



ACDA5004 – Project Management and Research Methods

Final Year Major Project Proposal

Final Year Major Project Proposal

ACDA5004

How Secure is the Average Home Network?

Contents

1.1	
Introduction	2
Background	2
Introduction	2
1.3 Objectives.....	4
1.4 Expected Outcomes	4
1.5 Research Methods	5
1.6 How will the objectives be completed?	5
Limitations, Issues, and Data Evaluation	6
Resources & Planning	7
Conclusion.....	8
Bibliography	8

Introduction

Background

The late 60's is where there was a boom in technology – this is because this is the time that the very first 'workable prototype' of the 'internet' was developed and was given the title of 'The Advanced Research Projects Agency Network', more commonly known as ARPANET; this development was funded by the United States' Department of Defense. ARPANET focused around using 'packet switching' which allowed multiple devices to communicate whilst connected to one network – this was the base for what we know today as a Local Area Network (LAN). [1] According to Evan Andrew's in his article regarding the invention of the internet, on October the 29th 1969, ARPANET delivered it's very first 'node-to' node message. The progression of the internet continued to develop through the years, and in 1983 ARPANET adopted the TCP/IP protocol completely – which is the very structure of the modern version of the internet. [1] Since then, developments in technology have come on what many may regard as 'leaps and bounds' – the state of today's current internet would be unbelievable to those who made the very grounds-work of what we have today. Billions of people can connect to each other with the click of a few buttons, communication is easier than ever.

The development of networks and broadband connection is fundamental to the development of modern society – but with such positive influences and uses, it does not come without its flaws. Where there are pros, there are cons, and as the internet is ever changing, so are the malicious in the world whose intent is to manifest their ill-will into networks - whether that be for their own personal gain or for any other reason – this is why network security is fundamental. As network security is growing increasingly more important by the day, it has been chosen as the subject of study for the major project which will be completed in the third year of study at UWTSD; the title of the study is '**How Secure Is the Average Home Network?**'.

Introduction

The particular area of study is network security, revolving around the need for network security and the actual efficiency of what is currently available – as the network is one of the most used 'products' around the globe, securing such a vast existence is vital; this particular study aims to investigate what measures are already in place to secure home networks and the very importance of each measure/product

implemented, along with investigating the advancements of network security over the near future.

According to Bhava Daya from the University of Florida, “there is a significant lack of security methods that can be easily implemented”. [2] They go on to discuss how there is an apparent “communication gap between developers of security technology and developers of networks’ [2]– this statement was made without any real substance and any facts/statistics to back up this claim, neither do they express how there is a lack of communication; making such a claim without providing any sort of evidence or any real substance almost de-values the reliability of the claims that are being made, regardless of Daya’s position at Florida University. Daya goes on to discuss IPV4 and IPV6 – highlighting the issues with IPV4, emphasizing on how ‘routing tables are constantly increasing in size’ and how the current methods to reduce the number of routing entries are only good for a duration of time. Daya quotes Sir Andress J in stating that there is a cap of a routing table is 2.1 million entries. [3] Daya uses a range of references whilst discussing the topic but it seems as though the references that were used were not particularly reliable, such as using ‘How Stuff Works’ as a viable reference whilst discussing network security, joined with the use of unreliable sources and primarily websites, Daya continues to back up their claims with little to no evidence – thus, this writer is not a reliable source.

Whilst Daya made claims like there being a lack of communication between security developers and network developers without any real substance, there does still lie the question “What is being done to secure the average home network?”. Network security can be deemed as a ‘subgroup of networking’ [4]– it includes securing all elements of the network, whether that be the networks physical infrastructure, or the network itself, network security is the protector of both. The network needs to be protected from a multitude of different kinds of attack, here are some examples:

- Theft
- Distributed Denial of Service Attacks – more commonly known as DDoS
- Malware
- Trojans
- Botnets
- Spyware

There are, of course a few other things in which the network needs to be protected from but listed above are some of the most popular.

The area of network security is a very interesting field – there are a multitude of ways in which networks can be secured (some methods popular, some more obscure) and there are no real, in-depth studies in to the efficiency of the modern home-network, and how network security professionals intend to continue developing and adapting to counter the continuously escalating threats. A report produced by Virginia Harrison and Jose Pagliery in 2015 states that in the year of 2014 ‘more than 317 million new pieces of malware were created’ [5], and according to ‘The Telegraph’ “12 million people suffered a computer virus attack within the last six months” [5] – this report was written in 2009. Moneysupermarket.com conducted research into malware and anti-virus – which found that 12 million had suffered such an attack, even though “95% of people claimed to use an antivirus/firewall software” – and a total of “39% described the assault as causing major disruption”. [6]

Such attacks happen all too often, the number of malwares being developed daily is rising continuously every year, with more and more people falling victims to such malicious actions – the primary question is “how efficient really is home security?” and because of this issue, this is a particularly important study, as there needs to be clear improvement.

1.3 Objectives

1. Discover how many people have fallen victim to malware & other attacks in the past 2 years
2. Analyse the current measures in place to protect home networks
3. Investigate the up and coming security measures
4. Evaluate the efficiency of home network security and recommend improvements

The primary way in which objectives 1-3 will be achieved will be through research, using all viable ways to obtain information such as: reports, books, websites, and articles – joined with this, an investigation will take place, with a sample number of people being asked about their own experience with malware & other attacks, joined with what security measures they have currently implemented on their own home network. The evaluation of home networks will be developed using the facts that were found during the study – based off whether security measures tackle and eradicate more attacks, than attacks gain success.

1.4 Expected Outcomes

The expected outcome of this study is to find a mixture of both competent and incompetent methods/software – with some functioning incredibly well, with the developers continuing to update their methods/software to keep up to date, but with some developers failing to keep up to date to combat the growing threats. It is expected that there will be a development within the near future in terms of the tools available to help combat some attacks – the hypothesis is the primary issue with the amount of people getting viruses on their devices is through lack of knowledge and awareness – tied in with obsolete methods of combat.

It is also an aim to analyse each current method and attempt to make recommendations – using the opinions/knowledge of specialists within the field, and the use of other assets such as reports and articles. At the end of the study, a complete, comprehensive report will be submitted, which will focus on the efficiency of current network security strategies/software, discussing why so many people fell victim to such attacks, and a report regarding all the improvements that could be made to the current system.

1.5 Research Methods

As this study focuses on the efficiency of methods/software, the type of philosophy that will be used within this report centers around positivism – this is because statistics will be relied upon heavily, primarily as it will need to be understood the success rates of specific methods/software, joined with this, as a survey will be given out for a number of people to complete, the results which will be found/used will be purely mathematical and will be used to base a conclusion off. In terms of the approach that will be completed, induction will take precedence, this is because the aim is to understand the opinion of the some of the professionals within the field and what they believe needs to be done to improve the current systems in place, and to collect the viewpoints of the public.

As the methods that will be used to gather information center around research and using other documentation to provide evidence for some points that are going to be made and draw an evaluation from, it is important to ensure the reliability of each source that is going to be used, joined with ensuring its validity. The internet is full of many different resources, articles, journal entries, and some PDF books but a lot of what you see is unreliable – for the final year project you have to ensure you can find information such as: the author, the publishing company/origins, when it was written, and some other defining factors which contribute to defining whether the source that is being used is reliable or not. Reliability within research is essential because it highlights the ‘consistency of a measure and the validity about how accurate the measure is’ [7]

1.6 How will the objectives be completed?

The first objective in this study is to get an understanding of the estimated amount of people that have fallen victim to malware attacks over the past two years, whilst it is understood that you cannot get a true, fully accurate reading for this particular piece of data (as some people will not have partaken in other widespread surveys, or discussed their issues privately), some understanding of the general amount can be understood by reviewing other studies/reports into malware attacks or network attacks – there is plenty of information that can be acquired using services online.

However, whilst some of the data that will be used to investigate this issue will be data from other reviews/reports etc.... this study will also include a study that will be conducted by the writer. The study will be a survey – the aim of this study is to understand the impact that malware can have on a select control amount of people, thus one is able to analyse the answers to the questions in as much depth as possible and know that the data is valid as it would have been first-person research.

The sample size of the survey will be 50 – these will be people from different parts of the world, however it is expected that the most concentrated country that will produce results will be Great Britain because it is the residence of the study-holder and family and friends will also be asked to fill in the survey (all of which are of different ages and genders). The survey will be conducted using Google Sheet’s survey – meaning that it is available online.

The second objective is to analyse all the standard, current network security methods that are in place in the average household – this will be done through a lot of research, this is because it is important to understand the variety of different security measures that are currently being used in different regions and how they're being implemented. There are, of course, many outdated means of security that are still being used. For this section, a lot of books and reports will be used to validate claims or generate evidence regarding the point. The survey that will be conducted will also help with understanding the security methods used, as a part of the survey will focus solely on what the person uses in their own home.

Objective three focuses on investigating what the future of network technology is – what ideas are up and coming, and what will the public be able to use as a widespread measure within the next few years. This primarily focuses around investigating the tech world – this section may take a lot more research, but it is also an aim to contact those who work within the field and are thought to be 'experts' within the field, or have a large amount of experience, to understand their opinion on the matter.

The fourth objective is simply an evaluation – there, the efficiency of the security of home networks will be evaluated, using information that was acquired throughout the entirety of the investigation – this evaluation will be developed and decided on using the information that was provided, it will be an unbiased summary of what was found throughout the duration.

Limitations, Issues, and Data Evaluation

Of course, network security is one of the most fundamental elements of any network – by conducting such an investigation, it is possible that some obscure elements of network security could be exposed through this investigation and should it fall into the wrong hands, this information could be used for malicious intent. Joined with this, part of the investigation is to find out the up and coming security measures, it is very likely that there will be some sort of limitation on the information available to be used within the report.

As this is an investigation-based study, the risks and limitations, along with legal issues, are very little and the limitations/risks that are evident are of very little risk and will not have that much of an affect on the outcome of the investigation. However, to combat the issues that were highlighted, the investigation will be kept secure using encryption and a key which the writer will only have access too. The data will also only be backed up on secure drives/clouds and USB's to prevent loss. In terms of gathering enough information to discuss the up and coming security measures, the only way in which this can be combatted is to find all means of study, resort to books, journals, and many other ways to gather information and ensure that as much information is found as possible.

The data that will have been collected will be evaluated by comparing the statistics of efficiency and success of different types of software/methods that are used widespread. Joined with this, the data that will be collected through the survey results will be analysed

and evaluated using statistics to enforce/backup points- explaining each of the results that are needed, in detail, and talking about what it means.

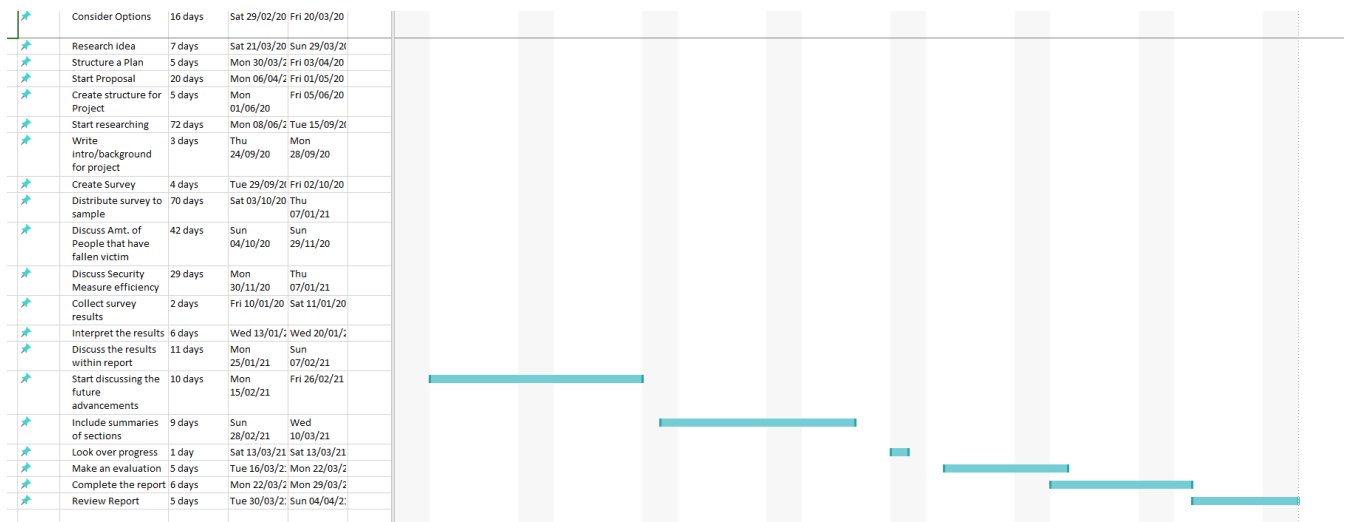
Resources & Planning

The resources that will be needed to complete this investigation are:

- A PC
- Internet Access
- Word
- Project
- Journals
- Books
- Google Sheets

Gantt Chart:

Research idea	7 days	Sat 21/03/20	Sun 29/03/20
Structure a Plan	5 days	Mon 30/03/20	Fri 03/04/20
Start Proposal	20 days	Mon 06/04/20	Fri 01/05/20
Create structure for Project	5 days	Mon 01/06/20	Fri 05/06/20
Start researching	72 days	Mon 08/06/20	Tue 15/09/20
Write intro/background for project	3 days	Thu 24/09/20	Mon 28/09/20
Create Survey	4 days	Tue 29/09/20	Fri 02/10/20
Distribute survey to sample	70 days	Sat 03/10/20	Thu 07/01/21
Discuss Amt. of People that have fallen victim	42 days	Sun 04/10/20	Sun 29/11/20
Discuss Security Measure efficiency	29 days	Mon 30/11/20	Thu 07/01/21
Collect survey results	2 days	Fri 10/01/21	Sat 11/01/21
Interpret the results	6 days	Wed 13/01/21	Wed 20/01/21
Discuss the results within report	11 days	Mon 25/01/21	Sun 07/02/21
Start discussing the future advancements	10 days	Mon 15/02/21	Fri 26/02/21
Include summaries of sections	9 days	Sun 28/02/21	Wed 10/03/21
Look over progress	1 day	Sat 13/03/21	Sat 13/03/21
Make an evaluation	5 days	Tue 16/03/21	Mon 22/03/21
Complete the report	6 days	Mon 22/03/21	Mon 29/03/21
Review Report	5 days	Tue 30/03/21	Sun 04/04/21



Conclusion

To summarize, the primary motive behind this investigation is to see whether the average home network security measures are reliable enough to protect people from attacks – it is also an aim to get an understanding of how many people are affected by malware and other types of attacks and understand why this is so. This study will be interesting to investigate because of the complexities and depth of the issues – it is tackling an every-day issue that many people encounter – it leaves you thinking “How efficient is home network security?”.

Bibliography

- [1] E. Andrews, “Who Invented the Internet?,” *HISTORY*, 2019.
- [2] B. Daya, “Network Security: History, Importance, and Future,” Florida, 2013.
- [3] A. J, “IPV6: The Next Internet Protocol,” [Online]. Available: www.usenix.com/publications/login/2005-.
- [4] P. Alto, “What is Network Security,” [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-network-security>.
- [5] J. P. Virginia Harrison.
- [6] U. Khan, “Computer Virus Attacks”.
- [7] F. Middleton, “Reliability Vs Validity: What's the difference?,” [Online]. Available: <https://www.scribbr.com/methodology/reliability-vs-validity/>.
- [8] H. o. Commons, Artist, *Broadband coverage and speeds: local statistics*, 2017. [Art]. UK Gov, 2017.

