Bachelor's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Herman Haugen Mo
Harald Nikolay Lund Olsen
Marcus Torvik

Multi-Perspective Issuance Corroboration

Bachelor's thesis in Computer Science
Supervisor: Sony George
May 2024

NTNU
Norwegian University of
Science and Technology

Herman Haugen Mo
Harald Nikolay Lund Olsen
Marcus Torvik

Multi-Perspective Issuance Corroboration

Bachelor's thesis in Computer Science
Supervisor: Sony George
May 2024

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Summary of Bachelor Project

Title	Multi-Perspective Issuance Corroboration
Project No.	35
Date	Spring 2024
Authors	Harald Nikolay Lund Olsen Herman Haugen Mo Marcus Torvik
Supervisor	Sony George
Client	Buypass
Contact Person	Mads Egil Henriksveen
Keywords	BGP, MPIC, Certificate Authority
Pages	65
Attachments	6
Availability	Public

Abstract

This bachelor thesis addresses the critical issue of Border Gateway Protocol (BGP) hijacking and its implications for Certificate Authorities. Initiated by Buypass, a root CA, the project focuses on the feasibility and effectiveness of implementing Multi-Perspective Issuance Corroboration (MPIC) as a mitigation strategy against BGP hijacking. By employing multiple geographically distributed vantage points, MPIC aims to enhance the security of domain control validation processes, thereby preventing unauthorized certificate issuance. Our research includes analysis of existing studies, simulation studies, and practical evaluations to assess the impact of MPIC. The findings suggest that MPIC significantly improves security and maximizes resilience when combined with other countermeasures. This thesis provides Buypass with actionable recommendations for implementing MPIC and improving overall security in their digital certificate issuance processes.

Sammendrag av Bachelorprosjekt

Tittel	Multi-Perspective Issuance Corroboration
Prosjekt Nr.	35
Dato	Vår 2024
Forfattere	Harald Nikolay Lund Olsen Herman Haugen Mo Marcus Torvik
Veileder	Sony George
Oppdragsgiver	Buypass
Kontaktperson	Mads Egil Henriksveen
Nøkkelord	BGP, MPIC, Certificate Authority
Antall sider	65
Antall vedlegg	6
Tilgjengelighet	Offentlig

Sammendrag

Denne bacheloroppgaven tar for seg det kritiske problemet med BGP-Hijacking og implikasjonene som følger for sertifikatutstedere. Igangsatt av Buypass, en rot-CA, fokuserer prosjektet på gjennomførbarheten og effektiviteten av implementering av Multi-Perspective Issuance Corroboration (MPIC) som en strategi for å motvirke BGP-Hijacking. Ved å bruke flere geografisk distribuerte perspektiver, har MPIC som mål å forbedre sikkerheten i prosesser for domenekontrollvalidering, og dermed forhindre uautorisert utstedelse av sertifikater. Vår oppgave inkluderer en omfattende litteraturgjennomgang, simuleringsstudier og praktiske evalueringer for å vurdere effekten av MPIC. Funnene tyder på at MPIC betydelig forbedrer sikkerheten og maksimerer motstandsdyktighet når det kombineres med andre tiltak. Denne oppgaven gir Buypass anbefalinger og strategier for implementering av MPIC og forbedring av den totale sikkerheten i deres digitale sertifikatutstedelsesprosesser.

Preface

This thesis is the result of our Bachelor of Engineering in Computer Science at the Norwegian University of Science and Technology (NTNU). Throughout this project, we have explored the complexities of BGP hijacking and investigated innovative solutions to enhance internet security.

First, we would like to thank our supervisor, Sony George, for his continuous support, insightful feedback, and valuable guidance. His expertise and encouragement have greatly influenced the direction and quality of our research.

We are also grateful to Mads Egil Henriksen, our contact person at Buypass. We want to thank Mads for his practical insights and steady support. His contributions have been essential in aligning our research with real-world applications and industry needs.

Additionally, we would like to thank Eigil Obrestad for helping us with access to NTNU's data center for our simulations.

This project has been a significant learning experience, and we hope our findings will contribute to the field of cybersecurity.

Herman Haugen Mo, Harald Nikolay Lund Olsen, Marcus Torvik

Spring 2024

Contents

List of Figures

List of Tables

Glossary

ACME Automated Certificate Management Environment, a protocol for automating interactions between certificate authorities and their users' web servers. 20, 56

AS Autonomous Systems, large networks or groups of networks under a common administration that share a common routing policy. 12–15, 17, 22, 45, 51, 57, 59

BGP Border Gateway Protocol, the protocol used to exchange routing information between autonomous systems on the Internet. 1, 3, 5, 8, 10, 12–17, 19, 21, 22, 24, 28, 30–32, 35, 40, 43, 49, 55, 61, 64

BGP hijacking When attackers maliciously reroute Internet traffic. 1–4, 6–8, 10, 12, 16–18, 20, 24, 27, 28, 30, 32, 33, 43, 47, 52, 54, 55, 58, 64

CA Certificate Authority, an entity that issues digital certificates. 1–3, 19, 23, 27, 38, 49, 50, 55, 60, 63–65

DNSSEC Domain Name System Security Extensions, a suite of specifications to secure certain kinds of information provided by the Domain Name System. 15, 23, 47, 51, 52, 54, 55, 62–64

Domain Validation Domain Validation, a process carried out by Certificate Authorities to verify the ownership of a domain name before issuing a digital certificate. 12, 19, 20, 23, 24, 27, 30, 32, 47, 51, 54, 56, 62, 65

eBGP External Border Gateway Protocol, the variant of BGP used to exchange routing information between different autonomous systems. 14, 31

Equally Specific Prefix a malicious IP prefix that is identical to the legitimate prefix announced by the rightful owner. 17, 33, 43

MPIC Multi-Perspective Issuance Corroboration, a method for validating domain control using multiple vantage points. 1, 15, 20, 23, 24, 26, 32, 43, 44, 47, 50–52, 55, 56

Prefix Prepending a technique where the attacker adds extra AS numbers to the AS path of a route announcement to manipulate routing decisions. 18

RPKI Resource Public Key Infrastructure, a framework designed to secure the Internet's routing infrastructure. 15, 18, 22, 47, 51, 54, 55, 61, 62, 64

SSL/TLS Allow web browsers to identify and establish encrypted network connections to web sites using the SSL/TLS protocol. 2, 18, 23

Subprefix a malicious IP prefix that is in a more specific subnet compared to the legitimate prefix announced by the rightful owner. 17, 40, 43

Chapter 1

Introduction

1.1 Problem Description

Buypass AS, a root Certificate Authority, has tasked us with addressing a critical security issue known as Border Gateway Protocol (BGP) Hijacking. BGP hijacking is a cyber threat where attackers redirect internet traffic to fraudulent destinations[1], compromising the validation processes used by Certificate Authorities (CA). This can lead to the issuance of fake digital certificates, which undermines internet security[2].

To combat this threat, Buypass, a root CA, is exploring the use of Multi-Perspective Issuance Corroboration (MPIC). MPIC uses multiple locations to verify domain control, making it harder for attackers to succeed in their hijacking attempts[3].

Our goal is to conduct a thorough analysis of the current landscape and provide Buypass with comprehensive recommendations for implementing MPIC. This involves understanding the problem in detail, reviewing existing research and technologies, and evaluating the effectiveness of MPIC through simulations and analysis of existing studies. Our research aims to equip Buypass with the necessary insights to enhance their security measures and contribute to overall internet safety.

1.2 Introducing Buypass

Buypass AS[1] is a Norwegian company that specializes in providing secure digital services. Established in 2001, Buypass has grown to become a trusted provider of electronic identification, payment solutions, and secure communication services.

[1] `https://www.buypass.no`

One of their key roles is acting as a root CA, issuing SSL/TLS certificates that are essential for encrypting internet traffic and verifying the authenticity of websites. These certificates help maintain trust and security in online transactions[4][5].

In addition to their CA services, Buypass offers a range of other digital security solutions:

- **Electronic Identification (eID):** Buypass provides robust electronic identification solutions used for secure login to various online services, ensuring that only authorized users can access sensitive information.
- **Payment Solutions:** They offer secure payment solutions for online and mobile transactions, ensuring that payments are processed safely and efficiently.
- **Digital Signatures:** Buypass enables digital signing of documents and transactions, providing a secure and legally binding way to sign contracts and other important documents electronically.
- **Authentication Services:** They provide multi-factor authentication (MFA) services to enhance the security of user accounts and protect against unauthorized access.

Buypass is also an active member of the CA/Browser Forum[6], an industry group that sets guidelines and standards for digital certificates[2]. This involvement demonstrates Buypass's commitment to staying at the forefront of security innovations and addressing emerging threats, such as BGP hijacking. By participating in this project, Buypass aims to explore advanced security measures like Multi-Perspective Issuance Corroboration (MPIC) to further protect their certificate issuance processes and enhance overall internet security.

1.3 Key Concepts

To provide a clear understanding for this thesis, it is important to define some key terms and concepts related to our study.

- **Digital Certificate**: A digital certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, the identity of its owner, and the digital signature of an entity that has verified the certificate's contents[7].

[2] `https://cabforum.org`

- **Certificate Authority (CA)**: A Certificate Authority is an entity that issues digital certificates. The CA is responsible for validating the identity of the certificate requester before issuing the certificate, thus ensuring the trustworthiness of the certificate[8][9].
- **Border Gateway Protocol (BGP)**: BGP is the protocol used to exchange routing information between different networks on the internet. It helps determine the best paths for data to travel across the complex web of interconnected networks[1].
- **BGP hijacking**: BGP hijacking is a type of cyber attack where malicious actors manipulate BGP routing tables to redirect internet traffic. This can lead to unauthorized access to sensitive data and compromise the validation processes used by CAs[10].
- **Multi-Perspective Issuance Corroboration (MPIC)**: MPIC is a security technique that involves using multiple, geographically distributed vantage points to verify domain control. By cross-verifying from different locations, MPIC reduces the risk of BGP hijacking affecting the certificate issuance process[3].
- **CA/Browser Forum**: The CA/Browser Forum is an industry consortium of Certificate Authorities and web browser vendors. It sets guidelines and standards for digital certificates to enhance internet security[11]. Buypass, as a member of this forum, contributes to developing solutions to combat emerging threats like BGP hijacking.

1.4 Intended Audience

The findings and recommendations in this thesis will be of interest to three key groups:

Buypass

Buypass AS, the commissioning entity, is the main beneficiary of this research. The insights gained from this study will help Buypass enhance its security measures against BGP hijacking. The recommendations provided will be helpful for their technical teams as they work to implement MPIC to secure their digital certificate issuance processes.

Industry Professionals

The thesis will also be relevant to professionals in the cybersecurity and network management industries. This includes other Certificate Authorities, members of the CA/Browser Forum, and organizations involved in internet infrastructure and security. The research will contribute to the broader understanding of BGP hijacking and potential countermeasures, helping to improve overall internet security practices.

Academic Community

This thesis will be of interest to researchers and students in the field of cybersecurity, network management, and internet infrastructure. The detailed analysis and evaluation of MPIC provide valuable insights that can support further academic research. By sharing our findings and recommendations, we aim to contribute to the academic discourse on BGP hijacking and digital certificate security, encouraging continued exploration and innovation in these areas.

1.5 Group Background and Motivations

Our research team consists of three members, Herman Haugen Mo, Harald Nikolay Lund Olsen, and Marcus Torvik. All three group members are students at the Norwegian University of Science and Technology (NTNU), studying Bachelor of Engineering in Computer Science. Given our interest in cybersecurity and networking, we decided to take on this project as a rare opportunity to work on internet-wide vulnerabilities and how to solve them. As a group, we have experience from relevant courses like **IIK3100 Ethical Hacking**, **IIKG2001 Software Security**, **IIKG1001 Cybersecurity and computer networks** and **IDATG2202 Operating Systems**.

1.6 Goals and Objectives

This section outlines the primary aims of our research and the specific objectives we seek to achieve. Our goals are divided into technical and scientific aspects, which guide the overall direction of the project. Additionally, we have set group objectives to ensure effective collaboration and project management.

1.6.1 Project Goals

Our project goals focus on understanding and addressing the security challenges posed by BGP hijacking. We aim to evaluate the effectiveness of MPIC and provide

Buypass with practical recommendations for implementation.

- **Develop a Comprehensive Understanding:** To gain an in-depth understanding of Border Gateway Protocol (BGP) Hijacking and its impact on Certificate Authorities (CAs).
- **Evaluate MPIC:** To assess the feasibility and effectiveness of MPIC in mitigating BGP hijacking risks.
- **Provide Recommendations:** To deliver actionable recommendations for Buypass on implementing MPIC to enhance their digital certificate issuance security.

1.6.2 Group Objectives

To ensure successful project execution, we have set group objectives focusing on collaboration, learning, and project management.

- **Effective Collaboration:** To work efficiently as a team, leveraging each member's strengths and expertise.
- **Skill Development:** To enhance our skills in network security, research, and technical writing.
- **Project Management:** To apply best practices in project management, ensuring timely completion of tasks and milestones.

1.7 Limitations

Our research is subject to several limitations that need to be considered:

1.7.1 Lack of Information

The relatively new field of MPIC [2] has limited studies available, with much of the existing research originating from Princeton University. This concentration of sources may limit the diversity of perspectives in our analysis. We rely on the most current and accessible sources, but we acknowledge that rapidly evolving technology could introduce new factors not covered in our study.

1.7.2 Time

A significant limitation for this project is the time constraint. We have a total of 5 months to complete our research, analysis, and provide recommendations. This limited timeframe restricts the depth of our investigation and the breadth of scenarios we can simulate. With more time, we could have engaged in more hands-on activities, such as assisting Buypass in the initial implementation of the first vantage point for MPIC. This would have allowed us to provide more practical insights and address implementation challenges in real-time.

1.7.3 Boundaries

The focus of our study is on a specific implementation of MPIC within the context of Buypass. While this provides valuable insights for Buypass, the findings may not be universally applicable to other Certificate Authorities or different contexts.

1.7.4 Self-implementation

Given the complexity and resource requirements, we are not developing a full-scale MPIC implementation ourselves. Our research is confined to a review of current literature, analysis of existing implementations, and theoretical evaluations.

1.8 Scope

This thesis focuses on the feasibility and effectiveness of implementing MPIC as a mitigation strategy against Border Gateway Protocol (BGP) Hijacking. The research includes a comprehensive review of current literature, analysis of current technologies, and simulations to evaluate MPIC. The study will cover:

- The principles and methods of BGP hijacking.
- The concept and implementation of MPIC.
- Evaluation of MPIC through simulations and existing studies.
- Recommendations for Buypass on implementing MPIC.

This study does not include the development of a full-scale MPIC system or address other cyber threats beyond BGP hijacking. The focus is specifically on MPIC as it pertains to Buypass's needs.

1.9 Our Contribution

Our primary contribution in this project is to act as an extension of Buypass's research team, focusing on providing a comprehensive set of recommendations for the implementation of MPIC. By conducting a thorough review of the current literature, analyzing current methodologies, and evaluating the feasibility and effectiveness of MPIC, we aim to equip Buypass with the necessary insights to enhance their digital certificate issuance process.

1.9.1 Key Contributions

- **Review of current literature:** We will conduct an extensive review of existing research on BGP hijacking and MPIC to understand the current state of the field and identify best practices.
- **Analysis and Evaluation:** Through detailed analysis and evaluation, we will assess the potential impact and effectiveness of MPIC in mitigating the risks associated with BGP hijacking.
- **Implementation Recommendations:** Based on our findings, we will develop a set of actionable recommendations for Buypass. These recommendations will cover practical aspects of implementing MPIC, addressing potential challenges, and suggesting solutions.
- **Presentation to Buypass:** We will present our findings and recommendations to the technical team at Buypass, providing them with a clear roadmap for implementing MPIC. This presentation will ensure that Buypass has a solid foundation for enhancing their security measures.
- **Illustrations, Graphs, and Tables:** We have created multiple illustrations, graphs, and tables to visually represent data and concepts, enhancing the clarity and comprehensibility of our findings and recommendations.

Our goal is to provide Buypass with a detailed and well-founded set of guidelines that will facilitate the successful implementation of MPIC, thereby improving the security of their digital certificate issuance process.

1.10 UN Sustainable Development Goal

Our research aligns with the **United Nations Sustainable Development Goal (SDG) 9: Industry, Innovation, and Infrastructure**. SDG 9 aims to build resilient infrastructure, promote inclusive and sustainable industrialization, and foster inno-

vation[12]. By enhancing the security of digital certificate issuance through the implementation of MPIC, we contribute to the development of a more secure and reliable internet infrastructure.

1.10.1 Key Alignments with SDG 9

- **Resilient Infrastructure:** Improving the security of digital certificates strengthens the overall resilience of internet infrastructure, making it less susceptible to cyber threats like BGP hijacking.
- **Innovation:** By exploring and recommending the implementation of MPIC, we promote innovative solutions to contemporary cybersecurity challenges, supporting the advancement of secure internet technologies.
- **Sustainable Industrialization:** Enhancing the security of digital communications supports sustainable industrialization by ensuring that businesses and industries can operate securely online, fostering trust in digital transactions.

Our project contributes to these global goals by addressing critical cybersecurity issues and providing practical solutions that enhance the integrity and reliability of digital infrastructure.

1.11 Diversion from Project Plan

Our initial project plan relied on Princeton University's open-source project to analyze the effectiveness of MPIC against BGP hijacking. We expected this tool to provide a robust framework for our analysis, streamlining our efforts towards evaluating and enhancing its methodologies. However, the release of this project was later postponed[13], necessitating a significant shift in our project's focus.

Anticipating the risk that the Princeton study might not be available, as outlined in our project plan, we were able to adapt to a new strategy. Without access to the expected tool, we redirected our efforts towards developing our own network simulations from scratch. This approach required a substantial investment of time and effort, as we constructed a simulation environment that reflected real-world BGP behaviors and vulnerabilities.

This shift, while challenging, offered valuable opportunities for deeper learning. Building and configuring the network environments allowed us to gain hands-on experience with BGP's inner workings and the intricacies of hijacking attacks. Through this process, we developed a deeper understanding of the both BGP and MPIC.

1.12 Project Structure and Methodology

1.12.1 Group Structure

Our group consists of three members. Each member played an important role in the project, contributing to both the research and the simulation aspects.

- **Herman Haugen Mo:** As the group leader, Herman was responsible for overall project coordination. He served as the primary point of contact with Mads Egil Henriksen from Buypass and our academic supervisor, Sony George. Herman ensured that the project stayed on track and facilitated communication between all parties involved.
- **Harald Nikolay Lund Olsen:** Harald was responsible for documenting meeting minutes. His records of our discussions and decisions ensured that we maintained a clear and detailed account of our progress.
- **Marcus Torvik:** Marcus handled the scheduling and sending of meeting invitations. His role was important in organizing our meetings and ensuring that all members were informed and available, helping to maintain a consistent workflow.

1.12.2 Methodology

Although our project involved limited amounts of coding, we adopted principles from the Scrum methodology to manage our tasks and ensure continuous progress. Scrum's emphasis on iterative development, regular communication, and flexibility was well-suited to our needs. We implemented the following practices:

- **Collaborative Research and Writing:** All team members were actively involved in conducting research and writing the report. This collaborative effort ensured a comprehensive and well-rounded analysis, with each member bringing their unique perspective and expertise to the table.
- **Simulation Work:** The simulation was a key component of our project, and all team members contributed to its development. By working together on the simulation, we were able to leverage our collective knowledge and skills to create a robust and accurate model.
- **Regular Meetings:** We held regular meetings to discuss our progress, address challenges, and plan our next steps. These meetings were important for maintaining momentum and ensuring that everyone was aligned with the project's objectives.

- **Documentation and Communication:** Harald's responsibility for meeting minutes and Marcus's role in managing meeting invitations ensured that our communication was organized and efficient. Detailed documentation of our meetings provided a valuable reference for tracking our decisions and progress.

1.12.3 Structure of the Thesis

This thesis is structured into several chapters, each addressing different aspects of our research. The organization of the thesis ensures a logical flow of information, from the background and theoretical foundations to the analysis and conclusions. The IMRaD (Introduction, Methods, Results, and Discussion) format[14] is suitable for this project, and the structure is as follows:

1. **Introduction:** This chapter provides an overview of the problem, introduces Buypass, and outlines the goals and structure of the thesis.

2. **Theory:** This chapter reviews the relevant literature and theoretical foundations related to BGP hijacking and digital certificate security. It lays the groundwork for understanding the problem and the proposed solutions. The purpose of this chapter is to ensure that readers have a solid understanding of the baseline theory necessary to comprehend the subsequent chapters.

3. **Methodology:** This chapter describes the methods and approaches used in our practical research, including the setup of simulations and experimental environments. These simulations are primarily intended for hands-on learning about the inner workings of BGP and common BGP hijacking methods. It is important to note that the results of our simulations are not used for any recommendations.

4. **Results:** This chapter provides a comprehensive review of existing studies and literature on MPIC and related technologies. We extract data from previous simulations conducted by Princeton to evaluate the effectiveness of MPIC, as our own simulations were not intended for generating results. This chapter also includes a study focusing on the implementation of MPIC at Let's Encrypt, offering insights into its practical application. Given the greater scale of the simulations performed by Princeton, this evaluation is a key component of our thesis.

5. **Discussion:** Based on the findings from the review, this chapter offers detailed recommendations and strategies for Buypass. It addresses potential challenges and provides practical solutions for implementing MPIC effectively.

6. **Conclusion:** This chapter summarizes the key findings and discusses the implications of our research.

The structure of the thesis is designed to provide a clear and logical progression of ideas, from the introduction of the problem to the presentation of our findings and recommendations.

Chapter 2

Theory

In this chapter, we provide the foundational knowledge necessary to understand the problem of BGP hijacking and its implications for digital certificate security. We delve into the technical aspects of BGP, explore the role of Autonomous Systems, and discuss the vulnerabilities associated with BGP. We also introduce the concept of Multi-Perspective Issuance Corroboration and examine supporting technologies and standards that enhance the security of Domain Validation processes

Our objective is to establish a comprehensive theoretical framework that supports the analysis and recommendations presented in later sections. This background knowledge is crucial for understanding the complexities of BGP hijacking and the solutions proposed to mitigate this threat.

2.1 Understanding the Border Gateway Protocol

The Border Gateway Protocol (BGP) is the principal routing protocol used to facilitate the exchange of routing information between autonomous systems (AS) on the Internet[1][15]. BGP is classified as a path vector protocol, which uniquely identifies the best paths for data transmission based on a range of metrics such as route length, reliability, and policy rules defined by network administrators. It plays a critical role in determining the manner in which routing decisions are made, ensuring that data packets find an efficient and reliable path across complex, interconnected network architectures.

In addition to data routing, BGP has a big part in maintaining the structure and efficiency of the Internet. By enabling routers to construct a table of IP network

paths, which in turn informs routing decisions, BGP optimizes the speed and efficiency with which data is routed. It is designed to handle the vast amount of information involved in mapping the routes of the global internet, managing thousands of routes in large networks. Moreover, BGP is dynamic, allowing for constant updates that respond to changes in network infrastructure, such as the addition or removal of routes.

BGP is essential for global internet connectivity, managing how data flows between internet regions, countries, and continents. Its capacity to handle network changes and maintain route consistency without requiring central coordination makes it a cornerstone of internet resilience and reliability. This decentralization allows the Internet to maintain high levels of performance and connectivity even in the face of hardware failures, network attacks, or other disruptions. The protocol's design and implementation impact almost every aspect of internet use, from the performance of streaming services to the reliability of global communications.

2.2 The Role of Autonomous Systems (ASes)

2.2.1 What are Autonomous Systems?

An AS is a collection of connected IP routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the internet[1] [16][17]. Essentially, an AS is a single administrative domain that has full control over its internal routing decisions. Organizations such as large ISPs, large corporations, or universities typically manage these systems, which are identified by a unique AS number (ASN) assigned by regional internet registries. The ASN facilitates global routing decisions and allows the autonomous system to exchange routing information with other neighboring autonomous systems via BGP[18][19][20][21].

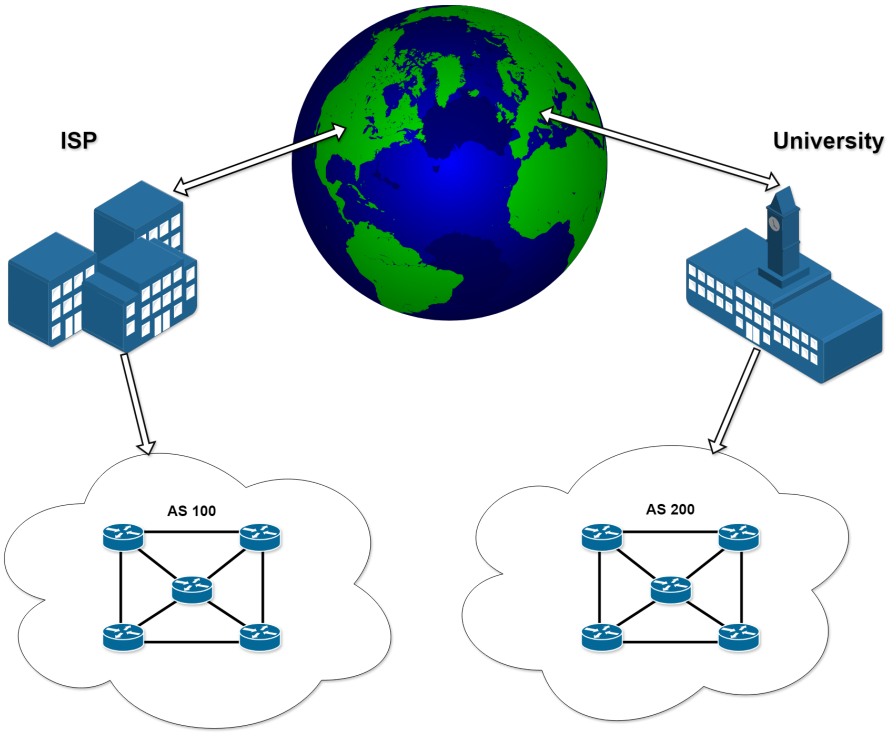


Figure 2.1: Examples of potential Autonomous Systems

2.2.2 ASes in the Context of BGP

Within the framework of BGP, autonomous systems are the backbone of internet connectivity. BGP is used for routing between ASes, which is known as External Border Gateway Protocol (eBGP) routing[22][23]. Each AS uses BGP to broadcast its presence and to announce the IP networks it encompasses to other ASes, facilitating interconnectivity and internet-wide routing of data. This process involves negotiating pathways that data packets travel from one AS to another, optimizing paths according to the routing policy defined by each AS. The protocol ensures that all participating ASes have the information necessary to route traffic both to and from areas within and beyond their local networks.

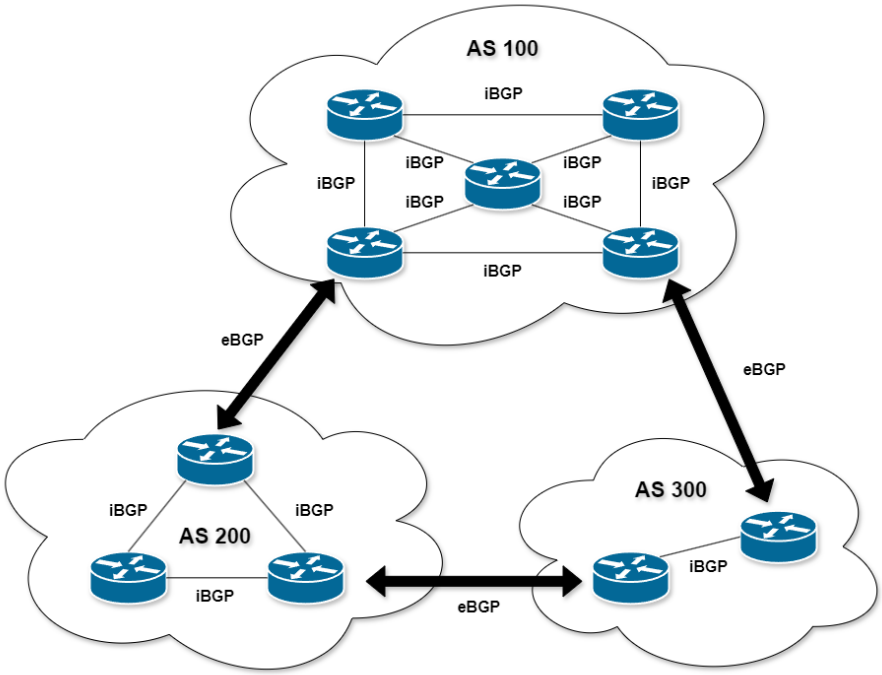


Figure 2.2: How AS's communicate

2.2.3 Vulnerabilities Associated with ASes

Despite their critical role in global connectivity, ASes are vulnerable to various security threats that can impact the entire internet. One significant vulnerability is the risk of route hijacking, where malicious entities advertise unauthorized routes to divert traffic through their AS for purposes of data interception or denial-of-service attacks[10][24]. Additionally, misconfigurations in AS routing can lead to route leaks where more specific routes are incorrectly announced, causing misdirected traffic and potential service disruptions. These vulnerabilities highlight the need for advanced mitigation techniques. The introduction of security enhancements such as RPKI (Resource Public Key Infrastructure) and DNSSEC (Domain Name System Security Extensions) has been important in addressing some of these issues[25][26]. However, given the evolving nature of threats, ongoing explorations into other robust solutions like MPIC (Multi-Perspective Issuance Corroboration) is essential. MPIC aims to provide an additional layer of security by indirectly verifying the legitimacy of BGP announcements from multiple vantage points using the corroboration results, thereby offering a promising approach to increase the resilience of ASes against such vulnerabilities[27].

2.3 BGP Hijacking

2.3.1 Definition and Significance

BGP hijacking, also known as prefix hijacking, occurs when malicious actors deliberately manipulate BGP routing tables by announcing unauthorized ownership of IP prefixes that they do not legitimately control[10][24][28]. This manipulation misdirects internet traffic through the hijacker's network, which can lead to interception or disruption of data flows. The significance of BGP hijacking stems from its potential to compromise the integrity of data transmission across the internet, impacting everything from individual privacy to the operations of entire businesses and governments.

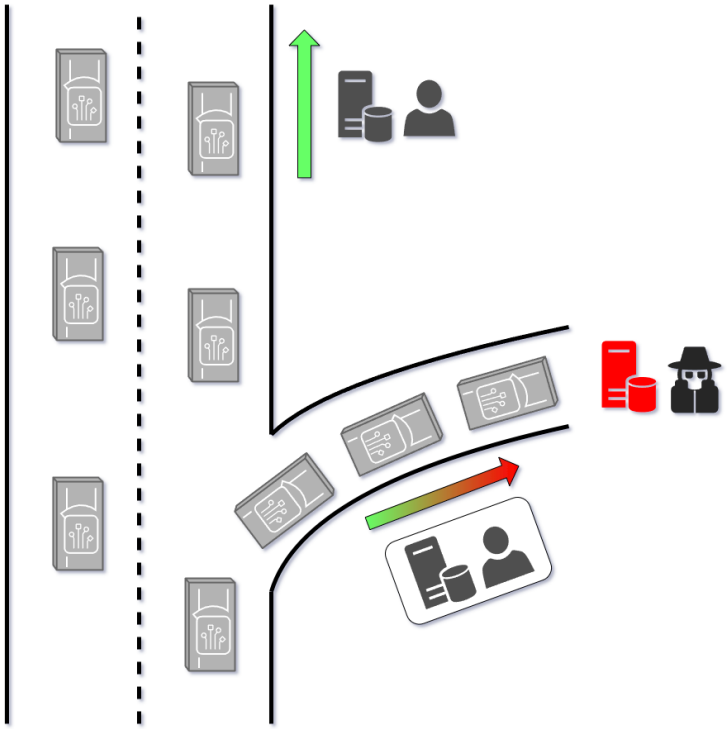


Figure 2.3: In this illustration, the cars (data) are tricked into taking an early exit (rerouted).

2.3.2 Mechanisms of BGP Hijacking

BGP hijacking exploits the trust-based nature of the BGP protocol, which lacks inherent security measures for validating the accuracy of routing announcements. There are several mechanisms through which BGP hijacking can occur:

- **Accidental Misconfiguration:** Administrators may unintentionally announce incorrect routing information, leading to unintentional hijacking[28].
- **Malicious Hijacking:** Attackers intentionally announce routes to IP prefixes they do not own, rerouting traffic through their devices for malicious purposes such as data interception and analysis[10].
- **AS Path Manipulation:** By altering the AS path information in a route announcement, attackers can make their route appear shorter and more attractive, encouraging other networks to route traffic through the compromised paths[24].

2.3.3 Types of BGP Hijacking Attacks

There are several common types of BGP hijacking attacks, each exploiting different vulnerabilities in the BGP routing process:

Equally Specific Prefix Hijacking:
Equally specific prefix hijacking occurs when a malicious AS announces an IP prefix that is identical to the legitimate prefix announced by the rightful owner[27]. Since BGP relies on the principle that the most specific prefix should be preferred, this type of attack can cause traffic to be split between the legitimate route and the hijacked route, depending on various factors such as path length, path preferences and network policies.

Example: In April 2010, China Telecom announced numerous prefixes belonging to various other networks, causing traffic destined for those networks to be misdirected through China Telecom's infrastructure for about 18 minutes. This incident affected around 15% of the internet's BGP routes.[29]

Subprefix Hijacking:
Subprefix hijacking involves the announcement of a more specific prefix within the range of a legitimate IP prefix[2]. For example, if the legitimate owner announces a prefix 192.0.2.0/24, an attacker might announce 192.0.2.0/25. Because BGP prefers more specific routes, the traffic destined for the original prefix will be redirected to the hijacker's route. This type of attack can be particularly effective and difficult to detect since the more specific prefix takes precedence over the broader legitimate prefix.

Example: In 2008, a Pakistani ISP announced a more specific prefix for YouTube's IP address range to block access within Pakistan. This misconfiguration accidentally propagated globally, leading to a worldwide YouTube outage for several hours.[30]

Recent studies indicate that MPIC is not effective against subprefix hijacking. While MPIC uses multiple vantage points to verify domain control, it primarily detects discrepancies in BGP announcements for equally specific prefixes. Subprefix hijacking remains problematic because the more specific prefix from the attacker still takes precedence, even when multiple vantage points are used for verification.

However, subprefix hijacking is less of an issue today due to several factors. Many ASes filter BGP announcements for prefixes longer than 24 bits, limiting the impact of very specific prefixes. Additionally, the implementation of RPKI has significantly improved routing security. RPKI cryptographically validates BGP announcements, preventing unauthorized announcements of specific prefixes and reducing the vulnerability of networks to subprefix hijacking.[25]

Prefix Prepending:
Prefix prepending is a technique used in BGP hijacking to manipulate the AS path length, enhancing the stealthiness and persistence of the attack[27]. An attacker adds extra AS numbers to the AS path of a route announcement, making it appear longer. This can be used in traditional attacks like equally specific prefix hijacking and subprefix hijacking to evade detection mechanisms that monitor changes in the origin AS. By making the AS path longer with the victim's AS number prepended, the hijacked route appears legitimate, reducing the likelihood of triggering alarms. Furthermore, this method can affect routing decisions, potentially making the attack less noticeable while still achieving its goals. However, it might attract less traffic due to the increased AS path length, as BGP routers typically prefer shorter paths.

2.3.4 Impact on Certificate Authorities and Web Security

BGP hijacking poses significant risks to certificate authorities and the overall security of web communications[2]. When traffic destined for a certificate authority is misrouted, it can lead to unauthorized issuance of digital certificates, thereby compromising the SSL/TLS authentication framework which is vital for web security. Additionally, if traffic to and from major websites is hijacked, attackers could potentially decrypt, manipulate, or steal user data. The integrity of encrypted sessions relies on the secure delivery of public key certificates, which can be undermined by

BGP hijacking, leading to broader implications for internet security, such as enabling phishing attacks or spreading malware.[2] Thus, enhancing the security measures in BGP and developing robust verification mechanisms like MPIC are vital to protect data integrity and maintain trust in digital communications.[3]

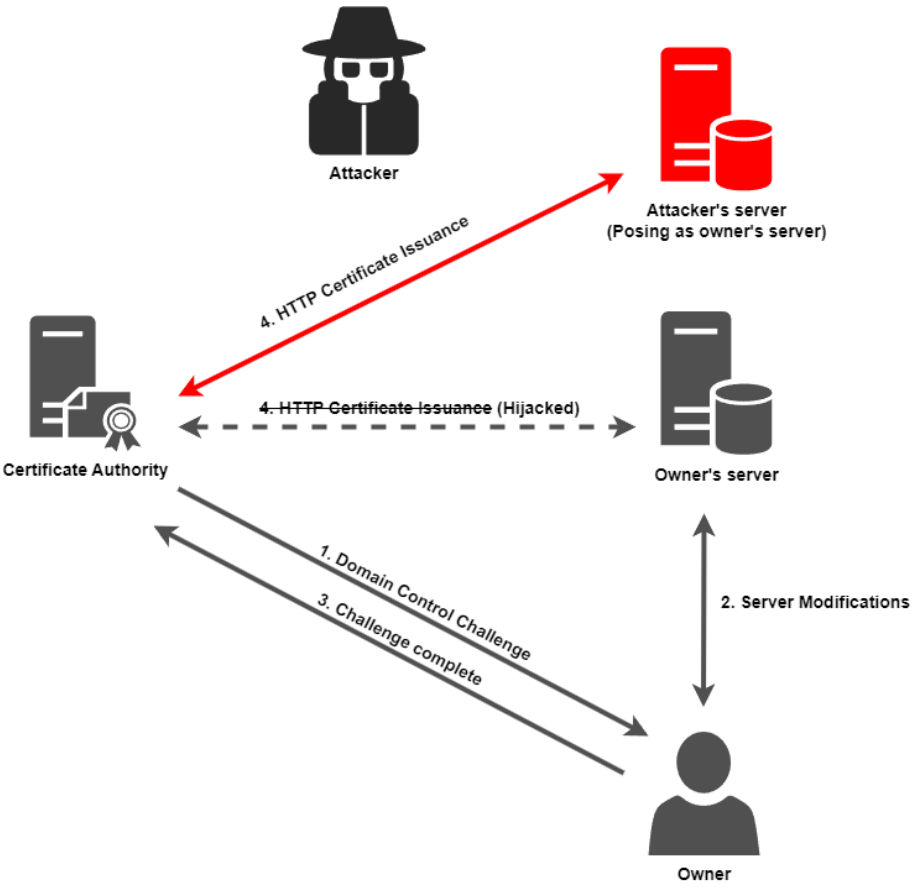


Figure 2.4: Hijack of HTTP certificate issuance.

2.4 Certificate Authorities and Domain Validation

Process of Domain Validation

Domain Validation is a critical process carried out by CAs to verify the ownership of a domain name before issuing a digital certificate[31]. Traditionally, this verification is performed using several methods:

- **Email Validation:** CAs send a verification link to an email address listed in the

domain's WHOIS record or to a standardized admin address at the domain.

- **DNS Record Validation:** The domain owner adds a specific TXT record to the DNS configuration of their domain.
- **HTTP Validation:** The domain owner places a specific file in the root directory of their website, which the CA can access via a standard URL.

To streamline these processes, Buypass employs the Automated Certificate Management Environment (ACME) protocol, which automates the interaction between certificate authorities and web servers seeking certificates[32]. ACME automates the generation and delivery of challenges, such as those used in DNS and HTTP validations, and validates the responses to ensure domain control. This automation significantly enhances the efficiency and accuracy of domain validation by standardizing the verification steps and minimizing human error.

2.4.1 Challenges in Current Validation Practices

Despite the automation and standardization provided by ACME, domain validation still faces significant challenges that can undermine its effectiveness:

- **Limited Verification:** Even with ACME, the standard domain validation processes primarily confirm control over the domain rather than verifying the identity of the person or organization controlling it. This can be insufficient for environments requiring high security[33].
- **Vulnerability to Domain Hijacking:** Advanced threats such as DNS hijacking can still pose risks, as attackers gaining temporary control over a domain could manipulate DNS or HTTP responses to fraudulently pass validation checks[27].
- **Dependencies on External Systems:** ACME's effectiveness is dependent on the proper functioning and security of external systems like DNS and web servers, where misconfigurations or security flaws could be exploited.

2.4.2 Concept and Operation of MPIC

Among the evolving vulnerabilities exposed by BGP hijacking, MPIC has been developed as a robust countermeasure[31]. This innovative approach is designed to enhance the reliability of Domain Validation processes carried out by CAs. Unlike traditional methods that generally verify domain control from a single vantage point, MPIC mandates verification from multiple, independent locations across the

internet. These locations are strategically diverse, both geographically and topologically, ensuring a comprehensive scrutiny that significantly diminishes the risk of single-point failures commonly exploited in attacks like DNS hijacking or the more complex BGP hijacking.

The operation of MPIC involves conducting simultaneous validations of a domain's control from these multiple vantage points. This process not only verifies the authenticity of domain ownership but also checks for any discrepancies in the information received from different vantage points. Given each vantage point has different routes to domains while validating, the chance that all vantage points are compromised will be exceedingly low. Such a methodology is crucial because it allows for the detection of anomalies that could indicate a security breach, such as traffic misrouting caused by a hijacked BGP session. By requiring consensus among multiple independent confirmations, MPIC drastically reduces the likelihood of issuing certificates based on fraudulent claims of domain ownership, thereby bolstering the integrity of web communications.

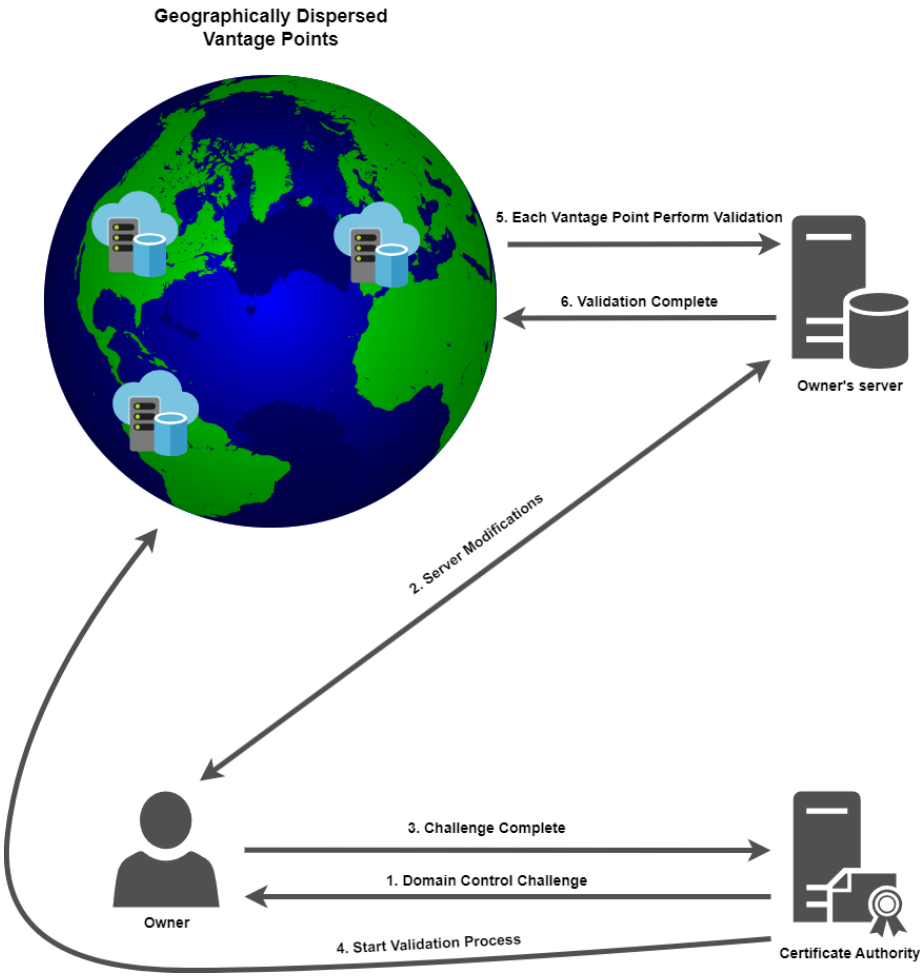


Figure 2.5: Illustration of MPIC

2.5 Supporting Technologies

2.5.1 RPKI

RPKI (Resource Public Key Infrastructure) is a security framework designed to secure the internet's routing infrastructure, specifically addressing the issue of route hijacking and misdirection[25]. RPKI uses cryptographic certificates to establish a chain of trust from the IP address holders to the route origin, authorizing which AS can announce specific IP prefixes. This helps in ensuring that only legitimate route announcements are accepted and propagated in the global routing system.

RPKI enhances the security of the BGP by providing a way to verify that a route

announcement is authorized by the legitimate holder of an IP block. This mechanism reduces the risk of route hijacking, where an AS falsely announces ownership of IP addresses that do not belong to it. By verifying the legitimacy of route announcements, RPKI helps maintain the integrity and stability of internet routing.

2.5.2 DNSSEC

DNSSEC (Domain Name System Security Extensions) is an enhancement to the traditional DNS protocol that aims to provide security when data is exchanged over the internet[26]. It adds layers of authentication to DNS responses by using digital signatures based on public key cryptography. This verification ensures that the received DNS data has not been tampered with during its transit and is exactly what the domain's DNS server originally sent. DNSSEC plays a crucial role in enhancing Domain Validation by protecting against DNS spoofing attacks, where false DNS information is used to redirect users. By verifying the authenticity of the DNS responses, DNSSEC helps ensure that the DV process is interacting with the actual domain's server.

2.6 CA/Browser Forum

The CA/Browser Forum is an industry consortium of certificate authorities and vendors of internet browsers that collaborates to establish guidelines and standards for the issuance and management of digital certificates[11]. Founded to provide a structured forum for continuous improvement and enhancement of internet security, the CA/Browser Forum develops policies that govern the issuance of SSL/TLS certificates. These policies are designed to standardize and elevate the security practices across all issuing bodies, ensuring a uniform level of trust and security in web communications.

Recognizing the critical need for enhanced validation processes, the CA/Browser Forum has decided to implement MPIC as a mandatory requirement for all certificate authorities[34]. The adoption of MPIC is set to redefine the standards for DV by introducing several key requirements that all CAs will need to adhere to. These requirements are designed not only to enhance the security and reliability of certificate issuance but also to ensure that these improvements are implemented uniformly across the industry.

2.6.1 CA/Browser Forum's Requirements

MPIC's deployment must strictly adhere to the specifications outlined in Ballot SC-067v2[34], a proposed update to the CA/Browser Forum's *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* document[35], which details the requirements for the issuance and management of Publicly-Trusted TLS Server Certificates. These requirements ensure that the methods used for domain control verification are robust, secure, and capable of mitigating potential threats such as BGP hijacking.

2.6.2 Verification Methods Compliance

According to SC-067, certificate authorities must perform Domain Validation and CAA[3] checks from multiple network perspectives for the applicable validation methods in the sections 3.2.2.4 and 3.2.2.5 of the baseline requirements document. MPIC meets this requirement through its use of multiple vantage points that collectively enhance the verification process. This approach significantly improves the accuracy and reliability of domain validation, which is why it was chosen to comply with the Forum's stipulations for robust verification methods.

2.6.3 Multi-Perspective Issuance Corroboration

According to section 3.2.2.9, the MPIC process requires certificate authorities to corroborate the determinations made by the Primary Network Perspective with multiple remote Network Perspectives before issuing a certificate, as this significantly enhances protection against equally-specific prefix BGP attacks. The requirements for the process are as follows:

- Certain methods for validating an applicant's ownership or control of a domain or IP address listed in a certificate require retrieving and processing CAA records from additional network perspectives before the certificate can be issued.
- A remote network perspective's CAA check respone must be interpreted as permission to issue to corroborate the primary perspective, regardless of whether the responsed from both perspectives are identical.
- A CA may consider a remote perspective as corroborating if one or both perspectives experience an acceptable CAA record lookup failure.

[3] A Certification Authority Authorization (CAA) record is used to specify which CAs are allowed to issue certificates for a domain[36].

- Each remote perspective needs to validate the presence of the expected domain control verification elements 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the used validation method.
- Each remote perspective needs to validate the CA's authority to issue to the requested domain(s).
- Section 3.2.2.4 and 3.2.2.5 outline the validation method that require the use of MPIC, and how a network perspective can corroborate the outcomes.
- Results or information from one network perspective must not be reused or cached when performing validation through subsequent perspectives.
- The network infrastructure providing internet connectivity to a network perspective may be administered by the same organization providing the perspectives computational services.
- All communications between network perspectives and the CA have to occur over secure, authenticated, and encrypted channels.
- Corroboration attempts from each network perspective has to at minimum record:
  - An identifier that uniquely identifies the network perspective used.
  - The attempted domain name and/or IP address.
  - The result of the attempt.
  - Quorum results for each domain or IP address represented in a certificate request(i.e "3/4", interpreted as "Three out of four attempted network perspectives corroborated the determinations made by the primary network perspective").
- CAs may immediately retry validating using the same validation method or an alternative method.
- When retrying validation, CAs must not rely on corroborations from previous attempts.
- The "Quorum Requirements" table outlines the quorum requirements related to MPIC.
  - **2-5 Network Perspectives:** 1 allowed non-corroborator.
  - **6+ Network Perspectives:** 2 allowed non-corroborators.
- If the CA does not rely on the same set of network perspectives for domain authorization or control, and CAA record checks, the quorum requirements must be met for both sets of perspectives.

- Remote network perspectives performing MPIC must rely upon networks that implement measures to mitigate BGP routing incidents in the global internet routing system.

To ensure distinctness of the network perspectives, the requirements specify that:

- DNS resolvers used by network perspectives must fall within the same Regional Internet Registry service region as the perspective relying upon it.
- The straight-line distance between any two DNS resolvers used in a corroboration attempt must be at least 500 km.
- Network perspectives must be considered "remote" and "distinct" if they are at least 500 km apart.
- The point where unencapsulated outbound DNS queries are first handed off to the network infrastructure providing internet connectivity to that DNS resolver determines the location of a DNS resolver.

2.6.4 Compliance Timeline

To ensure a systematic and controlled deployment of MPIC, the CA/Browser Forum guidelines provide a phased implementation timeline. This timeline is designed to progressively integrate MPIC within certificate authorities' operations, increasing the number of remote network perspectives over time to enhance the overall resilience and security of the certificate issuance process. The timeline is as follows:

- **Effective September 15, 2024**: Certificate Authorities (CAs) should begin implementing MPIC using at least two remote network perspectives. This initial phase is designed as a soft launch, allowing CAs to adjust their systems and processes to accommodate MPIC requirements without facing immediate compliance penalties.
- **Effective March 15, 2025**: CAs must have MPIC fully operational using at least two remote network perspectives. At this stage, the CA may proceed with certificate issuance even if the number of remote perspectives that do not corroborate the determinations made by the primary network perspective exceeds the allowed non-corroborations as defined in the Quorum Requirements table.
- **Effective September 15, 2025**: It becomes mandatory for CAs to not proceed with certificate issuance if the number of non-corroborations exceeds the limits set forth in the Quorum Requirements table. This marks a significant step in enforcing stricter control and reliability in the MPIC process.

- **Effective March 15, 2026**: CAs must use at least three remote network perspectives. The CA must not proceed with certificate issuance if the number of non-corroborations exceeds the limits set in the Quorum Requirements table and if the remote network perspectives that corroborate the determinations do not span at least two distinct Regional Internet Registries.
- **Effective June 15, 2026**: CAs must expand their implementation to include at least four remote network perspectives. The issuance of certificates must be contingent upon meeting the stricter criteria of non-corroborations and distribution across multiple Regional Internet Registries.
- **Effective December 15, 2026**: The CA must deploy MPIC using at least five remote network perspectives. This final stage in the timeline is critical for ensuring that the certificate issuance process is robust, with a broad geographic distribution of network perspectives and stringent adherence to the non-corroboration requirements.

This phased implementation timeline is crucial for CAs to plan and adapt their infrastructure gradually, ensuring that all systems are compliant with the evolving standards of the CA/Browser Forum. By progressively increasing the number of remote perspectives and tightening the corroboration requirements, the CA/Browser Forum aims to enhance the overall security and integrity of the Domain Validation process, thus mitigating risks associated with BGP hijacking and other sophisticated cyber threats. The compliance timeline ensures that certificate authorities transition smoothly into the more demanding requirements of MPIC, enabling them to maintain high security and trustworthiness in certificate issuance processes.

2.7 Overview of Current Literature

This subsection provides an overview of the key studies related to BGP hijacking and MPIC. Our focus is on three significant studies that have contributed to the understanding and development of MPIC and related technologies.

2.7.1 Cimaszewski et al. (2023)

Cimaszewski et al.'s study, titled *How Effective is Multiple-Vantage-Point Domain Control Validation?*[4], examines the effectiveness of using multiple vantage points for domain control validation. The authors investigate the robustness of this approach against BGP hijacking attacks, providing empirical data on its performance. Their

[4] `https://www.usenix.org/conference/usenixsecurity23/presentation/cimaszewski`

findings suggest that while multiple-vantage-point validation significantly enhances security, there are still challenges and limitations that need to be addressed to ensure comprehensive protection. This study serves as a primary focus of our thesis, providing a foundational understanding of the effectiveness of MPIC.

2.7.2 Birge-Lee et al. (2021)

The 2021 study by Birge-Lee et al., *Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt*[5], provides insights into the practical implementation of multi-vantage-point domain validation by Let's Encrypt. This study shares the experiences and lessons learned from deploying this technique at a large-scale Certificate Authority. The authors discuss the operational challenges, performance considerations, and the overall effectiveness of the multi-vantage-point approach in real-world scenarios.

2.7.3 Birge-Lee et al. (2018)

In their 2018 study, *Bamboozling Certificate Authorities with BGP*[6], Birge-Lee et al. explore the vulnerabilities in the TLS certificate issuance process that can be exploited through BGP hijacking. The study demonstrates how attackers can manipulate BGP routes to obtain unauthorized certificates, thus compromising the security of internet communications. The authors propose potential countermeasures, including the use of multiple validation perspectives to detect and prevent such attacks.

2.7.4 Focus of This Thesis

While these studies provide valuable insights into various aspects of BGP hijacking and MPIC, our thesis primarily focuses on two key studies. We rely on *How Effective is Multiple-Vantage-Point Domain Control Validation?* by Cimaszewski et al. (2023) for empirical data on the performance and effectiveness of MPIC. This study provides a comprehensive assessment of MPIC's ability to enhance domain validation security against BGP hijacking attacks. Additionally, we draw on *Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt* by Birge-Lee et al. (2021) for practical implementation tips and insights. This study offers valuable lessons and operational guidance that are crucial for Buypass as they consider implementing MPIC in their own digital certificate issuance processes. By synthesizing

[5] `https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee`

[6] `https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee`

findings from these studies, we aim to provide Buypass with actionable recommendations and guidelines.

Chapter 3

Methodology

In this chapter, we delve into the practical aspects of our research by conducting simulations to evaluate the effectiveness of Multi-Perspective Issuance Corroboration in mitigating BGP hijacking. Using GNS3, a robust network simulation tool[7], we replicate real-world network environments to test and observe the behavior of MPIC under various conditions.

These simulations serve a dual purpose. Firstly, they provide empirical evidence supporting the theoretical benefits of MPIC discussed in earlier sections. Secondly, they are a valuable learning tool, enhancing our understanding of BGP and MPIC through hands-on, practical research. By simulating different network scenarios, we gain deeper insights into the operational challenges and practical implications of implementing MPIC.

We will outline the setup and configuration of our simulated network environment, detailing the components used and the specific scenarios tested. Through these simulations, we aim to analyze the impact of MPIC on Domain Validation processes and highlight potential challenges and solutions for implementing MPIC in real-world settings. This practical exploration was crucial for translating theoretical insights into actionable recommendations for Buypass.

3.1 Network Simulation

After deciding on GNS3 as our simulation platform, we started a learning process to set up and manage the simulation environment effectively. The project involved

[7] `https://github.com/gns3`

integrating VyOS routers[8] and Ubuntu servers[9], each chosen for their specific roles and capabilities in network simulation. With our focus on external BGP (eBGP), we devoted significant time to understanding BGP attributes and routing policies.

3.2 Hosting and Environment Selection

For the hosting of our simulation project, we strategically chose NTNU's OpenStack data center[10], which provided several advantages. OpenStack[11], being a robust cloud infrastructure with extensive computing resources, enabled us to leverage high availability and scalability that are beneficial for conducting simulations that might change in resource consumption depending on how many network components we end up using[37][38][39]. We also preferred a cloud based simulation environment for the flexibility to collaborate effectively as a team, each from our individual workstations. The reliability and security of NTNU's data center also ensured that our project's data remained backed up and protected, mitigating the risks associated with potential data loss.

The choice of the Ubuntu server[12] with the Lubuntu desktop environment[13] to host our GNS3 simulation platform was based on several considerations. Ubuntu's widespread adoption in both academic and professional circles brings with it stability and a wide set of features[40][41]. We also preferred our main operating system to be the same as the network components in the GNS3 simulation, for the ease of testing scripts and specific tools outside the simulation environment before implementing them. Additionally, the lightweight nature of the Lubuntu desktop, being less resource-intensive, meant that more of the server's computational power could be dedicated to running the simulations rather than the overhead of the operating system's GUI[42][43].

3.3 GNS3 Components

In our network simulation using GNS3, we utilized VyOS routers and Ubuntu servers to create a topology that emulated the interconnections typical among autonomous systems. VyOS was chosen for its robust routing capabilities[14], while Ubuntu servers were deployed across different autonomous systems to perform various functions

[8] https://gns3.com/marketplace/appliances/vyos
[9] https://gns3.com/marketplace/featured/ubuntu-cloud-guest
[10] https://www.ntnu.no/wiki/display/skyhigh
[11] https://www.openstack.org
[12] https://cdimage.ubuntu.com/releases/jammy/release/
[13] https://lubuntu.me
[14] https://gns3.com/marketplace/appliances/vyos

related to our BGP hijacking simulations.

The server in the CA-AS was set up for superficial Domain Validation, as the inner workings of it are beyond the scope of this study. It communicated with servers in the vantage point ASes to enable cross-verification and comparison of route correctness and integrity. The Attacker-AS hosted a deceptive website to simulate the endpoint of illicit traffic redirection, whereas the Client-AS represented a legitimate website to assess the hijack's impact. This approach provided a controlled yet realistic network environment to observe BGP hijacking dynamics and evaluate countermeasures effectively.

3.4 Network Configurations

The network configurations involved setting up VyOS routers with multiple interfaces, firewall settings, NAT rules, and BGP configurations. Interfaces were assigned specific IP addresses and subnet masks to define network segments and establish connectivity between autonomous systems. Firewall rules controlled traffic flow, permitting essential services like HTTP on port 80 and enabling ICMP for network reachability tests.

BGP configurations included establishing peering relationships between routers in different autonomous systems, with specific BGP attributes configured to influence routing decisions. These peering sessions simulated the propagation of BGP announcements and tested the impact of hijacking attempts on route advertisement and selection. By analyzing route updates from vantage points, we assessed the reach and impact of the hijack and the effectiveness of MPIC as a mitigation strategy.

To simulate a real-world MPIC implementation, we followed these rules for vantage points:

- No vantage point should be a neighbor of the CA-AS.[31]
- All vantage points should have a unique route to the simulated client we want to validate.[31]
- None of the routes from a vantage point to the client should go through the CA-AS.[31][27]

The network size was determined based on the number of vantage points, ensuring unique paths for accurate simulation and analysis.

3.5 Simulating an Equally Specific BGP Prefix Attack

In our first network topology, we decided to simulate a Equally Specific Prefix BGP hijacking scenario in which an attacker is positioned closer to the CA-AS compared to the real client. Given that the Client-AS is one hop away from the CA-AS, the attacker would need to be a direct neighbor to the CA-AS. The specific relationship of the Attacker-AS to the Client-AS does not significantly impact this attack scenario, as the attacker's primary goal is not to redirect traffic to the real client. Nevertheless, we chose to position the Attacker-AS between the Client-AS and the CA-AS.

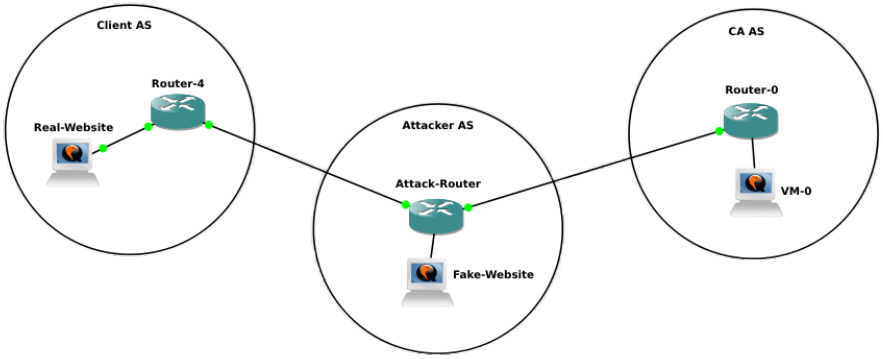


Figure 3.1: Initial build with the main AS's of the simulation

To enhance the accuracy of the simulation, we incorporated MPIC with three vantage points. These vantage points were strategically placed in various autonomous systems to provide the CA-AS with multiple perspectives on the routing paths. By checking the routing paths from these vantage points, the CA-AS could determine which webserver it was connected to, demonstrating the practical application of MPIC in detecting hijack attempts.

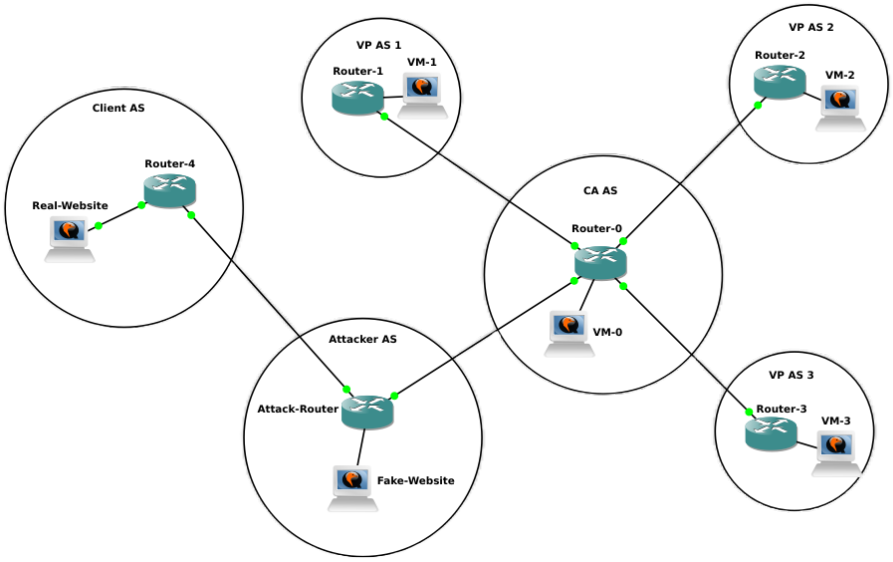


Figure 3.2: Building on the simulation with vantage point ASes

To more accurately simulate the internet, we introduced intermediary ASes between the primary ones, increasing the number of hops and the overall distance between nodes. This setup, shown in figure 3.3, created multiple paths for data to travel, making the simulation closer to real-world conditions and facilitating a more realistic simulation of BGP hijacking.

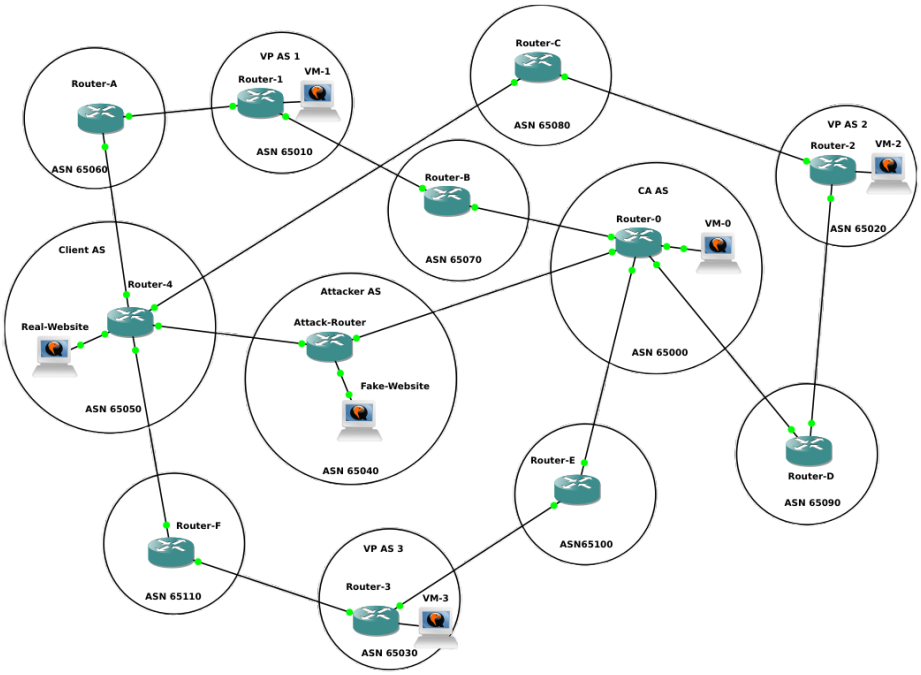


Figure 3.3: Complete simulation setup (equally specific prefix attack)

For the BGP configuration, we opted to announce the client's website using the prefix 192.168.4.0/24. This IP subnet is solely for representational purposes, as 192.168.x.x is typically a Class C private IP range and would not be used for public IP addresses[44]. After announcing this BGP prefix at the Client-AS router, a route to the client's website became visible on all AS routers. We tested this by using ping to check connectivity to the client website server from the CA's domain validation server, and also by using curl to retrieve the webserver's contents. Once we confirmed that the client's announcement was operational, we proceeded to announce the exact same prefix from the Attacker-AS webserver. In a real-world scenario, this would imply that the attacker is announcing a public IP subnet that they do not own, since a public IP subnet is uniquely assigned and cannot be legitimately used simultaneously by different entities.

Upon announcing the prefix from the Attacker-AS, we executed the same ping and curl commands. The ping command yielded the same results, as it targeted 192.168.4.2 (the webserver IP in the 24-bit subnet) and received a normal response. When we used curl to inspect the webserver's contents, it displayed content from the Attacker-AS's webserver. This differentiation was possible because we had distinct contents on the two webservers, aligning with our simulation plan. In practice, a CA would not use ping and curl to verify connectivity to a webserver; instead, it

would perform domain validations that we can, in this scenario, imagine as a binary response—either True (pass) or False (fail). For this simulation, it was practical to use a hardcoded string to identify which webserver we were connected to [15].

The webserver for the real website returns "DNS Validation Failed," and the webserver for the fake website returns "DNS Validation Passed." While this may seem counterintuitive, it's important to understand that the "validation" is merely symbolic. The goal is to simulate how BGP operates, not the actual validation mechanisms. Therefore, when the validation passes, it indicates that the system has been tricked and redirected. Conversely, when the validation fails (this is meant primarily for the vantage points) it means they have reached the real webserver. Symbolically, this signifies that the vantage points have identified route anomalies compared to the CA-AS, indicating a potential BGP hijack.

[15] See Appendix A Figure 1 for full validation script.

webserver_script.py

```
from http.server import BaseHTTPRequestHandler, HTTPServer


class HelloWorldHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(b"DNS Validation Passed\n")

def run(server_class=HTTPServer, handler_class=HelloWorldHandler, port=80):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f"Starting server on port {port}")
    httpd.serve_forever()

if __name__ == "__main__":
    run(port=80)
```

((a)) The webserver script for the fake website.

webserver_script.py

```
from http.server import BaseHTTPRequestHandler, HTTPServer


class HelloWorldHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(b"DNS Validation Failed\n")

def run(server_class=HTTPServer, handler_class=HelloWorldHandler, port=80):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f"Starting server on port {port}")
    httpd.serve_forever()

if __name__ == "__main__":
    run(port=80)
```

((b)) The webserver script for the real website.

Figure 3.4: The two webserver scripts used in the simulation.

Now, we have two different webservers in two distinct ASes, both announcing the same IP subnet prefix, 192.168.4.0/24, with both webservers located at 192.168.4.2/24. The Client-AS, hosting the legitimate webserver, is one hop away from the CA

AS, while the Attacker-AS, hosting the counterfeit website, is situated between the Client-AS and the CA-AS, making it a direct neighbour to the CA-AS. This proximity causes the CA-AS to prefer the route to the fake website in the Attacker-AS because it represents an equally specific prefix but offers a shorter path than the route to the legitimate website in the Client-AS. Without additional checks or mitigation measures, this scenario would successfully demonstrate a BGP hijacking attack, posing a real threat to CAs.

```
vyos@vyos:~$ show ip bgp
BGP table version is 10, local router ID is 192.168.255.1, vrf id 0
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0/24   0.0.0.0                  0         32768 i
*> 192.168.1.0/24   10.10.0.2                               0 65070 65010 i
*                   10.10.2.2                                0 65040 65050 65060 65010 i
*  192.168.2.0/24   10.10.2.2                                0 65040 65050 65080 65020 i
*>                  10.10.1.2                                0 65090 65020 i
*> 192.168.3.0/24   10.10.3.2                                0 65100 65030 i
*                   10.10.2.2                                0 65040 65050 65110 65030 i
*> 192.168.4.0/24   10.10.2.2               0                0 65040 i

Displayed  5 routes and 8 total paths
```

Figure 3.5: Here we can see that the path to the fake website is shorter than the path to the real website (the correct path to 192.168.4.0/24 should be 65040 65050 i).

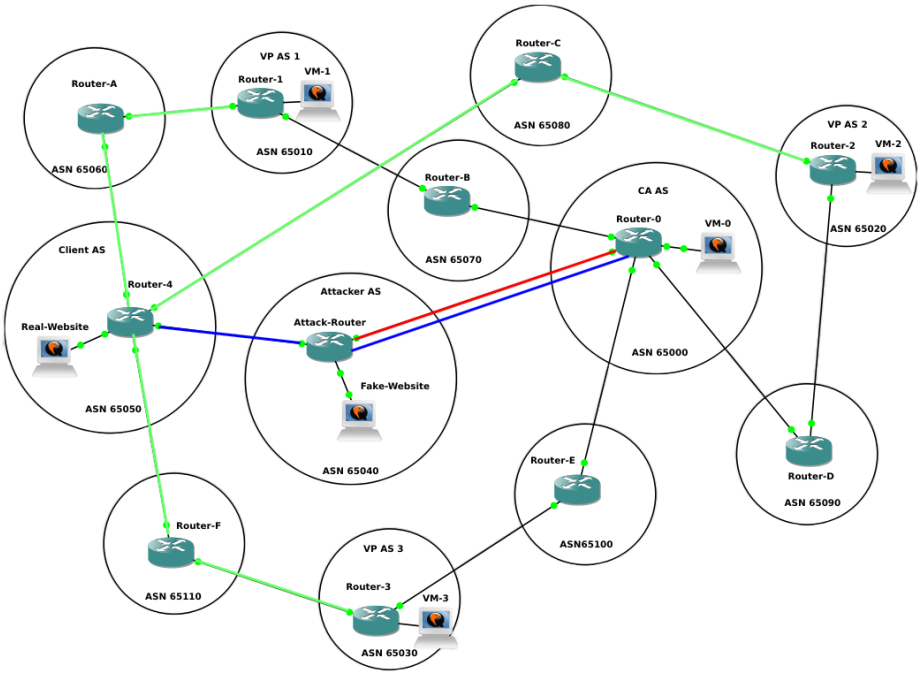


Figure 3.6: Blue represents the best and legitimate path, while red represents the hijacked path. Green represents the legitimate paths leading to the real website.

```
ubuntu@ubuntu-cloud:~$ ./mvp.sh 192.168.4.2
    Self AS: DNS Validation Passed
   VP AS 2: DNS Validation Failed
   VP AS 3: DNS Validation Failed
   VP AS 1: DNS Validation Failed


Validation FAILED. Potential BGP Hijack.
```

Figure 3.7: Validation results from the attack. The validation from the CA-AS passed, meaning that they connected to the fake webserver, while the validation from the VP's failed, meaning that they connected to the real webserver. In other words, the CA-AS got bamboozled. However, the additional perspectives from the vantage points did not, showing the utility of such an implementation.

```
ubuntu@ubuntu-cloud:~$ sudo python3 webserver.py
Starting server on port 80
192.168.0.2 - - [16/May/2024 14:16:35] "GET / HTTP/1.1" 200 -
```

((a)) The activity on the fake website from the CA-AS.

```
ubuntu@ubuntu-cloud:~$ sudo python3 webserver.py
Starting server on port 80
192.168.2.2 - - [16/May/2024 14:16:37] "GET / HTTP/1.1" 200 -
192.168.3.2 - - [16/May/2024 14:16:39] "GET / HTTP/1.1" 200 -
192.168.1.2 - - [16/May/2024 14:16:42] "GET / HTTP/1.1" 200 -
```

((b)) The activity on the real website from the vantage points.

Figure 3.8: Comparison of activity on the fake website and the real website.

3.6 Simulating a Subprefix BGP Attack

In addition to simulating an equally specific prefix BGP attack, we conducted a simulation of a Subprefix BGP attack. To set up this simulation, we utilized a slightly modified network topology from the simulation in the previous section. In this setup, the Attacker-AS has been moved further away from the CA-AS, and an additional AS has been added between the Attacker-AS and CA-AS. This configuration ensures that the route to the attacker has more hops (longer distance) than the route to the Client-AS, demonstrating the preference for more specific prefixes in BGP routing.

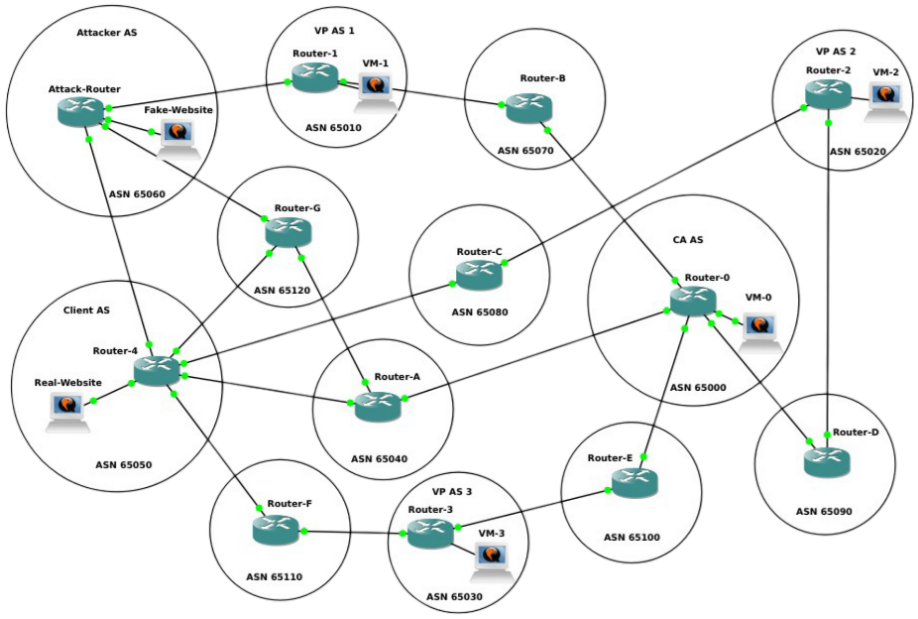


Figure 3.9: Complete simulation setup (subprefix attack)

The Client-AS announces the prefix 192.168.4.0/24, which establishes routes to the legitimate webserver across the network. The Attacker-AS, located further from the CA-AS, announces a more specific prefix (192.168.4.0/29). Due to BGP's preference for more specific prefixes, routers in the network update their tables to route traffic intended for the 192.168.4.0/24 prefix to the 192.168.4.0/29 prefix, effectively redirecting traffic to the attacker.

```
vyos@vyos:~$ show ip bgp
BGP table version is 6, local router ID is 192.168.255.1, vrf id 0
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.0.0/24   0.0.0.0                  0         32768 i
*> 192.168.1.0/24   10.10.0.2                             0 65070 65010 i
*> 192.168.2.0/24   10.10.1.2                             0 65090 65020 i
*> 192.168.3.0/24   10.10.3.2                             0 65100 65030 i
*> 192.168.4.0/24   10.10.2.2                             0 65040 65050 i
*> 192.168.4.0/29   10.10.2.2                             0 65040 65050 65060 i


Displayed  6 routes and 6 total paths
```

Figure 3.10: Here we can see that the path to the Client-AS is shorter (65040 65050 i) than the path to the Attacker-AS (65040 65050 65060 i).

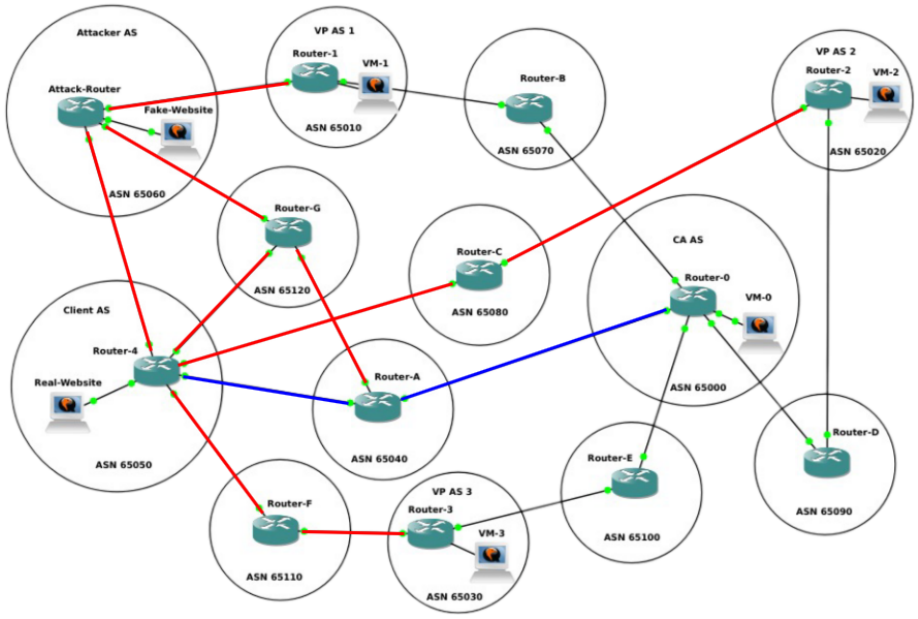


Figure 3.11: Blue represents the best and legitimate path, while red represents the hijacked path. Green represents the legitimate paths leading to the real website.

As a result, the CA-AS and all vantage points mistakenly connected to the attacker's webserver during the domain validation process. This misdirection is confirmed by the validation results, which show that the CA-AS and all vantage points passed, indicating a complete redirection across the board. The webserver logs further support this, showing successful connections from the CA-AS and vantage points to the attacker's server.

```
ubuntu@ubuntu-cloud:~$ ./mvp.sh 192.168.4.2
    Self AS: DNS Validation Passed
   VP AS 2: DNS Validation Passed
   VP AS 3: DNS Validation Passed
   VP AS 1: DNS Validation Passed


Validation Passed.
```

Figure 3.12: Validation results from the script run by the CA-AS, showing that the CA-AS and the VP's all reached the fake webserver.

```
ubuntu@ubuntu-cloud:~$ sudo python3 webserver.py
Starting server on port 80
192.168.0.2 - - [16/May/2024 13:45:00] "GET / HTTP/1.1" 200 -
192.168.2.2 - - [16/May/2024 13:45:01] "GET / HTTP/1.1" 200 -
192.168.3.2 - - [16/May/2024 13:45:03] "GET / HTTP/1.1" 200 -
192.168.1.2 - - [16/May/2024 13:45:04] "GET / HTTP/1.1" 200 -
```

Figure 3.13: Traffic to the fake webserver, confirming redirection.

This simulation shows the limitations of MPIC, as the additional vantage points would not have any effect on a subprefix attack. This is because a more specific prefix will always be preferred, meaning that no matter how many vantage points are implemented, they will all reach the more specific prefix in the end. However, as mentioned in the previous chapter, subprefix attacks are mostly a problem of the past, as effective mitigation strategies have been implemented (given how noisy such an attack is). MPIC is therefore not a "panacea", a remedy for all ills or difficulties[16], but one of several mitigation strategies that together will make BGP safer.

3.7 Analyzing the Results of BGP hijacking Simulations

The results from both BGP hijacking simulations—Equally Specific Prefix and Subprefix attacks—provide valuable insights into the effectiveness of different mitigation strategies and the inherent vulnerabilities of the BGP protocol.

3.7.1 Equally Specific BGP Prefix Attack Analysis

Simulation Setup and Execution:

- The attacker was placed as a direct neighbor to the CA-AS, while the Client-AS was one hop away.
- Both the Client-AS and the Attacker-AS announced the same prefix, 192.168.4.0/24.

Result Observations:

- The CA-AS preferred the shorter path to the Attacker-AS, thereby redirecting traffic to the attacker's webserver.
- Verification using ping showed normal responses, indicating that network connectivity was maintained.

[16]https://www.merriam-webster.com/dictionary/panacea

- The validation script displayed expected behaviour, showing that the CA-AS wan initially tricked by the Attacker-AS.

Effectiveness of MPIC:

- The use of MPIC with three vantage points revealed the effectiveness of detecting route anomalies.
- While the CA-AS was misdirected, the vantage points correctly identified the legitimate webserver, highlighting MPIC's capability in identifying discrepancies in routing paths.

Conclusions:

- This simulation demonstrated that BGP hijacking could be successfully executed when the attacker is positioned closer to the CA-AS.
- MPIC proved to be a valuable tool in detecting such attacks, showcasing its utility in enhancing network security through multiple routing perspectives.

3.7.2 Subprefix BGP Attack Analysis

Simulation Setup and Execution:

- In this scenario, the attacker announced a more specific prefix (192.168.4.0/29) from a position further from the CA-AS.
- The Client-AS continued to announce the original prefix, 192.168.4.0/24.

Result Observations:

- BGP's inherent preference for more specific prefixes resulted in all traffic intended for the 192.168.4.0/24 prefix being redirected to the attacker's 192.168.4.0/29 prefix.
- Both the CA-AS and the vantage points connected to the attacker's webserver, as evidenced by the validation results.

Limitations of MPIC:

- Unlike the equally specific prefix attack, MPIC was ineffective in detecting the subprefix attack.
- All routing paths favored the more specific prefix, underscoring a significant limitation in using MPIC alone for such attack scenarios.

Conclusions:

- The subprefix attack was highly effective due to BGP's preference for more specific routes.
- This demonstrated that MPIC and similar vantage point-based strategies are inadequate for mitigating subprefix attacks, necessitating additional security measures.

3.7.3 Comparative Analysis and Implications

MPIC Effectiveness:

- MPIC significantly enhances detection capabilities for equally specific prefix attacks by leveraging multiple routing perspectives.
- However, it falls short in scenarios involving subprefix attacks, where more specific routes are always preferred.

Realism of Simulations:

- The use of intermediary AS's and multiple vantage points made the simulations more reflective of real-world conditions.
- This approach provided an understanding of the dynamics and challenges associated with BGP hijacking.

BGP Vulnerabilities:

- Both simulations underscored critical vulnerabilities within the BGP protocol, particularly related to the trust model of BGP announcements.
- Effective mitigation requires a combination of strategies, as no single solution, including MPIC, can address all potential attack vectors.

In conclusion, while MPIC enhances the detection of certain BGP hijacking attacks, it is not a comprehensive solution. The simulations emphasize the need for a multi-faceted approach to secure BGP against diverse threats, ensuring a more resilient and secure network infrastructure.

3.8 Moving Forward With Results

Our simulations provided valuable insights into the behavior and effectiveness of MPIC in mitigating BGP hijacking attacks. However, it is essential to emphasize that

the methodology used in this thesis is not the primary basis for our results. Due to our limited resources, time and experience, we cannot claim to make significant contributions to the broader field. Instead, we have relied on existing, highly regarded studies to support our findings and recommendations.

Given our constraints, we utilized insights from these established studies to facilitate our simulations. This approach will ensure that our results are grounded in robust and credible research, despite our limitations. By leveraging established methodologies and findings, we are able to generate actionable recommendations for Buypass.

Chapter 4

Results

In this chapter, we will analyze what we have deemed to be the most important literature on the topic and evaluate the effectiveness of the Multi-Perspective Issuance Corroboration (MPIC) system. Using the insights gained from these studies, we will discuss MPIC's resilience against BGP hijacking, comparing the difference in resilience between the amount of vantage points used, and using single or multiple cloud providers. Following this, we will delve into the importance of supporting technologies such as RPKI and DNSSEC, and how they integrate with MPIC to bolster Domain Validation security. Lastly, we will explore its scalability and operational feasibility.

4.1 MPIC's Effectiveness

MPIC enhances how effectively networks can defend against BGP hijacking, showing considerable improvement when used together with traditional methods of Domain Validation. The MPIC system implemented at Let's Encrypt has secured the issuance of over 300 million TLS certificates, demonstrating its viability at Internet scale[31]. The system's open-source implementation was deployed in February 2020, showing negligible latency, low communication overhead, and a benign failure rate comparable to conventional single-vantage-point designs. Further analysis on the same system was performed by Princeton University in 2023. This study indicated that MPIC with three vantage points achieves an 88% success rate in mitigating attacks[17], which is substantially higher than the 76% success rate of systems using only one vantage point[27].

[17] See Figure 4.1 and 4.2 for resilience numbers under different Quorum policies

The Quorum policy is a security measure that requires a minimum number of independent verifications (corroborators) before a domain validation is accepted. This policy ensures that the validation process is robust and less likely to be compromised by a single faulty or malicious vantage point.[31]

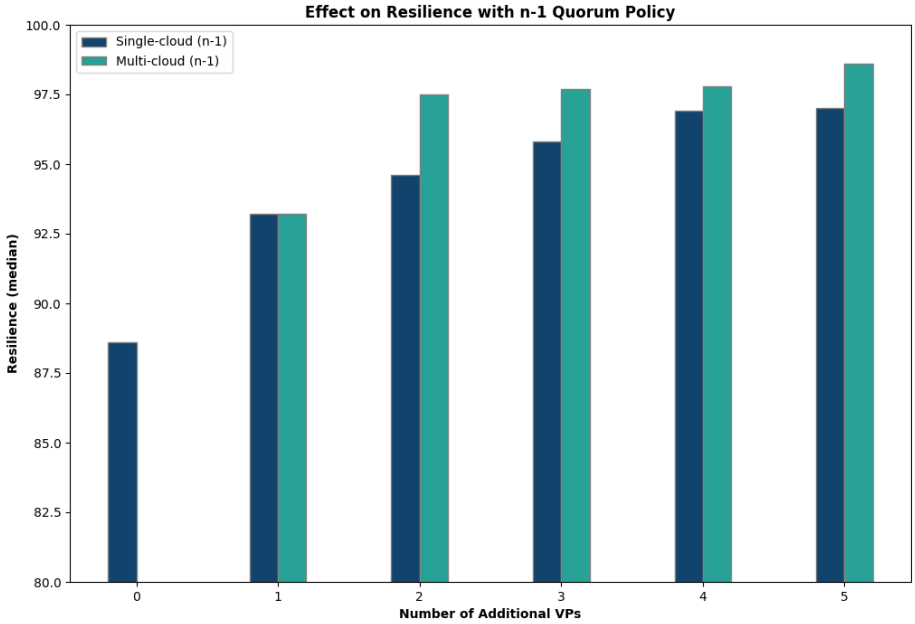


Figure 4.1: Bar chart plot of different number of vantage points effect on resilience with the Quorum policy set to $n-1$. Adapted from [27, Table 4].

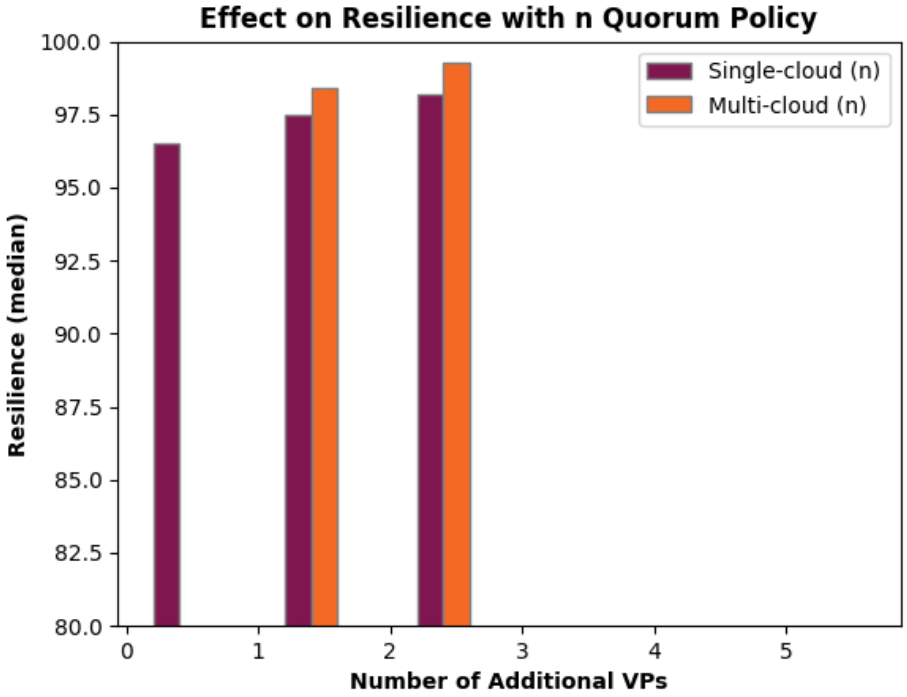


Figure 4.2: Bar chart plot of different number of vantage points effect on resilience with the Quorum Policy set to n. Adapted from [27, Table 4].

The system has shown resilience in real-world BGP hijack simulations, mitigating a vast majority of BGP attacks by using multiple vantage points[31], and has been instrumental in preventing bogus certificate issuance during BGP hijacking attempts[2]. Through the deployment of MPIC and a live BGP monitoring system, Let's Encrypt was able to secure domain control verification, demonstrating the success and feasibility of these countermeasures in a CA environment.

Cimaszewski et al. [27] also provides insights into the optimal selection of vantage point locations, which are pivotal for maximizing CA security against BGP hijacking. When considering all AWS vantage points surveyed in the study, the optimal locations with the largest resilience increase was found to be concentrated in Asia (Tokyo, Mumbai, and Sin- gapore), Northern Europe (Stockholm) and South America (Sao Paulo). It is important to note that these locations were evaluated based on Let's Encrypt having two vantage points in USA, and one in Europe. Their findings suggest that the geographic placement of vantage points critically influences their ability to detect and mitigate such attacks effectively. By analyzing various configurations, the study indicates that using eight strategically located vantage points can increase MPIC's resilience to 97% when using a single cloud provider.

4.1.1 Impact of Multiple Cloud Providers

The study also notes that the deployment strategy of vantage points across different cloud providers significantly impacts MPIC's effectiveness and resilience. For instance, using multiple cloud providers with a total of eight vantage points can increase it's resilience to 98.6%. Implementing a Quorum policy of n corroborators when using multi-cloud results in the highest resilience number, which is at 99.3% using only five vantage points in total (Figure 4.2). The n corroborators policy means that all involved vantage points must agree (corroborate) on the validation decision to consider it valid.

Provider	**AWS**	**GCP**	**Azure**
AWS	34%	10%	15%
GCP	10%	54%	25%
Azure	15%	25%	78%

Table 4.1: Average percentage of overlapping peers between different providers. Adapted from [27, Table 5].

The findings reveal that using multiple cloud providers enhances routing diversity, which is crucial for mitigating the risk of BGP hijacks that may affect a single provider's infrastructure. Table 4.1 showcases why this is, by comparing the fraction of overlapping peers between different providers. By diversifying the hosting of vantage points, CAs can prevent attackers from exploiting provider-specific vulnerabilities or routing biases. At five vantage points and a Quorum policy of $n-1$, the difference in resilience between single-cloud and multi-cloud is 2.9% (94.6% and 97.5%), but at eight vantage points the difference is reduced to 1.6% (97% and 98.6%) (Figure 4.1). Although the study also notes that while deploying additional vantage points within a single cloud provider can initially increase resilience, the benefit tends to plateau. For example, after adding a certain number of vantage points within a single provider like AWS, the resilience improvement levels off, demonstrating diminishing returns on further investments in the same infrastructure. In contrast, introducing vantage points across different providers, such as combining AWS with Google Cloud Platform or Microsoft Azure, continues to elevate resilience by covering a broader range of network paths and operational behaviors.

Even though using multiple cloud providers improves MPIC, Birge-Lee et al. [31] suggests that even with a single cloud provider, significant security improvements can be achieved by carefully selecting vantage points. This approach can be used to simplify billing and operational management while still maintaining compliance

with CA/Browser Forum requirements.

4.2 Importance of Supporting Technologies

Supporting technologies such as RPKI and DNSSEC are important for maximizing the effectiveness of MPIC systems in protecting Domain Validation processes against the threats of BGP hijacking. These technologies enhance the security framework of MPIC by providing layers of defense that address different aspects of the network and domain validation vulnerabilities.

The table below highlights the significant impact of these supporting technologies:

Princeton's Signigicant Findings
- Taking DNS into consideration causes a five-fold increase in the number of prefixes an adversary can target. - Considering the DNS attack surface drops the resilience of domains by 20% (from 95% to 75%) under multiple vantage point validation but 41% (from 83% to 42%) under single vantage point validation. - Current RPKI coverage improves the resilience of domains by 15% to 90% and full coverage could improve the resilience by 20% to 95%. - The resilience of Let's Encrypt's current deployment with three vantage points and a single cloud provider (AWS) is still 88.6% considering these factors

Table 4.2: Princeton's most significant findings about the supporting technologies. Adapted from [27, Table 1]

The findings emphazise the importance of RPKI and DNSSEC implementations in maintaining domain resilience, as DNS vulnerabilities and route hijacking can significantly compromise domain validation. Despite considering these factors, the resilience of Let's Encrypt's deployment with three vantage points and a single cloud provider remained strong, showcasing the effectiveness of combining MPIC with these supporting technologies.

4.2.1 Enhancing MPIC with RPKI

RPKI addresses the issue of route hijacking by enabling network operators to cryptographically verify that IP addresses are announced by legitimate ASes. This verification is benficial for MPIC, as it ensures the authenticity of routing information received from various vantage points. Table 4.2 highlights that RPKI deployment

can improve MPIC resilience by about 15%, underlining its significance in protecting against BGP hijacking. RPKI complements MPIC by providing an additional layer of security at the routing level. While MPIC validates domain control from multiple perspectives, RPKI ensures that these perspectives are based on legitimate route announcements. This combined approach enhances the overall security framework, making it more difficult for attackers to manipulate routing paths and compromise the validation process

Registration of RPKI-ROA records	**Figure**
Domains with at least 1 ROA-covered prefix	76.3%
Domains with all ROA-covered prefixes	26.2%
Target IPs with ROA records	60.0%

Table 4.3: Summary of RPKI-ROA Record Registration from the Princeton study's dataset. Adapted from [27, Table 2]

Table 4.3 summarizes the current state of RPKI-ROA record registration. While 76.3% of domains have at least one ROA-covered prefix, only 26.2% have all their prefixes covered. This partial adoption limits the full potential of RPKI in enhancing MPIC. However, even with these limitations, the 60% coverage of target IPs indicates a significant portion of the internet's routing infrastructure is benefiting from RPKI, which results in the addition of RPKI still showing significant improvements to domain resilience. Achieving full prefix coverage will further strengthen the security of MPIC[18].

4.2.2 Enhancing MPIC with DNSSEC

DNSSEC plays an important role in strengthening the security framework of MPIC systems by securing DNS responses essential for verifying domain control accurately across various locations. Despite its critical role, the adoption of DNSSEC is still limited, with only 5.6% (Table 4.4) of A records and 16.0%[27] of AAAA records fully protected. This underutilization exposes many domains to DNS spoofing attacks, where attackers manipulate DNS data to mislead domain validation efforts. By equipping DNS resolvers in MPIC systems to support DNSSEC, the integrity of the validation process is significantly improved, enhancing the reliability of validation outcomes and reducing susceptibility to spoofing attacks.

[18]It is important to note that RPKI prevents adversaries from claiming ownership of an IP prefix, but does not prevent advertising a bogus path to the prefix owner. The implementation of a new Internet architecture called SCION aims to eliminate routing attack threats but is not yet widespread enough to be usable[31].

Feature	Figure
Total number of certificates	810,000
Number of certs. successfully resolved	755,942
Total number of domains	1,354,318
% successful A record resolution	97.3
% successful AAAA record resolution	12.3
IP prefixes of domains	
Median number of prefixes in A records	1
Median number of prefixes in NS records	3
Little use of DNSSEC	
% domains full DNSSEC-signed	5.6

Table 4.4: An overview of the Princeton study DNS dataset, summarized. Adapted from [27, Table 2].

Table 4.4 highlights the current state of DNSSEC and RPKI adoption. The table shows that out of 810,000 certificates, 755,942 were successfully resolved, indicating a high success rate in DNS resolution. However, the success rate for A record resolution is 97.3%, whereas the success rate for AAAA record resolution is much lower at 12.3%, though this disparity is because of low IPv6 usage by the domain names surveyed.

Provider	Prop. of NS	ROA coverage
CLOUDFLARENET	28.3%	98.2%
AMAZON-02	14.4%	98.9%
AKAMAI-ASN2	7.1%	100%
NSONE	3.1%	50.0%
GODADDY-DNS	2.8%	100%
UltraDNS	2.8%	11.1%
Google, US	2.7%	100%
Total	61.2%	-

Table 4.5: Top nameserver hosting providers and the proportion of their network prefixes with valid ROA. Adapted from [27, Table 3].

Table 4.5 presents the ROA coverage for top nameserver hosting providers. High ROA coverage among these providers indicates better protection against route hijacking for their managed prefixes. For instance, providers like CLOUDFLARENET and AMAZON-02 have high ROA coverage percentages (98.2% and 98.9%, respectively), making them more reliable choices for ensuring secure routing. On the other hand, providers like UltraDNS have much lower ROA coverage (11.1%), which could pose a higher risk for route hijacking. This information can be used to make informed decisions about which nameserver hosting providers to use, based on their level of ROA implementation.

4.2.3 Combined Benefits for MPIC

Figure 4.3 illustrates the impact of integrating these technologies, showcasing that the DNS attack surface results in a median resilience drop of 19.0%, while implementing RPKI with the current level of internet RPKI coverage leads to a median resilience gain of 13.0%. This demonstrates that combining MPIC with RPKI and DNSSEC maximizes MPIC's effectiveness against BGP hijacking, and addresses the larger attack surface exposed by DNS vulnerabilities and routing exploits..

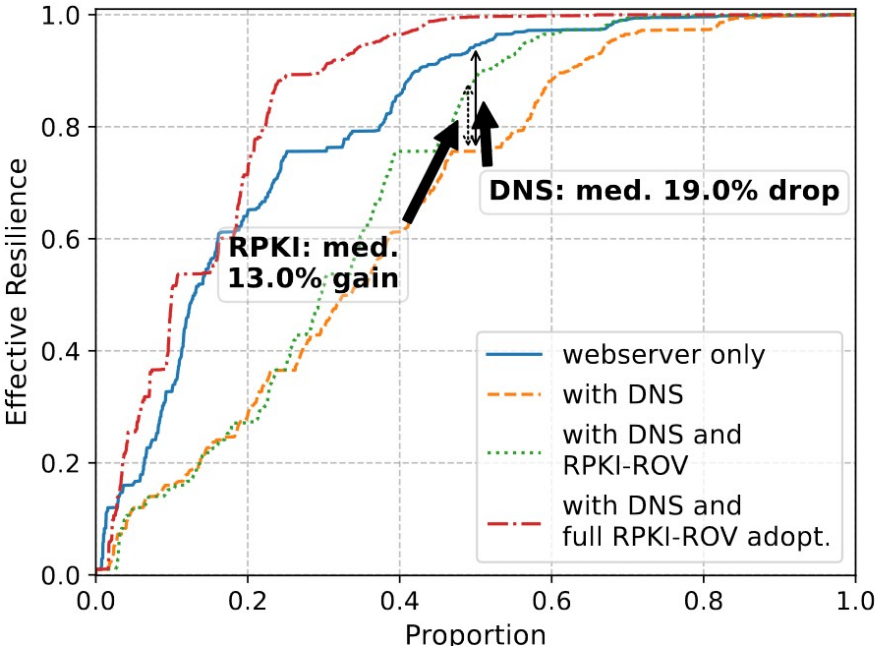


Figure 4.3: The resilience of Let's Encrypt's MPIC deployment under different conditions. Adapted from [27, Figure 5].

With these technologies complementing the protective features of MPIC, the system will also align with the broader security protocols recommended by internet governance bodies like the CA/Browser Forum. This alignment ensures that the security measures are comprehensive, covering various aspects of Domain Validation and securing them against an array of potential threats. As the internet landscape evolves and threats become more sophisticated, the continuous integration of advanced supporting technologies with systems like MPIC will be essential in maintaining robust defenses and ensuring the reliability and security of internet communications.

4.3 Operational Feasibility

MPIC has been incrementally deployed at Let's Encrypt, showing that it can be implemented in a live production environment with minimal changes to CA operations. The system balances security, manageability, performance, and benign failure rates, and has also shown low latency and communication overhead, making it suitable for large-scale deployments[31].

Additionally, the implementation of MPIC with the supporting technologies RPKI and DNSSEC may require significant updates to network protocols and systems. Despite this, the enhanced security outcomes justify the investment. MPIC is designed to be compatible with current internet governance frameworks, which facilitates its integration into various network architectures without disrupting existing operations. This strategic alignment of MPIC's design with operational practicality makes it a viable solution for enhancing security against BGP hijacking. Operational data from deployments across various setups indicate that MPIC's adaptability and compatibility with different network configurations and cloud environments play a crucial role in its feasibility and effectiveness as a security measure in dynamic operational contexts[31][2].

The scalability of MPIC is demonstrated by its ability to easily handle additional vantage points being added, with each addition providing incremental improvements in resilience against BGP attacks[27]. It is also indicated that strategic deployment across different geographic regions when using a single cloud provider can sufficiently increase resilience by optimizing route diversity and reducing the risk of localized attacks impacting all vantage points simultaneously. This capability ensures that MPIC can be adapted to both small and large-scale organizational needs, providing a solution if there are any limitations in budget or infrastructure.

Chapter 5

Discussion

In this section, we present a series of practical recommendations based on our analysis of Multi-Perspective Issuance Corroboration for Buypass. These recommendations are aimed at enhancing the security and efficiency of Buypass's certificate issuance process. We will detail strategies for implementing MPIC, including specific steps for integrating it with existing systems and suggestions for managing the deployment across multiple vantage points. Additionally, we discuss the necessary technical configurations, highlight the importance of compliance with current standards, and suggest measures for scalability and reliability. Our goal is to provide Buypass with clear, actionable advice that can be directly applied to improve their Domain Validation processes.

5.1 Strategic Recommendations for MPIC Implementation

For the implementation of MPIC within Buypass, we recommend a structured and phased adoption strategy that carefully integrates MPIC into the existing certificate issuance process. This strategy is designed to mitigate risks, test system robustness, and ensure a seamless transition to a more secure domain validation environment.

Preliminary Assessment and Planning:

- **Infrastructure and Configuration Review:** The effectiveness of MPIC, as discussed in chapter 4, relies heavily on thorough infrastructure assessment. We recommend beginning with a detailed assessment of Buypass's current infrastructure, particularly the existing ACME configurations used for domain validation. This review will help identify how MPIC can be integrated as

seamlessly as possible with the current validation process.

- **Resource and Technology Evaluation:** Our analysis in chapter 4 indicate that MPIC's deployment showed negligible latency and low communication overhead. Buypass should evaluate its technical resources, including server capacities and network configurations, to support the additional load from multiple vantage points. This evaluation helps in planning necessary upgrades and ensuring the infrastructure can handle the new validation processes effectively.
- **Risk and Compatibility Analysis:** Performing a risk and compatibility analysis is important to identify potential issues. Understanding and addressing risks early on can ensure the smooth functioning of the system during the pilot phase and beyond, maintaining system stability and performance.

Implementing First Vantage Point:

- **Infrastructure Preparation:** We recommend establishing the first vantage point by selecting a location with robust internet connectivity and minimal risk of network disruptions. This site will serve as the testbed for initial MPIC deployments. The location should be at least 500 kilometers away from the main point of validation. If the main point of validation is located in Oslo, the vantage point should at a minimum be outside of Scandinavia to fulfill this criteria. For optimal results, the direct path should be mostly landmass, as the strict 500 kilometer criteria does not take the amount of ASes in between the vantage point and the main point of validation into account.
- **Central Server Configuration:** It is important to configure a server in the main validation network at Buypass to receive and compare validation results from this and subsequent vantage points. This server will be the central hub where the domain validation decisions are finalized. Initially, this server should be in a separate test-environment away from the main validation server, to make sure there are no conflicts in the incoming validation requests.
- **System Configuration:** The vantage point needs to be equipped with the necessary hardware and software to perform domain validation. This includes setting up secure servers, network configurations, and installing ACME-compatible software that supports MPIC.

Pilot Testing:

- **Initial Testing:** Controlled pilot testing at the first vantage point should begin with a limited number of domains, focusing on those managed internally or by cooperative partners who are aware of the testing.
- **Monitoring and Data Collection:** Close monitoring of the system's performance, including response times, success rates, and any security anomalies, is important. Detailed logs and feedback should be collected for analysis. We recommend analyzing the data and feedback to identify any necessary adjustments in the system configuration, security measures, or the validation process itself.

Vantage Point Expansion:

- **Additional Vantage Points:** Once the pilot testing confirms that the initial setup is stable and effective, it is recommended to gradually introduce additional vantage points to minimize the impact on ongoing operations[31]. Ensure that each new site follows the same setup and security protocols as the first.
- **Synchronized Validation:** At this stage we recommend beginning conducting simultaneous validations from multiple vantage points for all new domain verification requests to validate the robustness and reliability of the MPIC system under normal operational loads.

Full-Scale Implementation:

- **Operational Integration:** With successful testing and stabilization from multiple vantage points, fully integrate MPIC into Buypass's standard domain validation process. This ensures that MPIC becomes a regular part of Buypass's operations, enhancing overall security and efficiency.

5.2 Technical Recommendations for MPIC Deployment

5.2.1 Vantage Point Selection Criteria

Selecting optimal vantage points is critical for the effective implementation of MPIC to ensure comprehensive coverage and minimize the risks of DNS and BGP hijacking. These are strategic criteria that we recommend Buypass to consider when deploying MPIC:

- **Geographic Diversity**: Vantage points should be distributed across various geographic locations to avoid localized network disruptions and biases in routing paths. As discussed in chapter 4, this diversity ensures that even if a BGP hijack affects one region, other vantage points can still provide accurate and unbiased data, thereby maintaining the integrity of MPIC's security measures.
- **Network Path Independence**: Each vantage point should be on a network path that is independent of the others. This setup minimizes the risk of a single point of failure affecting multiple vantage points simultaneously. Our analysis indicate that vantage points should not share common AS paths to the extent possible, to reduce the likelihood that a single malicious actor or compromised AS can impact multiple paths.
- **Cloud Provider Diversification**: To enhance resilience against provider-specific threats and outages, vantage points should not be concentrated within a single cloud provider's infrastructure. Using multiple providers can improve routing diversity, which is essential for detecting and mitigating potential hijacks. As mentioned in chapter 4, a combination of major cloud services, such as AWS, Google Cloud, and Azure, can be considered to optimize this aspect.
- **Strategic Network Placement**: Vantage points should be strategically placed near major internet exchange points or within well-connected ASes to ensure they have access to robust and comprehensive routing information. This placement helps in achieving a more accurate and timely detection of anomalous behaviors that could indicate a BGP hijacking attempt. In our analysis we found that the optimal locations to consider are Asia (Tokyo, Mumbai, and Sin- gapore), North-America (West and East Coast) and South America (Sao Paulo). These were the optimal locations for Let's Encrypt's implementation, but we asses that they are also optimal for Buypass, due to the locations being chosen based on the network size and amount of ASes in those areas, as well as distance.
- **DNS Resolver Configuration**: Each network perspective utilized by MPIC may use a recursive DNS resolver that is not co-located with it. However, it is mandatory that the DNS resolver used must fall within the same Regional Internet Registry service region as the network perspective relying upon it. Moreover, for any pair of DNS resolvers used in an MPIC attempt, the straight-line distance between the two states, provinces, or countries they reside in must be at least 500 km, ensuring significant geographical separation.

By adhering to these criteria, Buypass can optimize the deployment of MPIC vantage points to ensure a robust defense against DNS and BGP hijacking, significantly

enhancing the security of digital communications across its network. This strategic approach facilitates not only current operational needs but also accommodates future expansions and technological advancements, providing a scalable and reliable MPIC deployment.

5.2.2 System Configuration and Management

The deployment and management of MPIC within a CA requires adherence to a set of strategic configurations and operational protocols. These are designed to ensure robust security measures and to comply with the standards set forth by the CA/Browser Forum.

For effective MPIC operation, a CA should incorporate the following strategic approaches:

- **Corroborating Evidence Reuse**: A CA may reuse corroborating evidence for Certification Authority Authorization (CAA) record quorum compliance for a maximum of 398 days. This facilitates efficient management of validations and reduces redundant checks without compromising security.
- **CAA Record Retrieval Post-Certificate Issuance**: After issuing a certificate to a domain, remote network perspectives may omit retrieving and processing CAA records for its subdomains in subsequent certificate requests from the same applicant for up to a maximum of 398 days. This approach helps streamline the certificate issuance process while ensuring that the initial validations hold true for a reasonable period.
- **Quorum Requirements for Corroboration**: The quorum requirements dictate the number of allowed non-corroborations based on the number of distinct remote network perspectives utilized:
  - **2-5 Distinct Remote Network Perspectives**: 1 Allowed Non-Corroborations
  - **6+ Distinct Remote Network Perspectives**: 2 Allowed Non-Corroborations

These quorum requirements are essential to maintain the integrity and reliability of the MPIC process, ensuring that even if some discrepancies are observed, they do not undermine the overall security posture.

To support the technical needs of MPIC, the following operational protocols are recommended:

- **Internet Traffic Management**: All internet traffic via remote network perspectives must be forwarded through a network or set of networks that filter

all RPKI-invalid BGP routes as defined by RFC 6811[45]. This critical measure ensures that the routing infrastructure used in the validation process is secure and resilient against potential routing attacks.

- **Facility and Service Provider Requirements**: Network perspectives should ideally be hosted from facilities that are ISO/IEC 27001[46] certified or equivalent. They should rely on services covered in recognized security frameworks and audits such as SOC 2[47] or ENISA 715[48], ensuring that the operational environment adheres to high security and reliability standards.

- **Delegated Third Party Involvement**: If certain operations are delegated to third parties, the CA should obtain reasonable evidence to ascertain that these parties follow the outlined considerations. This ensures that even outsourced components of the MPIC process meet the necessary security standards without being directly under the CA's audit scope.

This approach to system configuration and management supports the operational needs of MPIC and also ensures compliance with the stringent standards set by the CA/Browser Forum, enhancing the overall security and trustworthiness of the certificate issuance process.

5.3 Reliability and Redundancy Measures

For Buypass, ensuring the reliability of the MPIC system is critical for continuous and secure operations. Focusing on the standardization of system setups and the integration of scalable infrastructure can significantly boost operational effectiveness and resilience. These strategies can help ensure smooth, continuous performance while improving system reliability and facilitating quick recovery in diverse operational scenarios.

5.3.1 System Standardization Across Vantage Points

Standardizing the configuration across all vantage points within the MPIC system is crucial for maintaining consistency and simplifying management[31]. When every node operates under the same configuration and adheres to the same security protocols, the process of conducting maintenance, troubleshooting, and applying updates becomes more streamlined. Uniform security patches, updates, and backup protocols can be deployed simultaneously across the entire network, minimizing downtime related to upgrades or recovery from system issues. Such standardization also benefits the training of technical staff. With a uniform system setup, staff training can be centralized and more focused, leading to quicker diagnostics and

resolutions when issues arise, and more efficient overall management. The consistency across systems reduces the risk of errors during manual interventions, as the procedures and safety checks developed apply universally across all components.

5.3.2 Scalable and Flexible Infrastructure

Implementing scalable and flexible infrastructure, particularly through cloud services, allows Certificate Authorities to dynamically adjust resources in response to current needs[27][31]. During periods of high demand, such as during extensive domain validation processes, cloud environments are capable of automatically provisioning additional computing power, storage, and bandwidth. This scalability ensures that the system can handle increased loads without performance degradation. Similarly, in times of lower demand, these resources can be scaled down to manage costs more effectively. Cloud platforms typically come equipped with features designed for disaster recovery and high availability. These features are important for managing system failovers automatically—transferring operations to backup systems or alternative sites without human intervention, thus maintaining uninterrupted service. This automatic failover and recovery capability is essential for continuing operations during unplanned outages or disruptions.

5.4 Future Research and Development Directions

As Buypass continues to refine its MPIC implementation, the integration of technologies such as RPKI and DNSSEC offers promising opportunities to elevate the security infrastructure. The efficacy of these technologies in enhancing Domain Validation processes is well-documented in chapter 4, which builds on the foundational research conducted by Princeton. This research provides compelling evidence that these technologies can significantly mitigate several of the more complex security vulnerabilities associated with domain validation systems.

5.4.1 RPKI

Integrating RPKI within the MPIC framework at Buypass could serve as a potent defense mechanism against prefix hijacking, which poses a significant threat to the integrity of domain validation operations. Chapter 4 highlighted that with RPKI securing routing information by authenticating that all route announcements are made by authorized entities, the incidence of traffic misdirection used in cyber attacks was significantly reduced.

While Buypass cannot implement RPKI independently—as it involves coordination with internet registries and service providers—the CA can advocate for and facilitate its broader adoption among network operators. Encouraging partners and providers to adopt RPKI would indirectly bolster the security of Buypass's MPIC operations. This advocacy could be supported by developing educational resources and tools to help partners implement RPKI, as well as supporting initiatives that promote RPKI adoption across the industry. Furthermore, Buypass can consider participating in research and development efforts aimed at enhancing the automation and efficiency of RPKI validations. This could involve collaborations with academic institutions or industry consortia to explore advanced cryptographic methods and the application of machine learning to predict and mitigate routing anomalies in real-time.

5.4.2 DNSSEC

Buypass can bolster the security of its MPIC framework by implementing DNSSEC within its operational DNS resolver. Given the vulnerabilities associated with DNS, such as spoofing highlighted in chapter 4, DNSSEC is essential for safeguarding DNS data integrity and authenticity. These threats can distort DNS responses and potentially lead to unauthorized certificate issuance.

By activating DNSSEC on its internal DNS resolver, Buypass enhance the verification process of DNS queries within its domain validation operations. Furthermore, when selecting any external DNS resolvers, Buypass should prioritize those that already support DNSSEC. This approach ensures that all external DNS queries associated with its services maintain a high security standard, providing an additional layer of protection against DNS-related attacks.

To streamline DNSSEC adoption, Buypass could develop automated tools for managing the complexities of DNSSEC, such as key management, which would simplify the process for users looking to implement DNSSEC on their domains[49].

Chapter 6

Conclusion

6.1 Summary of Findings

In this thesis, we have addressed the critical issue of Border Gateway Protocol (BGP) hijacking and its implications for Certificate Authorities (CAs). Our focus has been on the feasibility and effectiveness of implementing Multi-Perspective Issuance Corroboration (MPIC) as a mitigation strategy against BGP hijacking. We performed simulations and analyzed existing studies to evaluate the impact of MPIC.

Our findings indicate that MPIC significantly enhances the security of domain control validation processes by employing multiple geographically distributed vantage points. This approach reduces the risk of unauthorized certificate issuance, thereby improving overall internet security. However, it is clear that MPIC should be used in conjunction with other countermeasures, such as RPKI and DNSSEC, to maximize resilience against BGP hijacking and other cyber threats.

6.2 Practical Implications

The practical implications of our research are significant for Buypass and CAs. By implementing MPIC, Buypass can enhance its security measures against BGP hijacking, ensuring that its digital certificate issuance processes are more resilient to attacks. The detailed recommendations and implementation strategies provided in this thesis offer a clear roadmap for deploying MPIC effectively.

For the broader cybersecurity and network management community, our research contributes to the understanding of BGP hijacking and potential countermeasures. The insights gained from this study can help other Certificate Authorities, members

of the CA/Browser Forum, and organizations involved in internet infrastructure and security to adopt similar strategies, thereby enhancing the overall security of the internet.

6.3 Recommendations for Buypass

Based on our analysis, we recommend a structured and phased adoption strategy for implementing MPIC within Buypass. This includes:

- **Infrastructure and Configuration Review:** Conduct a thorough assessment of Buypass's current infrastructure to identify how MPIC can be integrated seamlessly with the existing validation process.
- **Resource and Technology Evaluation:** Evaluate technical resources, including server capacities and network configurations, to support the additional load from multiple vantage points.
- **Risk and Compatibility Analysis:** Identify and address potential issues related to the introduction of multiple vantage points, such as increased load and synchronization complexities.
- **Pilot Testing:** Begin with a controlled pilot testing phase at the first vantage point, closely monitoring performance and collecting detailed logs for analysis.
- **Vantage Point Expansion:** Gradually introduce additional vantage points to minimize the impact on ongoing operations, ensuring each new site follows the same setup and security protocols.
- **Full-Scale Implementation:** Fully integrate MPIC into Buypass's standard domain validation process once successful testing and stabilization have been achieved from multiple vantage points.

By following these steps, Buypass can effectively enhance its Domain Validation processes and improve its overall security posture against BGP hijacking.

6.4 Final Words

This thesis has been a significant learning experience for our team. We have gained a deep understanding of BGP hijacking, MPIC, and the complexities of enhancing internet security. We hope that our findings and recommendations will contribute to the field of cybersecurity and provide practical value to Buypass and other CAs.

References

[1] Cloudflare. *What is BGP? | BGP routing explained*. URL: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/.

[2] Henry Birge-Lee et al. *Bamboozling Certificate Authorities with BGP*. URL: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-birge-lee.pdf.

[3] petercooperjr. "Multi-Perspective Validation Geoblocking FAQ". In: *Let's Encrypt Community* (2024). URL: https://community.letsencrypt.org/t/multi-perspective-validation-geoblocking-faq/218158.

[4] SSL Support Team. "What is SSL/TLS: An In-Depth Guide". In: *SSL.com* (2023). URL: https://www.ssl.com/article/what-is-ssl-tls-an-in-depth-guide/.

[5] Buypass. *Hva er TLS/SSL?* URL: https://www.buypass.no/produkter/tls-ssl-sertifikater/ressurser-tls-ssl-sertifikater/guider/hva-er-ssl-tls.

[6] *Members CA/Browser Forum*. 2024. URL: https://cabforum.org/about/membership/members/.

[7] Fortinet. *What is a Digital Certificate?* URL: https://www.fortinet.com/resources/cyberglossary/digital-certificates.

[8] SSL Support Team. "What is a Certificate Authority (CA)?" In: *SSL.com* (2024). URL: https://www.ssl.com/article/what-is-a-certificate-authority-ca/.

[9] Wikipedia. *Certificate authority*. URL: https://en.wikipedia.org/wiki/Certificate_authority.

[10] Cloudflare. *What Is BGP Hijacking?* URL: https://www.cloudflare.com/en-gb/learning/security/glossary/bgp-hijacking/.

[11] digicert. *What is the CA/B Forum?* URL: https://www.digicert.com/faq/compliance/what-is-the-certification-authority-browser-forum.

[12] UN. *Sustainable Development Goals - Goal 9 - Industry, innovation and infrastructure*. URL: https://www.undp.org/sustainable-development-goals/industry-innovation-and-infrastructure.

[13] Henry Birge-Lee. "Announcing the Open Multi-Perspective Issuance Corroboration Project". In: *Freedom to Tinker* (2024). URL: https://freedom-to-tinker.com/2024/02/13/announcing-the-open-multi-perspective-issuance-corroboration-project/.

[14] Søk Skriv. *IMRaD-modellen*. URL: https://www.sokogskriv.no/skriving/imrad-modellen.html.

[15] AWS. *What is BGP?* URL: https://aws.amazon.com/what-is/border-gateway-protocol/.

[16] Cloudflare. *What is an autonomous system?* URL: https://www.cloudflare.com/en-gb/learning/network-layer/what-is-an-autonomous-system/.

[17] Javatpoint. *What is Autonomous System?* URL: https://www.javatpoint.com/what-is-autonomous-system.

[18] The Internet Numbers Registry for Africa. *Autonomous System Number (ASN)*. URL: https://afrinic.net/asn.

[19] American Registry for Internet Numbers. *Autonomous System Numbers*. URL: https://www.arin.net/resources/guide/asn/.

[20] NetworkLessons. *BGP - Autonomous System Number*. URL: https://notes.networklessons.com/bgp-autonomous-system-number.

[21] StackPath. *WHAT IS AN AUTONOMOUS SYSTEM NUMBER (ASN)?* URL: https://www.stackpath.com/edge-academy/what-is-an-autonomous-system-number-asn/.

[22] Ron Fuller, David Jansen, and Matthew McPherson. "BGP Basics: Internal And External BGP". In: *Network Computing* (2017). URL: https://www.networkcomputing.com/wan-networks/bgp-basics-internal-and-external-bgp.

[23] adware. "Difference between EBGP and IBGP". In: *GeeksforGeeks* (2020). URL: https://www.geeksforgeeks.org/difference-between-ebgp-and-ibgp/.

[24] Kentik. *BGP Hijacking: Understanding Threats to Internet Routing*. URL: https://www.kentik.com/kentipedia/bgp-hijacking/.

[25] Martin J Levy. "RPKI - The required cryptographic upgrade to BGP routing". In: *The Cloudflare Blog* (2018). URL: https://blog.cloudflare.com/rpki.

[26] Cloudflare. *How DNSSEC Works*. URL: https://www.cloudflare.com/en-gb/dns/dnssec/how-dnssec-works/.

[27] Grace Cimaszewski et al. *How Effective is Multiple-Vantage-Point Domain Control Validation?* URL: https://www.cs.princeton.edu/~jrex/papers/usenixsecurity23.pdf.

[28] CertiK. *BGP Hijacking: How Hackers Circumvent Internet Routing Security to Tear the Digital Fabric of Trust*. 2023. URL: https://www.certik.com/resources/blog/1NHvPnvZ8EUjVVs4KZ4L8h-bgp-hijacking-how-hackers-circumvent-internet-routing-security-to-tear-the.

[29] Philippa Gill. "Characterizing Large-scale Routing Anomalies - A Case Study of the China Telecom Incident". In: *The Citizen Lab* (2012). URL: https://citizenlab.ca/2012/12/characterizing-large-scale-routing-anomalies-a-case-study-of-the-china-telecom-incident/.

[30] RIPE NCC. *YouTube Hijacking: A RIPE NCC RIS case study*. URL: https://www.ripe.net/publications/news/youtube-hijacking-a-ripe-ncc-ris-case-study/.

[31] Henry Birge-Lee et al. *Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt*. URL: https://www.usenix.org/system/files/sec21-birge-lee.pdf.

[32] Buypass. *Hva er ACME-standarden og Buypass Go SSL?* URL: https://www.buypass.no/produkter/tls-ssl-sertifikater/les-mer-om-go-ssl-acme.

[33] Anastasios Arampatzis. "What Is ACME Protocol and How Does It Work?" In: *Venafi* (2024). URL: https://venafi.com/blog/what-acme-protocol-and-how-has-it-changed-pki/.

[34] *SC-067 V2: Require Multi-Perspective Issuance Corroboration (Version 2)*. 2024. URL: https://github.com/cabforum/servercert/pull/507.

[35] *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (Version 2.0.4)*. 2024. URL: https://cabforum.org/working-groups/server/baseline-requirements/documents/TLSBRv2.0.4.pdf.

[36] dnsimple Support. *What's a CAA record?* URL: https://support.dnsimple.com/articles/caa-record/#whats-a-caa-record.

[37] "What is OpenStack?" In: *Canonical Ubuntu* (2021). URL: https://ubuntu.com/openstack/what-is-openstack.

[38] Jiří Hanák. “Explained: How OpenStack works and six reasons you should have a cloud on this platform”. In: *MasterDC* (2016). URL: https://www.masterdc.com/blog/openstack-explained-how-does-openstack-work-advantages-reasons-for-cloud/.

[39] “OpenStack Caracal feature overview”. In: *define tech* (2024). URL: https://define-technology.com/openstack-caracal-feature-overview/.

[40] Alexia Emmanoulopoulou. “infographic: How many people use Ubuntu?” In: *Canonical Ubuntu* (2016). URL: https://ubuntu.com/blog/ubuntu-is-everywhere.

[41] “Six reasons why developers choose Ubuntu Desktop”. In: *Canonical Ubuntu* (2018). URL: https://rishi.fedorapeople.org/Desktop_Developers_WP_Canonical_Final.pdf.

[42] “Lubuntu - The fast and lean Linux distribution”. In: *Digital Guide Ionos* (2023). URL: https://www.ionos.com/digitalguide/server/configuration/lubuntu/.

[43] sanju6890. “Difference between Ubuntu and Lubuntu”. In: *GeeksforGeeks* (2021). URL: https://www.geeksforgeeks.org/difference-between-ubuntu-and-lubuntu/.

[44] geeksforgeeks.org. *Private IP Addresses in Networking*. URL: https://www.geeksforgeeks.org/private-ip-addresses-in-networking/d.

[45] P. Mohapatra et al. *BGP Prefix Origin Validation*. URL: https://datatracker.ietf.org/doc/html/rfc6811.

[46] P. Mohapatra et al. *ISO/IEC*. URL: https://www.iso.org/standard/27001.

[47] imperva. *SOC 2 Compliance*. URL: https://www.imperva.com/learn/data-security/soc-2-compliance/.

[48] enisa. *ENISA 71*. URL: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-9-opinion-on-final-accounts-2020.

[49] Cloudflare. *DNSSEC Complexities and Considerations*. URL: https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/.

Appendix

A Scripts

validation_script.sh

```bash
#!/bin/bash

# Check if an IP address is provided as a parameter
if [ "$#" -ne 1 ]; then
    echo "Usage: $0 <IP-to-curl>"
    exit 1
fi

# The first argument to the script is the IP to curl
IP="$1"
COMMAND="curl -sS $IP"

# Execute the command on VM-0 (the local machine) first
SELF_OUTPUT=$($COMMAND)
echo "    Self AS: $SELF_OUTPUT"

# Initialize a counter for "Fake Website" responses
FAKE_COUNT=0

# List of VMs and their IP addresses
declare -A VMs
VMs[VP AS 1]="ubuntu@192.168.1.2"
VMs[VP AS 2]="ubuntu@192.168.2.2"
VMs[VP AS 3]="ubuntu@192.168.3.2"

RED='\033[;31m'
GREEN='\033[;32m'
NC='\033[0m'

# Loop through the list of VMs and execute the command
for vm in "${!VMs[@]}"; do
    # Use SSH to run the command on the remote VM and capture the output
    OUTPUT=$(ssh -o StrictHostKeyChecking=no "${VMs[$vm]}" "$COMMAND")

    # Print the output
    if [ $? -eq 0 ]; then
        echo "   $vm: $OUTPUT"
        # Increment the fake count if the response is "Fake Website"
        if [ "$OUTPUT" == "DNS Validation Failed" ]; then
            ((FAKE_COUNT++))
        fi
    else
        echo "$vm failed to execute the command."
    fi
done

# Check if validation failed based on given conditions
if [[ "$SELF_OUTPUT" == "DNS Validation Failed" ]] || [[ "$FAKE_COUNT" -gt 1 ]]; then
    echo " "
    echo " "
    echo -e "Validation ${RED}FAILED${NC}. Potential BGP Hijack."
    echo " "
else
    echo " "
    echo " "
    echo "Validation ${GREEN}passed${NC}."
    echo " "
fi
```

Script run in the CA-AS to perform domain validation through the vantage point ASes

webserver_script.py

```
from http.server import BaseHTTPRequestHandler, HTTPServer


class HelloWorldHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(b"DNS Validation Failed\n")

def run(server_class=HTTPServer, handler_class=HelloWorldHandler, port=80):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f"Starting server on port {port}")
    httpd.serve_forever()

if __name__ == "__main__":
    run(port=80)
```

Script used to run the real web server in our simulation

webserver_script.py

```
from http.server import BaseHTTPRequestHandler, HTTPServer


class HelloWorldHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(b"DNS Validation Passed\n")

def run(server_class=HTTPServer, handler_class=HelloWorldHandler, port=80):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f"Starting server on port {port}")
    httpd.serve_forever()

if __name__ == "__main__":
    run(port=80)
```

Script used to run the fake web server in our simulation

B Project Plan

B.1 Goals and framework

Background

Border Gateway Protocol (BGP) Hijacking has emerged as a significant threat in the realm of internet security. BGP, the protocol controlling the routing of data across the internet, becomes vulnerable when malicious actors manipulate routing tables to divert internet traffic through their networks. This not only undermines the integrity of data transmission but also poses a specific risk to the issuance and validation of digital certificates by Certificate Authorities (CAs).

Recent incidents, such as the one detailed by Freedom to Tinker in March 2022, demonstrate the severity of BGP hijacking. In this instance, attackers illicitly acquired a certificate by deceiving a CA during the validation process, enabling them to steal a considerable amount of cryptocurrency. These incidents highlight the need for robust countermeasures against such attacks.

Buypass, as a root Certificate Authority (CA), plays a crucial role in this ecosystem. Trusted by web browsers and a member of the CA/Browser Forum, Buypass contributes to setting and maintaining security standards for certificate issuance and validation. The CA/Browser Forum, a voluntary consortium of various CAs and browser developers, is responsible for developing and prescribing security standards for CAs across the globe.

Given the rising threat of BGP hijacking, there is a growing discourse within the CA/Browser Forum and the broader internet security community about implementing mandatory measures to prevent such attacks. One such measure under consideration is Multiple-Vantage-Point Domain Control Validation, a technique designed to mitigate the risks associated with BGP hijacking by utilizing physically distributed points on the internet for domain validation.

This project aims to delve into the problem of BGP hijacking and its implications for certificate security, particularly focusing on the development of a prototype that leverages Multiple-Vantage-Point Domain Control Validation. Our exploration will include an analysis of existing solutions, like Cloudflare's API and the open-source project by Princeton University, to understand and improve upon the methodologies to counteract BGP hijacking in the context of CA operations.

Project goals

In the context of certificate security, BGP Hijacking allows attackers to divert a CA's domain validation efforts to their own network. This misdirection, especially during the DCV process, enables them to impersonate legitimate domain owners and wrongly obtain certificates

In addition to the technical development of the prototype, a significant goal of this project is research-oriented. We aim to gain a deeper understanding of the BGP Hijacking problem, its mechanisms, and the current landscape of countermeasures. This involves a thorough analysis of recent incidents, current security measures in place, and emerging technologies and methodologies in the field. The research will also encompass evaluating the effectiveness of the prototype and exploring potential improvements and adaptations for real-world application.

Framework

Our project approach combines theory, practical development, and real-world testing. We outline our framework as follows:

- **Theoretical Background:** We base our project on established cybersecurity concepts, focusing on BGP hijacking and its effects on certificate authorities. Our understanding and strategies will be informed by existing studies and standards in cybersecurity.
- **Research Methods:** Our approach includes both looking into past cases of BGP hijacking and examining current security solutions. We will use various data gathering and analysis methods to get a deep understanding of these topics.
- **Prototype Development:** A potential part of our project is building a prototype. We will go through stages of planning, designing, coding, testing, and improving it. The goal is to test if Multiple-Vantage-Point Domain Control Validation is a practical solution.
- **Empirical Analysis:** We plan to test the prototype in simulated environments to evaluate its performance. The analysis will include testing under various scenarios to assess robustness, scalability, and reliability against BGP hijacking attempts.
- **Interdisciplinary Integration:** Understanding that internet security covers various fields, our framework combines knowledge from computer science, network security, and cybersecurity policies. This comprehensive approach

makes sure that our prototype and findings are useful and can be applied in actual situations.

- **Collaborative Effort:** Our project benefits from collaboration with industry professionals and academic advisors. This collaboration aims to enhance the practical relevance of our research and ensure that the prototype aligns with industry standards and expectations.
- **Scrum Methodology:** We will incorporate Scrum, an agile project management framework, to ensure flexibility, iterative development, and continuous improvement. This approach will allow us to adapt to changing requirements and feedback throughout the project.

B.2 Scope

Subject Area

In the context of certificate security, BGP Hijacking allows attackers to divert a CA's domain validation efforts to their own network. This misdirection, especially during the DCV process, enables them to impersonate legitimate domain owners and wrongly obtain certificates.

This kind of attack undermines the trust model inherent in the SSL/TLS ecosystem, potentially allowing attackers to execute Man-in-the-Middle (MitM) attacks, where they can intercept, decrypt, and even modify encrypted communications. Such vulnerabilities necessitate the need for robust and advanced security protocols and vigilant network monitoring.

Efforts to mitigate these threats involve the implementation of more rigorous validation methods and the development of technologies to authenticate BGP routes. Notably, the industry has seen advancements in methods such as Extended Validation (EV) certificates, which involve a more comprehensive verification process and are less susceptible to being compromised through BGP hijacking.

Technologies and strategies being employed to mitigate BGP Hijacking and enhance certificate security include:

- **Resource Public Key Infrastructure (RPKI):** Used to authenticate the origin of BGP announcements, making it difficult for attackers to reroute traffic without detection.

- **Multi-perspective Validation:** Conducting domain control validation from multiple geographic and network locations to prevent attackers from intercepting all validation requests.
- **Extended Validation (EV) Certificates:** Require a more thorough verification process, enhancing security against fraudulent certificate issuance.
- **Automated Certificate Management Environment (ACME):** A protocol for automating interactions between CAs and web servers, ensuring secure certificate issuance and renewal.
- **DNS-Based Authentication of Named Entities (DANE):** A protocol to securely specify which TLS/SSL certificate or public key is associated with a domain, adding an extra layer of security.
- **Certificate Transparency Logs:** Publicly accessible logs that record all issued certificates, allowing for easy detection of fraudulent certificates.
- **BGP Monitoring and Alerting Systems:** Systems that monitor BGP announcements and alert network administrators of any suspicious activities.
- **Two-Factor Authentication for Domain Registrars:** Ensuring that changes to domain registration details are authenticated to prevent unauthorized changes.

Limitations

In our bachelor thesis focusing on BGP Hijacking from the perspective of a Certificate Authority, we, as computer science students, face several limitations primarily related to our current level of knowledge and experience. Firstly, there are gaps in our understanding of complex cybersecurity concepts and advanced tools like RPKI, given our developing expertise in handling sophisticated BGP hijacking threats. Our practical experience is also limited, as we have minimal exposure to real-world scenarios and hands-on application of security protocols in a professional setting. This could restrict our grasp of the complexities involved in combating BGP Hijacking.

Furthermore, our access to technical and financial resources is not on par with that of a professional CA, which may limit our ability to explore and test more advanced security solutions. Our limited exposure to professional networks and collaborations within the cybersecurity community could also impede our understanding of how various entities, like ISPs and domain registrars, work together to address security threats. Additionally, our familiarity with the legal and regulatory frameworks governing internet security and CA operations is still rudimentary, potentially affecting our consideration of these critical factors in our thesis.

Lastly, the rapid evolution of internet infrastructure and cybersecurity threats poses a significant challenge, especially for those of us who are still in the learning phase of our careers. These limitations underscore the challenges we face as computer science students in addressing a complex topic like BGP Hijacking in certificate security, and they emphasize the importance of continuous learning and gaining practical exposure.

Task Description

Our project primarily aims to gain a comprehensive understanding of the problem of BGP Hijacking and its implications for Certificate Authorities. In addition to this analytical goal, developing a prototype utilizing Multiple-Vantage-Point Domain Control Validation is a potential part of our endeavor. This approach involves exploring solutions like Cloudflare's API and Princeton University's upcoming open-source project.

The project is tailored for students with a combination of networking and programming skills and seeks to provide an in-depth analysis of the issue. The expected outcomes include a detailed insight into BGP Hijacking, an evaluation of current countermeasures, and a set of comprehensive options for the CA to effectively address this cybersecurity challenge. Through this process, we aim to contribute significantly to the field of internet security by enhancing the understanding and approach towards securing digital certificate issuance.

B.3 Project organization

Roles and responsebilities

The structure of our project team is designed to optimize efficiency, ensure clear communication, and facilitate the smooth progression of the project. The team is comprised of student members along with an advisor and an external collaborator who both provide guidance and expert insights. To ensure the success of our project, roles and responsibilities are assigned to each team member, aligning with their skills and interests. This division of labor allows for focused and efficient progress in each aspect of the project. Below this, the hierarchy and structure of our team is outlined:

- **Project Advisor (Sony George)**: University advisor who provides strategic direction, technical guidance, and oversight. He is the primary points of contact for high-level decisions and conflict resolution.

- **Team Leader (Herman Haugen Mo)**: Responsible for overall project management, coordination among team members, liaising with advisors, and ensuring adherence to timelines. Also coordinates the project, sets milestones, and ensures effective communication within the team and with external parties.
- **Research (All group members)**: Focuses on gathering and analyzing information on BGP hijacking, its impacts, current mitigation strategies, and case studies. They are the foundation of our project's theoretical base. Important to conduct thorough research, integrate findings, and present them to the team for informed decision-making.
- **Development (All group members)**: Handle the technical aspects of prototype development, including coding, implementation of algorithms, and integration of systems. Tasked with the creation and testing of the prototype.
- **Testing and Quality Assurance (All group members)**: Responsible for ensuring the prototype is rigorously tested and meets quality standards. Rigorously tests the prototype under various scenarios, document findings, and provide feedback for improvements. Also oversees the overall quality of both the research and the developed prototype, ensuring that all outputs meet the project's standards.
- **External Collaborator (Mads Egil Henriksen)**: Specialists from relevant fields who may provide specialized knowledge or resources, particularly in aspects of network security and BGP protocols.

Group rules and routines

Effective workflow management is key to the success of our project. To this end, we have established the following rules and routines:

- **Short daily Meeting**: We plan to collaborate each weekday, concluding our day with a concise meeting. In these meetings, we will share our daily progress and discuss plans for the next workday. This routine aims to maintain steady communication and coordinate our efforts effectively.
- **Communication Protocol**: Clear and timely communication through emails and a designated messaging platforms such as Teams and Discord for day-to-day interactions.
- **Decision-Making Process**: Major decisions to be made collectively during team meetings, with input from all members. The team leader will have the final say in case of deadlock.

- **Documentation**: We will ensure detailed documentation of our research and meetings, including agendas and meeting minutes, which will be stored systematically on Microsoft Teams. Additionally, for effective management and tracking of our code, we will implement version control using Git, with all repositories hosted on GitHub.
- **Conflict Resolution**: Any disagreements or conflicts within the team to be addressed promptly, first at the team level and, if unresolved, escalated to the project advisors.
- **Data Storage**: All data including files, documents and code will be stored on cloud storage solutions like Microsoft Office 365, Overleaf and GitHub. This allows for file history and automatic backup.

B.4 Planning, monitoring, reporting

Project management methodology

During the initial planning phase of our project, our team discussed what project management methodology would be most suitable to our project. We evaluated several methodologies, keeping in mind the unique challenges and dynamic nature of our project. Ultimately, we chose Scrum for its agile and flexible framework, which we believe aligns best with the evolving requirements of our research and development process.

Implementing Scrum in our project

By implementing scrum, we can create an environment that utilizes regular communication, quick adaptability, and continuous progress:

- **Regular team meetings**: Short daily meetings will be our primary method for obtaining progress updates, where each member will share their achievements, plans for the day, and any obstacles they face.
- **Sprint planning**: The project will be segmented into bi-weekly sprints. Each sprint will start with a planning meeting to clearly define the goals and tasks for the upcoming two weeks.
- **Sprint reviews and retrospectives**: At the end of each sprint, we will conduct a review session. These sessions will serve to evaluate our progress and the work done. Additionally, retrospective meetings will focus on our team's performance and collaboration, identifying potential areas for improvement.
- **Backlog grooming**: Maintain a project backlog that outlines all tasks. The backlog should be prioritized and refined to ensure the team is always working on the most valuable tasks.
- **Sprint workflows**: The sprints should be defined as time-boxed intervals where specific items from the backlog are completed. The processes of research, documentation, and development standards should support the iterative nature of the work being done.

In our scrum framework:

- Buypass will act as the product owner, providing insights and expectations for the project outcomes.
- The role of scrum master will rotate among team members, ensuring that everyone gains experience in this leadership role and maintains the team's focus on Scrum principles.
- All team members will contribute to research and development, collaboratively tackling the tasks set out in each sprint.

Main sections of the project

In alignment with our objectives, the project is structured into several key phases, each contributing to a comprehensive understanding and practical approach to mitigating BGP Hijacking:

1. **Research Phase:**
    - Deepen our knowledge about BGP hijacking, focusing on its impact on digital certificate issuance and validation.
    - Conduct a thorough review of existing literature, including current countermeasures, technological advancements, and case studies of past incidents.
2. **Exploratory Phase:**
    - Explore potential solutions such as Multiple-Vantage-Point Domain Control Validation, Cloudflare's API, and the upcoming open-source project by Princeton University.
    - Assess these solutions' feasibility and applicability in the context of a CA's operations.
3. **Prototype Development:**
    - If deemed beneficial, develop a prototype using selected solutions to test their effectiveness in a controlled environment.
    - This phase includes coding, implementation, and iterative refinement based on ongoing assessments.
4. **Analysis and Evaluation Phase:**
    - Analyze the data collected from the research and exploratory phases.
    - Evaluate the prototype's performance (if developed) against BGP hijacking scenarios.
    - Prepare a detailed report comprising our findings, insights, and comprehensive recommendations for CAs to enhance their security measures against BGP Hijacking.
5. **Final Compilation and Presentation:**
    - Consolidate all findings, analyses, and recommendations into a cohesive final report.

- Present our conclusions and suggested strategies, highlighting the practical implications for CAs and the broader internet security community.
- This structured approach ensures a focused and methodical exploration of the BGP Hijacking issue, enabling us to achieve our goals of understanding the problem, exploring potential solutions, and providing actionable recommendations.

Meeting plans

Effective communication and regular check-ins are vital for the smooth progression of our project. To this end, we have established a meeting schedule and an agenda for each meeting to ensure all team members are aligned and any issues are promptly addressed.

- **Daily Team Meetings**:
  - Every weekday before concluding our work.
  - Brief discussion on daily progress and plan for the next workday.
- **Weekly Meetings with External Collaborator**:
  - Every Friday at 10:00.
  - Agenda covers strategic guidance, feedback on recent progress, and resolution of complex issues.
- **Weekly Advisor Meetings**:
  - Every Friday at 12:00.
  - Agenda covers strategic guidance, feedback on recent progress, and resolution of complex issues.
- **Bi-weekly Scrum Sprint Meeting**:
  - Every second Thursday.
  - Comprehensive review of the progress from the Scrum sprint.
  - Planning the next Scrum sprint.
  - Discussing the team's performance and collaboration, identifying areas for improvement.
- **Emergency Meetings**:
  - Scheduled as needed in case of urgent issues or significant roadblocks.
  - Aimed at rapid problem-solving and decision-making to keep the project on track.

B.5 Development Practices and Resources

Development Routines

Adopting robust development routines is essential for the creation of a reliable and effective prototype. Our approach includes:

- **Coding Standards**: We will adhere to widely accepted coding standards for readability and maintainability. This includes consistent naming conventions, commenting practices, and code structuring.
- **Code Review Processes**: All code contributions will be subject to peer review before merging into the main branch. This ensures that all code is scrutinized for quality, functionality, and adherence to project standards.
- **Testing Protocols**: Rigorous testing will be an integral part of our development process. We will establish testing protocols that include unit tests, integration tests, and system tests, ensuring that every component of our prototype functions as intended.

Tools and Utilities

We are considering the following software and hardware resources for the potential development and testing of our prototype, although the final selection may vary as the project progresses:

- **Development Tools:** Python and Node.js are our primary choices for programming. We plan to use Git for version control and Visual Studio Code as our preferred Integrated Development Environment (IDE).
- **Network Simulation Tools:** We might utilize network simulators such as GNS3 or Cisco VIRL to create testing environments.
- **Testing and Analysis Tools:** Tools under consideration include Postman for API testing, Wireshark for analyzing network traffic, and PyTest or Jest for automated testing.
- **Documentation Tools:** We anticipate using Markdown editors and diagramming tools to produce clear and detailed documentation.
- **Hardware Resources:** We expect to require adequate computing resources, including CPUs, memory, and storage, and a reliable internet connection for development and testing purposes.

It's important to note that these choices are tentative and subject to change based on the evolving needs and direction of the project.

B.6 Risk

Risk Analysis

The following presents a risk analysis for our BGP hijacking countermeasure development project, categorizing potential problems according to their probability and consequence. We also propose measures to mitigate these risks. The risks are categorized into three levels: green (acceptable risk), yellow (moderate risk), and red (unacceptable risk).

Consequence	Probability				
	Rare	Unlikely	Possible	Likely	Certain
Catastrophic					
Major					
Moderate					
Minor					
Insignificant					

Risk matrix

Risk Scenario 1: Scope Creep
Description: There is a risk that due to poor planning or lack of clear communication, the project scope could expand beyond manageable limits, preventing the team from delivering the original objectives.

Probability: Possible

Consequence: Major

Overall Risk: Yellow

Measures: To minimize this risk any potential scope changes must be critically evaluated and unanimously agreed upon by all team members before proceeding.

Risk Scenario 2: Technical Challenges in Prototype Development
Description: Developing a prototype for detecting BGP hijacking might present unforeseen technical challenges due to the complexity of the task.

Probability: Likely

Consequence: Minor

Overall Risk: Yellow

Measures: Conduct in-depth research and self-study to enhance our understanding of BGP hijacking and related technologies. Utilize online resources and

forums for problem-solving and technical assistance. Implement an iterative development process, allowing for regular evaluation and adjustment of our approach based on feedback and testing results.

Risk Scenario 3: Data Loss
Description: Critical project data, code, or documentation could be lost due to hardware failure, software bugs, or human error.

Probability: Unlikely

Consequence: Major

Overall Risk: Yellow

Measures: Regular data backups, use of version control systems like Git, and cloud storage will be used to mitigate the risk of data loss.

Risk Scenario 4: Group Conflict
Description: Disagreements within the team could lead to delays or disruptions in the project.

Probability: Rare

Consequence: Moderate

Overall Risk: Yellow

Measures: Foster open communication and conflict resolution strategies within the team. If necessary, engage a mediator to facilitate discussion and resolve issues.

Risk Scenario 5: Sickness
Description: Sickness within the team that could lead to delays or disruptions in the project.

Probability: Possbile

Consequence: Minor

Overall Risk: Yellow

Measures: Clear and consistent communication between team members if sickness were to arise. If someone is sick, create a solution so that the sick team member can participate with what they can from home.

Risk Scenario 6: Princeton University open source project not released in time
Description: The open source project that is being worked on at Princeton University is not released in time for us to use it's findings for our project.

Probability: Possible

Consequence: Minor

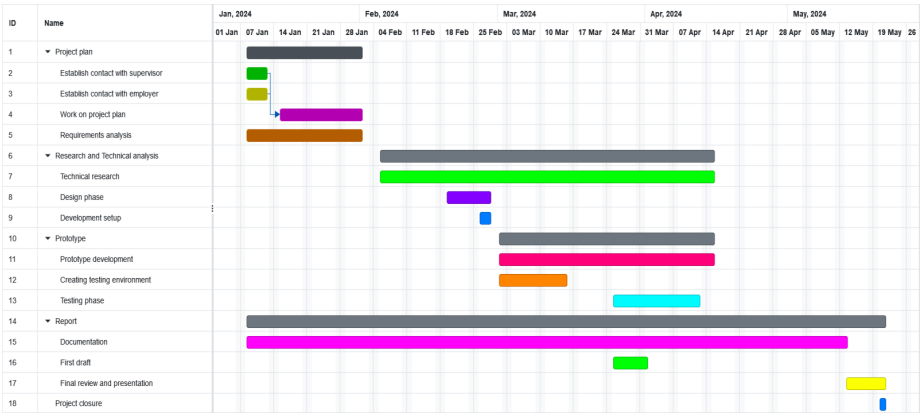
Overall Risk: Yellow

Measures: If the project isn't shared publicly on schedule, we will need to turn to other resources. This means we might miss out on using a resource we think

would benefit our research.

B.7 Implementation

Gantt chart



Implementation timeline in Gantt chart format.

Milestones and decision points

1. **Milestone 1 (December 15, 2023):** Start Communication with External Business and Advisor
    - Initiate talks with the company and our academic advisor to set up the project's framework.
2. **Milestone 2 (January 30, 2024):** Finalize Project Plan and Agreement
    - Complete and submit the detailed plan for the project and an agreement form.
3. **Milestone 3 (February 5, 2024):** Begin Research and Technical Analysis
    - Start detailed research and technical examination related to our project's focus area.
4. **Milestone 4 (February 28, 2024):** Decision on Using Princeton University's Project
    - Decide if we will include Princeton University's open source project in our work.
5. **Milestone 5 (March 15, 2024):** Decide on Prototype Development

- Make a decision about developing a prototype as part of our project.

6. **Milestone 6 (April 1, 2024):** First Draft of Report
    - Finish the first version of our project report.
7. **Milestone 7 (April 15, 2024):** Complete Prototype
    - Finish building the prototype, if we decide to create one.
8. **Milestone 8 (May 13, 2024):** Complete Final Report
    - Complete the final version of our project report.

C Project Agreement

NTNU
Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for datateknologi og informatikk
Veileder ved NTNU: Sony George e-post og tlf. sony.george@ntnu.no 611 35 211
Ekstern virksomhet: Bugpass Ekstern virksomhet sin kontaktperson, e-post og tlf.: Mads Egil Henriksveen, mads.henriksveen@bugpass.no
Student: Herman Haugen Mo Fødselsdato: 14/05/97
Ev. flere studenter[1] Marcus Torvik 07/08/00
Hamid Nikolay Lund Olsen 03/07/02

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 10/01/24
Sluttdato: 21/05/24

Oppgavens arbeidstittel er: Multi-Perspective Issurance Corroboration

[1] Dersom flere studenter skriver oppgave i fellesskap, kan alle føres opp her. Rettigheter ligger da i fellesskap mellom studentene. Dersom ekstern virksomhet i stedet ønsker at det skal inngås egen avtale med hver enkelt student, gjøres dette.

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:
Ingen utgifter planlagt

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[2]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

[2] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

X	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene: Se vedlegg

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: v Emrearnsaliz Dato: 5/2 - 24
Veileder ved NTNU: Dato: 31/01/2024
Ekstern virksomhet: 2024.01.30 Dato: '00'01+ 10:02:48
Student: Dato: 22/01/24
Ev. flere studenter 22/01/24
22/01/24

buypass

Tillegg til Prosjektavtale bacheloroppgave

Opphavs- og eiendomsrett

Eiendomsrett, opphavsrett og andre relevante materielle og immaterielle rettigheter til resultatet av bacheloroppgaven tilfaller oppdragsgiver, med mindre annet er særskilt avtalt.

Rettighetene omfatter også rett til endring og videreoverdragelse, jf. lov av 15. juni 2018 nr. 40 om opphavsrett til åndsverk mv. (åndsverkloven) § 68.

Studentene beholder rettighetene til egne verktøy og metodegrunnlag. Begge parter kan også utnytte generell kunnskap (know-how) som ikke er taushetsbelagt og som de har tilegnet seg i forbindelse med arbeidet.

5/2-24

Side 1 av 1

D Task Description

Oppgave 35 DIGSEC, BIDATA, BPROG 2-4 stk

Oppgavetittel: Multi-Perspective Issurance Corroboration

Bedrift:	Buypass AS
Kontaktperson:	Mads Henriksveen
E-post:	mads.henriksveen@buypass.no
Telefon:	95225672
Lokasjon:	Gjøvik

Beskrivelse av oppgaven

Buypass er en sertifikatutsteder (rot CA) som har tillitt hos nettlesere og er medlem i CA/Browser forum.

De siste årene har det dukket opp en ny trussel, Border Gateway Protocol (BGP) Hijacking, se for eksempel https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/. Det har vært vellykkede angrep den seneste tiden der angripere har skaffet seg et illegitimt sertifikat ved å benytte BPG-hijacking slik at sertifikatutstedere har blitt lurt under validering til å utstede sertifikatet, se https://freedom-to-tinker.com/2022/03/09/attackers-exploit-fundamental-flaw-in-the-webs-security-to-steal-2-million-in-cryptocurrency/.

Dette er nå ansett som en så alvorlig trussel at man snakker om å innføre obligatoriske tiltak som alle sertifikatutstedere må følge for å unngå dette. En måte å oppnå dette på er å ta det inn i standarder som utarbeides av CA/Browser forum. En av teknikkene som kan brukes er Multiple-Vantage-Point Domain Control Validation, se https://arxiv.org/abs/2302.08000 og https://blog.cloudflare.com/secure-certificate-issuance/. Her sørger man altså for å benytte flere fysisk distribuerte punkter på nettet når man skal gjennomføre oppslag som kan være sårbare for BGP-hijacking.

Vi ønsker å få litt bedre innsikt i problemstillingen og tiltak som kan gjøres for å forbedre dette. Vi vet at Cloudflare tilbyr et API som kan brukes for denne type mottiltak og Princeton University jobber med et open-source prosjekt som kan benyttes av sertifikatutstedere allerede fra tidlig neste år.

Vi ønsker at studentene går inn i problemstillingen og utvikler en prototype der man tester ut denne type løsninger for å gi innsikt i problemstillingen samt de tiltakene som kan iverksettes.

Oppgaven egner seg for en kombinert gruppe med både nettverks og programmeringskompetanse.

E Meeting Minutes

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

January 19, 2024

1 Meeting Details

Date: 19.01.19
Time: 10:00 - 10:30
Location: Microsoft Teams Meeting
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Prototype Selection**
   - Discussion on what to use as a prototype and exploring viable options.
2. **Tool and Programming Language Preferences**
   - Considerations for tools or programming languages best suited for the project.
   - Flexibility to adapt to the employer's software upon delivery.
3. **Scope Limitation**
   - Discussion on how to limit the scope of the project.
   - Decision to define the scope more clearly as the project progresses.
4. **Collaboration with Employer**
   - Opportunities for collaboration with the employer in relevant areas for the project plan.
5. **Meeting Frequency**
   - Next meeting scheduled for the following Friday.
   - Plan to establish a regular meeting schedule to be discussed in the next meeting.
6. **Preparation for Next Physical Meeting**
   - Confirmation of a physical meeting next Friday.
   - All members to send information to prepare for the meeting.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

January 26, 2024

1 Meeting Details

Date: 26.01.24
Time: 10:00 - 10:40
Location: Buypass Gjøvik Office
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Office Overview**
   - Presentation of the current draft of the project plan.
   - Mads finds the limitations section satisfactory; further review is planned post-meeting.
2. **Project Plan and Goals**
   - Task description and project goals align well with the published requirements.
   - Content development beyond what is written is at our discretion.
3. **Contractual Matters**
   - Mads to review the standard agreement, particularly copyright terms.
   - Addendum regarding copyright and property rights.
   - CEO Suna Lindstøl to sign the agreement.
4. **Finalizing and Signing the Agreement**
   - Agreement to be finalized today with the advisor.
   - Process for Mads receiving, signing, and forwarding the agreement.
5. **Meeting Schedule**
   - Weekly meetings set for Fridays at 10:00 AM.
   - Possibility of cancellation if necessary.
6. **Presentation and Requirements**
   - Brief overview by Mads on the "Strengthening Domain Validation Using Multi-perspective Issuance Corroboration." presentation.
   - Emphasis on meeting project requirements.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

January 26, 2024

1 Meeting Details

Date: 26.01.24
Time: 11:00 - 11:30
Location: NTNU A232
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Debrief with Buypass**
   - Reviewed the project plan with positive feedback; identified areas requiring adjustments in the collaboration agreement.
   - Discussed confidentiality constraints faced by a previous group due to copyright/security concerns, impacting disclosure of their work.
2. **Collaboration Agreement Revisions**
   - Agreed to send the revised sections of the collaboration agreement, as reviewed with Buypass, to Sony and Tom for their input.
   - Confirmed that while the project outcomes can be published, Buypass retains ownership over the work.
3. **Meeting Schedules**
   - Established a routine for regular meetings with Buypass.
   - Scheduled ongoing meetings with Sony every Friday, following discussions with Buypass.
4. **Work Tracking Mechanisms**
   - Evaluated the Excel sheet designed for tracking group working hours, defining essential metrics for recording time spent on project activities.
5. **Report Writing Schedule**
   - Set April as the official start month for compiling the report, noting the feasibility of drafting sections earlier as needed.
6. **Project Focus**
   - Highlighted that the project will primarily concentrate on research and documentation, with a secondary focus on exploring creative and innovative avenues.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

February 09, 2024

1 Meeting Details

Date: 09.02.24
Time: 09:30 - 10:00
Location: Microsoft Teams Meeting
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Project Status Update**
   - Presentation of the initial sections of the report, outlining the progress made thus far.
2. **Upcoming Open Source Project**
   - Mads mentioned that the Princeton open source project is expected to be released in March, which may provide relevant insights or resources.
3. **Domain Validation Initiatives**
   - Discussion on the Validation Sub Committee's efforts in domain validation, exploring potential relevance to our project.
4. **Research and Development**
   - Currently focusing on research and preliminary analysis. We anticipate having more detailed information and findings to present later in the project timeline.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

February 09, 2024

1 Meeting Details

Date: 09.02.24
Time: 11:00 - 11:30
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Report Outline and Initial Writing**
   - Commenced drafting the outline and began writing the background and theory sections of the report.
   - Presented the progress, including the outline and initial sections, to Sony for feedback.
2. **Defining the Report's Audience**
   - Identified the intended audience for the report to tailor the depth and scope of explanations accordingly.
   - Aim to ensure the report is comprehensible to individuals with a background in computer science.
3. **Content Development Strategy**
   - Focus on enriching the background section and initiating work on the implementation details.
   - Based on the audience's needs, strategize on the extent and manner of presenting information.
4. **Collaboration with External Projects**
   - Consider reaching out to the Princeton University open-source project for potential early access to support our research.
5. **Integration with Project Plan**
   - Permission granted to reiterate necessary elements from the project plan within the report.
6. **Citation and Referencing**
   - Emphasize the importance of citing sources meticulously, using boxed citations and direct links where applicable.
   - Non-citational material does not require strict ordering in the list of references or sources.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

February 23, 2024

1 Meeting Details

Date: 23.02.24
Time: 10:00 - 10:30
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Exploration of Implementation Approaches**
   - Conducted a review of various methods of implementation to identify the most suitable options for our project.
2. **Princeton Open Source Project Update**
   - Princeton University commenced work on their open-source project approximately two weeks ago, offering potential insights or collaboration opportunities for our research.
3. **Lets Encrypt Boulder Project**
   - Investigating the Lets Encrypt Boulder open-source project as a significant and complex initiative.
   - Ongoing efforts to understand how it might be integrated or utilized within our project due to its extensive scope.
4. **Accessing Expertise**
   - Mads has established contacts within Lets Encrypt, providing us with a valuable resource for inquiries related to our project's needs.
5. **Upcoming Briefing**
   - Scheduled a session next Friday to review and discuss the latest developments from Google, evaluating their applicability to our work.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

February 23, 2024

1 Meeting Details

Date: 23.02.24
Time: 11:00 - 11:30
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Princeton Project Announcement**
   - Noted Princeton University's recent announcement, marking the commencement of their open-source project.
2. **Lets Encrypt Alternative**
   - Discovered another promising project within Lets Encrypt, featuring a substantial codebase dedicated to certificate issuance.
3. **Project Scope and Timeline**
   - Acknowledged the challenge of addressing the breadth of the project within a three-month period.
   - Buypass has granted considerable flexibility, necessitating further efforts to define and narrow the project scope.
4. **Seeking Expertise**
   - Consideration of engaging an expert from NTNU to provide specialized knowledge and guidance for the project.
5. **Strategic Planning**
   - Plans to brainstorm potential solutions and approaches over the weekend.
   - A meeting with Sony is scheduled for Tuesday to discuss any difficulties or uncertainties encountered during the brainstorming process.
6. **Testing Methodology**
   - The company has proposed to assist with developing a testing method, although specific strategies will be determined at a later stage.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

February 27, 2024

1 Meeting Details

Date: 27.02.24
Time: 13:10 - 13:15
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Contact with a Network Expert**
   - Initiated a request to Sony for assistance in connecting with a network expert.
2. **Referral to Lars**
   - Sony recommended Lars, who manages IT networking at NTNU, as a potential source of expertise.
3. **Consultation with Tom**
   - Sony plans to consult Tom to ascertain the most effective strategy moving forward.
4. **Scheduling Flexibility**
   - Decisions regarding specific dates and times for meetings or consultations have been deferred, allowing for greater flexibility.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

March 01, 2024

1 Meeting Details

Date: 01.03.24
Time: 10:00 - 10:10
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Continuation of Report Writing**
   - Decided to proceed with writing the report, focusing on the background and theory sections related to BGP (Border Gateway Protocol).
2. **Exploring BGP Hijacking Simulation**
   - Evaluating the feasibility of simulating BGP hijacking, whether through setting up our own network or using servers.
3. **Review of Let's Encrypt Open Source Project**
   - Examined Let's Encrypt's open-source project but remain uncertain about its relevance to our work.
4. **Prototype and Simulation Ideas**
   - Presented our initial ideas for creating a prototype and conducting simulations.
5. **Future Focus on Testing**
   - Mads suggested that a deeper exploration into testing methodologies will be conducted later.
6. **Development of Sketches and Plans**
   - Planning to start looking at concrete sketches and plans possibly next week.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

March 08, 2024

1 Meeting Details

Date: 08.03.24
Time: 11:00 - 11:10
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Examination Preparation**
   - The team will prioritize preparation for the upcoming examination scheduled for the 13th, pausing other activities temporarily.
2. **Seeking a Network Expert**
   - Sony plans to consult with Tom, Kiran, or another contact to identify a network expert who can provide specialized assistance for our project.
3. **Recommended Resource on Report Writing**
   - Sony strongly recommends reviewing a specific lecture focused on report writing to enhance the quality of our documentation.
4. **Project Updates**
   - We intend to send further updates by the end of next week, following the exam.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

April 05, 2024

1 Meeting Details

Date: 05.04.24
Time: 10:00 - 10:15
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Simulation Environment Configuration**
   - This week, our efforts were concentrated on configuring the simulation environment using GNS3.
2. **Introduction to GNS3**
   - We provide a brief overview of how GNS3 operates as a network simulation tool.
3. **Topology Setup**
   - Successfully established the initial version of our network topology in GNS3.
4. **Simulation Timeline Inquiry**
   - In response to Mads's inquiry regarding the simulation readiness, we communicated that, while unable to commit to a definitive timeline, completing the setup is our current daily focus.
5. **Upcoming Physical Meeting**
   - Scheduled a physical meeting for next Wednesday to discuss and better understand Buypass's specific needs in relation to our project.
6. **Project Complexity and Interest**
   - Mads concurs that while the project's theme poses challenges, it remains a captivating subject.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

April 05, 2024

1 Meeting Details

Date: 05.04.24
Time: 11:00 - 11:15
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Consultation with Network Expert**
   - The interaction with the network expert provided us with sufficient information for our current needs, with no further questions at this stage.
2. **Importance of Presentation**
   - Sony highlighted the rarity of our project topic and advised that the manner of presentation would significantly impact its reception. Keeping the evaluation criteria in mind is essential.
3. **Communicating Novelty and Challenges**
   - It's crucial to articulate the novelty of our work and the challenges faced during implementation, using precise language to convey the project's pioneering nature.
4. **Opportunity for Innovation**
   - Sony suggested that our endeavor to create something new presents a valuable opportunity to enhance our project's merit and potentially improve our grade.
5. **Adherence to Project Plan**
   - Sony reassured us that deviating from the original project plan is acceptable, especially due to unforeseen changes, such as the delay in Princeton's project completion. It's important to document these changes clearly.
6. **Presentation Accessibility**
   - Ensuring the presentation is accessible to a general audience is vital. This may involve creating graphs or other visual aids to aid in comprehension and engagement.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

April 12, 2024

1 Meeting Details

Date: 12.04.24
Time: 14:45- 16:15
Location: Buypass's office in Gjøvik
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **CABF Ballot SC-067**
   - Proposal under CABF Ballot SC-067 to require domain validation and CAA checks from multiple network perspectives. This measure is expected to take additional time before it is finalized.
2. **Global Focus on BGP Hijacking**
   - There is a significant international focus on BGP Hijacking, with numerous stakeholders advocating for robust and secure implementations. In case of non-compliance or errors, CAs must log the incident in Bugzilla, which acts somewhat like a "wall of shame." See `wiki.mozilla.org/CA/Incident_Dashboard` for details.
3. **Buypass Operational Protocols**
   - Buypass issues certificates using domain names, avoiding IP addresses. The operational requirements include exceptions, making it complex to understand applicable standards.
   - The current validation methods used by Buypass include DNS and HTTP validation.
   - There is a requirement for network perspectives to be at least 500km apart in straight-line distance to be considered distinct.
4. **Routing and Validation Requirements**
   - All internet traffic must be forwarded via a network or set of networks that filter all RPKI-invalid BGP routes as defined by RFC 6811.
   - For our code in the simulation, t is not necessary to implement the full code for a website and validation processes. Instead, our focus will shift more towards the routing after we simulate BGP hijacking, exploring different outcomes using 0-X vantage points and comparing these.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

April 19, 2024

1 Meeting Details

Date: 19.04.24
Time: 11:00- 11:30
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Marcus Torvik, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Simulation Progress**
   - Significant efforts have been dedicated to the simulation aspect of our project. With substantial progress made, we are now shifting focus towards continuing the writing of the report.
2. **Aligning with Buypass's Expectations**
   - Sony inquired about our project's alignment with Buypass's expectations. We currently view our role as providing recommendations on potential implementations to Buypass. Furthermore, there is an understanding that Buypass aims to gain as much insight as possible from our research and findings.
3. **Preparation for Upcoming Presentation**
   - Scheduled for next Friday, we will deliver a presentation to Sony, showcasing our work and the intended approach for the final presentations.
   - This session will also serve as a mock evaluation, where Sony will pose potential "stupid" questions we might encounter during the actual evaluations. This practice is intended to enhance our preparedness and refine our presentation skills.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

April 26, 2024

1 Meeting Details

Date: 26.04.24
Time: 11:00- 11:10
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Completion of Simulation**
   - We have successfully concluded our simulation phase, extracting all possible insights and data.
2. **Report Finalization**
   - Our current focus has shifted to finalizing the report, incorporating the findings and analyses from the simulation.
3. **Preparation for Mock Presentation**
   - A mock presentation is scheduled with our advisor to refine our delivery and content ahead of the final presentation.
4. **Planned Presentation for Buypass**
   - We plan to deliver a similar presentation to Mads next week, who will bring relevant Buypass personnel who require the information.
   - This meeting will serve as a briefing to inform and update Buypass on our project's outcomes and recommendations.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

May 03, 2024

1 Meeting Details

Date: 03.05.24
Time: 10:00- 10:30
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Status Report to Mads**
   - Provided Mads with a brief update indicating our current focus on writing the report.
2. **Planning the Presentation for Buypass**
   - Discussed potential dates for the presentation, considering the 3rd or 4th of June.
   - Mads will confirm the exact date by next Friday.
   - He also plans to review the presentation preliminarily and will conduct an internal review round.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

May 03, 2024

1 Meeting Details

Date: 03.05.24
Time: 11:00- 11:30
Location: Microsoft Teams
Attendees: Sony George, Herman Haugen Mo, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Communication with Sony**
   - Sony inquired about our progress. We have assured him that he will be notified when the report is ready for review.
2. **Presentation Scheduling with Buypass**
   - Confirmed plans with Buypass to schedule our project presentation shortly before the official bachelor presentation.
3. **Preparation of Presentation Materials**
   - Discussed the necessity of creating a poster for our presentation. While we can request a template, it's important to note that only the report will be evaluated.
4. **Evaluation Criteria Explained by Sony**
   - Sony provided insights on how different components of our project connect with the evaluation criteria.
5. **Report Presentation Strategy**
   - Encouraged to create excitement within the report and effectively 'sell' our project. We aim to present our report in a manner that reflects the extensive effort involved.
6. **Inclusion of Project Plan in Report**
   - Plan to attach the project plan as an appendix and possibly include some reflective commentary in the report, although it is anticipated that this section may not be heavily scrutinized.

Meeting Minutes

Bachelor's Thesis - Multi-Perspective Issuance Corroboration

May 10, 2024

1 Meeting Details

Date: 10.05.24
Time: 10:00- 10:30
Location: Microsoft Teams
Attendees: Mads Egil Henriksveen, Herman Haugen Mo, Harald Nikolay Lund Olsen

2 Items Discussed

1. **Project Report Finalization**
   - Informed Mads that we are in the final stages of completing our report. The first draft has been prepared and is ready for review.
2. **Stable Requirement Specifications**
   - Mads confirmed that there are currently no changes to the project requirements.
3. **Upcoming Deadlines and Voting**
   - A deadline for certain project requirements is due today, and a vote on these requirements is expected to take place soon.
4. **Updates on External Projects**
   - Mads also shared news that there has been some progress in the Princeton project, indicating potential developments that could affect our project.

F Timesheets

Herman

Week	Day	Hours	Details	Total
50	Monday			5
	Tuesday			
	Wednesday	1	Meeting with supervisor	
	Thursday	1	Preperations for meeting	
	Friday	1	Meeting with Buypass	
	Saturday	2	Research	
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
51	Monday	2	Research	3
	Tuesday	1	Research	
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
52	Monday			0
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
1	Monday			2
	Tuesday			
	Wednesday			
	Thursday			
	Friday	2	Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
2	Monday			8
	Tuesday			
	Wednesday	4	Project plan	
	Thursday	4	Project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
3	Monday			6
	Tuesday			
	Wednesday	3	Meeting with supervisor / Project plan	
	Thursday	1	Project plan	
	Friday	2	Meeting with Buypass / Project plan	
	Saturday			

	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
4	Monday	2	Project plan / Standard agreement form	10
	Tuesday	3	Project plan	
	Wednesday	1	Project plan	
	Thursday	2	Project plan	
	Friday	2	Meeting with Buypass/Meeting with supervisor / standard agreement form	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
5	Monday	2	Project plan	14
	Tuesday	5	Project plan	
	Wednesday	6	Project plan / Standard agreement form	
	Thursday	1	Delivery of project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
6	Monday	3	Research	22
	Tuesday	3	Research	
	Wednesday	2	Research	
	Thursday	6	Report writing	
	Friday	8	Meeting with Buypass/Meeting with supervisor/Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
7	Monday	5	Report writing/Research	24
	Tuesday	5	Report writing/Research	
	Wednesday	3	Report writing/Research	
	Thursday	6	Report writing/Research	
	Friday	5	Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
8	Monday	4	Report writing/Research	23
	Tuesday	5	Report writing/Research	
	Wednesday	5	Report writing/Research	
	Thursday	3	Report writing/Research	
	Friday	6	Meeting with Buypass/Meeting with supervisor / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday	4	Report writing/Research	
	Tuesday	1	Meeting with supervisor	
	Wednesday	5	Report writing/Research	

9	Thursday	2	Report writing/Research	13
	Friday	1	Meeting with Buypass	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
10	Monday	4	Report writing/Research	25
	Tuesday	3	Report writing/Research	
	Wednesday	6	Report writing/Research	
	Thursday	6	Report writing/Research	
	Friday	6	Meeting with supervisor/Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
11	Monday	4	Report writing/Research	22
	Tuesday	3	Report writing/Research	
	Wednesday	6	Report writing/Research	
	Thursday	6	Report writing/Research	
	Friday	3	Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
12	Monday	4	Preperation for simulation / Report writing	18
	Tuesday	3	Preperation for simulation / Report writing	
	Wednesday	5	Preperation for simulation / Report writing	
	Thursday	3	Preperation for simulation / Report writing	
	Friday	3	Preperation for simulation / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
13	Monday		Easter	0
	Tuesday		Easter	
	Wednesday		Easter	
	Thursday		Easter	
	Friday		Easter	
	Saturday		Easter	
	Sunday		Easter	
Week	**Day**	**Hours**	**Details**	**Total**
14	Monday	6	Simulation setup	29
	Tuesday	6	Simulation setup	
	Wednesday	5	Simulation setup	
	Thursday	6	Simulation setup	
	Friday	6	Meeting with Buypass / Meeting with supervisor / Simulation setup	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday	7	Simulation work	

15	Tuesday	8	Simulation work	37
	Wednesday	7	Simulation work	
	Thursday	8	Simulation work	
	Friday	7	Meeting with Buypass / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
16	Monday	6	Simulation work / Report writing	34
	Tuesday	7	Simulation work / Report writing	
	Wednesday	7	Simulation work / Report writing	
	Thursday	8	Simulation work / Report writing	
	Friday	6	Meeting with Buypass / Meeting with supervisor / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
17	Monday	8	Simulation work / Report writing / Presentation work	37
	Tuesday	7	Simulation work / Report writing / Presentation work	
	Wednesday	6	Simulation work / Report writing / Presentation work	
	Thursday	8	Simulation work / Report writing / Presentation work	
	Friday	8	Meeting with Buypass / Mock presentation for supervisor / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
18	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting Buypass / Meeting supervisor/ Report Writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
19	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting with Buypass / Report writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
20	Monday	8	Report writing	57
	Tuesday	9	Report writing	
	Wednesday	9	Report writing	
	Thursday	9	Report writing	
	Friday		17. May	
	Saturday	11	Report writing / final touches	

	Sunday	11	Report writing / final touches	
Week	**Day**	**Hours**	**Details**	**Total**
21	Monday	12	Final touches / Delivery of project	12
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
			Total hours contributed to project:	**513**

Marcus

Week	Day	Hours	Details	Total
50	Monday			5
	Tuesday			
	Wednesday	1	Meeting with supervisor	
	Thursday	1	Preperations for meeting	
	Friday	1	Meeting with Buypass	
	Saturday	2	Research	
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
51	Monday	2	Research	5
	Tuesday	2	Research	
	Wednesday	1	Research	
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
52	Monday	2	Research	5
	Tuesday	2	Research	
	Wednesday			
	Thursday	1	Research	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
1	Monday	2	Research	6
	Tuesday	2	Research	
	Wednesday			
	Thursday	2	Research	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
2	Monday			8
	Tuesday			
	Wednesday	4	Project plan	
	Thursday	4	Project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
3	Monday			6
	Tuesday			
	Wednesday	3	Meeting with supervisor /Project plan	
	Thursday	1	Project plan	
	Friday	2	Meeting with Buypass / Project plan	
	Saturday			

	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
4	Monday	2	Project plan / Standard agreement form	11
	Tuesday	3	Project plan	
	Wednesday	1	Project plan	
	Thursday	2	Project plan	
	Friday	2	Meeting with Buypass/Meeting with supervisor/ Standard agreement form	
	Saturday			
	Sunday	1	Standard agreement form	
Week	**Day**	**Hours**	**Details**	**Total**
5	Monday	2	Project plan	14
	Tuesday	5	Project plan	
	Wednesday	6	Project plan / Standard agreement form	
	Thursday	1	Delivery of project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
6	Monday	2	Research	20
	Tuesday	3	Research	
	Wednesday	2	Research	
	Thursday	6	Report writing	
	Friday	7	Meeting with Buypass/Meeting with supervisor/Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
7	Monday	5	Report writing/Research	22
	Tuesday	4	Report writing/Research	
	Wednesday	3	Report writing/Research	
	Thursday	3	Report writing/Research	
	Friday	7	Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
8	Monday	5	Report writing/Research	21
	Tuesday	4	Report writing/Research	
	Wednesday	3	Report writing/Research	
	Thursday	3	Report writing/Research	
	Friday	6	Meeting with Buypass/Meeting with supervisor / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday	3	Report writing/Research	
	Tuesday	1	Meeting with supervisor	
	Wednesday	4	Report writing/Research	

9	Thursday	3	Report writing/Research	12
	Friday	1	Meeting with Buypass	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
10	Monday	4	Report writing/Research	26
	Tuesday	5	Report writing/Research	
	Wednesday	5	Report writing/Research	
	Thursday	6	Report writing/Research	
	Friday	6	Meeting with supervisor/Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
11	Monday	4	Report writing/Research	26
	Tuesday	6	Report writing/Research	
	Wednesday	6	Report writing/Research	
	Thursday	6	Report writing/Research	
	Friday	4	Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
12	Monday	4	Preperation for simulation / Report writing	18
	Tuesday	3	Preperation for simulation / Report writing	
	Wednesday	5	Preperation for simulation / Report writing	
	Thursday	3	Preperation for simulation / Report writing	
	Friday	3	Preperation for simulation / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
13	Monday		Easter	0
	Tuesday		Easter	
	Wednesday		Easter	
	Thursday		Easter	
	Friday		Easter	
	Saturday		Easter	
	Sunday		Easter	
Week	**Day**	**Hours**	**Details**	**Total**
14	Monday	6	Simulation setup	33
	Tuesday	8	Simulation setup	
	Wednesday	7	Simulation setup	
	Thursday	6	Simulation setup	
	Friday	6	Meeting with Buypass / Meeting with supervisor / Simulation setup	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday	7	Simulation work	

15	Tuesday	8	Simulation work	37
	Wednesday	7	Simulation work	
	Thursday	8	Simulation work	
	Friday	7	Meeting with Buypass / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
16	Monday	6	Simulation work/Report writing	34
	Tuesday	7	Simulation work/Report writing	
	Wednesday	7	Simulation work/Report writing	
	Thursday	8	Simulation work/Report writing	
	Friday	6	Meeting with Buypass / Meeting with supervisor / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
17	Monday	6	Simulation work / Report writing	21
	Tuesday	5	Simulation work / Report writing	
	Wednesday	4	Simulation work / Report writing	
	Thursday	6	Simulation work / Report writing	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
18	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting with Buypass / Meeting with supervisor / Report writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
19	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting with Buypass / Report writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
20	Monday	8	Report writing/Illustration production	57
	Tuesday	9	Report writing/Illustration production	
	Wednesday	9	Report writing/Illustration production	
	Thursday	9	Report writing/Illustration production	
	Friday		17. May	
	Saturday	11	Report writing / final touches	

	Sunday	11	Report writing / final touches	
Week	**Day**	**Hours**	**Details**	**Total**
21	Monday	12	Final touches / Delivery of project	12
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
			Total hours contributed to project:	**511**

Harald

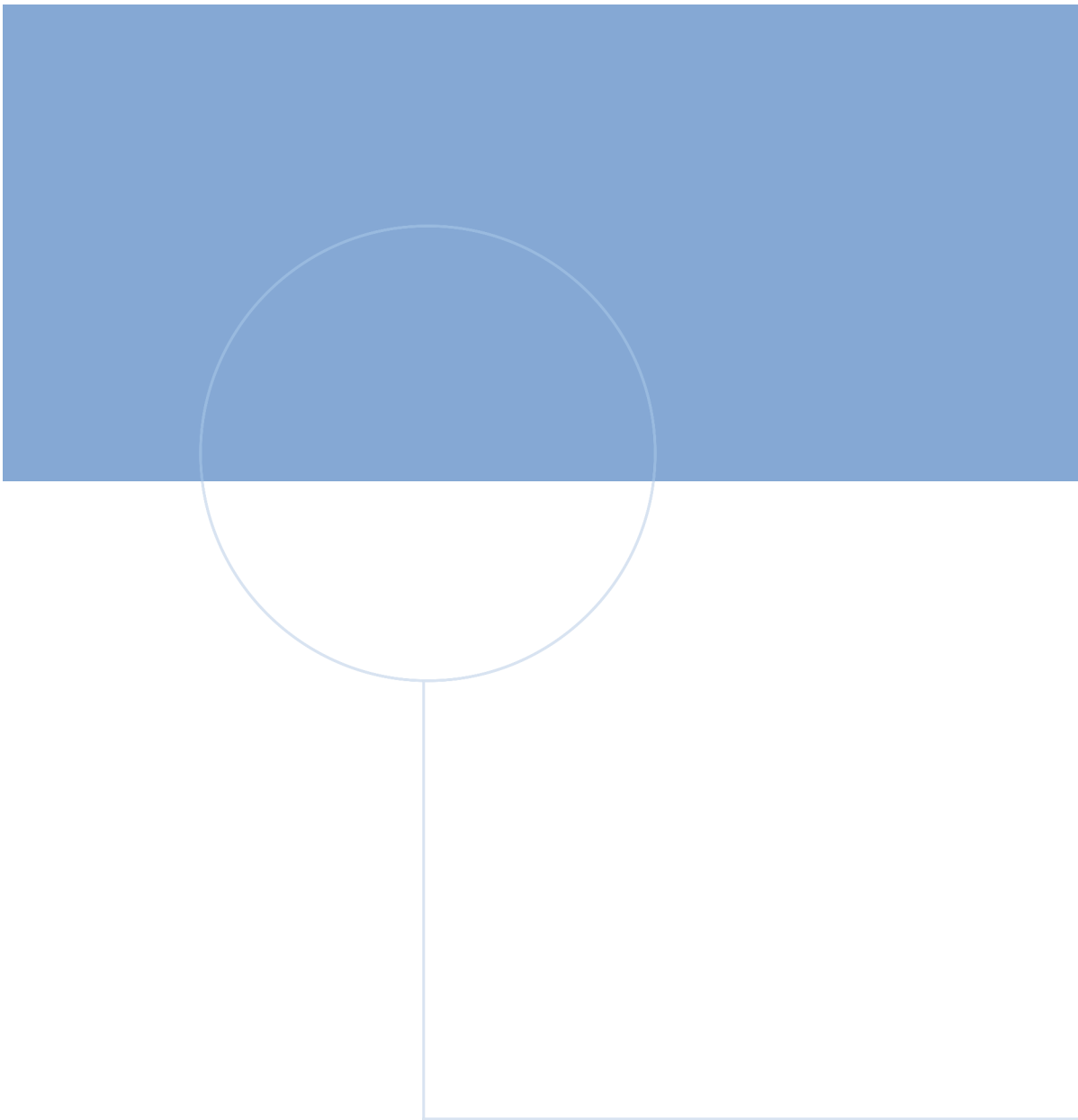
Week	Day	Hours	Details	Total
50	Monday			6
	Tuesday			
	Wednesday	1	Meeting with supervisor	
	Thursday	1	Preperations for meeting	
	Friday	1	Meeting with Buypass	
	Saturday	3	Research	
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
51	Monday	1	Research	2
	Tuesday	1	Research	
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
52	Monday			5
	Tuesday	2	Research	
	Wednesday			
	Thursday	3	Research	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
1	Monday			0
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
2	Monday			8
	Tuesday			
	Wednesday	4	Project plan	
	Thursday	4	Project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
3	Monday			7.5
	Tuesday			
	Wednesday	3.5	Meeting with supervisor/Project plan	
	Thursday	2	Project plan	
	Friday	2	Meeting with Buypass/Project plan	
	Saturday			

	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
4	Monday	2	Project plan / Standard agreement form	10
	Tuesday	3	Project plan	
	Wednesday	1	Project plan	
	Thursday	2	Project plan	
	Friday	2	Meeting with Buypass/Meeting with supervisor/ Standard agreement form	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
5	Monday	2	Project plan	14
	Tuesday	5	Project plan	
	Wednesday	6	Project plan / Standard agreement form	
	Thursday	1	Delivery of project plan	
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
6	Monday	2	Research	21
	Tuesday	3	Research	
	Wednesday	2	Research	
	Thursday	6	Report writing	
	Friday	8	Meeting with Buypass/Meeting with supervisor/Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
7	Monday	5	Report writing/Research	24
	Tuesday	4	Report writing/Research	
	Wednesday	3	Report writing/Research	
	Thursday	5	Report writing/Research	
	Friday	7	Report writing/Research	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
8	Monday	7	Report writing/Research	29
	Tuesday	5	Report writing/Research	
	Wednesday	8	Report writing/Research	
	Thursday	3	Report writing/Research	
	Friday	6	Meeting with Buypass/Meeting with supervisor/Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday			
	Tuesday	1	Meeting with supervisor	
	Wednesday			

9	Thursday			2
	Friday	1	Meeting with Buypass	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
10	Monday			33
	Tuesday			
	Wednesday	6	Report writing/Research	
	Thursday	7	Report writing/Research	
	Friday	8	Meeting with supervisor/Report writing/Research	
	Saturday	7	Report writing/Research	
	Sunday	5	Report writing/Research	
Week	**Day**	**Hours**	**Details**	**Total**
11	Monday			0
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
12	Monday	4	Preperation for simulation / Report writing	18
	Tuesday	3	Preperation for simulation / Report writing	
	Wednesday	5	Preperation for simulation / Report writing	
	Thursday	3	Preperation for simulation / Report writing	
	Friday	3	Preperation for simulation / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
13	Monday		Easter	0
	Tuesday		Easter	
	Wednesday		Easter	
	Thursday		Easter	
	Friday		Easter	
	Saturday		Easter	
	Sunday		Easter	
Week	**Day**	**Hours**	**Details**	**Total**
14	Monday	7	Simulation setup	32
	Tuesday	6	Simulation setup	
	Wednesday	6	Simulation setup	
	Thursday	6	Simulation setup	
	Friday	7	Meeting with Buypass / Meeting with supervisor / Simulation setup	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
	Monday	7	Simulation work	

15	Tuesday	8	Simulation work	36.5
	Wednesday	7	Simulation work	
	Thursday	7	Simulation work	
	Friday	7.5	Meeting with Buypass / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
16	Monday	5	Simulation work / Report writing	34
	Tuesday	7	Simulation work / Report writing	
	Wednesday	7	Simulation work / Report writing	
	Thursday	8	Simulation work / Report writing	
	Friday	7	Meeting with Buypass / Meeting with supervisor / Simulation work	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
17	Monday	8	Simulation work / Report writing / Presentation work	41
	Tuesday	8	Simulation work / Report writing / Presentation work	
	Wednesday	8	Simulation work / Report writing / Presentation work	
	Thursday	9	Simulation work / Report writing / Presentation work	
	Friday	8	Meeting with Buypass / Mock presentation for supervisor / Report writing	
	Saturday			
	Sunday			
Week	**Day**	**Hours**	**Details**	**Total**
18	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting with Buypass / Meeting with supervisor / Report writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
19	Monday	8	Report writing	56
	Tuesday	8	Report writing	
	Wednesday	8	Report writing	
	Thursday	8	Report writing	
	Friday	8	Meeting with Buypass / Report writing	
	Saturday	8	Report writing	
	Sunday	8	Report writing	
Week	**Day**	**Hours**	**Details**	**Total**
20	Monday	8	Report writing	56
	Tuesday	9	Report writing	
	Wednesday	8	Report writing	
	Thursday	9	Report writing	
	Friday		17. May	
	Saturday	11	Report writing / final touches	

	Sunday	11	Report writing / final touches	
Week	**Day**	**Hours**	**Details**	**Total**
21	Monday	12	Final touches / Delivery of project	12
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
	Sunday			
			Total hours contributed to project:	**503**



NTNU

Norwegian University of
Science and Technology