Increasing the Transparency, Accountability and Controllability of multi-domain networks with the UPIN framework

Rodrigo Bazo
University of Twente

Leonardo Boldrini
University of Amsterdam

Cristian Hesselman
SIDN Labs and University of Twente

Paola Grosso
University of Amsterdam

ABSTRACT

Demands for a more trustworthy Internet are constantly increasing, in particular to support emerging critical services such as intelligent urban transport systems and smart energy grids. Such cyber-physical systems 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 which the Internet security community currently focuses on (confidentiality, availability, and integrity). In this work-in-progress paper we propose the UPIN framework, which aims to fulfill these new trust requirements. The framework advances the state-of-the-art by defining components needed to incorporate transparency, accountability, and controllability into the Internet or other types of inter-domain networks. The framework is based on our analysis of a smart grid use case to understand the specific needs of critical service providers and a literature study on existing technologies. We also discuss our ongoing work, and the demands and challenges of implementing and deploying the UPIN framework.

1 INTRODUCTION

Communications services are increasingly a strategic asset in modern societies [4], they form the foundation for emerging safety-critical services such as smart energy grids, remote controlled robots, and intelligent urban transport systems. To deploy these kinds of services on a large scale, critical service providers and other users need to build on a multi-domain network that can provide significantly higher levels of confidence and trust than today's Internet. One way to accomplish this is through the Responsible Internet [14]. This new Internet security paradigm aims to provide users with more control over the network, both in terms of metadata about the network's structure and operation as well as how the network transports their data.

However, the current Internet infrastructure has inherent problems and limitations when it comes to transparency and control over routing of data. Primarily these limitations stem from the way the Internet was originally designed [3, 8].

TAURIN'21, August23, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8639-5/21/08.
https://doi.org/10.1145/3472951.3473506

In the course of the years significant research has been spent on overcoming these problems, mostly with revolutionary and evolutionary approaches. To the former belong solutions that require complete redesign of the network architecture (e.g. RINA [16]). For the latter, we can think of efforts that propose changes that more easily integrate with the current infrastructure (e.g. SCION [18]). The downside of revolutionary approaches is that they require huge revamp of the Internet architecture. In a realistic scenario this is nearly unfeasible to achieve due to the dependance of societies all over the world in the Internet. At the same time, we observe that critical service providers have a real demand for new Internet security capabilities. This is because they increasingly depend on the Internet as as a communications substrate to deliver their services, thus calling for new solutions that are feasible.

In this work-in-progress paper, we present UPIN (User-driven Path verification and control in Inter-domain Networks), an Internet framework that supports definition of network behaviour from its users. In UPIN, the user becomes the real driver of how the communication takes place. User requirements can vary from simple Key Performance Indicators (KPIs) to specific functions such as firewalling services, up to more advanced scenarios like avoiding particular regions or jurisdictions.

A key element to achieve our goals is the use of programmable networks such as based on P4 devices or network mechanisms such as Segment Routing. These technologies offer us the technical handles to steer traffic more flexibly and provide richer insights into network behaviour (control and verifiability functionalities respectively).

2 NEW INTERNET SECURITY REQUIREMENTS

Future Internet applications require higher levels of trust from the Internet infrastructure. In this section, we illustrate these demands using a smart energy grid and discuss two key security requirements that such applications introduce for the network. We expect that other cyberphysical systems (e.g., remote surgery robots and urban traffic management systems) will have similar requirements.

2.1 Smart Grid Example

Figure 1 shows a smart grid application which "integrates information and communication technologies with the power-delivery infrastructure, enabling two-way energy and communications flow" [17]. The smart grid operator in this example communicates with remote substations over the Internet, for instance to open or close power switches or to increase or lower voltage levels [9, 17]. The

Internet infrastructure in Figure 1 consists of six Autonomous Systems (ASs), A, B, C, D, and E. A is an AS managed by the grid operator, while B through E are managed by third parties. E is a wireless access network, for instance based on 5G. In reality, the Internet consists of over 70,000 ASs.

An example of a security requirement is the integrity of the energy distribution system, which is important for "avoiding outages and providing power to customers reliably and efficiently" [17]. The communications network plays a crucial role to meet those requirement because a compromised network can impact the availability of the grid, which should typically be at 99.9999%[9]. The network may for instance cause outages in the energy grid if malicious code in the network equipment of the third-party ASs (B through E) can drop, copy, reroute or modify traffic.

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 [13]. Also, there has been a long-standing debate around the alleged security weaknesses in 5G equipment [21] and (physical) hacks of Internet routers [23]. Another example is that not all router operators update their firmware, which can lead to security vulnerabilities at the network level [15].

The security of network equipment is particularly important in emerging decentralized energy grids, because the grid operator will likely need to use a multi-domain network to remotely manage a range of of geographically dispersed energy sources (e.g., windmill parks and solar farms) [9]. As a result, the grid operator will not know all AS's that transport its data. In Figure 1 the grid operator will have a contract with networks B and E since it connects to them directly, but it will likely not know intermediate ones (C and D) because it doesn't see the full path and will therefore have limited insight in the security posture of these intermediate operators. In addition, the set of intermediate ASs may change dynamically, for instance because of changing peering relations [6].

The alternative is that the grid operator runs its own communications network where it is in control of the equipment it puts in the network, but this will likely become economically infeasible because of increasing size and decentralized nature of energy grids.

2.2 Network Security Requirements

Based on the example of the smart energy grid, we observe two major requirements for a future network to support such critical infrastructures, which are in line with the concept of the Responsible Internet [14].

The first is that relying parties such as the grid operator will need more transparency and accountability from the network. This is particularly relevant in multi-domain scenarios when the relying party might not know the entire chain of network operators. For example, the grid operator in Figure 1 might want to know want to know if ASs B through E use routers that have been patched with the latest security updates [15], if the source code of the routers have backdoors or other vulnerabilities and if the routers are in a datacenter in a particular region).

The second requirement is that relying parties need more control over how the network transports their data and that it complies with their trust requirements. For example, the grid operator must be able to instruct the Internet that its traffic can only be transported by networks that run fully patched routers and went through a verifiable cybersecurity certification process (networks B, C, and D), for instance based on a scheme similar the EU's cybersecurity certification for 5G equipment [11]. This is currently not possible, because the Internet's routing system autonomously decides which network operators will handle the grid operator's instructions based on, e.g., the lowest number of network hops.

3 EXISTING TECHNOLOGIES

Deployed and experimental inter-domain networks and technologies only partly address the new security requirements of Section 2.2. We do see the need for a new design that explores existing technologies to fully satisfy the observed requirements on transparency, accountability and controllability on inter-domain networks. Using these three properties as key basis for the investigation, we harvest a handful of solutions through a literature review.

3.1 Cross-domain Transparency and Accountability

There are existing solutions that provide verifiable metadata about inter-domain networks, but to the best of our knowledge there is no overall framework that: (i) considers these properties in a network technology agnostic way; (ii) provides a generic metadata model that not only includes transparency of data paths but also of network equipment, domains and network management operations [14].

An example of an existing technology is SCION [18], which provides transparency and accountability of data paths in inter-domain networks based on the SCION protocol suite. It does however not fully meet our requirements because it does not consider the security attributes of network equipment and domains, which is what users like the energy grid operator in Figure 1 need to assess.

Another existing technology is remote attestation [1], which enables a verifier (e.g., the grid operator) to assess the trustworthiness of providers (e.g., AS B). In Figure 1, this would for instance involve AS B sending the grid operator a verifyable statement that it has patched all its routers, including a hardware-signed sequence of update operations to prove it, one per router. Another example is that the routers prove that they are in a certain geolocation by including their coordinates, signed by the root certificate of the country or region. Remote attestation is an active area of research, for instance in the Internet Engineering Task Force (IETF). However, to the best of our knowledge it has not been applied to make inter-domain networks more transparent and accountable.

Another existing technology are Programmable Data Planes (PDPs), for instance based on P4 [5]. They allow for custom packet processing and obtaining fine grained state information from routers and the forwarding path (e.g., routers traversed [12] or domains traversed [18]). We intend to use technologies like P4 to selectively include data plane measurements in the metadata of network equipment and domains.

Besides obtaining the metadata, users like the grid operator also need a way to automatically process it. We intend to leverage existing description languages for this purpose (e.g., the Network Description Language [22]) and extend them where needed.

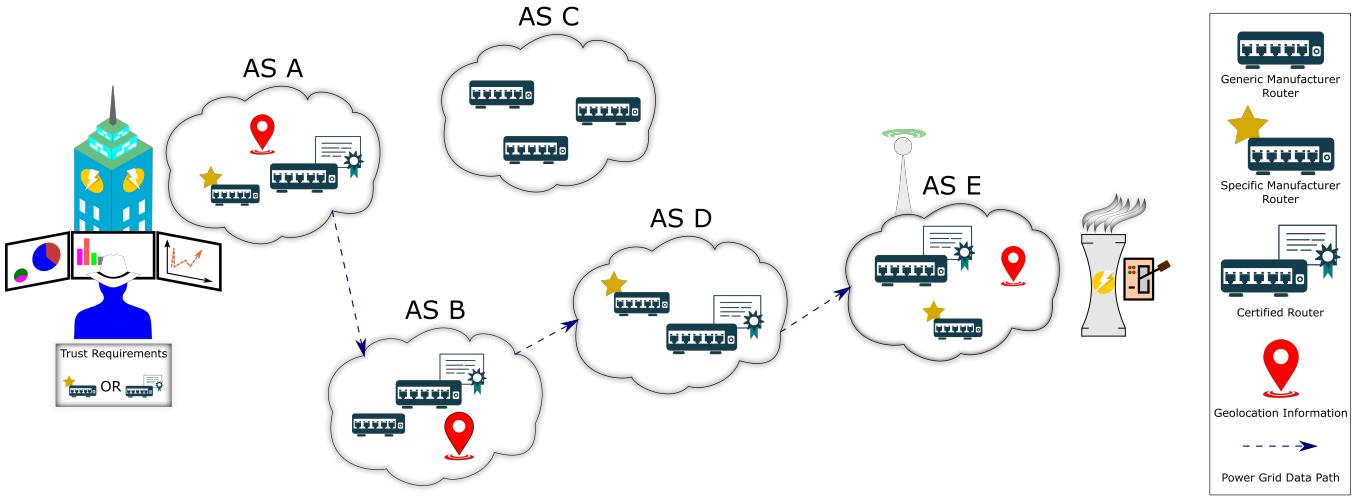

Figure 1: An Internet composed of five Autonomous Systems with specific properties each. A Power Grid operator manages A and wants to flip a switch at E, the data follows paths that satisfy the Power Grid's trust requirements.

3.2 Cross-domain Controllability

Path-Aware Networking (PAN) enables end-hosts to select the path they want for their data to follow at the level of ASs [20]. This functionality has been actively investigated and discussed under the Internet Research Task Force (IRTF) and the IETF in the last years [7]. PAN is already considered indispensable for constructing a secure Internet architecture and is implemented in several experimental Internet designs, such as SCION and NEBULA [2]. A PAN consists of two essential properties, namely Path Enforcement and Path Verification [7]. Path Enforcement consists of enforcing that selected path preferences are followed and Path Verification adds the capability of retrieving the paths taken by network packets for auditing. Path Enforcement can be achieved with the current Internet protocol suite, for instance using Segment Routing (SR) [10] and Multiprotocol Label Switching (MPLS) networks. Path Verification on the other hand, currently cannot be easily achieved without changing the packet processing logic of routers [7] or without any sort of tracing capabilities.

3.3 Summary of Findings

Table 1 summarizes our findings. For each one of the technologies we reviewed, we list their suitability to address each one of our requirements.

Table 1: Technologies and their capabilities for the observed Inter-domain requiremets.

Solution	Transparency	Accountability	Controllability
PDP	✓	✓	*x*
SR	*x*	*x*	✓
PAN	x	✓	✓

Through our survey we observe that there is not a single technology that satisfies all of our three requirements for inter-domain networks at the same time. This affirms our idea that a new design that combines aspects from these technologies is needed in order to achieve our requirements.

4 UPIN FRAMEWORK

The UPIN framework consists of a set of functions and components that, when coupled together, enable inter-domain networks to fullfill our requirements of transparency, accountability and controllability. Table 2 provides an overview of the key UPIN components.

Table 2: UPIN components and the requirements they fullfill.

Component	Transparency	Accountability	Controllability
Domain Explorer	✓	✓	✓
Path Controller	*x*	*x*	✓
Path Tracer	✓	✓	*x*
Path Verifier	✓	✓	*x*
Frontend	✓	✓	✓

4.1 UPIN-enabled domains

The core concept of the UPIN architecture is that of a UPIN enabled domain, which implements the UPIN components: Domain Explorer, Path Controller and Path Tracer, Path Verifier and Frontend.

The UPIN framework does not mandate the underlying data plane technology that is used in each domain. For example, one domain might support Segment Routing while another supports SCION. This means that the level of control and verifiability may differentiate between domains along the path. Furthermore, UPIN enabled domains can seamlessly coexist with non-UPIN domains; in this case UPIN operations can only be performed across UPIN-enabled domains and not across all domains along the whole path.

Figure 2 shows an example of a network composed of two UPIN-enabled domains. In this case the data flows from A in Domain 1 to

B in Domain 2. Messages in the data plane from A to B follow solid black lines, while messages issued by the UPIN components in the control plane follow the red dashed lines.

4.2 Domain Explorer

The Domain Explorer is responsible for obtaining and storing meta-data about the security, administrative and environmental properties of a domain's equipment and keeping that data updated. Examples of domain metadata include: source code of routers, composition of routers, router patching state and geographical characteristics such as a router's GPS location.

The Domain Explorer has a local view on its domain, which consists of deep and detailed knowledge on the domain and its nodes. Other domains can request metadata about a domain via the domain's Frontend, for instance to support inter-domain data transfer. For instance, this would be the case in Figure 2, where the Frontend in Domain 1 requests metadata about domain 2 through the latter's Frontend which interfaces with the Domain Explorer. The Domain Explorer also applies policies as to what metadata about the domain it wants to share with other domains. The domain operator defines these policies.

4.3 Path Controller

The Path Controller sets forwarding rules based on the user's preferences and sends them to routers present in the domain. For example, if the user in Figure 2 specifies that its traffic must avoid unpatched routers, the Path Controller steers the data accordingly. Likewise, if the user request has constraints on end-to-end latency or throughput, the Path Controller will setup the network accordingly.

The Path Controller component has a local scope, which means that it does not control the nodes belonging to other domains. The instructions that are sent to the nodes are dependent on the technology that the nodes use (e.g., Segment Routing).

4.4 Path Tracer

The Path Tracer gathers real-time measurements on the traffic in the data plane and stores traces and any information that could be useful for verification purposes, such as source and destination. Also in this case, tracers are technology independent, so a specific implementation of this component per domain is not necessary, but only tools that analyze it.

4.5 Path Verifier

The Path Verifier checks if the intent of the user is respected. To perform this verification task it uses the original request of the user and the traces gathered by the Path Tracer. The main challenge for this component is to determine the extent to which the properties of the actual data path meet the user's original request. The result of the verification procedure may not give an absolute certainty, for instance when the traces are incomplete or the transfer has passed through non-UPIN enabled domains.

The Path Verifier has a different verification grains which are defined by the user. They can range from hop-by-hop verification or for instance on a domain-by-domain. All it's components run locally in their own domain. In the domain where the user initiated the request, it will also need to put together the results of the local verification happening in other domains. This guarantees that we can perform an end-to-end compliance check.

4.6 Frontend

The Frontend is the means of communication between the user and a UPIN-enabled domain. Through the Frontend the user is able to configure desired settings (such as the geolocation of routers that their data must be routed through). Initially, the user sets up destinations and the system calculates available routes with the properties available for that route using meta-data obtained from the Domain Explorer. This way the user is able to clearly see if their trust requirements can be met for that destination. Furthermore, the user can configure behaviours in case that the configurations that are in place cannot be achieved anymore (e.g. due to changes in domains in the route).

Figure 2 illustrates that UPIN distinguishes two different types of network users: a user that actually sends the data (source A in Figure 2) and a user that formulates the trust requirements through the Frontend (e.g., a network administrator).

4.7 System Behaviour

Once a request for data transfer is issued by the user, the Path Controller and the Path Tracer components will guarantee the transfer occurs according to the request; the Path Verifier component will check if the intent of the user is respected. Via the Frontend the user also receives a confirmation from the Path Verifier if his intention was respected.

5 INITIAL EXPERIMENTS

We ran some initial experiments to demonstrate the feasibility of our framework in a simple single-domain setting. We chose to focus on the Path Control component and in particular we were interested in showing that we can give users the choice of functionalities that are applied to their traffic. We created two Virtual Network Functions (VNF), namely a firewall and a packet mirror, running on hosts in the networks.

In these initial experiments we made use of Segment Routing as UPINs underlying technology to steer the traffic to these specific network elements. The network topology used for this proof of concept consists of: a client that acts as a traffic generator and plays the role of the UPIN user; an SR-capable core, i.e. a set of routers and hosts belonging to the same domain where traffic goes through and where our steering actions take place; a server that acts as a receiver. We also have an SDN controller; this has the double purpose of (i) gathering the topology of the SR-capable domain from the Southbound Interface; (ii) receive instructions from an external machine through the Northbound Interface, in order to send the correct instructions to the SR capable core. More information on this network can be found in [19].

Our experiments showed that we can indeed steer traffic through the VNFs that we had loaded in the SR capable core; we also showed that it is possible to move the VNFs within the UPIN SR capable core without packet loss or performance degradation perceived from the client, except for a small change in latency. Finally, we also demonstrated that we can chain VNF functions and allow the

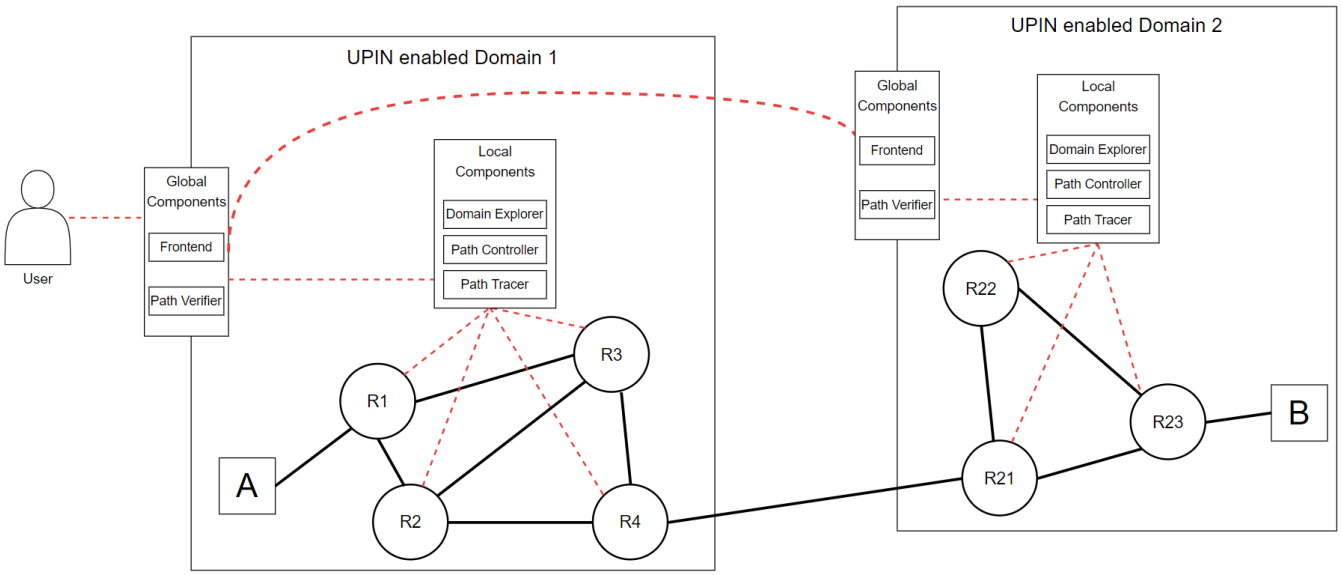

Figure 2: UPIN architecture across 2 domains. Black lines indicate links in the data plane, red lines in the control plane.

user to select and traverse them, a core functionality for the UPIN framework.

6 FINAL REMARKS

The Internet as we know today presents intrinsic risks when it comes to security of data in transit as users have limited insight in and control over how their data is being transported across on how their traffic is being transported across domains, which is a particular risk for the integrity of critical services such as smart energy grids or intelligent urban transport systems.

The Responsible Internet will help addressing this problem, but we showed that there is a technical gap that network operators need to close to make the Internet's network infrastructure more transparent, accountable and controllable. To accomplish this, network operators will need to share metadata about the security of their infrastructure, such as with users and other operators. This is a critical point that we will research in the future as we must evaluate how and how much information operators may want to share with third parties, as well as why would they do it. Investigation of the benefits of our proposal, both financial and operational, will also be conducted.

We propose the UPIN framework to organize required network functions in inter-domain networks, some of which can be implemented using existing technologies such as Segment Routing. We also discussed our initial experiments with one of the UPIN components (Path Controller) in a single-domain scenario. Our future experiments will focus on multi-domain scenarios, where we make use of different technologies, e.g. Segment Routing on one domain and P4 hardware on another domain. We intend also to evaluate the use of SCION as a mean of communication across domains. We will develop an initial version of a router that implements the UPIN framework using P4 and deploy and test it in the 2STiC testbed [12]. The 2STiC testbed is a national multi-domain setup of P4-programmable routers interconnected in a star-shaped network, deployed across six sites in Netherlands and interconnected by SURF's optical network.

The main research areas that we will explore further are translation of a user's request into network behaviour, standardization in communication across domains, interoperability between different technologies (i.e. routing mechanisms) present in different domains, trust assessment and evaluation. Lastly, attestation and verification of information provided by other domains is also a point of interest for future works.

ACKNOWLEDGEMENTS

This research received funding from the Dutch Research Council (NWO) under the project UPIN.

REFERENCES

[1] Tigist Abera, N Asokan, Lucas Davi, Farinaz Koushanfar, Andrew Paverd, Ahmad-Reza Sadeghi, and Gene Tsudik. 2016. Things, trouble, trust: on building trust in IoT systems. In *Proceedings of the 53rd Annual Design Automation Conference*. 1–6.

[2] Tom Anderson, Ken Birman, Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael J Freedman, Andreas Haeberlen, Zachary G Ives, Arvind Krishnamurthy, et al. 2014. A brief overview of the NEBULA future internet architecture. *ACM SIGCOMM Computer Communication Review* 44, 3 (2014), 81–86.

[3] Thomas Anderson, Larry Peterson, Scott Shenker, and Jonathan Turner. 2005. Overcoming the Internet impasse through virtualization. *Computer* 38, 4 (2005), 34–41.

[4] Fabio Bisogni, Simona Cavallini, Luisa Franchina, and Giovanni Saja. 2012. The European perspective of telecommunications as a critical infrastructure. In *International Conference on Critical Infrastructure Protection*. Springer, 3–15.

[5] Pat Bosshart, Dan Daly, Glen Gibb, Martin Izzard, Nick McKeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese, et al. 2014. P4: Programming protocol-independent packet processors. *ACM SIGCOMM Computer Communication Review* 44, 3 (2014), 87–95.

[6] Timm Böttger, Felix Cuadrado, and Steve Uhlig. 2018. Looking for hypergiants in peeringDB. *ACM SIGCOMM Computer Communication Review* 48, 3 (2018), 13–19.

[7] Kai Bu, Avery Laird, Yutian Yang, Linfeng Cheng, Jiaqing Luo, Yingjiu Li, and Kui Ren. 2020. Unveiling the Mystery of Internet Packet Forwarding: A Survey

of Network Path Validation. *ACM Computing Surveys (CSUR)* 53, 5 (2020), 1–34.

[8] NM Mosharaf Kabir Chowdhury and Raouf Boutaba. 2010. A survey of network virtualization. *Computer Networks* 54, 5 (2010), 862–876.

[9] Justyna Joanna Chromik. 2019. Process-aware SCADA traffic monitoring: A local approach. (2019).

[10] Clarence Filsfils, Nagendra Kumar Nainar, Carlos Pignataro, Juan Camilo Cardona, and Pierre Francois. 2015. The segment routing architecture. In *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.

[11] European Union Agency for Cybersecurity. [n. d.]. Securing EU's Vision on 5G: Cybersecurity Certification. ([n. d.]). https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification, Publish in: Feburary 2021, Accessed in: May 2021.

[12] Paola Grosso, Cristian Hesselman, Luuk Hendriks, Joseph Hill, Stavros Konstantras, Ronald van der Pol, Victor Reijs, Joeri de Ruiter, and Caspar Schutijser. 2021. A national programmable infrastructure to experiment with next-generation networks. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM2021)*. Accepted.

[13] The Guardian. [n. d.]. Huawei 'may have eavesdropped on Dutch mobile network's calls'. ([n. d.]). 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.

[14] Cristian Hesselman, Paola Grosso, Ralph Holz, Fernando Kuipers, Janet Hui Xue, Mattijs Jonker, Joeri de Ruiter, Anna Sperotto, Roland van Rijswijk-Deij, Giovane C. M. Moura, Aiko Pras, and Cees de Laat. 2020. A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management* 28, 4 (2020), 882–922. https://doi.org/10.1007/s10922-020-09564-7

[15] SIDN Labs. [n. d.]. Analysing vulnerabilities in the network infrastructure. ([n. d.]). https://www.sidnlabs.nl/en/news-and-blogs/analysing-vulnerabilities-in-the-network-infrastructure, Published in: November 2020, Accessed in: May 2021.

[16] Vincenzo Maffione, Francesco Salvestrini, Eduard Grasa, Leonardo Bergesio, and Miquel Tarzan. 2016. A software development kit to exploit RINA programmability. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, 1–7.

[17] National Institute of Standards and Technology. [n. d.]. Guidelines for Smart Grid Cybersecurity. ([n. d.]). https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final (Appendix E, use-case 24), Published in: September 2014, Accessed in: May 2021.

[18] Adrian Perrig, Pawel Szalachowski, Raphael M Reischuk, and Laurent Chuat. 2017. *SCION: a secure Internet architecture*. Springer.

[19] Cees Portegies, Marijke Kaat, and Paola Grosso. 2021. Supporting VNF chains: an implementation using Segment Routing and PCEP. In *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 1–5.

[20] Simon Scherrer, Markus Legner, Adrian Perrig, and Stefan Schmid. 2021. Enabling Novel Interconnection Agreements with Path-Aware Networking Architectures. *arXiv preprint arXiv:2104.02346* (2021).

[21] New York Times. [n. d.]. E.U. Recommends Limiting, but Not Banning, Huawei in 5G Rollout. ([n. d.]). https://www.nytimes.com/2020/01/29/world/europe/eu-huawei-5g.html, Published in: January 2020, Accessed in: May 2021.

[22] Jeroen Van der Ham, Paola Grosso, Ronald Van der Pol, Andree Toonk, and Cees De Laat. 2007. Using the network description language in optical networks. In *2007 10th IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 199–205.

[23] Wired. [n. d.]. NSA Laughs at PCs, Prefers Hacking Routers and Switches. ([n. d.]). https://www.wired.com/2013/09/nsa-router-hacking/, Acessed in: May 2021.