

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

The Ivory Tower Syndrome: Operators' Reflections on Academic BGP Security Solutions

Aleeza Suhel Inamdar, *Saarland University;* Tobias Fiebig, *TU Wien;*
Mannat Kaur, *Max-Planck-Institut für Informatik*

https://www.usenix.org/conference/usenixsecurity26/presentation/inamdar

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

The Ivory Tower Syndrome: Operators' Reflections on Academic BGP Security Solutions

Aleeza Suhel Inamdar
Saarland University

Tobias Fiebig
TU Wien

Mannat Kaur
Max-Planck-Institut für Informatik

Abstract

The Border Gateway Protocol (BGP) is the backbone of Internet routing, primarily used for exchanging network reachability information between autonomous systems on the Internet. BGP leverages a trust-based framework, where networks rely on each other's routing information implicitly. However, the initial design of BGP lacks in-built security mechanisms, thus making it vulnerable to various attacks and possibly network failures. Over the years, academics have introduced several solutions to enhance BGP security and address these vulnerabilities such as Resource Public Key Infrastructure (RPKI), Secure Border Gateway Protocol, and BGPsec. However, academic solutions may not always be readily applied by network operators. It is, therefore, important to understand the existing challenges in the transition from academic research to widespread implementation. We engaged with 12 network operators via online focus groups, focusing on their work experiences in implementing various BGP security mechanisms. All participants noted a gap between academic research and industry needs, indicating misaligned priorities. To bridge this gap, they suggested more collaboration between the two domains – particularly through increased researcher involvement in the network operators' community. We propose ways to foster such collaboration and urge the research community to reflect on the purpose behind publishing.

1 Introduction

Our increasing trust and dependence on the Internet for communication, financial transactions, and vital infrastructure has led to a rise in the complexity and prevalence of digital threats in today's globalized world. New attack surfaces constantly appear as digital transformation accelerates. With the use of innovative techniques such as supply chain attacks and zero-day exploits, adversaries have become more sophisticated.

Over the past decade, attacks on the core routing infrastructure of the Internet have become more prevalent, usually as an 'end-to-a-means'. For example, we have witnessed attackers rerouting packets to attack 'crypto' currency exchanges [3] and other payment services [101]. Similarly, governments use rerouting of Internet traffic for various forms of censorship [11], which sometimes lead to global effects. Such attacks on routing infrastructure are usually enabled by the limited security guarantees which BGP (Border Gateway Protocol), the protocol used to exchange routing information between independent networks, each being an AS (Autonomous System), has by design [95]. Being a protocol from the times of the 'early Internet', BGP essentially works based on trust between operators [39]. Even today, security is mostly rooted in operators applying filters regarding the network paths they accept from ASes to which they are directly connected [33].

With the increasingly apparent threat that arises from insufficient route-origin-validation (ROV), i.e., ensuring that a network path one receives from neighbors is actually *authorized*, technology has been developed to provide more integrity and especially authorization for routes. Given the critical role of BGP in Internet routing, proposals to move beyond unsigned filters [33] and towards cryptographically signed authoritative sources of truth for route and path authorization have been proposed and implemented. The most prevalent by now is certainly the Resource Public Key Infrastructure (RPKI) [69], a repository enabling ROV by publishing route-origin-authorization (ROA) objects, and in the future AS Provider Authorization (ASPA) [5]. In contrast, e.g., BGPsec [70], has seen limited deployment. Nevertheless, all three together are necessary to ensure full path integrity.

With the high-stakes involved in routing security, the topic also gathered interest from the academic community. In parallel to the afore mentioned technologies, work in academia investigates options for attacking BGP [10, 82, 106], measuring the prevalence of attacks like prefix hijacks [52, 81, 88], and deployment of security technologies like RPKI ROV [24, 43, 63, 74, 96]. Additionally, there has been an abundance of proposed mitigations [83, 98, 111].

However, while proposals like 'secure BGP' (S-BGP) [61] have been around for decades, solutions proposed in academia often see limited adoption and recognition from the indus-

try. In fact, anecdotally, operators are often frustrated with academic contributions [35], especially in the area of BGP security. This begs the serious question whether academic BGP security work as a whole goes into the right direction, or, produces encapsulated output for an academic circle alone–despite usually claiming direct practical impact.

Contributions: With this paper, we examine this question by conducting focus group discussions to gather operators' perspectives on academic BGP security work. Specifically, we make the following contributions:

- Using a qualitative methodology, we identify a gap between academic work on BGP security and industry perspectives, limiting academic work's applicability and practical relevance.
- We explore network operators' perspectives on this gap and present their suggestions for bringing academia and industry closer together in the context of BGP operations.
- We trace the impracticality of academic BGP solutions to the fast-paced and often elitist academic culture.
- We discuss how this gap further connects to an insufficient influx of young network engineers, highlighting the looming challenge for Internet operations in the near future as the previous generation of operators retires.
- In human-centered security, expert users remain understudied, with prior work focusing mainly on their views on technical systems and workplaces. By examining operators' perspectives on academic work, we highlight another factor to consider when creating systems and solutions for those who are expected to use them.

2 Background

Here we introduce definitions, provide a *very* high-level overview of how BGP, in essence, works, and introduce several BGP security technologies from academia and industry.

Operator: 'Operator' refers to system and network administrators - those who manage *"computers, networks, and the people who use them"* [76]. They are responsible for running and expanding all systems [59]. This entails installing and configuring new hard- and software, update systems and servers, software development, deploying new tools etc. [59]. We specifically invited system and network operators who had work experience with BGP operations (see Sec. 3.3).

Academic Research: Throughout this work and in the interview questions, we use the terms 'academic research' and 'academic papers' to refer primarily to peer-reviewed publications in first and second tier academic network security venues, including—but not limited to—IEEE (S&P, EuroS&P), ACM (CCS, IMC, SIGCOMM), USENIX (Security, NSDI, ATC) conferences, and other academic venues like, e.g., NDSS, ACSAC and RAID.

2.1 A Primer on BGP

The Internet is a network of interconnected networks [65], each referred to as an Autonomous Systems (AS) [48], usually identified by a unique 32bit (formerly limited to 16bit [56]) number. Networks use Internet Protocol (IP) version 4 [91] and 6 [30] addresses to make hosts [25], i.e., computers and other systems, globally reachable [44]. IPv4 addresses have a length of 32bit [91], while IPv6 addresses are 128bit long [30] to mitigate the issue of IPv4 exhaustion [92]. A network usually encompasses a set of IP addresses in one or more 'prefixes' [42], i.e., blocks of IP addresses where the first N bit are the same, with N being the 'prefix length'. For example, '192.0.2.0/24' is an IPv4 prefix of all addresses where the first 24bit are the same, i.e., the IPv4 addresses from 192.0.2.0 to 192.0.2.255. IP addresses and AS numbers are assigned to networks by regional internet registries (RIRs) [54].

The Border Gateway Protocol (BGP) is currently the only protocol routers of different ASes use to exchange information on which AS 'has a route' for a prefix, i.e., is able to forward network packets to a specific IP address given its prefix [95].

Two connected routers ('neighbors') can exchange routing information over a 'BGP session'. On a high level, each router 'advertises' all prefixes for which it has a 'route' to its neighbors. Here, there is a distinction between a router, or rather an AS, 'originating' a prefix, and it 're-advertising' a prefix originated by another AS. Each advertised (or 'exported') route, also called 'network layer reachability information (NLRI)', carries various attributes. The most crucial aspects are the prefix and prefix length itself. Among the additional attributes found in NLRI, the AS_PATH is the most relevant. This field contains a list of all ASes an announced NLRI traversed. At its very core, BGP uses the Bellman-Ford algorithm [8], i.e. a path-vector [80] algorithm, to compute the best path for packets towards a specific prefix. The main decision criteria here are prefix length (more specific, i.e., longer prefixes are preferred) and the AS_PATH length, where the shortest path usually wins [94]. Beyond that, BGP is a policy-based routing protocol, i.e., allows operators to turn various additional knobs to influence route selection.

Finally, route propagation usually follows a tree structure. Simplified and omitting corner cases, an AS has 'upstreams', 'peers', and 'downstreams' [4]. Routes originated by an AS or learned from a downstream should be advertised to all peers. Routes learned from peers and upstreams should only be announced to downstreams. ASes that are so large that they do not have any upstreams are also called 'Tier-1 ASes [33]. This creates a 'valley-free' structure of route propagation [103].

2.2 An overview of Securing BGP

In the initial design of BGP, security was not a primary concern. This enables attacks such as confidentiality violations, replay attacks, message spoofing, denial of service attacks,

man-in-the-middle attacks, prefix hijacking, and route leaks [20, 21, 87, 108]. Securing BGP relates to different aspects of the protocol [33]: (i) Securing the BGP Speaker, (ii) Securing sessions between neighbors, (iii) Securing which routes are imported and exported, and, (iv) Securing which forwarding decisions are made based on routing information, i.e., preventing the forwarding of spoofed packets [6, 34, 102].

Securing Speakers and Sessions: Securing BGP speakers themselves boils down to basic network security measures, ensuring that no unauthorized traffic reaches the management interfaces and control plane. For securing BGP sessions, MD5 based session authentication has been the defacto standard [49], which only slowly is being replaced by TCP-AO [105], if it is used at all. In academia, most work here relates to attacks on speakers, e.g., by leveraging fragmentation [27, 28].

Securing Announcements: The main threat in the context of BGP are malicious announcements, which lead to traffic that should not traverse them suddenly traversing them, enabling on-path attacks on all affected network traffic. This is usually accomplished by falsely originating a route, e.g., with a shorter prefix, or–if the attack's objective is geographically limited–a shorter prefix [45, 51]. Various more specific implementations of these attacks exist under different circumstances (forged-origin hijacks, prepend-hijacks, etc.) [52, 81, 88]. Traditionally, especially route import has been secured via filter-lists generated from Internet Routing Registry (IRR) data published by RIRs via their corresponding databases [33]. However, filtering practices have been lax [19, 20, 57], and these databases are not cryptographically signed.

Methods like BGPsec [70, 73] and secure BGP (S-BGP) [61] were proposed to reduce the overhead of generating these filters, while also introducing cryptographic signatures to protect authorization information's integrity. The Resource Public Key Infrastructure (RPKI) developed in Internet Engineering Task Force (IETF) in the Secure Inter-Domain Routing (SIDR) Working Group [69] is the most widely deployed method to accomplish this. Using RPKI, network operators can generate cryptographically signed Route Origin Authorizations (ROAs) that bind IP address prefixes to their corresponding originating ASes [18]. Furthermore, currently, ASPA records are being finalized in SIDROPS [5], which—together with RPKI and BGPsec—will finally allow fully securing AS_PATH information.

Academic work on announcement security encompasses direct attacks on the routing ecosystem, e.g., attacks utilizing forms of prefix hijacks [3, 7, 10, 82, 106], work measuring various forms of prefix hijacking [52, 81, 88], measurements of the deployment state of, e.g., RPKI validation, as well as proposals to improve ROV and announcement security in general [19, 20, 24, 43, 57, 63, 74, 96]. Here, secure BGP (S-BGP) is one of the pre-cursers of RPKI, using two Public Key Infrastructures (PKIs) based on X.509 (v3) certificates to build trust relationships [61].

Securing Forwarding: Besides announcement security, ensuring that ASes do not *send* packets they are not supposed to send is an important goal. Packets with forged source addresses ('spoofed' packets) are a major issue on the Internet, enabling, e.g., amplification DDoS attacks [26, 97]. As such, ASes should ensure that they only forward packets from clients and downstreams authorized to send from those addresses [6, 34, 102].

Academic work regularly performs measurements to assess the prevalence of spoofed traffic [75, 85], or which try do identify which ASes allow spoofing [9, 41, 78, 79, 90]. Additionally, recent academic work concerns various methods and enhancements to BGP to make source address validation (SAV) easier [111].

Possible Harm of Disconnected Academic Work: In the context of securing announcements and measuring, e.g., route leaks or hijacks, inaccurate academic work can create noise via an abundance of claimed events (leaks/hijacks). This could lead to notification fatigue [107], and reputation damage for parties incorrectly claimed to have executed leaks/hijacks, see also MANRS (https://manrs.org/). Similarly, incorrect claims of insufficient address validation can negatively impact an operator's reputation. Especially, source address validation measurements often cause non-negligible additional network load. Lastly, based on anecdotes, there are concerns among operators that a high level of academic 'noise' on the subject sways organizations to dedicate resources to resolve issues which may rest on inaccurate assumptions.

3 Methodology

We use a qualitative approach to study the perspectives and experiences of network operators involved in BGP operations.

3.1 Research Questions

The overarching research question driving this study was: *What are the operators' perspectives on the practical feasibility of BGP security solutions proposed in academic papers?*

We split this question into two independent sub-questions, to be answered from the ***perspective of network operators***:

RQ1: To what extent is scientific literature considering the expertise of network operators while formulating new theories/methodologies for BGP security?

RQ2: Is there a gap between academic work and the requirements of network operators? If yes, what are the reasons and what steps could be taken to bridge this gap?

3.2 Focus Group Design

Focus groups involve moderated group discussions on specific topics or concepts through a mediated conversation based on the individual experiences, opinions and attitudes [89]. Asynchronous Online Focus Groups (AOFGs) are a data collection method in which participants respond to questions in an online platform over a designated period [115]. They have proven to be a practical and flexible qualitative approach [31] that is effective in soliciting the perspectives of professionals [68]. We opted for AOFGs because an asynchronous format allows one to contribute at their own convenience. This suits our participants, who tend to be busy [32, 59] and overworked [60]. We did not provide remuneration as sysadmins are generally well paid for their work, but are short on time [32].

We followed a semi-structured interview approach containing four main open-ended questions (see Apd. D). These allow participants to respond freely and discuss topics that they find more relevant. In addition, we shared the Code of Conduct at the start of the discussions to foster a respectful environment for the participants (see Apd. B). We also conducted trial focus groups to evaluate our interview protocol and asynchronous approach.

3.3 Participant Recruitment

We aimed to engage with network and system administrators willing to share their day-to-day experiences, specifically regarding BGP operations. We crafted study invites and circulated them via RIPE NCC, NANOG, ARIN, LACNIC, APNIC mailing lists, and other platforms such as LinkedIn, Telegram, X, Mastadon and Discord. Additionally, fliers (see Apd. E) were distributed at IETF 121 and RIPE 89 meetings to attract participants. Since the chosen method was online and asynchronous, we aimed to recruit people from a wide geographic area to increase the diversity of the responses. The invitation contained a registration link to enable participants to register and select their desired start date for the focus group. We had a total of 31 responses to this form.

We sent interested participants the study description, instructions on how to participate in the discussion, and the informed consent form. Tab. 1 shows the list of 12 participants who actively participated in the focus group discussions. Five additional participants joined the Mattermost channel but did not participate in the focus group discussions. Tab. 1 includes Participant Q01 who expressed interest in participating in the study but was unable to join the focus group. We remedied this by sharing with them a written questionnaire with the same questions as the focus groups. Participant Q01's responses were considered as additional input, i.e. we did not consider Q01's input for theme generation but performed an additional analysis to verify whether or not their responses fit our already generated codebook and themes (which they did).

Furthermore, we received feedback from several participants that the 'paperwork' required by participation, specifically the consent form, felt like prohibitive overhead. Several participants and prospective participants noted out-of-band that this formal requirement likely reduced our participant pool. We note this as an additional tension between academia and operators' general attitude, see also Dietrich et al. [32].

3.4 Asynchronous Online Focus Groups

Twelve people participated in six focus groups. Each discussion began with an introduction of the moderators and the research process. The Code of Conduct (see Apd. B) was posted in the group to enable a respectful and open environment for discussion. Participants joined with pseudonyms and were asked to introduce their professional role without revealing their names. Each focus group lasted approximately four to five weeks, and a total of four open-ended questions (see Apd. D) were asked, roughly one each week, allowing the participant ample time and flexibility to respond. Follow-up questions were asked based on the participants' responses, to elicit further details and clarifications. Four focus groups had 2 participants, one had 3, and one had 1. The group sizes were based on the availability of participants at the same point in time. As for the group with one participant, we had no-shows but did not want to lose the opportunity to solicit input from experienced participants.

3.5 Data Analysis

Reflexive thematic analysis (TA) is a qualitative data analysis process that examines and reports patterns in the data [13, 14]. It emphasizes on the importance of the researcher's interpretation and reflexivity (Sec. 3.5), and offers a systematic approach to comprehend qualitative data. We opted for inductive TA, which is a data-driven approach where codes are developed directly from the data without a predefined codebook, thus allowing for a comprehensive data exploration and theme development [15]. In line with TA, we opted for a single coder approach. However, theme development was done in regular consultation with the research team.

Phase 1 - *data familiarization* - involved an extensive and repeated review of the transcripts collected from focus group discussions. To ensure confidentiality and privacy of all participants, the data collected was pseudononymized. All personally identifiable information (PII) like names, details of the organizations and any information that could be used to potentially identify a participant was removed from the transcripts. Phase 2 - *coding* - required labelling the data with 'codes', enabling systematic categorization. This gives direction on how to organize the data so that meaning can be constructed and presented in a structured way. For this, an internally-hosted instance of ATLAS.ti[1] was used. In line with an inductive coding approach, we coded all relevant and interesting responses,

[1] ATLAS.ti: https://atlasti.com/

ID	Gender	Education	Job Title	Job Sector	Location	Org. Size	Exp. (y)
P01	Male	Msc. (Computer Science), IT Law	Industry Principal	IT Security	Australia	18 Billion in Revenue	23
P02	Male	University	Chief Executive Officer	IXP	Cambodia	10 Employees	20+
P03	Male	University Degree	Managing Director	Telecommunication	Austria	SME	32
P04	Male	Programming, Eng., Networks	Consultant, Infra. Services	Education and Government	Canada	15 Employees (dept.)	35
P05	Male	Telecom Engineer	Chief Technology Officer	Datacenter, Network and Telecom	Switzerland	5 Employees	29
P06	∅	Undergraduate Computer Science	Network Engineer	ISP	Remote	~30 Employees	10
P07	∅	University	∅	Internet Industry	Germany	Individual	37
P08	Male	BSc	"Employee IT serv." (HPC/mI)	IT Services	Germany	700 Employees	10+
P09	Male	BSc, LL.M, MCA, Ph.D	Senior Sec. Research Engineer	Security Engineer	India	10,000 Employees	18
P10	Male	College/Industry Training	Senior Network Engineer	IXP/ISP Networks	UK	5 Employees	30
P11	∅	Apprenticeship, University Dropout	Associate Infra. Operation	ISP and Services	Switzerland	15 Employees	25
P12	Male	3y Apprenticeship Electronics	Senior Advisor	Computer Networking, Healthcare	Norway	800+ Employees	23
Q01	Male	B.E. CCIE	Network Architect	FMCG	India	25,000 Employees	20

Table 1: List of Participants. ∅ = no response

not limiting ourselves to specific responses relating to our research questions. Semantic and latent codes [16] were used, leading to a total set of 178 codes. In phase 3 - *generating initial themes* - we clustered related codes based on commonalities and shared concepts using an online whiteboard[2], and created initial themes. The codes were refined and redundancy was removed by combining codes that shared the same ideas.

During phase 4 - *developing and reviewing themes* - the clusters were iteratively refined by reassigning codes between clusters to ensure the best fit, as well as renaming the clusters to more accurately reflect the core concepts they represented. Some clusters were divided into sub-clusters to identify any specific trends or variations within broader themes as well as to capture finer details. The frequency of occurrence of the codes was also taken into account to understand their relative significance. Phase 5 - *refining, defining and naming themes* - was about finalizing the themes and sub-themes, and identifying the interconnections by going back and forth between the transcripts and the codes. Certain codes fit into different clusters better than others, and some even fit into more than one cluster. In order to weave everything together and present a coherent story, we systematically reported our themes (Tab. 2) as per phase 6 - *writing up* - and connected our findings to relevant work in the domain.

Reflexivity and Positionality Our team comprised of experts in system administration, computer security, human factors and qualitative research techniques. The interviewer's IT security background enabled them to deeply engage with the participants on technical topics. Another team member with over a decade of experience running Internet infrastructure guided the design of the study and assisted in recruitment via their contacts in various networking communities. Our research was motivated by the belief that the improvement of network operations and security processes are reliant on strong collaboration between academia and industry.

[2]Miro: https://miro.com/online-whiteboard/

Theme	Sub-theme(s)
The Reality of BGP Operations	1. The Rulebook: Standards 2. The Changing Face of Expertise in BGP Operations 3. Day-to-Day Challenges in BGP Security Operations 4. Proposed Solutions and Strategies
BGP Innovation: Finding New Ideas	1. To Adopt or Not: Factors that Sway Decisions 2. From Paper to Practice
The Academia - Industry Divide	
Crossing the Divide	1. Embracing Gradual Change 2. Enhancing Communication and Collaboration 3. Optimizing the Format 4. Reflecting on Practical Relevance

Table 2: Themes and sub-themes

3.6 Saturation and Completeness

Data saturation was continuously evaluated until the input of the participants started to converge. This convergence was observed for certain (sub)themes: sources of new BGP solutions, factors influencing the adoption of these solutions, the academia-industry gap, and possibilities to bridge this gap.

Achieving saturation for responses related to operational realities and challenges in BGP proved difficult since participants came from various backgrounds and industry sectors, with varying day-to-day responsibilities and priorities.

4 Results

Here, we present the four main themes from our data (see Table 2), and answer our research questions in Sec. 5.

4.1 The Reality of BGP Operations

The first theme is about a perceived disconnect between operational reality, i.e., how things really are versus the mental model researchers seem to have of BGP operations.

P04: *"Do not trust that your lab directors have a goddamn clue how the Internet operates."*

P04 explains that operational teams often become frustrated when non-operational decision-makers dictate orders without understanding the technical nuances of global routing. This connects to a perception by operators that management decisions of those outside of day-to-day operations already tend to conflict with operational realities, an effect also noted in prior work [59, 86]. This frustration further amplifies when non-operationally involved academics provide solutions.

The operational landscape is defined by practical pressures such as tight deadlines and instant problem-solving. In such scenarios, balancing skepticism and pragmatism in organizational decision making can be challenging. Yet again, P04 indicates that changes to a system are often a result of urgent and/or unexpected requirements. Often, BGP solutions are implemented with a "just make it work" mentality existing across several organizations, which may ignore in-depth analyses or long-term developments.

Moreover, organizations usually prioritize revenue generating activities [37]. This leads to a cautious approach towards changes that may induce network disruptions. P08 argues that unless absolutely necessary, one should not tinker with a running system:

P08[3]: *"never change a running system."*

M02[4]: *"@<P08> is there ever a situation where you would change a running system?"*

P08: "*for bpg [sic] - operations/security requirements.*"

The underlying argument is that BGP configurations are either too critical or too complex, leading to hesitance when making changes that are not strictly operationally necessary. P10 and P02 concur that operators are reluctant to make changes to a BGP configuration that somehow works just fine. The "don't touch a running system"-attitude is also illustrated in previous work [59] which implied that system administrators often prefer to let things be if they are operating fine instead of applying changes that may alter the system state. P04 emphasizes this point, questioning whether changes that are intended as improvements are indeed that.

P04: *"Ultimately, change costs money and time, and from that perspective, very few "improvements" actually are mprovements [sic]."*

When the overlooked aspects of cost and time are considered, a so called "improvement" may not necessarily be beneficial. P07 concurs with this as well, underlining the importance of critically evaluating and weighing the cost of the hidden elements associated with a proposed change. Therefore implying that there may be instances in which preserving the status quo is more cost-effective than seeking change for the sole purpose of improvement.

Numerous complexities arise in network operations as operators are often torn between operational and organizational factors. P03 indicates that *"this industry has learned to think in business-cases everywhere"* and therefore often prioritizes value for money over security and long-term stability. Similarly, P03 believes *"IP needed to be cheap - so the industry made it cheap"*, again emphasizing that organizations prioritize generating revenue. Hence, a strong financial justification is necessary to justify a change.

4.1.1 The Rulebook: Standards

Standards and frameworks lay the foundation for stability, interoperability, and security in the constantly evolving fields of network and routing security. They help to ensure that security measures are consistently applied, lowering the probability of vulnerabilities in BGP operations. Standards are often developed by recognized bodies such as Information Security Standard (ISO), National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF). Although often encouraged by several organizations, these may or may not be mandatory depending on the organizations regulatory requirements.

For BGP related operations, work by the IETF seems to be most relevant, or as P09 claims: *"BGP implementations follows RFC standards [sic][5], hence minimum set of requirements are met"*. Similarly, P03 suggests that operators prioritize and rely on these established standards. The implementation of technologies or solutions within organizational networks highly depends on whether they are recognized by the networking community as important.

P03: "*My work urges me to wait on things until they are ready and the community has accepted it as to-be-done or as to-be-standard - then I take it into my own world.*"

Similarly, P04 shares that *"Until what you're proposing is at least a standards-track Draft[6], I really don't even want to hear about it."*, indicating trust and confidence in community-established standards.

4.1.2 Changing Face of Expertise in BGP Operations

Several participants noted difficulty in finding new talent in the field of network operations, linking it to the work itself not being 'trendy', like, e.g., 'LLMs'. P03 noted that this leads to a growing knowledge gap between retiring experts and emerging engineers since knowledge is concentrated within the older generation:

P03: *"the most critical mission is to learn [sic] these skills to a younger next generation of students/engineers as those who know are broadly on the way to retire in the next 10-20 years - and imho there is a big gap behind those in generation distribution of knowledge ..."*

[3] P08 refers to the Participant

[4] M02 refers to the second moderator

[5] We acknowledge that RFCs are not, per se, standards and come in various different tracks and document statuses [2, 12, 29, 47, 53, 64]

[6] A specific line of documents that, ultimately, may become an 'Internet Standard' [2, 12, 29, 47, 53, 64].

This impacts operational efficiency and exacerbates the distrust between operational teams and non-operational decision-makers. Such decisions, in the opinion of operators, frequently put budgetary limitations ahead of technical stability, e.g., when deciding to *not* hire a new junior for a team. This raises doubts about management's appreciation of the complexities of BGP operations, as they make risk acceptance decisions without fully understanding the implications, similar to findings of Munot et al. [86].

The overall result of this retirement driven loss of in-house expertise leads to organizations having to, as P08 put it, *"rely on hiring externals"*, i.e., consultants. This 'capability loss', predominantly in specialized niches of IT operations has been previously discussed in the literature [36, 38]. However, it also highlights that a specific set of practical experience is necessary for BGP operations, highlighting again the point that academics may also lack this operational expertise as previously discussed in the literature [35].

4.1.3 Day-to-Day Challenges in BGP Operations

Managing networks is a continuous process, often riddled with tasks that may not have an immediate benefit to the network *continuing to work*. For example, during mergers and acquisitions, it might be necessary to clean up a significant number of stale Internet Routing Registry (IRR) records as a result of the acquiring company's outdated IRR databases. P06 indicates that operators tend to find it naturally burdensome to *"unwind years of legacy configurations"*. Networks are evolving, demanding the systematic removal of these obsolete records following extensive analysis and revision. Yet, they are left untouched because they "somehow work".

As BGP lacks built-in security mechanics [21], leaving it far too often vulnerable to a variety of attacks [109], BGP security is incorporated in layers on top of the protocol, making it even more complex. This, in turn, further increases operational complexity, and creates a wider chance for errors to occur. In fact, several participants reported on the difficulties and misconfiguration-opportunities introduced by, e.g., RPKI. P03 frequently sees *"[...] rpki invalid creation from those who run rpki roa, but operate different asn themself"*. Similarly, P06 often comes across misconfigured RPKI however, *"More often it is not configured at all."*

With BGP security being difficult, participants were quick to identify insufficient training or technical aptitude by operators as the major issue in deploying RPKI: P06 notes that *"probably the single biggest factor that influences all of these issues is lack of familiarity"*. Similarly, five participants agreed to a statement by P02 that the *"primary challenge is educational"*. In fact, throughout all focus-groups, the core issue seen on the surface was, as P02 puts it, *"underskilled Engineers try to run or hold up a BGP based network"*. This effectively reduces the technical challenge of BGP security to a personal responsibility (and failure). The underlying perspective (human error as personal failure) is an outdated, yet still common, perspective on human factors [58].

Beyond personal responsibility, within an organization, management of BGP is significantly impacted by internal decision-making processes, corporate priorities, and organizational politics. P02 draws attention to the issue of BGP's ambiguous *"administrative ownership"*. It is uncertain who in the organization is in charge of managing BGP operations. This causes a delay in the implementation of RPKI and the management of other BGP objects, like ROAs. Hence, digging deeper, it in fact turns out that the more critical issue is even more socially inclined: *"getting people to care"* (P04).

P02: "*The challenges we face are less about BGP itself and more about its practical application and understanding.*"

However, also considering the aforementioned points on financial priority setting and the role of decision makers, this means that there is little room for the necessary work to, e.g., implement RPKI *properly*. This mindset of *"my Internet is fine, so why should I care"* (P04) exposes a cognitive prejudice called normalcy bias [114], in which people fail to acknowledge the likelihood of infrequent but disastrous circumstances simply because they haven't witnessed them personally. This ultimately leads to the observed operational challenges and an overall reactive approach to security [58].

4.1.4 Proposed Solutions and Strategies

Participant P03 proposes extensive training to fully understand BGP. P12 mentioned post-incident audits as a crucial part of incident response to capture lessons learned and find tangible action items to reduce complexity, as also proposed in related work [32]. However, the bulk of recommendations center around technical solutions. Network design techniques to improve resilience and reduce the effect of failures are covered by P06. These include *"Avoiding single points of failure"* (P06) to ensure that failure of no single server or device will disrupt the entire network, and to *"reduce the blast radius"* (P06), reducing the number of affected devices in the event of failure. However, such methods are not easily implemented in larger, grown, networks.

Another technical solution regularly discussed by operators is automation. For instance, P07 relies on automation for frequently changing the 'max prefix' value on peerings. Max prefix limits the number of prefixes a router may receive from its neighbour. This way, the router terminates the connection in case of an (accidental) route leak. According to P07, PeeringDB[7], a publicly accessible database that facilitates peering, offers an API their automation can use to obtain information on specific peers. In addition, P12 asserts that with the help of a template, automation adds consistency in their configuration. Similarly, P01 illustrates that, in the context of routers, *"IDs are best kept to autogenerated"*. However, no participant discusses the necessary technical capabilities to properly build and maintain automation systems in the first place.

[7] PeeringDB Website: https://www.peeringdb.com/

4.2 BGP Innovation: Finding New Ideas

The second theme relates to how participants identify new technologies and options for routing security. P04 and P11 claim that they often learn about new and interesting BGP advancements during informal conversations such as *"offline discussions, beers"*. Similarly, five participants note that newer technologies can be learned by *"existing (or potential) BGP peers"* (P04). Involvement with the *"local community of network operators"* (P12) may also serve as a good source. P07 and P11 encourage the use of *"RFCs"*, and *"Mailinglists'* such as those of DENOG (German Network Operator Group), NANOG (North-American Network Operator Group), and RIPE-Lists. Six participants (P04, P07, P11, P03, P06 and P12), also suggest that conferences such as RIPE meetings, NOGs, RIPE and the IETF are a great source to discover recent developments in BGP security.

4.2.1 To Adopt or Not: Factors that Sway Decisions

The decision to adopt or implement new technologies is influenced by operational, financial and organizational factors and varies from operator to operator. The *"features and functionalities"* (P01), and *"Flexibility and Future-Proofing"* (P09) offered by the technology plays an important role in judging whether or not to implement that particular solution. Similarly, factors such as *"cost"* (P09), *"Operational Complexity"* (P09), *"Ease of adoption"* (P11), and *"Security Effectiveness"* (P09) also stood out in the focus groups discussions.

P06 and P12 suggest that *"vendor support and maturity matters"* (P06) and *"other documents recomending [sic] this feauture [sic]/solution, and configuration guides will also affect decision making"* (P12). P11 adds that *"It needs to make sense in our infra"*. Similarly, the *"Compatibility and Interoperability"* (P09) offered by the solution with the current organizational structure and requirements matters. The *"Time/effort it takes"* (P07) to deploy a solution, *"Community and Peer Adoption"* (P09), the probability of risk involved in deploying a solution and *"Business requirement's"* (P01) are also contributing factors.

There were opposing views on automation. P04 would like to have a solution that *"Can be automated"*, whereas P07 argues that they do not prefer automated processes in the network because *"they've been burned badly in the past by automation run amok"*. They explain that their *"strong negative view"* of automation is *"about perception, not reality - but because of the nature of our entity, perception is very important"*. P04 points out that even a flawless protocol, designed with careful consideration, succeeds or fails depending on whether people are willing to adopt it. Rather than the technology itself, the biggest challenge lies in persuading individuals of its benefits.

P04: *"the most theoretically perfect protocol or system still has to convince tens of thousands of people to *do something* that most won't understand, don't have time for, are getting criticized by their managers for "wasting time on", etc."*

Operators find learning new technology to be time-consuming and tedious. This leads to reservations from the operators' side when academics only engage the operational community after developing a 'solution'. From the operators' perspective it may appear notable overhead—already for *understanding* the solution—is put on them, while the researchers appear to not have attempted to sufficiently understand the problem itself and the practical requirements around it, an effect also discussed in prior work [58].

Finally, personal experience and familiarity play a role in adopting new technologies. P11 acknowledges that their positive view on academic papers may be influenced by their previous work. They are more inclined to it since they have previously advocated for these projects.

4.2.2 From Paper to Practice

Academic research has proposed or supported several enhancements to BGP, for example S-BGP [61] and BGPsec [71]. In academia, the goal switches from immediate problem-solving to understanding the "why's" behind reoccurring problems, and proposing elegant solutions. This is echoed by P03, who thinks that *"research is often a professional way to summarize problems and structure possible solutions"*, recognizing the value of academic work. Similarly, P01 acknowledges that research papers are *"certainly helpful"*. Despite their statement that academic work cannot be solely depended on, P01 states that these are an excellent point of reference to acquire new ideas and learn about the latest frameworks. P03 asserts that academic solutions might be helpful, but argue that a subset of existing work was written *"just for the sake of it"*, without considering whether or not they would truly offer beneficial solutions.

Several participants also expressed skepticism towards academic papers. As per them, the solutions offered by academia are inadequate and impractical in terms of the challenges faced in the field. P06 notes that the current format of academic papers is not flexible enough to provide actionable steps for implementation to practitioners. Operators often feel as though research papers are *"Too long"* (P07). P11 adds that *"Either the scale isn't right, or the topic is really working for an exploration, not many of them could be applied in the real world"*.

4.3 The Academia - Industry Divide

Participants regularly voiced that academia and industry are indeed divided, not owing to hostility, but as a result of distinct priorities and timelines. Academia relies on a theoretical approach, long-term problem-solving, and conceptual models, whereas network operators prioritize practical efficiency,

real-time problem-solving, and solutions that can meet the demands of day-to-day operations.

P09 notes an *"unaccidental"* gap between industry and academia, especially in the field of routing security. P09 has been on both sides and witnessed the struggles of attempting to implement academic research in real-world situations. As such, they note that *"there has to be some gap"* (P09) between academia and industry. Similarly, P03 indicates the existence of two distinct, disconnected worlds with minimal overlap, each having their respective priorities and approaches. They claim that *"people crossing the lines are the minority"* (P03) highlighting how uncommon it is to come across individuals who actively participate in both domains. P04 claims to have *"seen MANY solutions in search of a problem"*. The missing practical inclination of academic research is made more evident by P07's remark:

P07: "Research papers are written by researchers for other researchers."

The participant claims that research papers are written keeping in mind fellow researchers, as compared to operators that could utilize the presented solutions in practice. The focus on academic language and theoretical advancement indicates that researchers may also utilize their work to establish reputation in the academic community, thereby creating a silo-ed stream of work on routing security, decoupled from actual requirements in practice.

Several barriers exist in the practical implementation of academic solutions. In fact, P04 goes as far as to claim that academia has an *"[...] "ivory tower" syndrome [...]"*. Researchers often operate in an isolated environment, oblivious to the real-world challenges faced by network operators. This metaphor, again, suggests that academics could be seen as as operating in idealistic, theoretical circumstances without having a full grasp of the practical challenges associated with daily networking operations.

P04: "All the problems are ultimately communication and understanding, the classic "ivory tower" syndrome. Academia as a whole vastly, enormously, and consistently overestimates how much network operators care about research."

P04 believes that academics largely overestimate the significance of research to network operators, indicating that, despite their exemplary nature, academic publications often attract the attention of operators because they dismiss the real-world problems that operators face.

Several participants highlight the missing communication and collaboration between academics and operators, P04 hints at as well. For example, P03 reflects missing communication and collaboration between the two realms: *"my feeling is that industriy [sic] and academia are too disconnected"*. P03 further points out the gap between academia and practical application, and expresses operators' displeasure when academic insights are offered without genuine understanding or collaboration.

P03: "it always looks strange when you see researchers coming with some talks who have never been in this community and then come over to tell the elite engineers of our industry how academia thinks how they have to do their job - this is an example of how it should not happen."

Their responses indicate that researchers who do not have first-hand experience in the industry might not have sufficient practical knowledge to fully understand the difficulties faced by network operators. The expression *"telling elite engineers how to do their job"* (P03) shows both, operators feeling patronized when academics suggest ideas without taking into account their expertise, but also the underlying (over)confidence of operator culture [59, 60]. Nevertheless, professionals with years of practical expertise may feel as though researchers are dismissing their knowledge by imposing theoretical concepts on them. However, contextualizing this strong statement, the participant follows up that this is an example of *"how it should not happen"* (P03), indicating that mutual understanding and respect also occur between academics and researchers.

The responses of P03 relate to the insider - outsider dilemma [77]. The community of operators have their own norms and expectations. Hence, when an 'outsider' begins to contribute to the group, this may cause some resistance.

The academic outside perspective ties in with a misunderstanding of the scope of proposed changes. Solutions may be *theoretically* sound, but too disruptive to be rolled out at once, while not considering a gradual roll-out. For example, P06 highlights that the changes required to implement academic solutions in practice are often *"large and potentially disruptive"* (P06). This connects with an academic mindset assuming that–once the concept has been demonstrated–practitioners will 'fill in the gaps'. P07 ties this to a missing practical inclination in academia, stating,*"Operators need solutions to fix real world problems quickly"*.

Operators are also sceptical of the motivation behind publishing papers, seeing it in obtaining a degree, obtaining funding, or building a career. For example, P08 is not convinced that research fulfills its purpose of leading to actual improvements, while also sharing a concern that publications are simply done to *"get a degree"*.

P08: "you fail to deliver if you publish for your own shelf only [...] and the only reason you publish is to get a degree"

Especially the incentive system around funding is seen critical by operators. Participants voiced their concern about how funding plays a crucial role in bending the rules of academia, thus influencing its outcomes, especially due to conflicts of interest when for-profit organizations finance research. Still, participants also note that in an ideal scenario, *"that shouldn't be the case"* (P11), but maintain that in reality this may pose a risk. Despite being critical of funding incentives, participants also acknowledge the necessity for researchers to focus on matters that will attract funding:

P11: "I understand that academic research isn't simple, also on the financing part. I suspect that some " sponsoring "

or support money for research groups might come from some for-profit sources, and those might want to affect the outcome of the results [...]"

When work is published, operators note that it still remains difficult to find relevant work. As P03 notes: *"there is no structured index I'm aware of"*. Or, as P10 states:

P10: "The fact that they don't come across my desk very often maybe says something about a disconnect between academics and people working with it operationally every day."

As such, even open access papers may be *practically* unavailable to operators, as it becomes difficult to find relevant work, as it is *"not advertised"* (P12)[8] and findable for operators. Overall, this also strengthens the perception of academia as an exclusive 'in-group', or, as P08 notes: *"if you are not in this part of research, you do not know the papers"* (P08).

4.4 Crossing The Divide

The previous sections focused on our themes describing the *divide* between academia and industry in BGP security work. Our last theme presents a more positive commentary from our participants, focused on bridging that gap.

4.4.1 Embracing Gradual Change

The practical requirements of the industry necessitate a more gradual approach to proposed changes in a well-structured manner. Operators prefer *"modular or incremental solutions which are easy to deploy rather than a full blown solution at scale"* (P01). Similarly, P06 suggests having *"a breakdown of incremental steps"*, indicating that the use of modular solutions allows for smaller changes[9]. In this manner, the probability of unexpected network disruptions, is reduced.

However, we note as authors, that this proposed approach is fundamentally difficult to implement in research. For one, researchers often lack the operational experience to correctly asses the right change sizes, see Sec. 4.1. Furthermore, academia favors 'groundbreaking' and 'innovative' insights, i.e., 'big-leap' papers, while following relatively strict 'success timelines', e.g., for graduation or tenure [35].

4.4.2 Enhancing Communication and Collaboration

Overall, our participants were positive of enhancing communication and collaboration between academia and industry. Six participants explicitly encourage collaboration between academia and industry. P01 encourages academics to collaborate with network operators, IXPs and other industry professionals while developing research questions to ensure that they fully capture the realities of BGP operations. P04 states that it is a good idea to *"Involve practitioners early"* to shape the research and allow researchers to build impactful and practical solutions. Similarly, P09 recommends researchers to *"Invite Subject Matter Experts from Industry to share their experience and challenges"* early on in order to help academics understand the operational and technological barriers that practitioners come across, like financial limitations, legacy systems, and risk management.

For getting into contact with operators, our participants recommend a continuous involvement and community building by regularly attending IETF, RIPE and other NOGs' conferences and meetings. The participant pointed out that *"initiatives for academia at ripe [sic] like the RACI program"* (P03) for students and researchers may lower the entry barriers for participating in such events. However, our participants were also adamant that researchers should not treat this as a unidirectional conversation, but that researchers should actively engage these communities and become a part of them. Researchers should, as P07 puts it, *"Not just talk and present, but LISTEN"* to discover challenges faced by operators and incorporate these into the research to make it practical.

4.4.3 Optimizing the Format

P12 notes that *"research needs to have a format that goes a bit more directly to how it can be applied , like a configuration guide or BCP document. As for the research it self it needs to be presented in a way that operators can quickly get a summary, and possible applications/solutions."*

For a bigger impact in practice, research work must be presented in a more actionable manner, like a *"blueprint"* (P06). This means presenting it with clear instructions on how it can be implemented. P12 recommends proposing operational changes as a summary and to-the-point 'Best Current Practice' (BCP) document in order to offer practically useful information to network operators. This would enable implementation without having to interpret the often prohibitively complicated academic language used in papers. Similarly, P08 expresses a preference for practical resources that are easily available in contrast to traditional research papers.

4.4.4 Reflecting on Practical Relevance

Participant P01 suggests that researchers need to truly understand the needs of the industry and try to incorporate these into their proposals to increase the practical relevance and also the likeliness of deployment into production networks:

P03 prompts researchers to *"intigrate [sic] things like MANRS into the academic teaching/researching"*, so that, over time, research and education align closer with industry practices. This ties in with the generally low operational experience of academics, which–in turn–makes it difficult to correctly assess the realism of scenarios and solutions (see Sec. 4.1) and the recommendation to interact with operators earlier and long-terms (see Sec. 4.4.2).

[8] Please note that 'advertising' does not translate to the 'over-hyping' often seen with vulnerabilities in security work.

[9] See also the 'small badge principle' [104].

5 Discussion

In this section, we answer our research questions, discuss our results, further explore the *'Ivory Tower'* syndrome, and document the limitations of our study.

5.1 Research Outcome

Our overarching research question was: *What are the operators' perspectives on the practical feasibility of BGP security solutions proposed in academic papers?* From our data analysis, see Sec. 4, we find that operators perceive academic work on BGP security–despite providing an interesting reference point–to regularly not necessarily be directly practically viable. Without exception, all participants expressed that there is a gap between academic research and real-world operations. Next, we will dive into the two sub-questions (***RQ1*** and ***RQ2***).

RQ1: **Consideration of 'the Practice' in Research:** Our participants frequently noted, see Sec. 4.2.2 and 4.3, that they perceive researchers lack the expertise of industry professionals. While, on the one hand, this can be expected [35], it also contributes to the *"Ivory Tower"* syndrome ascribed by one participant. Academic research is generally a more theoretical endeavour, making it more disconnected from real-world operational needs by default. As conjectured in prior work [35], this leads to academics identifying 'the wrong problem', and subsequently designing a solution for that. Furthermore, even if 'the right problem' is identified, the solution might not find the right balance between the problems severity, and the scalability and deployment challenges a new solution incurs in different production environments. Beyond those more technical and operational requirements, production networks also have to adhere to financial requirements and need to honor logistical limitations of the real world. As per our participants, this is a stark conflict with the focus of academic work on the theoretical *feasibility* alone.

Ultimately, the insufficient integration of operators' perspectives leads to a perception among operators that scientific literature does not account for their experiences and expertise. Operators' perception of some work being produced solely for attaining funding, a degree, or other academic accolades also contributes to operators not feeling heard by the scientific research community. Instead, if academics, e.g., attend operator centric conferences or meetings, the impression emerges that they are there to 'tell operators how to do it', instead of listening, learning, and exchanging ideas.

As such, we find that operators do not feel like scientific literature sufficiently considers their expertise when proposing new theories or methodologies in the area of BGP security.

RQ2 pt. 1: **The Academia / Industry Gap:** All of our participants voiced that they do see a gap between academic work and industry needs. The reasons for this are tightly connected to the answer to ***RQ1*** in Sec. 5.1: According to our participants, researchers lack the practical experience to correctly assess which problem *do* need solving. Furthermore, this lack of experience leads to solutions to 'the right' problem that are ineffective or infeasible in practice.

Due to these mismatches, operators partially even doubt academics' motivation when conducting research, assuming misaligned priorities of academics such as publishing for personal reasons, i.e., attaining academic credentials for a promotion or degree, influence of funding bodies, or an attempt to conduct research to justify further funding. In addition, academic work is often not easy to read for operators, due to the often unnecessarily verbose and complex language used in academic writing, as well as due to the formatting of papers that includes text considered 'redundant' by operators. This, in turn, leads to proposals from academia often–if operators are even aware of them–being rejected or ignored.

We acknowledge that not all academic research is meant to be directly practically applicable. In fact, papers presenting opinions, describing challenges, developing new theories or replicating prior findings are essential to the scientific corpus. Such diversity makes a crucial contribution to the global scientific discourse. However, for researchers aiming for a practical engineering impact, we summarize our participants' suggestions for bridging this gap in the following section.

RQ2 pt. 2: **Bridging the gap:** To bridge the gap between academia and industry (see Sec. 5.1), especially for something as intricate as BGP, effective collaboration is crucial. We summarize our participants' suggestions for that:

1. Researchers should either gain practical experience themselves (e.g., through industry internships or practice-oriented coursework as recently reported by RIPE [50]) or engage with operators early and continuously throughout the research cycle—to ensure that the right problems are addressed and that proposed solutions are practically feasible. This can be done through active, sustained participation in relevant operational communities (e.g., IETF, RIPE, NOGs), approached with a "listen and learn" mindset rather than as detached presenters. Where direct engagement is not feasible, involving researchers with operational experience can help assess practical viability.

2. For researchers seeking to develop solutions that are practically viable and directly applicable to network operations, attention must be paid to how research outcomes are communicated. While it is unrealistic to fundamentally change academic writing conventions, distilling key contributions and sharing them in industry-oriented venues—such as RIPE Labs[10] or the APNIC Blog[11]—in a practical, stepwise manner can help create a bridge between academia and industry. This recommendation complements prior work highlighting the organizational factors that shape the adoption and deployment of security solutions in network operations [59, 60, 86].

[10] https://labs.ripe.net/
[11] https://blog.apnic.net/

5.2 The Missing Link

Our participants' responses also hinted at an issue expanding beyond scientific research. Academics, usually, also serve as lecturers, educating the next generation of engineers. However, the perceived limited practical experience when it comes to network operations also expands to teaching, which regularly is perceived as 'theoretical', or 'studying computer science with a pencil'. Networking concepts like BGP are taught in a theoretical manner without considering that students may eventually be responsible for operating networks in the real world.

With no practical exposure, students are left with insufficient understanding of BGP and may not fully understand its nuances. Additionally, also from the side of operators, there is an underlying expectation that "niche" technologies like BGP should be "learnt on our own". Even for those who are genuinely interested in networking, there is a noticeable scarcity of accessible, entry-level resources[12].

This issue is further aggravated by the perception that networking is "uncool" or "not trendy enough". While this is, essentially, directly related to the visibility paradox of system operations [60] (invisible and taken for granted if everything works, highly visible and reprimanded when issues occur), it also worsens the skill shortage in networking.

As BGP plays a vital role in the Internet infrastructure, having enough capable and experienced engineers is essential to maintaining our global digital infrastructure and digital sovereignty [37]. With the impending retirement of many older engineers in the next 10-20 years, there is a chance that the essential expertise that maintains the Internet will be lost.

5.3 The Eye of the 'Ivory Tower'

Several recommendations made in Sec. 5.1 require a long-term commitment to a single topic and, similarly important, community building. As noted in the literature [35], long-term planning may not be necessarily be feasible in the constraints of academic realities. Under the current system, publishing *more* is seen as an opportunity to gain recognition among fellow academics. Additionally, timelines–N years for a PhD, N years to tenure, x papers for the next promotion–may not allow for the necessary long-term commitment.

The implications of this stretch beyond research being unable to follow (necessary) recommendations to make BGP security more aligned with practice. Operators also perceive the pressures and implications created by this academic environment. For example, during the focus group discussion, a participant expressed frustration with researchers that attempt to address real world issues, claiming to understand the needs of operators, while not being involved in community discussions, essentially reverting to *"sales & marketing"* to get papers published. This leads to a picture of academia being stuck in a self-serving 'publish or perish' loop, ultimately promoting technosolutionism.

The 'Ivory Tower Syndrome' is further exacerbated by the (perceived) influence of the struggle for third-party funding. During the discussions, a participant prompted that research must uphold the foundational principles of Internet operation, including accessibility, freedom of speech, and openness. However, especially when competing with sensationalized areas like 'AI' and 'cloud computing', researchers may again have to revert to *"sales & marketing"* to compete with these fields. In turn, this approach seeds doubts among practitioners whether researchers are committed to those values, if they would, e.g., conflict with funding agencies' positions[13].

We argue that a transparent approach to funding (including selection) is the most viable approach to reduce those doubts by practitioners. Ethical and moral principals are vital while funding research to ensure that research is conducted in the interest of advancing technology rather than being another means for personal or business gains. Similarly, researchers may experience discrimination based on gender, race, or color, while diversity and inclusion in funding decisions can lead to a wider range of fresh perspectives and ideas that are likely to benefit interests globally. Hence, keeping the funding sources *and* selection procedures transparent and publicly auditable is essential to maintain the integrity of academic research–and efficacy of BGP security related work.

In summary, to address root-causes of the 'Ivory Tower' syndrome, and to create high-quality and socially relevant work, researchers would require room and time for reflection and thoroughly understanding the intricacies of the complex socio-technical system that is BGP and, ultimately, the Internet. However, such slow scholarship is not compatible with the ever-increasing demands of neo-liberal universities [84].

5.4 Limitations

Our study included 13 participants from nine countries, with over half (7/13) based in Europe. While this geographic diversity is notable, the findings are not intended to be generalizable to the global population of network operators. As a qualitative study, our goal was to explore operators' perspectives in depth; however, the predominantly European and male participant pool may unintentionally foreground a male- and Eurocentric perspective.

While qualitative research is inherently subjective, we treated researcher–participant intersubjectivity as an analytic asset [46]. Participation was voluntary and not financially incentivized to support candid, interest-driven responses, and anonymity and confidentiality were maintained throughout the study. Finally, since our approach relied on participant

[12] https://ripe86.ripe.net/archives/video/1119/

[13] See, also, the U.S. government's actions against language concerning equitable participation and rights in grant applications and papers.

inputs and words, this leaves room for the use of LLM assistance. To mitigate this, we kept the conversations semi-formal so that people felt enabled to respond in the same way.

6 Industry Perspectives: Why BGP is Different

Here we briefly discuss related work on the academia-industry gap and operators' perspective related studies. For references to BGP security related studies, please see Sec. 2.

Over the past decade, work on experts' perspectives has kept up its growth after having been neglected for a long time [58]. Work around experts, industry, and academic contributions can generally be clustered into two groups: *i)* Work studying a specific artifact, or implementation, e.g., through usability studies, or, *ii)* Work investigating a broader gap between academia and industry.

6.1 Industry Perspectives on Specific Artifacts

This group of work is either concerned with specific artifacts, or processes, and strives to understand *how* industry experts interact with it, mostly to improve the process/artifact. For example, Acar et al. study how usable cryptographic APIs in common libraries are [1]. Similarly, Krombholz et al. study experts' perspectives on HTTPS, and challenges when deploying HTTPS [66, 67]. On the process side, early work from 2007 on secure development by Woon et al. is a good example, asking why secure development practices are often not implemented in practice [112]. Similarly, more recently in 2022, Braz et al. ask a similar question to better understand how security is considered during code review [17]. Other notable work includes work on operators' perspective on security misconfigurations [32], software update behavior [72], and analysts behavior during malware analysis [113].

6.2 Studying the Academia-Industry Gap

Going from specific artifacts to bridging the gap, a recent work by Reichmann et al. [93] constitutes a hybrid between both categories. While starting from a usability analysis of VeraCrypt, the authors observe a disconnect between academic suggestions and their implementation in practice. Hence, the work then turns towards this specific gap.

More generally, the issue of the perceived academia-industry gap in IT related fields has been discussed for at least a decade. For example, in 2017, Celikkan & Sahin [23] provided perspectives from a general educational-science perspectives, suggesting closer collaboration and more dynamically updated curricula to bridge this gap. Similar to the work by Reichmann [93]–in terms of moving from the artifact to a systemic perspective–Huaman et al. study implementers' perspectives on the overall complexity of the cryptographic ecosystem, specifically observing the inherent (and often contradicting) complexity of standards and recommendations [55]. Similarly, Fischer et al. investigate the challenges for bringing research outputs in the field of cryptography to actual products [40].

6.3 BGP: Same, but different

That there *is* a gap between research and practice in BGP security is out of the question. This gap is, for example, already acknowledged by Kent et al. in 2000 [62], when introducing S-BGP, explicitly noting the challenges academic solutions introduce for implementation and operational consistency.

Earlier work listed above generally works on an assumption that, after all, suggestions from academia will be–and in fact regularly are–improvements. In contrast, we find that for BGP security work, academia does not necessarily know 'best'. This also means that common patterns and solutions towards 'bridging the gap' through education and training [22, 99, 100] are trying to bridge the wrong side of the gap.

Instead, our work aligns closer with findings by Wan et al. from AI-based vulnerability management systems [110], tracing shortcomings in academic proposals back to assumptions made on scalability requirements in practice, a strongly siloed corner-case focus of academic solutions, and often unclear resource and budget requirements.

7 Conclusion

We present the results of a qualitative study on operators' perspectives on academic BGP security research. We find that practitioners do not perceive academic work to sufficiently consider network operators' perspectives and practical requirements when developing research questions and new academic proposals for securing BGP (***RQ1***). Based on our participants' responses we identify how this leads to an industry-academia gap in BGP security, that is amplified by limited practical experience of academics and, as coined by an operator, the *'Ivory Tower Syndrome'* (***RQ2 pt. 1***).

On a more positive note, our participants shared recommendations how academics can bridge this gap (***RQ2 pt. 2***). However, essential recommendations, e.g., collaborating long-term with operators to deepen practical experience, or continuously participating in and contributing to (*'listen not talk'*) operator communities are difficult to implement in an output-driven academic system. This concern is also voiced by operators, who perceiving academic work to not be driven by a genuine pursuit of understanding and meaningful improvement, but instead by attempts to quickly generate output to satisfy funding, career, or graduation requirements. As such, we argue that careful and impactful engagement with BGP and BGP security requires a more considerate approach to research and academic work, that leaves room for the necessary community engagement and practical engagement with the subject.

Ethical Considerations

We ensured that high ethical standards were constantly upheld during this study. We submitted our research design, data management plan and the planned informed consent form (see Apd. A) to our institution's ethics review board, following which the project was granted approval. In addition, we present below the stakeholder-based ethics considerations, based on which we decided to pursue this line of research.

Study participants The main stakeholder in this study are those who volunteered to participate. Ensuring the privacy and confidentiality of participants was central to our study design. We set up an internally-hosted instance of Mattermost[14] for conducting the online focus groups, which was administered by one of the authors, allowing to improve participant's privacy by enabling pseudoanonymization during the online focus groups and data analysis. All personal and sensitive data, such as participant names and contact information, were not shared with third parties and deleted after project completion. In addition, we formulated a code of conduct (see Apd. B) to foster a respectable environment for the discussions. The participants were informed of the data collection, data processing and data storage procedures–along with the project summary (see Apd. C)–via the informed consent forms. Consent forms (see Apd. A) were provided to participants in advance, at the time of initial contact for interview scheduling.

To mitigate any possible distress arising from discussing workplace experiences related to network operations and security, participants were informed (see Apd. A) that they can refuse to answer any questions and withdraw from the study at any time. In addition, a code of conduct (see Apd. B) was shared during each focus group to foster a respectable group environment. Finally, to mitigate risks associated with data breaches, all data was stored on internal servers. We deidentified the focus group transcripts after data collection and deleted the original transcripts. We also deleted all PII (email addresses and signed consent forms) after project completion.

Computer security researchers While not directly involved in the study as participants, our work refers to security researchers in several ways, making them a secondary stakeholder in this study. In particular, our study is motivated by the discussion of BGP security research that might be disconnected from practical relevance. However, we made sure to not point fingers by mentioning any specific work but discuss this disconnect in general. In addition, the findings and recommendations presented in this study are largely aimed at the academic community, i.e. security researchers. We present these recommendations in particular to those researchers who seek to develop solutions that are practically viable for network operations.

[14] https://mattermost.com/

Research team Since our team comprises computer security researchers, we also consider ourselves a stakeholder in this study. Participant critiques of academic research practices and academic community in general can create a psychological burden on the research team. To mitigate this, the researchers relied on other team members for support and approached participant input as an opportunity for learning and growth. We encourage our fellow researchers, similarly, to see the participant insights and recommendations presented in this work as a different perceptive that can offer opportunities for reflection and growth.

Open Science

Our study dataset comprises transcripts of our focus group conversations. These transcripts, while deidentified, may contain personally-sensitive information such as participants' pseudonyms or specific workplace related information or anecdotes. During our study, participants were informed that their input will only be anonymously quoted in the research outputs, and the deidentified transcripts will not be shared beyond the study team and will be deleted one year after project completion. To ensure high ethical standards, and prevent any harm to our research participants, we cannot share our qualitative dataset. However, our qualitative codebook created based on interview transcripts is shared in App. E.

References

[1] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky. "Comparing the usability of cryptographic apis". In: *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2017.

[2] H. Alvestrand and R. Housley. *IESG Procedures for Handling of Independent and IRTF Stream Submissions*. RFC 5742. IETF, Dec. 2009. URL: http://tools.ietf.org/rfc/rfc5742.txt.

[3] M. Apostolaki, A. Zohar, and L. Vanbever. "Hijacking bitcoin: Routing attacks on cryptocurrencies". In: *2017 IEEE symposium on security and privacy (SP)*. IEEE. 2017.

[4] A. Azimov, E. Bogomazov, R. Bush, K. Patel, and K. Sriram. *Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages*. RFC 9234. IETF, May 2022. URL: http://tools.ietf.org/rfc/rfc9234.txt.

[5] A. Azimov, E. Bogomazov, R. Bush, K. Patel, J. Snijders, and K. Sriram. *BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects*. Internet-Draft draft-ietf-sidrops-aspa-verification-22. Work in Progress. Internet Engineering Task Force, Mar. 2025. 20 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/22/.

[6] F. Baker and P. Savola. *Ingress Filtering for Multihomed Networks*. RFC 3704. IETF, Mar. 2004. URL: http://tools.ietf.org/rfc/rfc3704.txt.

[7] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker. "Low-resource routing attacks against Tor". In: *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. 2007.

[8] R. Bellman. "On a routing problem". In: *Quarterly of applied mathematics* 16.1 (1958).

[9] R. Beverly and S. Bauer. “The Spoofer project: Inferring the extent of source address filtering on the Internet”. In: *Usenix Sruti*. 2005.

[10] H. Birge-Lee, Y. Sun, A. Edmundson, J. Rexford, and P. Mittal. “Bamboozling certificate authorities with {BGP}”. In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018.

[11] S. Bortzmeyer. “Le Pakistan pirate YouTube”. In: *Blog de Stéphane Bortzmeyer* (2008).

[12] S. Bradner. *The Internet Standards Process – Revision 3*. RFC 2026. IETF, Oct. 1996. URL: http://tools.ietf.org/rfc/rfc2026.txt.

[13] V. Braun and V. Clarke. “Reflecting on reflexive thematic analysis”. In: *Qualitative research in sport, exercise and health* 11.4 (2019).

[14] V. Braun and V. Clarke. “One size fits all? What counts as quality practice in (reflexive) thematic analysis?” In: *Qualitative research in psychology* 18.3 (2021).

[15] V. Braun and V. Clarke. *Conceptual and design thinking for thematic analysis. Qualitative Psychology, 9 (1), 3–26*. 2022.

[16] V. Braun and V. Clarke. “Thematic analysis”. In: *Encyclopedia of quality of life and well-being research*. 2024.

[17] L. Braz and A. Bacchelli. “Software security during modern code review: the developer’s perspective”. In: *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2022.

[18] R. Bush. *Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)*. RFC 7115. IETF, Jan. 2014. URL: http://tools.ietf.org/rfc/rfc7115.txt.

[19] K. Butler, T. Farley, P. McDaniel, and J. Rexford. “A survey of BGP security”. In: *ACM, draft version* 5 (2004).

[20] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford. “A survey of BGP security issues and solutions”. In: *Proceedings of the IEEE* 98.1 (2009).

[21] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford. “A Survey of BGP Security Issues and Solutions”. In: *Proceedings of the IEEE* 98.1 (2010). DOI: 10.1109/JPROC.2009.2034031.

[22] J. C. Carver and R. Prikladnicki. “Industry–Academia Collaboration in Software Engineering”. In: *IEEE Software* 35.5 (2018). DOI: 10.1109/MS.2018.3571250.

[23] U. Celikkan and Y. Sahin. “Perceived information gap between academia and industry: A qualitative study”. In: *EDULEARN17 Proceedings*. IATED. 2017.

[24] T. Chung, E. Aben, T. Bruijnzeels, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, R. v. Rijswijk-Deij, J. Rula, et al. “RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins”. In: *Proceedings of the Internet Measurement Conference*. 2019.

[25] S. Crocker. *New Host-Host Protocol*. RFC 33. IETF, Feb. 1970. URL: http://tools.ietf.org/rfc/rfc0033.txt.

[26] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. “Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks”. In: *Proceedings of the 2014 Conference on Internet Measurement Conference*. 2014.

[27] T. Dai, P. Jeitner, H. Shulman, and M. Waidner. “From IP to transport and beyond: cross-layer attacks against applications”. In: *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 2021.

[28] T. Dai, P. Jeitner, H. Shulman, and M. Waidner. “The hijackers guide to the galaxy:{Off-Path} taking over internet resources”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021.

[29] L. Daigle and I. A. Board. *The RFC Series and RFC Editor*. RFC 4844. IETF, July 2007. URL: http://tools.ietf.org/rfc/rfc4844.txt.

[30] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 8200. IETF, July 2017. URL: http://tools.ietf.org/rfc/rfc8200.txt.

[31] C. A. DiCamillo, R. D. Schmidt, S. T. Gonzalez, S. M. St. George, and V. E. Horigian. “Asynchronous Online Focus Groups: An Effective Approach to Engage Young Adult Women in Discussions on Mental Health Problems”. In: *International journal of qualitative methods* 25 (2026).

[32] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig. “Investigating system operators’ perspective on security misconfigurations”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018.

[33] J. Durand, I. Pepelnjak, and G. Doering. *BGP Operations and Security*. RFC 7454. IETF, Feb. 2015. URL: http://tools.ietf.org/rfc/rfc7454.txt.

[34] P. Ferguson and D. Senie. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. RFC 2827. IETF, May 2000. URL: http://tools.ietf.org/rfc/rfc2827.txt.

[35] T. Fiebig. “Crisis, Ethics, Reliability & a measurement. network: Reflections on Active Network Measurements in Academia”. In: *Proceedings of the Applied Networking Research Workshop*. 2023.

[36] T. Fiebig. “Report on the Security State of Networks of Max-Planck Institutes: Findings and Recommendations”. In: (2023).

[37] T. Fiebig and D. Aschenbrenner. “13 propositions on an internet for a" burning world"”. In: *Proceedings of the ACM SIGCOMM Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet*. 2022.

[38] T. Fiebig, S. Gürses, C. H. Gañán, E. Kotkamp, F. Kuipers, M. Lindorfer, M. Prisse, and T. Sari. “Heads in the Clouds? Measuring Universities’ Migration to Public Clouds: Implications for Privacy & Academic Freedom”. In: *Proceedings on privacy enhancing technologies symposium*. 2. 2023.

[39] T. Fiebig, F. Lichtblau, F. Streibelt, T. Krüger, P. Lexis, R. Bush, and A. Feldmann. “Learning from the past: designing secure network protocols”. In: *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden* (2018).

[40] K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, and A. Sasse. “The challenges of bringing cryptography from research papers to products: Results from an interview study with experts”. In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024.

[41] O. Fonseca, Í. Cunha, E. Fazzion, W. Meira, B. A. da Silva, R. A. Ferreira, and E. Katz-Bassett. “Identifying networks vulnerable to IP spoofing”. In: *IEEE Transactions on Network and Service Management* 18.3 (2021).

[42] V. Fuller and T. Li. *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*. RFC 4632. IETF, Aug. 2006. URL: http://tools.ietf.org/rfc/rfc4632.txt.

[43] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman. “Are We There Yet? On RPKI’s Deployment and Security”. In: *NDSS*. 2017.

[44] T. Gillespie. “Engineering a Principle: ‘End-to-End’in the Design of the Internet”. In: *Social Studies of Science* 36.3 (2006).

[45] V. Giotsas and S. Zhou. “Valley-free violation in internet routing—analysis based on bgp community data”. In: *2012 IEEE International Conference on Communications (ICC)*. IEEE. 2012.

[46] B. Gough and A. Madill. “Subjectivity in psychological science: from problem to prospect.” In: *Psychological methods* 17.3 (2012).

[47] J. Halpern, L. Daigle, and O. Kolkman. *RFC Streams, Headers, and Boilerplates*. RFC 7841. IETF, May 2016. URL: http://tools.ietf.org/rfc/rfc7841.txt.

[48] J. Hawkinson and T. Bates. *Guidelines for creation, selection, and registration of an Autonomous System (AS)*. RFC 1930. IETF, Mar. 1996. URL: http://tools.ietf.org/rfc/rfc1930.txt.

[49] A. Heffernan. *Protection of BGP Sessions via the TCP MD5 Signature Option*. RFC 2385. IETF, Aug. 1998. URL: http://tools.ietf.org/rfc/rfc2385.txt.

[50] T. Heinrich. *Hands-On the Network: Our Experience with RouterLab*. Apr. 2025. URL: https://labs.ripe.net/author/tiago-heinrich/hands-on-the-network-our-experience-with-routerlab/.

[51] R. Hiran, N. Carlsson, and P. Gill. "Characterizing large-scale routing anomalies: A case study of the china telecom incident". In: *Passive and Active Measurement: 14th International Conference, PAM 2013, Hong Kong, China, March 18-19, 2013. Proceedings 14*. Springer. 2013.

[52] T. Holterbach, T. Alfroy, A. Phokeer, A. Dainotti, and C. Pelsser. "A system to detect Forged-Origin BGP hijacks". In: *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. 2024.

[53] R. Housley, D. Crocker, and E. Burger. *Reducing the Standards Track to Two Maturity Levels*. RFC 6410. IETF, Oct. 2011. URL: http://tools.ietf.org/rfc/rfc6410.txt.

[54] R. Housley, J. Curran, G. Huston, and D. Conrad. *The Internet Numbers Registry System*. RFC 7020. IETF, Aug. 2013. URL: http://tools.ietf.org/rfc/rfc7020.txt.

[55] N. Huaman, J. Suray, J. H. Klemmer, M. Fourné, S. Klivan, I. Trummová, Y. Acar, and S. Fahl. ""You have to read 50 different RFCs that contradict each other": An Interview Study on the Experiences of Implementing Cryptographic Standards". In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024.

[56] G. Huston. *Autonomous System (AS) Number Reservation for Documentation Use*. RFC 5398. IETF, Dec. 2008. URL: http://tools.ietf.org/rfc/rfc5398.txt.

[57] G. Huston, M. Rossi, and G. Armitage. "Securing BGP—A literature survey". In: *IEEE Communications Surveys & Tutorials* 13.2 (2010).

[58] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig. "Human factors in security research: Lessons learned from 2008-2018". In: *arXiv preprint arXiv:2103.13287* (2021).

[59] M. Kaur, S. Parkin, M. Janssen, and T. Fiebig. ""I needed to solve their overwhelmness": How System Administration Work was Affected by COVID-19". In: *Proceedings of the ACM on Human-Computer Interaction* 6.CSCW2 (2022).

[60] M. Kaur, H. Sri Ramulu, Y. Acar, and T. Fiebig. ""Oh yes! overpreparing for meetings is my jam:)": The Gendered Experiences of System Administrators". In: *Proceedings of the ACM on Human-Computer Interaction* 7.CSCW1 (2023).

[61] S. Kent, C. Lynn, and K. Seo. "Secure border gateway protocol (S-BGP)". In: *IEEE Journal on Selected areas in Communications* 18.4 (2000).

[62] S. T. Kent, C. Lynn, J. Mikkelson, and K. Seo. "Secure Border Gateway Protocol (S-BGP)-Real World Performance and Deployment Issues." In: *NDSS*. 2000.

[63] S. K. Khadka, S. Bayhan, R. Holz, and C. Hesselman. "Assessing the security of Internet paths: A case study of Dutch critical infrastructures". In: *Proceedings of the 2024 Applied Networking Research Workshop*. 2024.

[64] O. Kolkman, S. Bradner, and S. Turner. *Characterization of Proposed Standards*. RFC 7127. IETF, Jan. 2014. URL: http://tools.ietf.org/rfc/rfc7127.txt.

[65] E. Krol and E. Hoffman. *FYI on "What is the Internet?"* RFC 1462. IETF, May 1993. URL: http://tools.ietf.org/rfc/rfc1462.txt.

[66] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. Von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA"–End User and Administrator Mental Models of HTTPS". In: *2019 IEEE Symposium on security and privacy (SP)*. IEEE. 2019.

[67] K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl. ""I Have No Idea What I'm Doing"-On the Usability of Deploying {HTTPS}". In: *26th USENIX Security Symposium (USENIX Security 17)*. 2017.

[68] K. LaForge, M. Gray, E. Stack, C. J. Livingston, and C. Hildebran. "Using asynchronous online focus groups to capture healthcare professional opinions". In: *International Journal of Qualitative Methods* 21 (2022).

[69] M. Lepinski and S. Kent. *An Infrastructure to Support Secure Internet Routing*. RFC 6480. IETF, Feb. 2012. URL: http://tools.ietf.org/rfc/rfc6480.txt.

[70] M. Lepinski and K. Sriram. *BGPsec Protocol Specification*. RFC 8205. IETF, Sept. 2017. URL: http://tools.ietf.org/rfc/rfc8205.txt.

[71] M. Lepinski and K. Sriram. *BGPSEC protocol specification*. Tech. rep. 2017.

[72] F. Li, L. Rogers, A. Mathur, N. Malkin, and M. Chetty. "Keepers of the machines: Examining how system administrators manage software updates for multiple machines". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019.

[73] Q. Li, J. Liu, Y.-C. Hu, M. Xu, and J. Wu. "Bgp with bgpsec: Attacks and countermeasures". In: *IEEE Network* 33.4 (2018).

[74] W. Li, Z. Lin, M. I. Ashiq, E. Aben, R. Fontugne, A. Phokeer, and T. Chung. "RoVista: Measuring and analyzing the route origin validation (ROV) in RPKI". In: *Proceedings of the 2023 ACM on Internet Measurement Conference*. 2023.

[75] F. Lichtblau, F. Streibelt, T. Krüger, P. Richter, and A. Feldmann. "Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses". In: *Proceedings of the 2017 Internet Measurement Conference*. 2017.

[76] T. A. Limoncelli, T. Limoncelli, C. J. Hogan, and S. R. Chalup. *The practice of system and network administration*. Pearson Education, 2007.

[77] J. Lindvall and D. Rueda. "The insider–outsider dilemma". In: *British Journal of Political Science* 44.2 (2014).

[78] Q. Lone, M. Luckie, M. Korczyński, H. Asghari, M. Javed, and M. Van Eeten. "Using crowdsourcing marketplaces for network measurements: The case of spoofer". In: *2018 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE. 2018.

[79] Q. Lone, M. Luckie, M. Korczyński, and M. Van Eeten. "Using loops observed in traceroute to infer the ability to spoof". In: *Passive and Active Measurement: 18th International Conference, PAM 2017, Sydney, NSW, Australia, March 30-31, 2017, Proceedings 18*. Springer. 2017.

[80] D. Medhi and K. Ramasamy. *Network routing: algorithms, protocols, and architectures*. Morgan kaufmann, 2017.

[81] A. Milolidakis, T. Bühler, K. Wang, M. Chiesa, L. Vanbever, and S. Vissicchio. "On the effectiveness of bgp hijackers that evade public route collectors". In: *IEEE Access* 11 (2023).

[82] A. Mitseva, A. Panchenko, and T. Engel. "The state of affairs in BGP security: A survey of attacks and defenses". In: *Computer Communications* 124 (2018).

[83] C. Morris, A. Herzberg, B. Wang, and S. Secondo. "Bgp-isec: Improved security of internet routing against post-rov attacks". In: *Network and Distributed System Security (NDSS) Symposium 2024*. Internet Society. 2024.

[84] A. Mountz, A. Bonds, B. Mansfield, J. Loyd, J. Hyndman, M. Walton-Roberts, R. Basu, R. Whitson, R. Hawkins, T. Hamilton, et al. "For slow scholarship: A feminist politics of resistance through collective action in the neoliberal university". In: *ACME: An International Journal for Critical Geographies* 14.4 (2015).

[85] L. Müller, M. Luckie, B. Huffaker, K. Claffy, and M. Barcellos. "Challenges in inferring spoofed traffic at IXPs". In: *Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies*. 2019.

[86] S. Munot, T. Fiebig, and M. Kaur. ""You just wanna sign on the dotted line and hope for the best": Navigating the Cloudscapes of Higher Education". In: *Proceedings of the ACM on Human-Computer Interaction* 9.CSCW1 (2025).

[87] S. L. Murphy. *RFC 4272: BGP Security Vulnerabilities Analysis*. 2006.

[88] B. Al-Musawi, P. Branch, and G. Armitage. "BGP anomaly detection techniques: A survey". In: *IEEE Communications Surveys & Tutorials* 19.1 (2016).

[89] T. O. Nyumba, K. Wilson, C. J. Derrick, and N. Mukherjee. "The use of focus group discussion methodology: Insights from two decades of application in conservation". In: *Methods in Ecology and evolution* 9.1 (2018).

[90] L. Pan, J. Yang, L. He, Z. Wang, L. Nie, G. Song, and Y. Liu. "Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels". In: (2023).

[91] J. Postel. *Internet Protocol*. RFC 791. IETF, Sept. 1981. URL: http://tools.ietf.org/rfc/rfc0791.txt.

[92] L. Prehn, F. Lichtblau, and A. Feldmann. "When wells run dry: the 2020 IPv4 address market". In: *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*. 2020.

[93] F. Reichmann, A. Buckmann, K. Fischer, M. A. Sasse, and A. Naiakshina. "Bridging the Gap Between Usable Security Research and Open-Source Practice-Lessons From a Long-Term Engagement With VeraCrypt". In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 2025.

[94] Y. Rekhter and T. Li. *A Border Gateway Protocol 4 (BGP-4)*. RFC 1771. IETF, Mar. 1995. URL: http://tools.ietf.org/rfc/rfc1771.txt.

[95] Y. Rekhter, T. Li, and S. Hares. *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. IETF, Jan. 2006. URL: http://tools.ietf.org/rfc/rfc4271.txt.

[96] A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett, T. C. Schmidt, and M. Wählisch. "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering". In: *ACM SIGCOMM Computer Communication Review* 48.1 (2018).

[97] C. Rossow. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." In: *NDSS*. 2014.

[98] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel, and D. Mohaisen. "RouteChain: Towards blockchain-based secure and efficient BGP routing". In: *Computer Networks* 217 (2022).

[99] A. Sandberg, L. Pareto, and T. Arts. "Agile Collaborative Research: Action Principles for Industry-Academia Collaboration". In: *IEEE Software* 28.4 (2011). DOI: 10.1109/MS.2011.49.

[100] A. Sannö, A. E. Öberg, E. Flores-Garcia, and M. Jackson. "Increasing the impact of industry–academia collaboration through co-production". In: *Technology Innovation Management Review* 9.4 (2019).

[101] P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos. "A survey among network operators on BGP prefix hijacking". In: *ACM SIGCOMM Computer Communication Review* 48.1 (2018).

[102] K. Sriram, D. Montgomery, and J. Haas. *Enhanced Feasible-Path Unicast Reverse Path Forwarding*. RFC 8704. IETF, Feb. 2020. URL: http://tools.ietf.org/rfc/rfc8704.txt.

[103] K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, and B. Dickson. *Problem Definition and Classification of BGP Route Leaks*. RFC 7908. IETF, June 2016. URL: http://tools.ietf.org/rfc/rfc7908.txt.

[104] S. R. C. Thomas A. Limoncelli Christina J. Hogan. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT (3rd Edition)*. Addison-Wesley, 2017.

[105] J. Touch, A. Mankin, and R. Bonica. *The TCP Authentication Option*. RFC 5925. IETF, June 2010. URL: http://tools.ietf.org/rfc/rfc5925.txt.

[106] P.-A. Vervier, O. Thonnard, and M. Dacier. "Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks." In: *NDSS*. 2015.

[107] F. Voutsas, J. Violos, and A. Leivadeas. "Mitigating alert fatigue in cloud monitoring systems: A machine learning perspective". In: *Computer Networks* 250 (2024).

[108] M. Wählisch, O. Maennel, and T. C. Schmidt. "Towards detecting BGP route hijacking using the RPKI". In: *SIGCOMM Comput. Commun. Rev.* 42.4 (Aug. 2012). DOI: 10.1145/2377677.2377702. URL: https://doi.org/10.1145/2377677.2377702.

[109] M. Wählisch, O. Maennel, and T. C. Schmidt. "Towards detecting BGP route hijacking using the RPKI". In: *ACM SIGCOMM Computer Communication Review* 42.4 (2012).

[110] S. Wan, J. Saxe, C. Gomes, S. Chennabasappa, A. Rath, K. Sun, and X. Wang. "Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia". In: *arXiv preprint arXiv:2405.02435* (2024).

[111] X. Wang, Z. Liu, Q. Li, Y. Guo, S. Ling, J. Zhan, Y. Xu, K. Xu, and J. Wu. "Secure Inter-domain Routing and Forwarding via Verifiable Forwarding Commitments". In: *arXiv preprint arXiv:2309.13271* (2023).

[112] I. M. Woon and A. Kankanhalli. "Investigation of IS professionals' intention to practise secure development of applications". In: *International Journal of Human-Computer Studies* 65.1 (2007).

[113] R. Yamagishi, S. Fujii, S. Yasuda, T. Sato, and A. A. Hasegawa. "Collaborative Work in Malware Analysis: Understanding the Roles and Challenges of Malware Analysts". In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 2025.

[114] K. Yamori. "Revisiting the concept of normalcy bias." In: *Japanese Journal of Experimental Social Psychology* (2009).

[115] M. Zwaanswijk and S. van Dulmen. "Advantages of asynchronous online focus groups and face-to-face focus groups as perceived by child, adolescent and adult participants: a survey study". In: *BMC research notes* 7 (2014).

A Informed Consent Form

A.1 General Agreement - Research Goals, Participation Tasks & Voluntary Participation

1. I have read and understood the study information or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I

can withdraw from the study at any time, without having to give a reason.
3. I understand that taking part in the study involves:
    - Engaging in a focus group discussion conducted via a secure digital platform (Mattermost)
    - Having the chat transcripts from this discussion recorded and preserved for research purposes

A.2 Potential Risks of Participating (Including Data Protection)

1. I understand that taking part in the study also involves collecting specific personally identifiable information (PII) and associated personally identifiable research data (PIRD) such as:
    - Email Address
    - Job Title and Description
    - Educational Background
    - Gender Identity
2. I understand that the following steps will be taken to minimise the threat of a data breach, and protect my identity in the event of such a breach:
    - All data collected including the chat transcripts and PII will only be stored internally on protected servers
3. I understand that personal information collected about me that can identify me will not be shared beyond the study team.
4. I understand that the (identifiable) personal data I provide will be destroyed after the completion of the study

A.3 Research Publication, Dissemination and Application

1. I understand that after the research study the de-dentified information I provide will be used for:
    - Comparing theoretical concepts with practical applications in professional settings
    - Analyzing potential gaps between academic literature and real-life operations in the field
    - Identifying areas where academic research may need to be updated or expanded based on current industry practices
    - Developing insights that could bridge the divide between theoretical knowledge and practical implementation
    - Contributing to the body of knowledge in [specific field or industry] by highlighting real-world perspectives
    - Informing future research directions and potentially influencing curriculum development in relevant academic programs
2. I agree that my responses, views or other input can be quoted anonymously in research outputs

B Code of Conduct

To ensure a productive and respectful environment for all participants, please adhere to the following guidelines:

1. Respect and Privacy:
- Treat all participants with respect and courtesy.
- Disagree respectfully if you have a different viewpoint.
2. Participation:
- Log in during the study period (typically 1 week) to respond to questions and engage with other participants.
- We encourage you to share your honest insights and experiences in detail as well as engage in group discussions as it will be helpful for collecting rich qualitative data for our study.
- We encourage you to respond to other participants' comments, building on ideas or offering different perspectives.
- You may ignore a question if you do not feel comfortable in responding to it.
- Use the platform's features to indicate agreement (e.g. with emojis) or to quote others' responses when relevant.
- Please participate at your convenience and try to engage regularly throughout the study period.
- If you do not feel comfortable or wish to withdraw from the study, please inform the moderator.
3. Content:
- Avoid sharing offensive, discriminatory, or inappropriate content.
- Do not promote personal businesses or agendas unrelated to the research topic.
- We reserve the right to remove anyone from the group in case of the following:
    - Disrespectful communication towards others participants
    - Verbal/written abuse towards others participants
    - Bullying or intimidation
    - Harassment or discrimination (gender, race, sexual, etc)
4. Support:
- Use the private messaging feature if you need to communicate directly with the moderators about sensitive issues.
- If you encounter technical issues, you may contact Aleeza using the private messaging feature.

By participating in this focus group, you agree to abide by this code of conduct.

C Project Description in the Consent Form

The purpose of this research study is to review both academic literature and practical experiences of network operators with a focus on BGP security. The data collected will be used to identify the potential gap between these publications and the day-to-day experiences of network operators.

D Focus Group Structure

To begin the focus group discussions, the participants were first welcomed and briefed about the aim of the study. Following this, the moderators were introduced. Then, we described how the study would be carried out and shared the code of conduct with the participants to ensure the discussion ran smoothly. Further, we asked the participants to optionally provide short, anonymous introductions without revealing any PII. Finally, laying the foundation for our discussion, we were prepared to pose the questions stated below. We followed a semi-structured interview approach, i.e. the set of questions presented below acted as a guide and were **not** strictly followed. The follow-up questions are **optional** and highly dependent on the participants' responses.

1. In your day-to-day work, particularly regarding BGP and routing security in your organization's network, what are the main challenges you encounter?

   Optional follow-up prompts:

   - Could you please elaborate on these issues with some examples?
   - If not already mentioned- Do you encounter BGP Security misconfigurations? If already mentioned, then go to follow-ups:
   - What factors do you think contribute to these misconfigurations?
   - If yes, how often and how were they handled?

2. Do you think academic research papers proposing BGP security solutions adequately address the types of challenges /misconfigurations you encounter in practice?

   Optional follow-up prompts:

   - Only ask if yes, can you provide examples where academic research has been particularly useful in your practice?
   - If no- why not? can you please elaborate?

3. What are the key factors that influence your decision to adopt or reject new BGP/ routing security techniques/solutions?

   Optional follow-up prompts:

   - If academic research is not brought up- Do you consult/leverage academic research to make business decisions and enhance your practical tasks?
   - If not, what prevents you from doing so?
   - If yes, How do you consult or leverage academic research in your work? Or in what ways does it help you?
   - How relevant do you find the theories, frameworks, and models presented in academic literature to the practical problems you encounter in your organization?

4. What do you think the research community could do differently to make their BGP security studies more relevant and applicable for practitioners like yourself?

   Optional follow-up prompts:

   - What changes would you like to see in terms of research focus, methodology, dissemination, or collaboration?
   - How, in your opinion, can communication and collaboration between researchers and network operators be improved?
   - How, in your opinion, can academics better understand and incorporate operational realities in their work?

Following the questions, we concluded the focus group by thanking the participants for their participation and valuable feedback. The participants were provided with the researcher's email address in case they wanted to contact us with further inquiries or share additional thoughts.

E Focus Group Invite

Fig. 1 shows the flyer that we created to attract participants to our study.

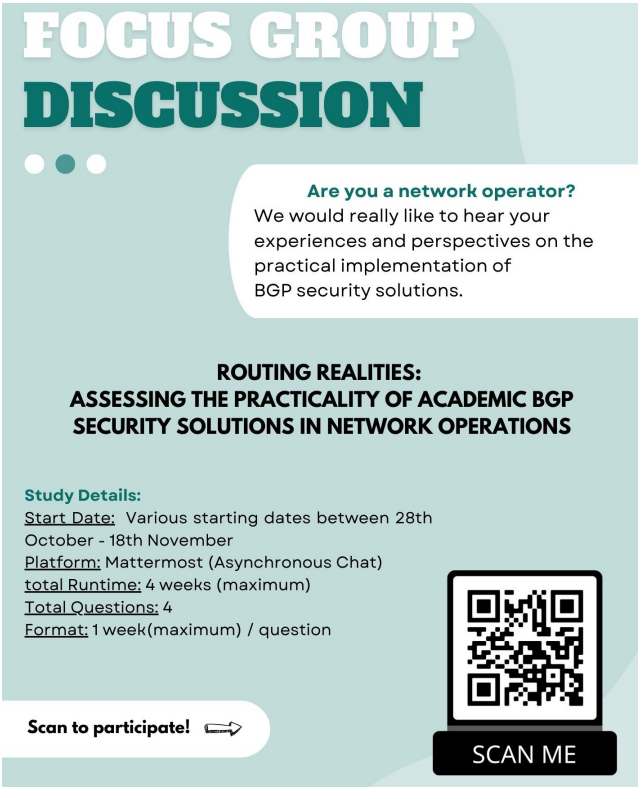


Figure 1: Flyer to Attract Participants

Table 3: Codebook Overview

Theme: ***Operational Realities***

Changing Face of Expertise		**Decision Making in BGP**		**Standards**		**Outsourcing BGP**	
Cost cutting	1	Deadlines drive action	1	Security requirements from frameworks	2	BGP is outsourced to third party	1
Distrust in non operational decision makers	1	Operational caution due to fear of network disruption	3	Reliance on established standards	3	Outsourcing due to lack of BGP knowledge within the organization	1
Reliance on basic BGP setups in junior-led networks	1	Commercial interest of providers may influence BGP configs	1	MANRS	2		
		Skepticism Toward "Improvements"	3				
		Investment vs. cost mindset	1				

Theme: ***Challenges in BGP***

Consequences of Misconfigurations		**Knowledge Factor**		**Organizational Web**		**Proposed Solutions**	
Blockhole	1	Educational gaps in effective BGP usage	3	Testing BGP in labs is a challenge	1	BGP Training is must	1
Outage due to unfiltered session	1	Lack of basic BGP knowledge	2	Unclear administrative ownership	1	Structured debugging approach to BGP	1
Service disruption	1	Economic constraints are a barrier for knowledge acquisition	1	Working around vendor limitations in new deployments	2	Post-incident audit	1
Brute Force Attack	1			Addressing legacy config issues	1	Static filtering	1
						System-based fixes	1
						Automation	3
Uncategorized:							
Increase awareness among people	1	Typing Errors	2	Misconfigured RPKI	2	Complexity in BGP	2
Insufficient support for security in BGP	1	Route leaks	2	Stuck routes	1	Inter-AS vs. intra-AS routing	1

Theme: ***Sources of BGP technologies & Factors Affecting their Adoption***

Sources		**Technical/Organizational Factors**				**Human Factors**	
Interpersonal	2	Features and functionalities	1	Automation	2	Behavioral barriers in implementing impractical protocol design	1
Learning from others	5	Flexibility and adaptability	2	Incident Response and Recovery	1	Extractive ways of knowledge production	1
Involvement with the local community	1	Cost	2	Strategic alignment w/ vendor/partner	2	Familiarity bias in adoption of solutions	1
Online	4	Operational Complexity	3	Time/effort it takes	1	Knowledge disparity due to role-specific exposure to networking practices	1
RFCs	2	Security Effectiveness	5	Community and Peer Adoption	1	Variation in expertise leads to inconsistent problem solving	1
Mailinglists	1	Vendor & Documentation Support	4	Probability of risk involved	1	Subjective adoption of new tech	1
Conferences - RIPE, NOGs	6	Compatibility and Interoperability	2	Good documentation and configuration examples	2		
Vendor documentation	3	Scalability of the solution	2	Business requirements	2		

Theme: ***Views on Research Papers***

Industry solutions might be proprietary in nature	1	Academic papers may/may not be invoked in the decision making process	2	Broad nature of academic papers	2	Operations doesn't care about research	1
Most operators don't consult research papers	4	Operators prefer to read standards like RFCs over research	1	RFCs may or may not be incorporated by Vendors	1	Independent advancement of technology	1
Scale limitations cause inconsideration of academic papers	1	Limited real-world application of academic solutions	1	Views on research papers: Research papers may not have the best format	1	Research papers are too long	1
Research papers don't provide adequate solutions to operational problems	1	Missing centralized knowledge repository	1	Deployment challenges in heterogeneous environments	1	Some exceptions - operators actually implemented solutions	1
Research is a good way to provide structured solutions	1	Views on research papers: Publish for selfish reasons	1				

Theme: ***Gap between Academia and Operations***

Academia has ivory tower syndrome	1	Theory - Practice disconnect	1	Missing practical inclination in research	1	Innovation without practical justification	1
Industry and academia disconnect	2	Authority vs practical experience	1	On-the-job learning	1		

Theme: ***Reasons Behind the Gap***

Implementation Barriers		**Lack of Accessibility**		**Funding Influence**			
Unupdated solutions lose relevance	1	The real barrier is access, not interest	3	Behavioral barriers in implementing impractical protocol design	1		
Solutions proposed by academia require significant changes	2	There exists access barriers to research papers	3	Funding pressure vs. Research integrity	1		
Academic solutions do not easily translate into actionable steps	1	Search engine results don't contain research papers	1	Risk of funding bias in research	1		
Operators prefer actionable workarounds over research	1						

Theme: ***Steps to Bridge the Gap***

Incremental Solutions		**Enhance Communication and Collaboration**		**Optimize Format**		**Practical Relevance**	
More modular and incremental changes	2	Collaborate with experts	1	Improve format of solutions	3	More practical-driven solutions	1
		Collaborate with vendors - Arista, Cisco, etc	1			Integrate academia with the networking community	1
		Involvement with local communities before PhD	1			Talk to small actors	1
		Involve operators early while formulating solutions	2			Simulation tools to mimic presented solutions	1
		Talking to Operators	2			Consensual decision making	1
		Initiatives at RIPE - RACI program support students & young researchers	1				
		Work with IEFT/NANGOG/RIPE	3				
		Understand the needs of the 'real' world	3				