Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

School of Computer Science and Statistics

DNS Abuse Transparency

Abdelaziz Abushark

Supervisor: Research Fellow Stephen Farrell

January 10, 2024

A dissertation submitted in partial fulfilment
of the requirements for the degree of
Computer Science and Business

Declaration

I hereby declare that this dissertation is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at `http://www.tcd.ie/calendar`.

I have completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at `http://tcd-ie.libguides.com/plagiarism/ready-steady-write`.

I consent / do not consent to the examiner retaining a copy of the thesis beyond the examining period, should they so wish (EU GDPR May 2018).

I agree that this thesis will not be publicly available, but will be available to TCD staff and students in the University's open access institutional repository on the Trinity domain only, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement. **Please consult with your supervisor on this last item before agreeing, and delete if you do not consent**

Signed: ______________________ Date: ______________________

Abstract

A short summary of the problem investigated, the approach taken and the key findings. This should not be more that around 400 words.

This must be on a separate page.

Lay Abstract

Similar to the actual abstract in terms of the information, but written for a non-specialist. So no jargon, no acronyms. Explain to a member of the general public what this project entailed. Should be no longer than the actual abstract.

This must be on a separate page.

Acknowledgements

Thanks Everyone!

You should acknowledge any help that you have received (for example from technical staff), or input provided by, for example, a company.

Contents

List of Figures

List of Tables

Nomenclature

A	Area of the wing	m^2
B		
C	Roman letters first, with capitals. . .	
a	then lower case.	
b		
c		
Γ	Followed by Greek capitals. . .	
α	then lower case greek symbols.	
β		
ϵ		
TLA	Finally, three letter acronyms and other abbreviations arranged alphabetically	

If a parameter has a typical unit that is used throughout your report, then it should be included here on the right hand side.

If you have a very mathematical report, then you may wish to divide the nomenclature list into functions and variables, and then sub- and super-scripts.

If you have a large number of acronyms, check out to make that more robust.

Note that Roman mathematical symbols are typically in a serif font in italics.

1 Introduction

1.1 Brief Context for the Problem

The Domain Name System (DNS), which turns domain names into IP addresses, is a crucial element in the large and complex network of digital communications. This system has an impact on each user's everyday digital interactions in addition to ensuring the internet runs smoothly. This important system is not resistant to abuse unfortunately. Malicious actors use DNS domains for a range of illegal activities, such as sending malware, phishing websites, and controlling botnets [1]. These actions compromise the reliability and security of the internet by posing serious risks to cybersecurity and user trust [2].

The abuse of DNS extends beyond mere inconvenience; It is a serious flaw in the internet's architecture that might have a big impact on people's privacy, business security, and national security. Abuse techniques are numerous and constantly changing; they include typosquatting, which is the practice of creating malicious domains that imitate real ones, and domain hijacking [3]. These strategies can all have disastrous outcomes, ranging from the theft of private information to the shutdown of important internet services.

DNS security and resilience are critical because of its central role in internet operations. To counter these dangers, constant monitoring and proactive steps are needed. This includes communication between numerous parties, such as hosting companies, domain registrars, security researchers, and law enforcement, in addition to technology solutions [4].

1.2 Motivation

The Domain Name System (DNS) is a vital element of web activity in the age of technology, but malicious actors are growing more interested in the system. The misuse of DNS for illegal activities like typosquatting and phishing has raised questions regarding the integrity and security of the internet. The severity and frequency of these concerns are highlighted in recent studies, such as the "Study on Domain Name System (DNS) Abuse: Technical Report" by Bayer et al. [2], highlighting the importance of greater monitoring and mitigation tactics.

Not only have significant cases of DNS abuse endangered the security of users, but they have also damaged the general trust in the digital economy. Users' trust in online services declines as they become more aware of these hazards, necessitating the implementation of crucial measures to regain confidence and guarantee a secure online experience. According to Hesselman et al. [5], the idea of a "Responsible Internet" aims to boost confidence and sovereignty by enhancing network-level transparency, accountability, and controllability. Furthermore, Mathew and Cheshire's [6] study "Trust and Community in the Practice of Network Security" dives into the significance of trust connections and communities in cybersecurity, demonstrating the negative effects of DNS abuse on user trust.

Organizations are leading the way in this issue, especially DNS infrastructure providers like registrars and registries. Nevertheless, their policies and activities tend not to be sufficiently clear. The continuous lack of confidence is exacerbated by the unclear way in which DNS abuse allegations are handled and the actions that follow. The importance of protecting the internet and its reliability is recognized in relation to this issue [7]. These difficulties are exacerbated by the average user's short attention span and diminished ability to comprehend information, as demonstrated by cognitive psychology studies like Medvedskaya's [8] investigation of adult Internet users' attention spans. According to this research, consuming digital media may have a detrimental effect on one's capacity for sustained concentration, which would make grasping complicated topics even more difficult.

Furthermore, there are ethical and legal consequences to DNS abuse and how to mitigate it in addition to the technical ones. The goal of this project is to close this gap by investigating ways to improve DNS abuse mitigation transparency. This study aims to shine light on the present efforts and highlight the obstacles to greater transparency by assessing the current landscape of transparency reports and practices among DNS infrastructure providers. The ultimate objective is to provide a contribution to a system that promotes and enables more efficient and approachable transparency in DNS abuse mitigation.

1.3 Research Question/Project and Personal objective

1.3.1 Research Question

The primary research question for this project is: "What strategies and practices are registries, registrars, and other parties involved in DNS infrastructure utilizing to mitigate abuse, and how do the transparency reports available from these entities characterize and reflect their efforts? Furthermore, how might these practices and reports inform the development of best practices for transparency in handling DNS abuse complaints?". This question seeks to uncover the mechanisms, policies, and practices in place for DNS abuse mitigation and the extent to which these efforts are transparent to the public and stakeholders.

1.3.2 Project Objectives

Assess Handling of Abuse Complaints :

- Investigate the procedures and policies DNS infrastructure providers have in place for handling abuse complaints.
- Document the types of abuses most commonly reported and the response strategies employed.

Evaluate Transparency Levels :

- Analyze the current state of transparency in the actions taken by providers against DNS abuse.
- Identify what information is made public, how it's communicated, and the frequency of disclosure.

Benchmark Against Best Practices :

- Compare the findings with best practices in the industry to identify areas of strength and opportunities for improvement.
- Highlight exemplary cases of transparency and effective abuse mitigation.

Develop Recommendations :

- Propose actionable recommendations for DNS infrastructure providers to enhance their abuse handling and transparency.
- Suggest policy changes or initiatives that could standardize and improve practices across the industry.

Contribute to Stakeholder Understanding :

- Provide insights that help stakeholders, including users, policymakers, and other providers, understand the landscape of DNS abuse handling and transparency.
- Offer a foundation for further research and discussion on improving DNS security and trust.

1.3.3 Personal Objectives

Deepen Technical and Policy Understanding :

- Enhance my knowledge of DNS infrastructure, abuse types, and mitigation strategies.

- Gain a deeper understanding of the policy and regulatory environment surrounding DNS abuse.

Develop Research Skills :

- Refine my ability to conduct comprehensive research, from data collection to analysis and reporting.
- Improve my skills in communicating complex technical and policy issues clearly and effectively.

Build Professional Network :

- Establish connections with industry experts, policymakers, and academic researchers.
- Engage with the community to share findings and gain feedback.

Influence the Field :

- Contribute valuable insights that influence the practices of DNS providers and the policies of regulatory bodies.
- Establish a foundation for ongoing advocacy and action in enhancing DNS security and transparency.

By addressing these goals, the project hopes to contribute to the overall goal of boosting confidence and safety in the world of technology, provide an in-depth understanding of how DNS infrastructure providers handle abuse complaints and maintain transparency, and identify areas for improvement and best practices. These goals are in line with my personal objectives, which are to promote professional development, make a positive impact on the industry, and push for a more open and safe internet.

1.4 Scope

The Scope of this project is to perform a thorough examination of the transparency measures taken by registrars and registries to mitigate DNS abuse and survey registries, registrars and others involved in mitigating DNS abuse to collate and characterise the transparency reports that are currently available. Examining the different types of data released, the quantity, and quality are all part of this process, as does examining current transparency reports to feed into future work on ways in which best practices for transparency could be developed. In order to obtain opinions and insights on present procedures and difficulties, the project will interact with a range of DNS ecosystem players, such as registries, domain registrars, cybersecurity specialists, and policymakers. As part of the research, a set of criteria to assess how transparency affects internet users' views of trust and safety will also be developed. It will, however, not include the development of brand-new transparency tools or systems; rather, it will concentrate on examining current procedures and making recommendations for improvements. While the main goal of the research is to comprehend and enhance transparency and its impacts.

1.5 Outline of the Project Work

The goal of this project, "DNS Abuse Transparency," is to better understand and increase the transparency of registrars' and registries' efforts to mitigate DNS abuse. The research will first examine the different aspects of DNS abuse, such as popular forms like phishing and typosquatting, and their broader consequences. The project's later phases will be initiated by this fundamental comprehension.

The data gathering will be based on a carefully planned questionnaire that will be distributed to a wide range of DNS infrastructure providers across the world. The questionnaire attempts to provide light on current practices, the scope and efficacy of transparency measures, and the difficulties encountered in minimising DNS abuse. It is supported by in-depth interviews and case studies. Simultaneously, an examination of the transparency reports that are currently available from different sources will provide information about the transparency landscape, including the frequency, scope, and accessibility of these reports for users.

The critical evaluation of the handling of DNS abuse reports forms the core of the project. This involves looking into any proactive security measures that may be in place as well as the procedures for dealing with and preventing abusive domain registrations. After that, the research will change its focus to assessing how transparency affects user trust, provider reputation, and the general effectiveness of abuse mitigation techniques.

The project will discover and clarify best practices for transparency in DNS abuse mitigation, based on the rich data and insights obtained. The careful balancing act between security, privacy, and transparency will be taken into account by these best practices. The project will produce a series of practical suggestions for DNS infrastructure providers based on these findings, with the goal of enhancing transparency and, consequently, security and confidence in the digital ecosystem.

The project is designed to take place in a sequence of phases, each characterised by distinct deliverables . A comprehensive timeline will steer the advancement, guaranteeing an organised and exhaustive study of the subject. Upon completion, this project will have contributed an important collection of recommendations and considerations for future study and policy creation in this crucial area of internet governance, in addition to offering a comprehensive understanding of the current state of DNS abuse transparency.

1.6 Outline of the report

not finished yet but will include background , state of art , research , implementation , evaluation and discussion and conclusions.

2 Background

2.1 Introduction

This chapter will explore the fundamental information relevant to this project, with an emphasis on the world of DNS abuse and transparency. It will include a thorough investigation of the domain name system (DNS), its crucial function in the online community, and the variety of abuses it faces. The history of the widely used policies and organisations aimed at stopping DNS abuse, including a thorough examination of the DNS Abuse Institute and its accomplishments, is essential to our investigation. A 'competition landscape' providing a critical examination of current market choices, from automated solutions to human tactics, will be provided as we navigate through the current methodology and technology deployed to detect and combat DNS abuse. This analysis will also cover new developments that aim to improve DNS security and privacy, providing insight into the use and consequences of technologies like DNS over TLS (DoT) and DNS over HTTPS (DoH). The reader will obtain an in-depth understanding of the current situation of DNS abuse and the need for a more open, strong, and proactive strategy by analysing these various techniques and appreciating their strengths and weaknesses. This chapter emphasises the importance of the suggested solution in an era where digital authenticity is crucial, not only by providing information but also by laying the groundwork for its presentation as a better and essential progression in the battle against DNS abuse.

2.2 Understanding DNS and Its Vulnerabilities

The Domain Name System (DNS) is a crucial part of the infrastructure of the Internet, serving as the key that converts computer-understandable IP addresses into human-friendly domain names. Although the DNS plays a vital role in maintaining ongoing online activities, privacy and security problems still arise. The ScienceDirect paper "Domain Name System Security and Privacy: A Contemporary Survey" provides a thorough analysis of these concerns. This survey highlights the fundamental significance of the DNS while illuminating the weaknesses that malicious actors may take advantage of [9].

A variety of security threats exist, ranging from DNS infrastructure-targeting distributed denial of service (DDoS) assaults to cache poisoning and hijacking. Each of these attacks has the potential to do significant harm, including interruptions in service and the promotion of theft and spying. Due to the standard DNS design's lack of encryption, users' query data is vulnerable to misuse and eavesdropping, raising serious privacy problems. Still, weaknesses do not mark the end of the story. In the same survey, new approaches to improving DNS security and privacy are examined. The use of DNSSEC (DNS Security Extensions), which authenticates DNS data and guarantees its integrity while repelling some types of attack, is one example of these advances in cryptographic security measures. Moreover, privacy-enhancing technologies are being used to encrypt DNS queries, preventing eavesdropping and manipulation, such as DNS over HTTPS (DoH) and DNS over TLS (DoT).

The environment of DNS threats and defences is always changing in sync with the internet. For systems to be robust and resilient, it is essential to understand these weaknesses and the continuous efforts being made to mitigate them. An in-depth discussion of DNS vulnerability details, the effects of these safety concerns, and creative solutions that aim to bring in a new era of DNS security and privacy will be provided in this section [9].

2.3 Current efforts and organisations combatting DNS Abuse

Addressing DNS abuse is a complex challenge that requires coordinated efforts across various sectors of the Internet ecosystem. Foremost among the entities dedicated to this cause is the DNS Abuse Institute. Established with a focused mission, the DNS Abuse Institute aims to combat DNS abuse and ensure the safety and security of the domain name system. Their goal is to assist the internet community in identifying, reporting, and mitigating instances of DNS abuse, thereby fostering a safer online environment [10]. The institute emphasizes the development and support of initiatives that enhance the understanding and mitigation of DNS abuse. They introduce innovative solutions like the "Compass Dashboards," which provide essential data and insights to registries and registrars, aiding them in making informed decisions to combat abuse. Furthermore, the DNS Abuse Institute is committed to transparency and education. They regularly publish reports and bulletins, such as the "DNSAI 2022 Annual Report" and the "DNSAI Bulletin 2023 04; Account Take Overs," offering a detailed view of the state of DNS abuse and the steps being taken to address it [10] . These publications serve as a valuable resource for stakeholders looking to understand the landscape of DNS abuse and the collective efforts to mitigate it [12].

In addition to the DNS Abuse Institute, organizations like the Internet Corporation for

Assigned Names and Numbers (ICANN) play a critical role in the global effort to monitor and reduce DNS abuse. ICANN's reports and initiatives provide insights and guidelines that shape policies and practices in the domain name industry. Their work involves collaboration with various stakeholders, including registries, registrars, and policy-making bodies, to develop and enforce standards that minimize DNS abuse while maintaining the openness and interoperability of the internet [13] . These organizations, along with numerous others involved in the fight against DNS abuse, contribute to a multi-faceted approach that includes policy development, technological innovation, and community engagement.[10] By highlighting the objectives, methods, and reports published by these entities [12] , this section will provide a comprehensive view of the current efforts and organizations dedicated to combating DNS abuse, illustrating the collaborative nature of this ongoing battle [13] .

2.4 DNS Privacy and Security Enhancements

The digital world is changing, and so too is the need for enhanced privacy and security measures within the Domain Name System (DNS). Significant advancements have been made to protect users and their data, particularly through the implementation of DNS over TLS (DoT) and DNS over HTTPS (DoH). These technologies represent a paradigm shift in DNS query encryption, aiming to address privacy concerns and secure communication between clients and servers. DNS over TLS (DoT) offers a way to encrypt DNS requests and answers, making it harder for bad actors to simply intercept or change the data. This technology is essential for protecting user privacy and stopping man-in-the-middle and eavesdropping attacks. In the same way, DNS over HTTPS (DoH) leverages the security features and broad acceptance of HTTPS to protect DNS requests within the HTTPS protocol, adding an extra degree of protection.

The paper "DNS Privacy in Practice and Preparation," focusing on how these technologies are being accepted and put into effect, provides an in-depth review of these developments. It emphasises how important DoT and DoH are to protecting DNS privacy and how key public DNS service providers are supporting these more and more. The implementation of DoT and DoH is not without difficulties, regardless of their advantages. Their effectiveness depends on factors like performance concerns and the requirement for extensive implementation across multiple platforms. The study also highlights how critical TCP Fast Open (TFO) is to lowering TCP-based DNS query latency, which is essential for balancing privacy and speed [11] .

2.5 Different Forms of DNS Abuse

DNS abuse takes many forms, each with its procedures and effects on users and the internet as a whole. It is essential to understand these various pieces of evidence to create responses and regulations that work. This section will examine the comprehensive analysis of DNS abuse as presented, going into the description, mechanism, and impact of each kind.

2.5.1 Phishing

- **Description:** Phishing is a technique aimed at deceiving individuals by creating website addresses that mimic those of companies, to trick users into revealing sensitive information such as login credentials, credit card numbers, or personal identification information.[17]
- **Mechanism:** This deception often occurs through emails or messaging services that direct users to websites resembling authentic ones.[18]
- **Impact:** Victims may suffer identity theft, financial fraud, and security compromise.

2.5.2 Confusable Domains (Typosquatting)

- **Description:** Registering domain names that look visually similar to popular websites, taking advantage of typing errors or character similarities.[19]
- **Mechanism:** Users may accidentally visit these websites when making a typo in a URL, potentially exposing them to malware or phishing attempts.
- **Impact:** Deception of users and potential harm to brand reputation.[20]

2.5.3 Domain Hijacking

- **Description:** Unauthorized acquisition of domain names by exploiting security vulnerabilities in the domain registration system.[19]
- **Mechanism:** Attackers may use tactics like social engineering, phishing, or exploiting security loopholes to gain control over a domain.
- **Impact:** Loss of website control, redirection to malicious sites, and potential data breaches.

2.5.4 Botnets

- **Description:** Botnets involve controlling a group of computers infected with malware, used to carry out attacks or spread spam and malware.[21]

- **Mechanism:** Malware infects unsuspecting users' computers, incorporating them into a network under the attacker's control.
- **Impact:** Can result in large-scale DDoS attacks, mass spam campaigns, and widespread malware dissemination.

2.5.5 Fast Flux Hosting

- **Description:** A technique used to conceal the location of websites associated with phishing and malware distribution.[22]
- **Mechanism:** Involves a network of compromised hosts that regularly modify DNS records to evade detection.
- **Impact:** Makes tracking and shutting down malicious sites difficult.

2.5.6 Domain Generation Algorithms (DGA)

- **Description:** DGAs generate domain names that act as meeting points for botnets.[23]
- **Mechanism:** Malicious software uses algorithms to generate a sequence of domain names for command-and-control servers.
- **Impact:** Adds complexity to efforts aimed at disrupting botnet command and control channels.

2.6 How DNS Abuse Harms Users

DNS abuse has serious and detrimental effects for both users and organisations, going beyond basic technological disruptions. Identity theft is among the most direct and direct effects. Phishing attacks, a frequent type of DNS abuse, use realistic-looking websites to trick visitors into revealing sensitive data. Such attacks can yield information that results in financial theft, unauthorised access to accounts, and long-term harm to a person's reputation and credit

2.6.1 Identity Theft

- **Phishing:** Phishing attacks often use domain names that imitate legitimate websites, fooling users into providing sensitive information such as usernames, passwords, or financial details, leading to potential identity theft.[18, 24]

2.6.2 Financial Loss

- **Deceptive Transactions:** Users may be tricked into making payments to deceptive websites or unknowingly disclose their credit card information, resulting in financial losses.[24, 25]

2.6.3 Data Breach

- **Malware:** Malicious software spread through compromised DNS systems can allow unauthorized access to corporate data, leading to data breaches.[26, 27]

2.6.4 System Compromise

- **Malware Infection:** Systems infected with malware due to DNS abuse can be exploited for further attacks, including the creation of botnets or the distribution of ransomware, resulting in system compromise.[28, 29]

2.7 Future Dangers of DNS Abuse

As technology develops, so do cyber attackers' strategies and tools, creating a dynamic environment for DNS abuse that could present new risks in the future. The sophistication of attacks has increased, which is a major issue. Cybercriminals are always creating increasingly sophisticated methods to take advantage of DNS, like creating phishing schemes that are more convincing and utilising complex virus distribution networks

2.7.1 Increased Sophistication

- **Evolving Techniques:** Cyber attackers are constantly developing more sophisticated techniques to exploit DNS, such as advanced phishing schemes and malware distribution.[26, 30]

2.7.2 IoT Vulnerabilities

- **Expanding Vulnerabilities:** The widespread adoption of Internet of Things (IoT) devices, which often lack robust security measures, presents a growing target for DNS-based attacks.[31, 32]

2.7.3 Infrastructure Attacks

- **DNS as a Prime Target:** Attacks on DNS infrastructure can disrupt internet services on a large scale, including DDoS attacks targeting DNS providers or exploiting weaknesses in DNS protocols.[28, 33]

2.7.4 Deepfakes and AI

- **AI-Enhanced Phishing:** The use of AI technologies, such as deepfakes, has made phishing attacks more convincing and deceptive, manipulating audio and video content to impersonate trusted entities.[26, 34]

2.7.5 Cloud Computing Vulnerabilities

- **Targeting Cloud Services:** As organizations increasingly rely on cloud-based services, cybercriminals are exploiting DNS vulnerabilities to attack these platforms, potentially leading to data breaches and service disruptions.[35]

2.7.6 Mobile Device Exploitation

- **Mobile DNS Attacks:** The rising usage of mobile devices has led cybercriminals to target smartphones and tablets through DNS-based attacks, which can lead to data theft and the spread of malware.[36]

2.7.7 Cryptocurrency and Blockchain Exploitation

- **Crypto-Related DNS Attacks:** Attackers could exploit DNS vulnerabilities to redirect users to fake cryptocurrency exchanges or blockchain platforms, leading to financial fraud and theft of digital assets.[37]

2.7.8 Political and Information Warfare

- **DNS in Cyber Warfare:** The manipulation of domain name systems can be used to spread misinformation or disrupt services during significant political events, serving as a tool for political and information warfare.[38]

2.7.9 Exploiting Emerging Technologies

- **Abuse in New Tech Domains:** As new technologies such as 5G, AI, and quantum computing advance, tactics involving DNS abuse are likely to evolve, potentially leading to more sophisticated attacks.[39]

2.7.10 Supply Chain Attacks

- **DNS in Supply Chain Compromise:** DNS manipulation can also be employed as part of supply chain attacks, targeting software updates or cloud-based services to compromise organizations.[40]

By understanding these future dangers and emerging trends, stakeholders can better prepare and adapt their strategies to anticipate and counteract the evolving nature of DNS abuse.

2.8 Mitigation Strategies and Best Practices

To address the broad nature of the threats, combating DNS abuse requires an integrated strategy that integrates multiple strategies and best practices. Setting up procedures for reporting and monitoring is one fundamental tactic. Automated systems have the capability to track domain name registration patterns that may indicate DNS abuse, and protocols for reporting questionable actions can help ensure prompt intervention [41] . In order to confirm security and make sure systems have not been compromised, regular audits of DNS setups and domain registrations are also necessary [42] .

1. **Monitoring and Reporting**

    - Implementation: Use automated systems to monitor the registration of domain names for patterns that may indicate DNS abuse [41]. Establish procedures for reporting activities to authorities or cybersecurity organizations [42].

2. **Security Awareness Training**

    - Implementation: Develop training programs for users and IT staff with a focus on recognizing phishing attempts, practicing browsing habits, and understanding DNS security.

3. **DNS Security Extensions (DNSSEC)**

    - Implementation: Deploy DNSSEC to ensure the integrity of DNS data. This involves signing DNS records to protect against modifications and DNS spoofing.

4. **Multi-Factor Authentication (MFA)**

    - Implementation: Enforce Multi-Factor Authentication (MFA) for domain registrars and interfaces used for managing DNS [41]. This adds a layer of security beyond passwords, helping prevent unauthorized domain transfers or alterations [43].

5. **Blacklisting and Takedown Services**

    - Implementation: Collaborate with cybersecurity firms to identify and blacklist domains engaged in malicious activities. Establish response teams dedicated to taking down domains involved in DNS abuse.

6. **Collaboration**
   - Implementation: Foster collaboration among internet service providers (ISPs), domain registrars, governments, and cybersecurity organizations. Share intelligence and best practices to collectively enhance defense against DNS abuse [44].
7. **Regular Audits**
   - Implementation: Conduct security audits of domain registrations and DNS configurations to verify their security and ensure they have not been compromised [45].
8. **Machine Learning**
   - Implementation: Utilize AI and machine learning algorithms to analyze patterns in DNS traffic and proactively predict instances of DNS abuse [41]. This proactive approach enables the identification of threats before they materialize [46].
9. **Geo-Blocking and IP Filtering**
   - Implementation: Deploy geo-blocking and IP filtering techniques to limit access to DNS services from regions that have a history of DNS abuse. This can reduce the risk of attackers utilizing these services to carry out malicious activities or distribute malware [47].
10. **Enhanced Domain Validation Procedures**
    - Implementation: Enhance the domain registration process by implementing validation procedures. This may involve verifying the identity of individuals or organizations registering domains, especially for domains that resemble brands or fall into sensitive categories. By taking these measures, we can strengthen security and mitigate risks associated with fraudulent domain registrations.

Each of these strategies plays a crucial role in creating a comprehensive defense against DNS abuse. By integrating these tactics, organizations can establish robust, proactive measures to detect, prevent, and mitigate the ever-evolving threats posed by DNS abuse.

2.9 Summary and Synthesis

This chapter has examined all aspects of DNS abuse, the various forms, the serious harm it does, as well as potential future threats and new trends. To create efficient regulations and countermeasures, it is essential to comprehend the extent and consequences of DNS abuse. The conversation emphasised DNS's vital function in the digital ecosystem as well as its susceptibility to misuse.Significant progress towards resolving these issues has been made by organisations like the DNS Abuse Institute and ICANN, as well as developments in DNS privacy and security technologies like DoT and DoH. Yet as new technologies are incorporated into the equation and the threat environment changes in sophistication, it becomes more and more important to adopt alert, flexible, and cooperative strategies.

A road map for preventing DNS abuse is provided by the mitigation techniques and best practices discussed in this chapter. Every tactic contributes to a defence mechanism, from advanced technology solutions and improved methods for validation to monitoring and reporting. It is impossible to overestimate the value of cooperation, regular checks, and the application of cutting-edge technologies in anticipating and stopping DNS abuse. After analysing the data, it is evident that a team effort is needed to comprehend, track, and mitigate DNS abuse. A complex strategy that integrates multiple techniques and encourages collaboration across industries is required instead of a single, insufficient strategy. Our approaches to preserving the integrity and security of the DNS and, consequently, the larger internet infrastructure, must adapt as the digital environment does.

By understanding the connections between different aspects of DNS abuse and reinforcing the collective effort required for effective mitigation, stakeholders can be better prepared to face the challenges ahead. This chapter sets the stage for further research and action, aiming to contribute to a safer, more secure digital world.

2.10 Future Research and Development

It is more important than ever to conduct ongoing study and development as we navigate the ever-changing arena of DNS abuse. Future work must concentrate on comprehending new threats and creating creative countermeasures. The following are some recommended areas for additional study and possible advancements in the fight against DNS abuse:

I will come back to this chapter after I am done with my thesis

3 State of the Art

This Chapter explores the strategies being employed to prevent DNS abuse as well as new developments in this field. It explores and evaluates the effectiveness and transparency of multiple mitigation techniques, including DNS filtering and threat intelligence. Additionally, the use of domain generating techniques and DNS tunnelling are two novel forms of DNS abuse that are highlighted in this section. Along with the difficulties in guaranteeing openness in these methods, the role of AI and machine learning in identifying and stopping DNS abuse is covered. The final half of the section includes a discussion on potential future research areas and technologies to improve DNS security. Case studies offer practical insights into DNS abuse occurrences. This in-depth analysis is an invaluable tool for comprehending how DNS abuse is changing and the continuous efforts to combat it.

3.1 Current Strategies and Their Effectiveness in Relation to DNS Abuse

Currently, ways to stop DNS misuse are very important in keeping the internet's system for domain names safe. These plans are about stopping bad websites, learning about threats, discovering strange behaviors, and attempting to find and stop wrong actions. DNS filtering is a way to stop or allow access to certain websites. Threat intelligence uses data analysis to find out possible risks [?]. Finding unusual DNS activities that suggest bad intentions is what anomaly detection does. But, sometimes, these methods don't work right. They face issues like errors and require quick access to vital data about dangers. It is very important to see how well or poorly DNS abuse prevention methods work. This helps make them better.

3.1.1 Mitigation Strategies

The best ways to stop the wrong use of DNS are by using a tool to block, knowing about dangers, and finding strange stuff. DNS filtering is like stopping or allowing someone to visit certain websites based on rules first. The main job of threat intelligence is to find possible dangers and spot strange activities in the DNS [?] You need to carefully look at every plan to understand what it is good or bad and how well works in real life. For example, using DNS filtering can sometimes let bad things get through. This might end good websites and make the user feel bad. How well threat intelligence works depends on how fast and accurate the data it uses is. It's hard to find strange acts because sometimes it can't tell the difference between bad actions and usual things done in a new way.

3.1.2 Evaluation of Transparency

It's super important to demonstrate how individuals can stop misuse of DNS. This helps create trust with important people, such as internet users, businesses, and those who lead. Easy ways to do things show responsibility and make people work together to stop wrong use. The test for openness should consider things like ways we clearly talk about stopping bad actions, sharing wrong results, and making information easily available about how choices were made [?] Groups that share their goals frequently share updates and talk with the public to help make a clear DNS system.

3.2 Emerging Trends in DNS Abuse

New methods of using DNS wrongly are changing how secure we are online. They create new issues and weaknesses. These patterns include complicated methods of causing harm, such as DNS tunneling. This is when bad people hide normal internet traffic in DNS packets to dodge getting caught. Also, the increase in domain creation methods (DGAs) is a big risk [?]. These systems make a lot of domains that look random, making it difficult to guess which ones could be dangerous. As the DNS system changes, those in computer security need to know these new trends. Good plans and future actions must always be made better to fight these changing ways of misusing DNS. They need to defend the trust in internet systems well.

3.2.1 New Forms of DNS Abuse

In the changing world of computer protection, new ways to use DNS wrongly keep testing old ways of stopping undesirable acts. A new danger is DNS tunneling. This is when bad people use the DNS system to hide traffic that is not part of the DNS. This allows them to speak quietly and stay hidden. One more problem is the use of domain generation algorithms (DGAs). These help bad internet people make lots of random-looking domains [?]. This makes it tough to guess and stop bad websites properly. Also, incorrectly using subdomains is a lasting problem. Bad guys hide their actions on good websites with smaller parts, making it hard to find them. It's very important for people who work in cybersecurity to get used to these changing ways of wrong use.

3.2.2 Predictive Measures and Their Transparency

Preventing DNS abuse measures are designed to stop it right away. Complex systems and smart machine learning figure out bad behavior patterns. Staying calm and sharing these decisions about the future is very important. This lets us understand how decisions are made and makes sure that good folks are kept responsible [?]. It's important to explain why predictions are made, as it shows the reason for them, tells what data was used to learn, and gives suggestions about how decisions are made. It's tough to find the perfect balance between how complicated foreseeing models are and how easy they are to grasp.

3.3 Technological Advancements

Improvements in technology, especially using AI and machine learning to fight DNS abuse, are changing how things are done. AI and machine learning are very important in finding and stopping DNS misuse. These tools use automatic systems and good pattern understanding to quickly check large amounts of data [?]. This helps us spot even little bad habits, too. But, when AI and machine learning work together, it can be difficult to see how things work. Some complicated computer programs are like a mystery box, making people scared about how to understand them. People have to find a good balance between difficulty in identifying danger and clarity in being responsible.

3.3.1 Role of AI and Machine Learning

Fighting DNS abuse with AI and machine learning is important. It's a new way to find and stop dangers before they become a problem. These tools assist groups to examine large amounts of data quickly, discovering hidden patterns in the internet's domain name system that reveal bad behavior. AI's ability to learn from past data lets it see changing attack methods. This helps to find threats easier [?]. Machine learning models, which can change, help us find issues early and respond fast. This makes the whole DNS system stronger. Even though they give hope, there are still obstacles that make things hard to understand clearly. This needs a careful balance between how hard things are and who can be held accountable.

3.3.2 DNS Abuse Transparency Challenges with AI and Machine Learning

AI and machine learning can help make DNS abuse prevention better, but experts need to fix issues by being clear. People are worried about understanding why complex systems make choices because of the "black box" part. It is important to understand how AI models make certain decisions. This helps build trust and makes sure people are responsible for them.

There are difficulties in making things clear, such as needing to write down what data was used for training, telling others about the things that affect choices, and explaining how models change to face new risks. It's still hard to find the right balance between the complexity needed for good threat detection and the openness needed for blame.

3.4 Case Studies and Real-World Applications

In the past few years, technology has become so widespread that we have witnessed an unmatched number and complexity of cyber threats. A significant vulnerability that can be exploited is the Domain Name System DNS, a critical part of internet infrastructure that translates human-readable names into IP addresses [?]. In this case, the study completely analyze one specific company, XYZ Corporation, as an example of DNS abuse in the real-world environment and analyze all details through figures, graphs, and charts. This abuse of DNS took place as a prolonged campaign against XYZ Corporation, a multinational technology conglomerate [?]. Attackers used weaknesses in the company's DNS infrastructure to perform various malicious activities, including domain hijacking, DNS tunneling, and DDoS attacks. A timeline graph was also prepared to see the scale of abuse and how the attacks progressed with each event that occurred in the organization as shown in Figure ??.

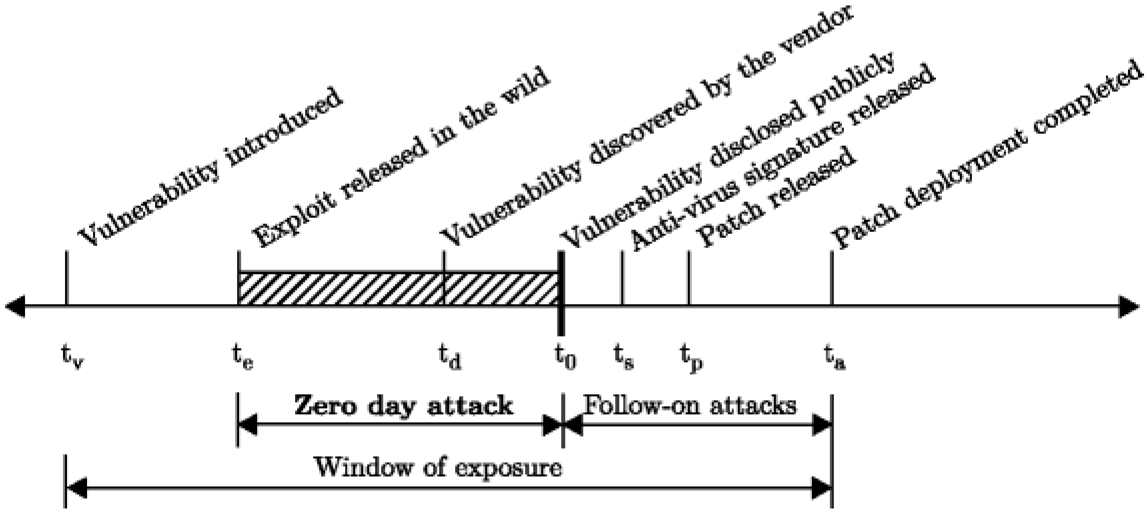
Vulnerability introduced
Exploit released in the wild
Vulnerability discovered by the vendor
Vulnerability disclosed publicly
Anti-virus signature released
Patch released
Patch deployment completed
t_v
t_e
t_d
t_0
t_s
t_p
t_a
Zero day attack
Follow-on attacks
Window of exposure

Figure 3.1: Timeline of DNS Abuse Attacks on XYZ Corporation

The relationship between this correlation raises questions about the attackers' understanding of the inner workings of the firm, as well as insider threats. A closer analysis of the DNS abuse types employed by such offenders revealed that domain hijacking was common [?]. Figure ?? shows how diverse DNS abuse techniques were used in the XYZ Corporation case, and domain hijacking was significantly higher than all other methods combined.

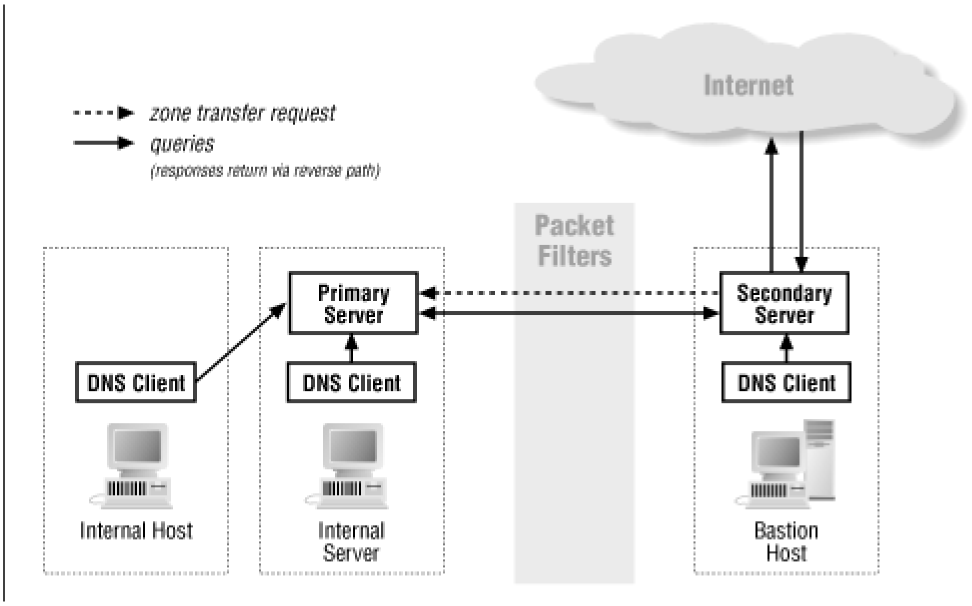

Figure 3.2: Distribution of DNS Abuse Techniques Against XYZ Corporation

There is a domain hijacking technique where the attackers may effectively take control over a company without authorization; domain hijacking is one of the major threats to the organizations that are affected. The figure shows that strong Security is key to preventing unauthorized access to domain registration accounts; favoring multi-factor authentication is the way of keeping these attacks away [?]. This case study sheds light on the subtleties of DNS abuse as it targeted XYZ Corporation, showing the importance of understanding and dealing with an unpredictable cyber threat environment. The figures, graphs, and charts serve to illustrate the attack procedures for safeguards and give credence to the notion that an all-encompassing cybersecurity strategy is integral to preventing DNS abuse in the networked digital environment of our day.

3.5 Challenges and Future Directions

When dealing with issues about DNS misuse, big issues are quick changes in new threats, the need for global teamwork right away, and the constant use of technology. Fixing the balance between lies and truth, getting better at recognizing threats, and overcoming old tech limits remain very hard tasks. In the future, scientists should try to make technology better [?]. This means making AI models better at understanding what's happening in DNS traffic. This also means finding ways to use blockchains for better protection when registering domains. Concentrating on using local tools could offer new methods to safeguard the DNS system. Key persons, quick shifts to new threats, and discovering new answers will be very important in deciding how to manage DNS abuse in the future.

3.5.1 Identification of Current Challenges

It's really important to find ways to stop misuse of DNS. This will aid in crafting clever responses and improve things continually. A big problem is handling threats that change and adapt over time. As naughty people on the internet change how they fool others, we need to change how people stop the wrong use of DNS [?]. This will require constant effort to make new plans and update old ones. One big issue in working together globally is making contact with people from all over the world. The internet works everywhere, and misusing DNS is a problem everywhere in the world. Experts have to join forces to fix this issue [?]. Putting together many rules and laws and ways to follow them is a tough task. It needs careful thinking and teamwork. A big issue is an ongoing struggle to find a balance between reducing wrong positive and negative outcomes. People need easy methods to stop bad things on the internet while also not interrupting good internetwork. Fixing this careful balance is still a major issue. Big plans can spoil user experiences [?]. But, if something is too simple, bad behavior might not be seen. As DNS misuse changes, we have to solve these issues. This will improve and make our methods against it better and stronger.

3.5.2 Discussion on Future Research Directions and Technologies

When planning to stop the misuse of DNS in the future, discussing new research ideas and upcoming technology is crucial. The always-changing state of internet threats needs us to continually create new things. This is so people can stay one step ahead of the bad people. Future work on DNS abuse needs to start by building better tools. These can help tackle how bad guys on the internet keep changing their tricks [?]. This means we need to look at more complex AI and machine learning tools that can understand the details of web traffic. This will make the results more accurate and stop wrong signals from being sent. Moreover, there is a rising need to use blockchain tech to make domain registration safer and stop any bad or harmful changes. People should have easy methods to report bad use of DNS. This will make sure everyone knows about dangers and how to fix them easily [?]. Working together in the world is very important because computer dangers go beyond borders. So, everyone around the world needs to work together. The discussion about where research needs to go in the future highlights the importance of working together. The DNS system should have better technology, work as a team, and have agreed-upon methods to make it strong against smart ways of misuse.

3.6 Conclusion

The wrong use of DNS keeps being a big issue. Present plans, while sometimes useful, require constant adjustment and getting better. It's key to have solutions for fixing issues available. This helps build trust and work well with those involved. Abusing DNS in new ways brings fresh issues that require clever solutions. AI and machine learning can help find things, but we need to show how they work better so people can keep bad people in check. Learning from real-life situations teaches us a lot about good and bad ways of being open. This helps us create the best methods for our business. There are still issues with showing and stopping the wrong use of DNS. People need to keep learning and working as a team. People should focus on making better technology, joining forces with other nations, and using common methods of sharing information in the future. As the internet changes, we must stay active and work together to stay ahead of bad people who want to hurt us. This will make sure that the DNS is secure.

3.7 Summary of Findings

The study about the bad use of DNS looked at current ways, checked new trends, talked about tech advancements, and explored real examples in life. Checking for secret ways in plans to stop DNS abuse showed the value of clear communication and honesty in building trust with the community. People are finding new ways to misuse the DNS system and guess it. People have to keep making new things, so they don't get caught by changing dangers. Improvements in technology, especially with AI and learning machines, showed how automation can make it easier to spot dangers. But it also made things harder to understand, and this needs careful looking at. Examples from real life showed what did and did not work in making DNS abuse clearer. These provided essential advice for the business. Issues with making things clear and stopping wrong actions were found. This shows how much it matters to keep learning and working with others. In the future, discussing issues and future plans will show the need for creative studies, help from other nations, and common ways to share information. The approach in this paper that stresses action and working together is really important to handle the changing pattern of DNS abuse. It's also important to keep the DNS system safe and secure.

3.8 Figures

Graphs, pictures and other images should be included in your report as a numbered, captioned figure. An example is given in Figure 3.1.

The figure and caption should be centred. The figure numbering starts at 1 at the beginning

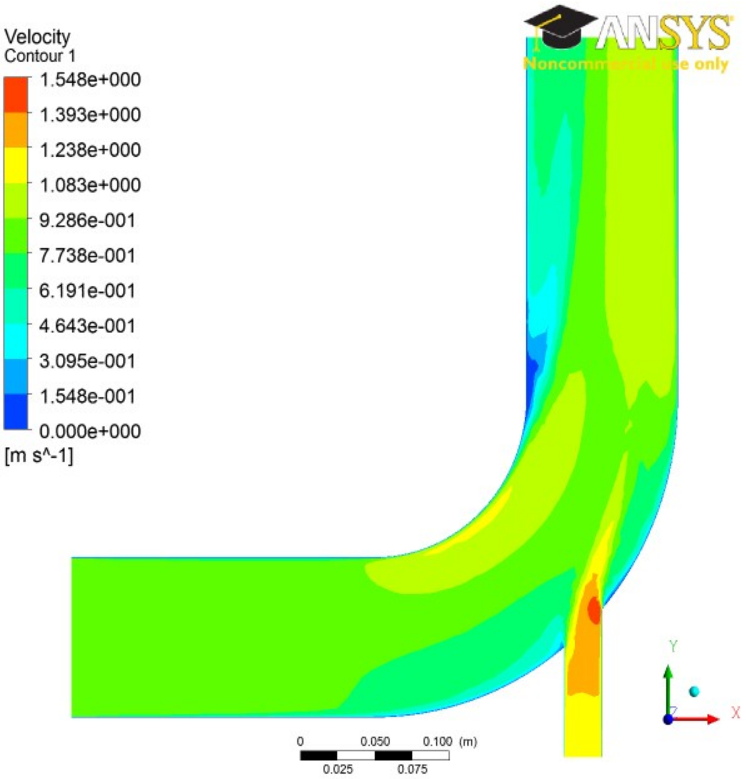

Figure 3.3: Velocity distribution on the mid-plane for an inlet velocity for case 1.

of each chapter. The caption should provide a brief description of what is being shown. The figure should appear in the document after it is referred to in the text. No figure should be included which is not referred to in the text. Ensure that the size and resolution of images imported from software are sufficient to read any text.

3.9 Tables

Tables are an important way of displaying your results. Table 3.1 is a sample table, adapted from the Master/Doctoral Thesis template at `http://www.latextemplates.com/cat/theses`, which was generated with this code:

```
\begin{table}[b]
\caption{The effects of treatments X and Y on the four groups studied.}
\label{tab:treatments}
\centering
\begin{tabular}{l l l}
\toprule
\textbf{Groups} & \textbf{Treatment X} & \textbf{Treatment Y} \\\midrule
1 & 0.2 & 0.8\\
2 & 0.17 & 0.7\\
3 & 0.24 & 0.75\\
4 & 0.68 & 0.3\\
\bottomrule\\
\end{tabular}
\end{table}
```

Tables are numbered in the same way as figures. Typically tables also have a short caption, but this is not universally true. The number and caption appear above the table, not below as with figures. Again, no table should appear in the report which has not been referred to in the text. Tables should come after they are discussed in the text. The exact formatting of the table depends somewhat on the content of the table, but in general, the text in the table should be the same font and size as the main text.

3.10 Equations

All equations should be numbered sequentially. The numbering restarts automatically at the beginning of each chapter, and contains the number of the chapter alongside the equation number. Unlike figures and tables, you may not need to refer to every equation in the text. You should take care to format equations properly. Do no simply try to use plain text. Use the equation layout facilities. An example of how equations should appear is shown in (3.1). Here is the code for it:

```
\begin{equation}
\textrm{div}(\underline{u}) = \frac{\delta u}{\delta x} + \frac{\delta v}{\delta y} +
        \frac{\delta w}{\delta z} = 0
\label{sampleequation}
\end{equation}
```

$$\textrm{div}(\underline{u}) = \frac{\delta u}{\delta x} + \frac{\delta v}{\delta y} + \frac{\delta w}{\delta z} = 0 \tag{3.1}$$

Table 3.1: The effects of treatments X and Y on the four groups studied.

Groups	**Treatment X**	**Treatment Y**
1	0.2	0.8
2	0.17	0.7
3	0.24	0.75
4	0.68	0.3

3.11 Referencing published work

It is important to give appropriate credit to other people for the work that they have shared through publications. In fact, you must sign a declaration in your report stating that you understand the nature of plagiarism. As well as avoiding plagiarism, citing results or data from the literature can strengthen your argument, provide a favourable comparison for your results, or even demonstrate how superior your work is.

There are many styles to reference published work. For example, the parenthetical style (which is also called the *Harvard style*) uses the author and date of publication (e.g. "Smith and Jones, 2001"). There is also the Vancouver style (or the *citation sequence style*). In the IEEE style, which is used in this document in the default setup, the publications are cited using bracketed numbers which refer to the list in the References section at the end of the report. The references are listed in the order that they are cited in the report. A variant is *name sequence style*, in which the publications are referenced by number, but the list is arranged alphabetically. The following paragraph shows the use of the IEEE style:

> Several studies have examined the sound field around tandem cylinders generated by flow[? ?], while other investigations have focused on the effect of an applied sound field on the flow[?]. Papers from conference proceedings[?], books[?] and technical reports[?] can be dealt with in the same style.

The IEEE style has the advantage that it is a little more compact in the text and does not distract from the flow of the sentence if there are a lot of citations. However, it has the disadvantage that it is not immediately clear to the reader what particular work has been referenced. You can use author names directly and discuss the work of Finnegan et al. [?] similar to this sentence to make it more readable.

It actually does not matter which particular referencing style is used as long as three important considerations are observed:

- the referencing style used throughout the document is consistent;
- all material used or discussed in the text is properly cited;
- nothing is included in the reference list that has not been cited.

Check with your supervisor as they may have a strong opinion on what you should use

This template has a suitable referencing style already set up – you should use it and use the built-in BibTeX system to manage your references. See above for examples of how to cite a reference and look in the `sample.bib` file to see BibTeX references. It is strongly recommended that you use a bibliographic tool, such as EndNote (check out https://www.tcd.ie/library/support/endnote/), as this will facilitate compliance with these three requirements. Endnote can help you build you .bib file. Remember Google Scholar and other search engines will give you BibTeX references for lots of academic publications. Be aware that Web of Science is more reliable for giving the full record for the BibTeX entry. Otherwise, you can easily make up your own based on the examples in that file.

4 LaTeX

LaTeX, or more properly "LaTeX 2ε", is a very useful document processing program. It is very widely used, widely available, stable and free. Famously, TeX, upon which LaTeX is built, was originally developed by the eminent American mathematician Donald Knuth because he was tired of ugly mathematics books [?]. Although it has a learning curve (made much less forbidding by online tools and resources – see below), it allows the writer to concentrate more fully on the content, and takes care of most everything else.

While it can be used as a word processor, it is a *typesetting* system, and Knuth's idea was that it could be used to produce beautiful looking books:

> *LaTeX is a macro package which enables authors to typeset and print their work at the highest typographical quality, using a predefined, professional layout.*[1]

LaTeX has great facilities for setting out equations and a powerful and very widely supported bibliographic system called BibTeX, which takes the pain out of referencing.

Three useful online resources make LaTeX much better:

(1) An excellent online LaTeX environment called "Overleaf" is available at `http://www.overleaf.com` and runs in a modern web browser. It's got this template available – search for a TCD template. Overleaf can work in conjunction with Dropbox, Google Drive and, in beta, GitHub.

(2) Google Scholar, at `http://scholar.google.com`, provides BibTeX entries for most of the academic references it finds.

(3) An indispensable and very fine introduction to using LaTeX called *"The not so short introduction to LATEX 2ε"* by [?] is online at `https://doi.org/10.3929/ethz-a-004398225`. Browse it before you use LaTeX for the first time and read it carefully when you get down to business.

Other tools worth mentioning include:

[1] This is from [?]. Did we mention that you should minimise your use of footnotes?

- `Draw.io` – an online drawing package that can output PDFs to Google Drive – see `https://www.draw.io`.

5 Evaluation

6 Conclusion

7 Findings

This document provides a template for the preparation of final year project reports. The objective is to provide clear guidance to you, the students, and also to provide uniformity to the project reports, to facilitate equitable grading. This LaTeX template uses a sans-serif font to aid accessibility..

The font colour for Chapter headings is "Pantone Blue", which is the colour used in TCD documents. The page number appears at the bottom of each page starting at 1 on the first page of the Introduction chapter. If you are not familiar with concepts like styles, captioning, cross-referencing, and how to generate tables of contents, figures etc. in LaTeX, the Overleaf guides are a useful start at:
`https://www.overleaf.com/learn/latex/Learn_LaTeX_in_30_minutes`

7.1 Headings, sections and subsections

Chapters should be divided into appropriate subsections. LaTeX makes the numbering much easier and it is all built in. Headings should incorporate the Chapter number into them as is done here.

7.1.1 Subsection name style

The subsections, if used, should be numbered sequentially within each section. You should really try to avoid using sub- subsections, but if you do they should not be numbered.

7.2 Length of the report

The page margins is set to 2.54 cm top, bottom, left and right. There may be a table or figure for which it is sensible to deviate from these margins, but in general the main text should be formatted within the specified margins. The body of the report should be organised into several chapters. There are a number of chapters that you must have: an introduction; a background or literature review chapter; and a conclusion chapter. The focus of the other chapters will depend on your specific project. Refer to the issued guidelines for the page limit. This limit does not usually include the front matter, references list and any appendices. In other words, from the first page of the Introduction to the last page of the Conclusions chapters must be less than the given limit for MAI. If you exceed these page limits or deviate significantly from this format, you will lose marks.

7.3 Contents of the Introduction

The introduction presents the nature of the problem under consideration, the context of the problem to the wider field and the scope of the project. The objectives of the project should be clearly stated.

7.4 Contents of the background chapter

Bibliography

[1] J. So *et al.*, "Domains do change their spots: Quantifying potential abuse of residual trust," 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9833609

[2] J. Bayer *et al.*, "Study on domain name system (dns) abuse: Technical report," 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1/language-en

[3] D. Tatang *et al.*, "The evolution of dns-based email authentication: Measuring adoption and finding flaws," 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3471621.3471842

[4] G. Holdmann *et al.*, "Renewable energy integration in alaska's remote islanded microgrids: Economic drivers, technical strategies, technological niche development, and policy implications," 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8801901

[5] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, J. H. Xue, M. Jonker, and C. D. Laat, "A responsible internet to increase trust in the digital world," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 882–928, 2020. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10922-020-09564-7.pdf

[6] A. Mathew and C. Cheshire, "Trust and community in the practice of network security," 2016.

[7] V. Cerf, "Preserving the internet," *Communications of the ACM*, vol. 65, no. 4, pp. 6–7, 2022. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3522782

[8] E. I. Medvedskaya, "Features of the attention span in adult internet users," 2022. [Online]. Available: https://journals.rudn.ru/psychology-pedagogics/article/view/31393

[9] A. Khormali, J. Park, H. Alasmary, A. Anwar, M. Saad, and D. Mohaisen, "Domain name system security and privacy: A contemporary survey," *ScienceDirect*, 2023, accessed: 13/10/2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128620313001

[10] "Home - dns abuse institute," *DNS Abuse Institute*, 2023, accessed: 13/10/2023. [Online]. Available: https://dnsabuseinstitute.org/

[11] C. Deccio and J. Davis, "Dns privacy in practice and preparation," *ACM Digital Library*, 2023, accessed: 13/10/2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3359989.3365435

[12] "September 2022 report - dns abuse institute," *DNS Abuse Institute*, 2022, accessed: 13/10/2023. [Online]. Available: https://dnsabuseinstitute.org/wp-content/uploads/2022/09/DNSAI-Intelligence-Report-September-2022-FINAL.pdf

[13] S. Tajalizadehkhoob and R. Weinstein, "Icann reports dns abuse is trending downward globally," *ICANN*, 2022, accessed: 13/10/2023. [Online]. Available: https://www.icann.org/resources/press-material/release-2022-05-17-en

[14] K. Hynek, T. Cejka, A. Wasicek, J. Luxemburk, and D. Vekshin, "Summary of dns over https abuse," *IEEE Xplore*, 2023, accessed: 13/10/2023. [Online]. Available: https://ieeexplore.ieee.org/document/9775718

[15] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on dns encryption: Current development, malware misuse, and inference techniques," *arXiv*, 2023, accessed: 13/10/2023. [Online]. Available: https://arxiv.org/pdf/2201.00900v1.pdf

[16] "Webinar: Understanding and combating dns abuse - encouraging best practice," *ICANN*, 2023, accessed: 13/10/2023. [Online]. Available: https://features.icann.org/event/icann-organization/webinar-understanding-and-combating-dns-abuse-%E2%80%93-encouraging-best-practice

[17] WebinarCare, "Dns security statistics 2023 - everything you need to know," https://webinarcare.com/best-dns-security-software/dns-security-statistics/, 2023, accessed: 25/10/2023.

[18] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006.

[19] International Trademark Association (INTA), "Inta board resolution on domain name system abuse may 2023," https://www.inta.org/wp-content/uploads/public-files/advocacy/board-resolutions/INTA-Board-Resolution-on-Domain-Name-System-Abuse-May-2023.pdf, 2023, accessed: 25/10/2023.

[20] B. Edelman, "Typosquatting: Unintended adventures in browsing," *McAfee Security Journal*, pp. 34–7, 2008.

[21] D. H. B. C. F. CITP, A. L. CISSP, and C. B. CISSP, "Is your pc a zombie? here's how to avoid the attentions of blacklisters and vampire slayers."

[22] H.-T. Lin, Y.-Y. Lin, and J.-W. Chiang, "Genetic-based real-time fast-flux service networks detection," *Computer Networks*, vol. 57, no. 2, pp. 501–513, 2013.

[23] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon, "From {Throw-Away} traffic to bots: Detecting the rise of {DGA-Based} malware," in *21st USENIX Security Symposium (USENIX Security 12)*, 2012, pp. 491–506.

[24] GoDaddy, "Demystifying dns abuse | the godaddy blog," https://www.godaddy.com/resources/skills/demystifying-dns-abuse-understanding-the-digital-threat-landscape, 2023, accessed: 25/10/2023.

[25] R. Böhme, *The economics of information security and privacy*. Springer, 2013.

[26] ICANN, "The last four years in retrospect: A brief review of dns abuse trends," https://www.icann.org/en/system/files/files/last-four-years-retrospect-brief-review-dns-abuse-trends-22mar22-en.pdf, 2022, accessed: 25/10/2023.

[27] K. Fowler, *Data breach preparation and response: breaches are certain, impact is not*. Syngress, 2016.

[28] dotmagazine, "Dns abuse: Everyone's problem - building trustworthiness," https://www.dotmagazine.online/issues/the-heart-of-it/building-trustworthiness/dns-abuse, 2022, accessed: 25/10/2023.

[29] J. Saxe and H. Sanders, *Malware data science: attack detection and attribution*. No Starch Press, 2018.

[30] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*, illustrated ed. McGraw-Hill Education, 2014.

[31] CircleID, "A look at dns trends and what the future may hold," https://circleid.com/posts/20201028-a-look-at-dns-trends-and-what-the-future-may-hold/, 2020, accessed: 25/10/2023.

[32] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2015, pp. 336–341.

[33] M. Dooley and T. Rooney, *DNS Security Management*. John Wiley & Sons, 2017.

[34] N. Schick, *Deep fakes and the infocalypse: What you urgently need to know*. Hachette UK, 2020.

[35] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. " O'Reilly Media, Inc.", 2009.

[36] M. H. Au and R. Choo, *Mobile security and privacy: Advances, challenges and future research directions*. Syngress, 2016.

[37] I. Bashir and N. Prusty, *Advanced Blockchain Development: Build highly secure, decentralized applications and conduct secure transactions*. Packt Publishing Ltd, 2019.

[38] M. Chapple and D. Seidl, *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning, 2021.

[39] T. Brunner, "Cybersecurity in beyond 5g: use cases, current approaches, trends, and challenges," *Communication Systems XIV*, p. 28, 2021.

[40] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems," *Technovation*, vol. 34, no. 7, pp. 342–353, 2014.

[41] ICANN, "Dnssec – what is it and why is it important?" https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en, accessed: 25/10/2023.

[42] M. W. Lucas, *TLS Mastery: Beastie Edition*. Tilted Windmill Press, 2021.

[43] S. G. Moghaddam, A. Nasiri, and M. Sharifi, "Ecco mnemonic authentication–two-factor authentication method with ease-of-use," *International Journal of Computer Network and Information Security*, vol. 6, no. 7, p. 11, 2014.

[44] F. Skopik, *Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level*. CRC Press, 2017.

[45] A. S. Coronado, "It auditing: Using controls to protect information assets , by chris davis, mike schiller, and kevin wheeler," 2014.

[46] E. Tsukerman, *Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python*. Packt Publishing Ltd, 2019.

[47] J. Meese, "Edited by ramon lobato," 2016, printer: Print on Demand.

A1 Appendix

The Domain Name System (DNS) plays a role, in the infrastructure of the internet by converting user domain names into IP addresses. However due to its use and importance it has become a target for actors seeking to exploit it. These abuses range from setting up phishing websites to taking advantage of DNS for activities like typosquatting. The responsibility for mitigating abuse primarily lies with DNS infrastructure providers, such as registrars and registries. These entities respond to reports of abuse by taking down confirmed domain names or proactively blocking the registration of harmful ones. While these actions are essential for maintaining the security and integrity of DNS they also raise questions about how transparent these measures

Transparency in the context of mitigating DNS abuse refers to the disclosure of actions taken by registries and registrars including the criteria and reasoning behind their decisions. Currently there is prevalence in publishing transparency reports related to this matter leading to a lack of clarity and understanding, about the processes involved in combating DNS abuse. This project aims to address this issue through a survey involving registries registrars and other stakeholders actively engaged in mitigating DNS abuse.

The main objective of the survey is to collect organize and describe the transparency reports they're presently accessible. This will help us gain an understanding of the status of transparency, in mitigating DNS abuse.

A1.1 Appendix numbering

Appendices are numbered sequentially, A1, A2, A3... The sections, figures and tables within appendices are numbered in the same way as in the main text. For example, the first figure in Appendix A1 would be Figure A1.1. Equations continue the numbering from the main text.