyse historic & modern attack/defence landscape - Analysis of literature malware/threats
- Explanation of entry vectors and profiling
- Explanation of malware mechanisms

Synthesis

- Investigate antivirus systems w/ comparison
- Investigate IDS/IPS systems w/ comparison
- Illustrate proof of concept IDS & implementation of technologies

Evaluation

- Discussion of meaningful defence

Product

- Dissertation Paper
- Experiment and PoC Design/Testing
- IDS Source Code
- Experimentation Result Documentation w/ Metric Justification

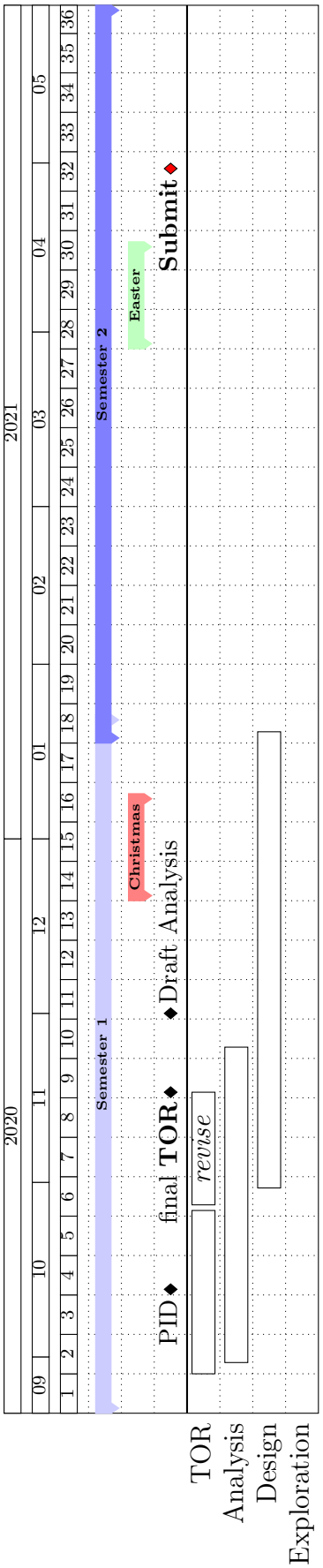
Fitness for Purpose

- There must be analysis of both sides
- There must be comparison of feasible solutions
- The program must be functional to a proof of concept level

Build Quality

- Experiment design quality
- Code quality & testing
- Quality of analysis & synthesis
- Quality of meaningful mitigation

8 Project Plan



9 Bibliography

J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes. Systematic approach to cyber resilience operationalization in smes. *IEEE Access*, 8:174200–174221, 2020. doi: 10.1109/ACCESS.2020.3026063.

Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra. A game of "cut and mouse": Bypassing antivirus by simulating user inputs. page 456–465, 2019. doi: 10.1145/3359789.3359844. URL `https://doi.org/10.1145/3359789.3359844`.

Mikko Hypponen and Linus Nyman. The internet of (vulnerable) things: On hypponen's law, security engineering, and iot legislation. *Technology Innovation Management Review*, 7:5–11, 04 2017. doi: 10.22215/timreview/1066.

Posted by John Love and John Love. A brief history of malware-its evolution and impact, Sep 2019. URL `https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/#:~:text=Itsoriginstemsfromtwo,allofauser'sfiles.`

Ciarán Mc Mahon. In defence of the human factor. *Frontiers in Psychology*, 11, 07 2020. doi: 10.3389/fpsyg.2020.01390.

John Michener, Steven Mohan, James Astrachan, and David Hale. 'snake-oil security claims' the systematic misrepresentation of product security in the e-commerce arena. *SSRN Electronic Journal*, 06 2010. doi: 10.2139/ssrn.1616728.

10 Risk Assessment Form

Risk	Mitigation
Malware reaches internet, and spreads into the wild	No direct internet access
Malware breaches hypervisor	Dedicated ESXI machine or live cd with disconnected drives (if at home). Modern and up to date hypervisor that is ring 3. Disabling of VMware tools. Defense in depth
Malware reaches local network	Use of virtualized custom network (no bridged!)
Malware persists on VM	Reverting to earlier snapshot / Scrubbing drive
Malware spreads in transit	Encrypted zips with password
Malware reaches router	No connected network cables or WIFI, static addressing
Malware spreads to shared folders	Avoid use of shared folders, have samples encrypted on snapshot, no downloads needed.
Malware detects VM, does not run	Install common apps, artificially use pc, increase RAM, remove additions/VMware tools, fake internet server (steps needed to bypass average VM checks)
Attacks act on the wrong target	All attacks will be done inside the virtualized network, that cannot reach the outside, this includes potential Kali/parrotOS. I will have a defined addressing scheme as part of the experiment