Remote validation of router attributes in Path-Aware Inter-domain networks

Rodrigo Bazo[1] <*r.bazo@utwente.nl*> and
Cristian Hesselman[1,2] <*cristian.hesselman@sidn.nl*>

[1] University of Twente
[2] SIDN Labs

Abstract. Trust requirements on the Internet are increasing. The adoption of online services by critical service providers and deployment of cyberphysical systems are some of the drivers behind that. In order to increase the trust in Inter-domain networks such as the Internet, some of it's limitations must be assessed. One of the most concerning limitations of the current Internet is it's black-box nature. For instance, users have no insight on how and who handles their data. The users must completely trust the network to send their data to the desired destination. This lack of transparency is a threat to the user's trust as the users cannot assess the network equipment security that their data travels through. Furthermore, there is no accountability on behalf of operators, which further keeps the user in the dark regarding where their data is travelling. In this research report, I detail and discuss my ongoing research status on building a Path-Aware solution for Inter-domain networks based on router attributes. Most specifically, I specify the problem which I am investigating and clarify the research goals, as well as discussing the current Research Questions which guide the work.

Keywords: Network Security · Network Transparency · Network Accountability · Path-Aware Networking

1 Introduction

The current Internet has inherent limitations and vulnerabilities due to the way it was originally designed [1, 5]. For instance, one limitation is that users have no knowledge nor control of the paths that their data follow on the internet and one vulnerability are known BGP hijacks which have been observed in the wild. Despite this, the Internet is a huge success and societies all over the globe depend on it for their correct functioning [3]. Societies' dependencies on the Internet will increase further as critical services such as energy grids and mobility services start building on the Internet as well.

2 Problem Statement

The problem I am addressing is the lack of accountability and transparency that the current Internet provides in terms of router attributes. For instance, Internet

users cannot check routers that they data traverses. Users such as critical service providers demand higher levels of trust from the Internet. For instance, these users may want to verify and control where their data travels before reaching it's destination. This is currently not possible to achieve, and is made even harder due to the black-boxed nature of the Internet [7].

One dimension of the problem space is vulnerable network equipment, which is a continuous worry from of users as they cannot remotely assess the security of equipment [8]. This is important because the Internet is a network of networks, so user data will be transported by multiple different network operators for the same communication session. Insecure network equipment is a realistic operational concern. For example, an equipment supplier of a large Dutch telecom operator might allegedly have monitored calls in the operator's network [6]. Also, there has been a long-standing debate around the alleged security weaknesses in 5G equipment and (physical) hacks of Internet routers [11]. Another example is that not all router operators update their firmware, which can lead to security vulnerabilities at the network level. Lastly, the black boxed nature of the Internet also applies to network operators, which provide no insight into their infrastructure. This also a challenge to overcome in order to offer a more trustful Internet.

Emerging critical services such as intelligent urban transport systems and smart energy grids require more insight into the properties of network operators (e.g., in terms of the security posture of their equipment) and more control over which network operators transport their data, thus going well beyond the traditional security paradigm that the Internet currently focus on (confidentiality, availability and integrity). This increased requirements arise from the nature of such systems, since they interact more closely with the real-world and many times are responsible for human lives [7].

Dealing with the problem of a black-box and unaccountable Internet is particularly hard since the Internet as a whole was not designed to contain these properties and revolutionizing the Internet is nearly impossible due to the magnitude and dependence of the society on it. Furthermore, some users may not even be aware that such functionalities are essential to the future Internet.

Achieving Path-Awareness [10] on Inter-domain networks is a milestone to be achieved in order to assess this problem, that is, adapt and expand the current Internet infrastructure to be able to know the path that packets follow. In order to achieve a path-aware network, transparency is a hard requirement. And with a Path-Aware network in place, higher levels of accountability can be achieved [4]. Several proposals for future Internet architectures (e.g. SCION [9] and NEBULA [2]) already embed Path-Awareness within their mechanics, however they cannot easily operate together with the current Internet, and function as alternative protocols for isolated networks.

3 Research Goals

The main goal of my work is: *Research solutions for enabling a scalable path-aware solution based router attributes on Inter-domain networks.*

The current work is part of a larger project called UPIN (User-driven Path Verification and Control on Inter-domain Networks). This project aims at investigating methods for enabling users to control and verify data paths in multi-domain scenarios, with the goal of increasing the trust for critical service providers to more safely operate in networks like the Internet through the concepts of Transparency, Accountabillity and Controllability. The project is being conducted jointly by the University of Amsterdam, responsible for researching mainly control mechanisms for Inter-domain networks (Controllability), and by the University of Twente, responsible for responsible for researching verification mechanisms (Transparency and Accountability), which is the focus of the present work.

4 Research Question 1: What are the barriers towards expanding the Internet with Path-Awareness based on router attributes?

This is the overarching question of this research. This question is major to the work and originates the other research questions as well. Answering it is important because thoroughly investigating and understanding existing barriers is crucial in order understand how to design a Path-Aware extension to the current Internet. The **approach** I will take to answer this question is by conducting literature reviews, surveys with potential users and through experimentation and results analysis. Further research questions are intrinsically tied to this question as their answers also provide answers to this one.

5 Research Question 2: What is the grain of Transparency needed in order to achieve Path-Awareness based on router attributes in Inter-domain networks?

This is an essential question to answer. Transparency of network equipment is a hard requirement in order to achieve the goal of my work. However, this is a hard task to overcome because network providers may not want to share insights on their equipment. For instance, operators may not want to provide insights about their routers and firmware versions as this would be a security breach. On the other hand, transparency of network equipment safety is of interest of both operators and users. So it is essential to understand how much transparency is too much or too few. The **approach** to answer this question will be through literature reviews, surveys with industry related personnel and by investigating and designing means for domains and operators to share this kind of data

without compromising their security. By answering this question I intend to obtain important information regarding transparency which is needed in order to design, implement and experiment with Path-Aware solution.

6 Research Question 3: What are existing technologies that enable Path-Awareness and Transparency in Inter-domain networks and how can they solve our problem?

This question is important to answer because I need to understand which technologies already exist that try to solve similar problems, and how well they operate. The **approach** for answering this question will be reviewing the literature for existing technologies and techniques, followed by experimenting with these technologies, making necessary adaptations and collecting measurements and results. The output to this question are designs and evaluations of developed Path-Aware solutions for Inter-domain networks, using information collected in Research Question 2 and further polishing the answer to that question as well.

7 Research Question 4: Who would benefit from a Path-Aware Internet and what are their requirements?

Lastly but not least, understanding who would benefit from our goals is crucial in two ways: (i) reach out to users that may not be aware that they need such functions from the network and clarify the necessity of these properties to them; (ii) harvest requirements from users in order to understand how transparency and accountability can be used to fulfill their requirements. For answering this question the approach I'll use is to review existing literature of existing critical service providers network security requirements and conducting surveys with researchers from critical services areas and industry partners which work in related critical fields.

8 Research Status and Future Works

We already achieved a group of milestones to the current date. First and foremost, a first version of the proposed architecture was already developed and documented in the form of an article. This article was submitted to a workshop on Technologies, Applications, and Uses of a Responsible Internet (TAURIN) at SIGCOMM 2021. The article contains a review on existing technologies that assist in achieving the goals described in this paper. The first version of the architecture was created based on this review of existing technologies and analysis of a use-case of a critical service provider. We also submitted and had approved an extended abstract and poster to ICT.OPEN 2021, working towards spreading the idea of the research, collaborate and collect feedback.

A group of milestones are already envisioned for the near-future. Initial experimentation with the existing technologies reviewed in the TAURIN article will be conducted and familiarization with the project's testbed is the first next step. In the following months, surveys and literature reviews with partners will be conducted in order to extract requirements and prospect more potential users for the work. These new results will then be documented and written as an article to be submitted to a conference yet to be defined.

References

1. Anderson, T., Peterson, L., Shenker, S., Turner, J.: Overcoming the internet impasse through virtualization. Computer **38**(4), 34–41 (2005). https://doi.org/10.1109/MC.2005.136
2. Anderson, T., Birman, K., Broberg, R., Caesar, M., Comer, D., Cotton, C., Freedman, M.J., Haeberlen, A., Ives, Z.G., Krishnamurthy, A., et al.: The nebula future internet architecture. In: The Future Internet Assembly. pp. 16–26. Springer (2013)
3. Bisogni, F., Cavallini, S., Franchina, L., Saja, G.: The european perspective of telecommunications as a critical infrastructure. In: International Conference on Critical Infrastructure Protection. pp. 3–15. Springer (2012)
4. Bu, K., Laird, A., Yang, Y., Cheng, L., Luo, J., Li, Y., Ren, K.: Unveiling the mystery of internet packet forwarding: A survey of network path validation. ACM Computing Surveys (CSUR) **53**(5), 1–34 (2020)
5. Chowdhury, N.M.K., Boutaba, R.: A survey of network virtualization. Computer Networks **54**(5), 862–876 (2010)
6. Guardian, T.: Huawei 'may have eavesdropped on dutch mobile network's calls', https://www.theguardian.com/technology/2021/apr/19/huawei-may-have-eavesdropped-on-dutch-mobile-networks-calls, Published in: April 2021, Accessed in: May 2021
7. Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J.H., Jonker, M., de Ruiter, J., Sperotto, A., van Rijswijk-Deij, R., Moura, G.C.M., Pras, A., de Laat, C.: A responsible internet to increase trust in the digital world. Journal of Network and Systems Management **28**(4), 882–922 (2020), https://doi.org/10.1007/s10922-020-09564-7
8. Labs, S.: Analysing vulnerabilities in the network infrastructure, https://www.sidnlabs.nl/en/news-and-blogs/analysing-vulnerabilities-in-the-network-infrastructure, Published in: November 2020, Accessed in: July 2021
9. Perrig, A., Szalachowski, P., Reischuk, R.M., Chuat, L.: SCION: a secure Internet architecture. Springer (2017)
10. Scherrer, S., Legner, M., Perrig, A., Schmid, S.: Enabling novel interconnection agreements with path-aware networking architectures. arXiv preprint arXiv:2104.02346 (2021)
11. Times, N.Y.: E.u. recommends limiting, but not banning, huawei in 5g rollout, https://www.nytimes.com/2020/01/29/world/europe/eu-huawei-5g.html, Published in: January 2020, Accessed in: May 2021