KV6003 Investigation into infrastructure defence in relation to emerging threats

Individual General Computing Project - Terms of Reference

Carl Slatter

1st December 2020

1 Background

We must find new ways of solving existing and new problems in the world, often with technology. This is useful for convenience, and quality of life, but does pose a problem for security. There is Hypponen's law in IOT security that states, the more you add in terms of functionality, the more that must be secured. (Hypponen and Nyman, 2017) This law is applicable to infrastructure also, potentially to a larger impact due to the scalability of network infrastructure. It is a 'cat and mouse' game of which defence is paramount. (Genç et al., 2019)

Cyber-Security is really "Managed insecurity" (Man, 2019). 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.

Developing realistic solutions for smaller businesses is crucial. They are more at risk, with less resources for security. (Carías et al., 2020) The is a culture of security snake-oil, scare-ware, and supposed all-in-one solutions rather than overarching defence-in-depth. This is evident in the numerous adverts that claim much and only deliver a specific defence. (Michener et al., 2010) I must look at current solutions with a critical eye and 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)

2 Proposed Work

I will create a proof of concept intrusion detection system that can detect a few pattern based attacks, conducting the research necessary, including experiment of threats vs defence. This will be a proof of concept to show my understanding, rather than a product. It will also illustrate the scale that corporate products can run at, including extra methods that are out of scope for me. 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.

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. By looking at both sides of infrastructure with a purple team perspective, I can gain a deep understanding of the landscape we have currently and moving forwards. I intend to discover different cyber attack types, and how they have innovated over the years. Defences catch up over time, it will be eye-opening to see the historic methodology, and how the two sides try to out-smart each other. (Love and Love, 2019)

The dissertation will have the approach of being an overview, as it is the best way to cover the bigger picture. I will go into relative depth where it is necessary.

An investigation into threats would be pointless without a practical defence, I will compare and analyse both endpoint and infrastructure defences in relation to both a sample of threats, and to one another.

Details of the experiments will come in the synthesis, as it entirely depends on my research to which exact direction I go in. Malware analysis is something I haven't had much experience in, though I have be interested for a while now. It will benefit my defence capability greatly. There will be a dedicated computer for this kind of analysis, likely using a VMware hypervisor for containment and infrastructure management, with more details in the synthesis.

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.

I will then analyse this data and draw sensible conclusions based upon the research and practical work.

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 (Variable order)

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. **Create a secure malware analysis lab**

9. **Investigate IDS/IPS systems w/ comparison**
10. **Formulate showcase proof of concept IDS (Language, libraries, attack detection choice)**
11. **Investigate antivirus systems w/ comparison**
12. **Discussion of meaningful defence**

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.

Secure Environment Setup - Discussion of the malware analysis lab created will be conducted, including choices of approach and software.

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 in relation to set defences.

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 in relation to set defences.

Proof of Concept IDS - I will talk about the choices made regarding it's development, what I used and how it performs in relation to what I have learnt.

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

- Discussion of the secure malware analysis lab
- 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

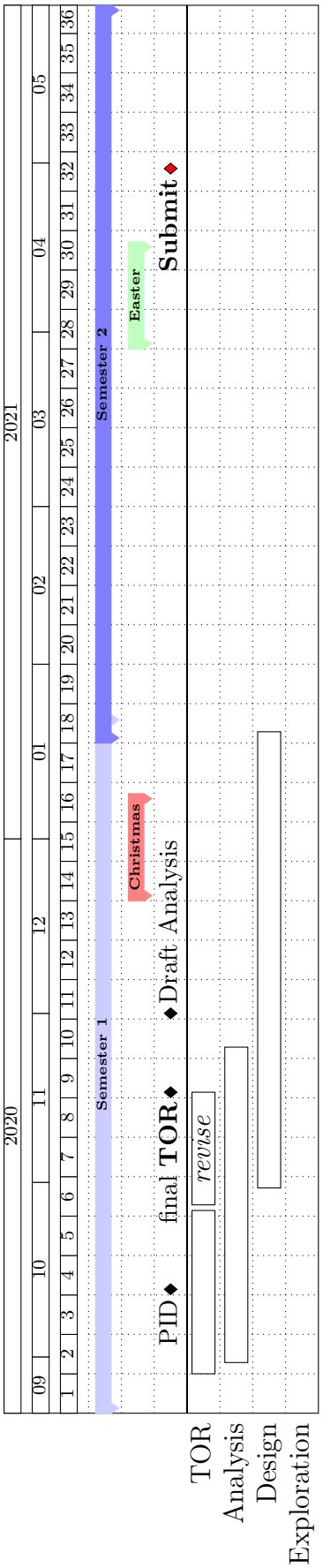
Fitness for Purpose

- 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

Bogdan botezatu$_2$019, 2019. *URL*.

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. 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. 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. 10.22215/timreview/1066.

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

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. 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