Schengen Routing: A Compliance Analysis

Daniel Dönni, Guilherme Sperb Machado, Christos Tsiaras, Burkhard Stiller

Schengen Routing: A Compliance Analysis

Daniel Dönni, Guilherme Sperb Machado,
Christos Tsiaras, Burkhard Stiller

University of Zurich, Department of Informatics,
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland
doenni|machado|tsiaras|stiller@ifi.uzh.ch

Abstract. Schengen Routing was proposed as a countermeasure to traffic monitoring activities practiced by intelligence agencies. This work here presents the results of a larger-scale measurement performed to quantify Schengen Routing compliance in today's Internet. Based on 3388 TCP, UDP, and ICMP traceroute measurements executed from RIPE Atlas probes located in over 1100 different Autonomous Systems (AS) in the Schengen Area, it was found that 34.5% to 39.7% of these routes are Schengen-compliant, while compliance levels vary from 0% to 80% among countries. Finally, an approach was developed that allows end-users to determine whether a specific route to a host is Schengen-compliant or not.

Keywords: Schengen Routing, Geo-location, Compliance checks

1 Introduction

The affair involving Edward Snowden and the National Security Agency (NSA) in 2013 demonstrated that wiretapping large amounts of Internet traffic data was not only possible, but also applied on a regular basis by various intelligence agencies in violation of privacy laws [13]. However, the controversy only came into broader political debate by the time it was alleged that several European state heads had become victims of the wiretapping activities themselves [2].

In the context of the political and technical debate that followed, the idea of *Schengen Routing* demonstrated to be a possible amendment to protect communications across Europe. The term *Schengen* refers to the treaty targeted at reducing border controls and implementing a harmonized legal framework [9]. Those countries, who signed the Schengen Treaty, form the Schengen Area. Table 1 shows the current Schengen members. It is important to highlight that the Schengen Area is not equivalent to the European Union (EU), since some countries belonging to the EU are not part of Schengen (*e.g.,* United Kingdom), while Schengen also comprises non-EU countries (*e.g.,* Switzerland).

Schengen Routing refers to the practice of routing Internet traffic between hosts located in the Schengen Area, not leaving the borders of countries part of the Schengen Treaty. Such Internet traffic not leaving the Schengen Area is more difficult to be wiretapped by non-Schengen intelligence agencies, since

Table 1. Schengen members as of January 2015

Country Code	Country Name	Country Code	Country Name
AT	Austria	IT	Italy
BE	Belgium	LI	Liechtenstein
CH	Switzerland	LT	Lithuania
CZ	Czech Republic	LU	Luxemburg
DE	Germany	LV	Latvia
DK	Denmark	MT	Malta
EE	Estonia	NL	Netherlands
ES	Spain	NO	Norway
FI	Finland	PL	Poland
FR	France	PT	Portugal
GR	Greece	SE	Sweden
HU	Hungary	SI	Slovenia
IS	Island	SK	Slovakia

the Internet traffic remains still unencrypted. However, this traffic remains still vulnerable to wiretapping activities that may occur within Schengen [16].

An implementation of Schengen routing requires the reconfiguration of routing tables and the renegotiation of transit and peering agreements. The effort required depends significantly on the degree to which current routing already complies with Schengen routing or not. However, there is no previous work available, which measured a Schengen routing compliance through active measurements by analyzing TCP, ICMP, and UDP traffic. Thus, this paper answers the following question: What is the Schengen routing compliance or non-compliance percentage of current traffic among Schengen countries based on the observation of active measurements?

For that a large number of traceroute measurements was executed by applying RIPE Atlas [17] probes located in Autonomous Systems (AS) within Schengen to a well-known host in Switzerland, being part of the Schengen Area. ASes were chosen as the unit of analysis, because ASes are collections of network devices managed by a single administrative authority that can decide to cooperate with government agencies or not. IP addresses of nodes along a network path can be determined by using the traceroute tool. By means of a database, such as GeoLite [10], IP addresses obtained can be related to ASes and countries and, thus, placed in- or outside Schengen. Next to these measurements, a tool termed chkroute has been developed, allowing end-users to find out whether specific routes are Schengen-compliant.

This paper is structured as follows. Section 2 presents related work. The approach applied and evaluations performed are described in Sections 3 and 4, respectively. Section 5 presents the chkroute tool developed. Finally, Section 6 summarizes the work, draws conclusions, and outlines future steps.

2 Related Work

The most detailed work analyzing routes leaving the Schengen Area was performed by [16]. Publically accessible BGP routing tables were obtained and, based on BGP routing entries, a graph of ASes was generated. Based on these graphs, traffic routes were established and analyzed to assess whether traffic between two peers within the Schengen Area would leave the area, thus, pointing on non-compliant Schengen Area routes. It was assumed that an AS belongs to a particular country, if the majority of its allocated Internet Protocol (IP) address space is bound to that country. Therefore, if an AS hosts IP addresses used in countries X, Y, and Z, but more than 50% is allocated to country X, the AS is considered to be located in country X. Such an assumption simplifies the full process of binding ASes to particular countries. However, it may present non-realistic results, since some ASes can present logical connections to several countries that not necessarily reflect the true country of origin of such an AS [19]. Those results show that, *e.g.,* in Belgium, Switzerland, and Spain, more than one third of available routes are operating via ASes located outside the respective country. It is further found that the number of routes leaving the Schengen Area substantially varies among countries, *e.g.,* 0% in Iceland and 35.38% in Belgium.

Another approach analyzed the content of BGP routing tables [12]. The respective outcomes are beneficial due to 3 reasons:

1. BGP looking glasses are servers running specific software designed to retrieve routing information. These servers are found in a considerable number of strategic ASes around the globe.
2. Evaluating BGP routing tables is a passive and, thus, less intrusive approach to form an AS graph.
3. BGP routing tables present a wider view of routing possibilities within each AS.

The major disadvantage of this approach is the lack of certainty that a packet will follow the inferred AS graph to a specific destination as the information may be incomplete or out of date.

Therefore, active measurements involving tools such as, *e.g.*, traceroute, are employed to discover Internet routes that are being used in practice for particular protocols and traffic [3]. Moreover, traceroute measurements are able to (1) reveal multiple routers within an AS and not only an AS-level graph representation, and (2) provide a real time result of the current network hops from source to destination. Thus, Paris traceroute [1] provides a more realistic routing map compared to the classic traceroute tool, solving problems caused by the current vast deployment of load balancers in the Internet. Paris traceroute addresses per-flow load balancers, varying header fields, such as the TCP/ICMP sequence number, the UDP checksum, and the ICMP identifier. The chkroute tool uses Paris traceroute to collect routing information (*i.e.*, IP addresses of network hops) from the source to the destination, and uses the GeoLite database [10] to map IP address ranges to ASes. Table 2 summarizes major characteristics of chkroute and [16] to analyze Schengen Routing compliance.

Table 2. Characteristics comparison of approaches analyzing Schengen Routing compliance

Approaches	Characteristics			
	Based on Active Measurements	**Based on Passive Measurements**	**Uses GeoLite Database**	**Provide Compliance in Real Time**
[16]	no	yes	yes	no
chkroute	no	yes	yes	yes

A major disadvantage of Schengen routing is that Internet traffic remains unencrypted. As a consequence, it is still vulnerable to wiretapping activities from within Schengen. A wide-spread use of end-to-end encryption would resolve this issue [16].

3 Approach

To measure Schengen routing compliance, a larger-scale measurement has been performed. RIPE Atlas [17] was chosen as a measurement platform due to its high AS coverage. ASes were selected for anlysis, because they appear as units controlled by a single administrative entity defining routing policies that has the capability to coopreate with intelligence agencies or not.

3.1 Test-bed Selection

To perform real-life measurements at a larger scale, a suitable test-bed is needed. Test-beds had to meet two requirements to be taken into consideration:

1. The test-bed had to be able to run traceroute measurements to retrieve IP addresses of nodes along a routing path.
2. The test-bed had to provide a high AS coverage in the Schengen Area.

Several test-beds could have been used to perform larger-scale measurements: Planet-Lab [15], EMANICSLab [8], Bismark [18], and RIPE Atlas [17].

On one hand, Planet-Lab [15] and EMANICSLab [8] provide administrative access to the machines and, therefore, allow for full control over all aspects of the experiment. On the other hand, the number of ASes currently covered by these test-beds in Europe is lower when compared to RIPE Atlas: EMANICSLab provide nodes in 11 different ASes, while Planet-Lab provides nodes in 69 ASes. In contrast, RIPE Atlas provides 1306 ASes in the Schengen Area alone. Since Planet-Lab and EMANICSLab nodes are predominantly located in academic and research networks, such a distribution may not necessarily be representative for assessing Schengen routing compliance in the Schengen Internet as a whole [7].

The project Bismark [18] allows researchers to perform measurements from home routers equipped with a modified openWRT firmware [14]. The project cannot be used to study Schengen compliance, since there are only 178 routers globally available, and even less within Schengen as of 2014 [18].

RIPE Atlas is a measurement infrastructure initiated and coordinated by RIPE NCC [17]. According to RIPE's website, "RIPE NCC is building the largest measurement infrastructure ever made" [17]. The RIPE Atlas measurement infrastructure is based on a large number of low-cost measurement nodes given away for free to volunteers willing to host those probes in their private, institutional, or public networks. In exchange for hosting a probe, volunteers get access to measurement statistics and obtain credits that can be traded for running user-defined measurements on the infrastructure. The RIPE Atlas measurement infrastructure provides the best AS coverage by a substantial margin (1306 different ASes in Schengen alone) and was, therefore, chosen for the Schengen routing compliance analysis.

3.2 AS Selection

To determine to what extent traffic complies with Schengen Routing, a list of ASes in the Schengen Area had to be selected. Maxmind provides a free geolocation database named GeoLite [10], which maps IP address ranges to ASes and countries. The respective information is provided in two separate files. The first file contains IP address ranges in a long representation along with an AS number (*e.g.,* 5 10 AS1). The second file contains IP address ranges in a long representation along with a country code (*e.g.,* 5 10 CH). Based on this information, the number of IP addresses per AS and country was calculated (*e.g.,* AS1 has 10 - 5 + 1 = 6 IP addresses in CH (Switzerland)). These AS and country ranges did not always match and had to be divided into matching subranges in these cases. The logic for calculating the number of IP addresses per country remained the same. ASes were included in the measurement effort, if they had at least one IP address in a Schengen country. The resulting number of ASes in the Schengen Area was 9967 (*cf.* Table 3).

Table 3. Number of ASes after results processing (T: TCP, U: UDP, I: ICMP)

Original	Not	No Probes			Failed/Error			Outside Schengen			Remaining		
	Covered	T	U	I	T	U	I	T	U	I	T	U	I
9967	8661	44	47	50	25	24	25	105	104	106	1132	1131	1125

3.3 Measurement Execution

All traceroute measurements were executed using the RIPE Atlas measurement infrastructure. RIPE Atlas allows to specify an AS number as a measurement source and selects a suitable probe with an IP address within the AS automatically. The target IP address of all traceroute measurements was a machine located within Schengen at the premises of University of Zurich, Switzerland (within AS 559). Measurement requests were submitted for all 9967 ASes determined in Section 3.2 for the ICMP, TCP, and UDP protocol in turn. For each protocol, RIPE Atlas performed three traceroute measurements automatically.

These measurements were limited to one target host and three traceroute measurements per protocol because the number of measurements that can be performed on RIPE Atlas is limited by the credit earned by the respective volunteer.

3.4 Results Processing

All results obtained from these measurements were processed in several steps (see Table 3).

1. Measurement requests were submitted for 9967 ASes, out of which 8661 ASes were not covered by RIPE Atlas. They could, therefore, not be taken into consideration.
2. RIPE Atlas could not find suitable probing devices in all ASes covered. These ASes could not be taken into consideration.
3. Some measurements failed or produced invalid results (*e.g.*, error messages rather than measurement data) and were excluded.
4. ASes may have IP address ranges advertised in several countries, especially in ASes with large number of IP address subnets. Because RIPE Atlas chooses IP addresses within the AS at its discrection, an IP address outside the Schengen Area may be selected. Measurements executed from probes having IP addresses located outside the Schengen Area were excluded.

After this results processing, 1132 TCP, 1131 UDP, and 1125 ICMP valid measurements remained for an evaluation. The unprocessed traceroute files obtained from RIPE Atlas measurements have been made publically available [5].

4 Evaluation

These results obtained were classified with respect to Schengen routing compliance as follows:

1. Measurements containing at least one IP address located outside the Schengen Area were classified as "Non-compliant" (NC).
2. Measurements containing only IP addresses inside the Schengen Area were classified as "Compliant" (C).

3. Measurements containing IP addresses for which no country information was available or for which traceroute did not produce an IP address were classified as "Unknown" (U), if all other IP addresses were located within Schengen and "Non-Compliant" otherwise

To determine the geographic location of an IP address, Maxmind's GeoLite database [10] was used, the same database as was used for the AS selection process described in Section 3.2. Figure 1 provides an overview of those results found. Light gray shades represent higher Schengen routing compliance levels while dark gray shades stand for lower compliance levels.

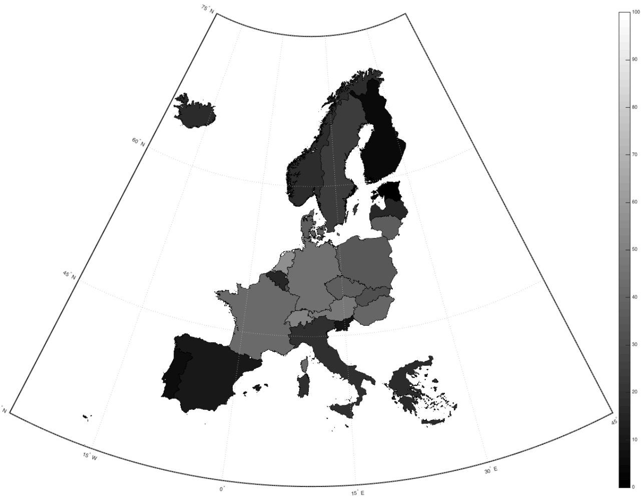


Fig. 1. Schengen routing compliance levels

All detailed results are shown in Table 4. The "R" column ranks the Schengen countries – represented by their ISO code – according to the relative amount of compliant TCP routes. TCP was chosen for ranking, since it is the most frequently used transport protocol in the Internet as of today. The "ASes" column represents the number of ASes for which traceroute measurements have been performed. "T" represents the total number of measurements that were performed for the respective country and protocol. "C", "NC", and "U" show the amount of routes that were compliant, non-compliant, and unknown, respectively. For each of these categories the absolute and relative values are provided.

4.1 Results Analysis

This section discusses the results presented in Table 4, providing insight into compliant, non-compliant, and unknown routes.

Table 4. Schengen Routing compliance analysis

		TCP								UDP								ICMP							
R	ISO	ASes	T	C	C (%)	NC	NC (%)	U	U (%)	ASes	T	C	C (%)	NC	NC (%)	U	U (%)	ASes	T	C	C (%)	NC	NC (%)	U	U (%)
1	LI	5	15	12	80.0%	0	0.0%	3	20.0%	4	12	9	75.0%	3	25.0%	0	0.0%	5	15	12	80.0%	3	20.0%	0	0.0%
2	NL	88	264	148	56.1%	51	19.3%	65	24.6%	88	264	165	62.5%	65	24.6%	34	12.9%	88	264	161	61.0%	68	25.8%	35	13.3%
3	CH	66	198	102	51.5%	30	15.2%	66	33.3%	67	201	126	62.7%	39	19.4%	36	17.9%	66	198	132	66.7%	44	22.2%	22	11.1%
4	AT	56	168	79	47.0%	42	25.0%	47	28.0%	56	168	77	45.8%	59	35.1%	32	19.0%	56	168	89	53.0%	64	38.1%	15	8.9%
5	DE	192	576	253	43.9%	187	32.5%	136	23.6%	189	567	266	46.9%	198	34.9%	103	18.2%	188	564	280	49.6%	210	37.2%	74	13.1%
6	FR	115	345	143	41.4%	91	26.4%	111	32.2%	117	351	155	44.2%	94	26.8%	102	29.1%	114	342	170	49.7%	111	32.5%	61	17.8%
7	HU	20	60	24	40.0%	23	38.3%	13	21.7%	21	63	28	44.4%	26	41.3%	9	14.3%	20	60	27	45.0%	27	45.0%	6	10.0%
8	CZ	81	243	90	37.0%	76	31.3%	77	31.7%	80	240	91	37.9%	83	34.6%	66	27.5%	81	243	102	42.0%	94	38.7%	47	19.3%
9	DK	38	114	42	36.8%	30	26.3%	42	36.8%	38	114	53	46.5%	33	28.9%	28	24.6%	38	114	53	46.5%	36	31.6%	25	21.9%
10	LT	11	33	12	36.4%	12	36.4%	9	27.3%	11	33	13	39.4%	11	33.3%	9	27.3%	11	33	13	39.4%	12	36.4%	8	24.2%
11	PL	78	234	81	34.6%	96	41.0%	57	24.4%	78	234	73	31.2%	108	46.2%	53	22.6%	78	234	78	33.3%	117	50.0%	39	16.7%
12	LU	19	57	18	31.6%	27	47.4%	12	21.1%	19	57	15	26.3%	30	52.6%	12	21.1%	19	57	17	29.8%	33	57.9%	7	12.3%
13	SK	13	39	12	30.8%	13	33.3%	14	35.9%	13	39	12	30.8%	16	41.0%	11	28.2%	13	39	12	30.8%	19	48.7%	8	20.5%
14	SE	58	174	41	23.6%	53	30.5%	80	46.0%	58	174	72	41.4%	63	36.2%	39	22.4%	59	177	69	39.0%	69	39.0%	39	22.0%
15	IT	70	210	39	18.6%	66	31.4%	105	50.0%	70	210	43	20.5%	78	37.1%	89	42.4%	69	207	45	21.7%	77	37.2%	85	41.1%
16	NO	41	123	21	17.1%	51	41.5%	51	41.5%	41	123	17	13.8%	65	52.8%	41	33.3%	40	120	21	17.5%	62	51.7%	37	30.8%
17	GR	24	72	12	16.7%	44	61.1%	16	22.2%	24	72	12	16.7%	40	55.6%	20	27.8%	24	72	12	16.7%	46	63.9%	14	19.4%
	IS	6	18	3	16.7%	7	38.9%	8	44.4%	6	18	3	16.7%	9	50.0%	6	33.3%	6	18	3	16.7%	9	50.0%	6	33.3%
19	LV	13	39	6	15.4%	24	61.5%	9	23.1%	13	39	3	7.7%	29	74.4%	7	17.9%	13	39	3	7.7%	33	84.6%	3	7.7%
20	BE	27	81	12	14.8%	40	49.4%	29	35.8%	27	81	9	11.1%	52	64.2%	20	24.7%	26	78	14	17.9%	58	74.4%	6	7.7%
21	ES	43	129	12	9.3%	56	43.4%	61	47.3%	43	129	14	10.9%	73	56.6%	42	32.6%	42	126	16	12.7%	83	65.9%	27	21.4%
22	SI	16	48	4	8.3%	28	58.3%	16	33.3%	15	45	6	13.3%	35	77.8%	4	8.9%	16	48	6	12.5%	39	81.3%	3	6.3%
23	PT	13	39	2	5.1%	26	66.7%	11	28.2%	13	39	3	7.7%	28	71.8%	8	20.5%	13	39	3	7.7%	31	79.5%	5	12.8%
24	FI	25	75	3	4.0%	42	56.0%	30	40.0%	26	78	3	3.8%	45	57.7%	30	38.5%	26	78	3	3.8%	51	65.4%	24	30.8%
25	EE	11	33	0	0.0%	27	81.8%	6	18.2%	11	33	0	0.0%	27	81.8%	6	18.2%	11	33	0	0.0%	28	84.8%	5	15.2%
	MT	3	9	0	0.0%	6	66.7%	3	33.3%	3	9	0	0.0%	5	55.6%	4	44.4%	3	9	0	0.0%	5	55.6%	4	44.4%
	Total	1132	3396	1171	34.5%	1148	33.8%	1077	31.7%	1131	3393	1268	37.4%	1314	38.7%	811	23.9%	1125	3375	1341	39.7%	1429	42.3%	605	17.9%

Overall compliance levels range from 34.5% in the TCP case, to 37.4% in the UDP, and 39.7% in the ICMP case. The variation among countries is substantial, though, it ranges from 0% (TCP), 0% (UDP) and 0% (ICMP) in the case of Malta (MT) to 80% (TCP), 75% (UDP), and 80% (ICMP) in the case of Liechtenstein (LI). These results show that no country is fully compliant with Schengen routing for those active measurement results.

Overall non-compliance levels range from 33.8% in the TCP case to 38.7% in the UDP and 42.3% in the ICMP case. As it happens for the compliance level, the variation among countries is considerable, it ranges from 0% (TCP) and 20% (ICMP) in the case of Liechtenstein (LI) and 19.4% (UDP) in the case of Switzerland (CH) to 81.8% (TCP), 81.8% (UDP), and 84.8% (ICMP) in the case of Estonia (EE).

The relative amount of unknown routes ranges from 31.7% in the TCP case to 23.9% in the UDP and 17.9% in the ICMP case. The variation among countries is less pronounced for unknown routes compared to compliant and non-compliant routes, in the TCP case results range from 18.2% in Estonia (EE) to 50% in Italy (IT), in the UDP case they range from 0% in Liechtenstein (LI) to 42.4% in Italy (IT), and in the ICMP case results range from 0% in Liechtenstein (LI) to 41.1% in Italy (IT).

The core finding is that compliance levels vary significantly among individual countries and range from a very low to a very high compliance. As a consequence, overall values are of limited use. The second finding is that there is no significant variation among transport protocols with respect to the relative amount of compliant, non-compliant, and unknown routes.

4.2 Comparative Analysis

While the work [16] used a passive approach based on publically available BGP routing table information, countries were ranked according to a Schengen routing compliance score, which represents the relative amount of routes that do not comply with Schengen routing [16]. Although the geo-location information is taken from Maxmind's GeoLite database [10] in both cases, the comparison of both sets of results obtained are compared and shown in Table 5. The relative amount of non-compliant routes obtained using active measurements in the chkroute approach exceeds in almost all cases the amount obtained using the model based on BGP routing table data. An analysis discussing the reasons resulting in those differences found between [16] and the chkroute approach is omitted at this point, because the routing data used to produce results in [16] is not available.

5 Design and Implementation of the chkroute Tool

While those results presented are useful to obtain a general understanding of compliance levels in each of the individual Schengen countries, end-users are more interested to learn whether specific routes are compliant with Schengen

Table 5. Non-compliant routes according to Pohlmann et al. [16] vs. chkroute

Country Code	Country	Pohlmann et al. [16]	chkroute
BE	Belgium	35.38%	49.4%
LI	Liechtenstein	29.41%	0.0%
CH	Switzerland	23.48%	15.2%
ES	Spain	21.27%	43.4%
LU	Luxembourg	21.15%	47.4%
FR	France	19.13%	26.4%
MT	Malta	17.86%	66.7%
FI	Finland	16.58%	56.0%
CZ	CzechRepublic	16.31%	31.3%
SE	Sweden	14.92%	30.5%
NL	Netherlands	13.07%	19.3%
DE	Germany	12.26%	32.5%
NO	Norway	10.31%	41.5%
GR	Greece	8.67%	61.1%
EE	Estonia	6.78%	81.8%
SK	Slovakia	6.25%	33.3%
LT	Lithuania	5.50%	36.4%
IT	Italy	3.70%	31.4%
AT	Austria	3.23%	25.0%
DK	Denmark	1.75%	26.3%
PL	Poland	1.43%	41.0%
PT	Portugal	1.39%	66.7%
LV	Latvia	1.34%	61.5%
SI	Slovenia	1.15%	58.3%
HU	Hungary	0.49%	38.3%
IS	Iceland	0.00%	38.9%

Routing or not. Therefore, *chkroute* was designed and prototyped. The tool chkroute assesses whether a specific route complies to Schengen Routing or not and is available at [6].

The tool's architecture consists out of the 3 components depicted in Figure 2. The client desires to verify a route. The target host or IP address represents the endpoint of the route. The geo-location server stores location and compliance information about IP addresses. The compliance checks for routes are performed in four steps.

1. The client runs traceroute to the target host.
2. The client collects responses from hops along the path.
3. The client submits hops to the geo-location server.
4. The geo-location server analyzes these hops and sends country and compliance information back to the client, which prints the result.

A sample run of chkroute is shown in Figure 3. The chkroute command is executed from a client at University of Zurich towards a server of the University of Federal Armed Forces in Munich. Both hosts are located in Schengen. The output produces a hop count, an IP address, the country code, Schengen routing compliance information (Yes ("Y"), No ("N"), and Unknown ("Unknown")), and the AS number.

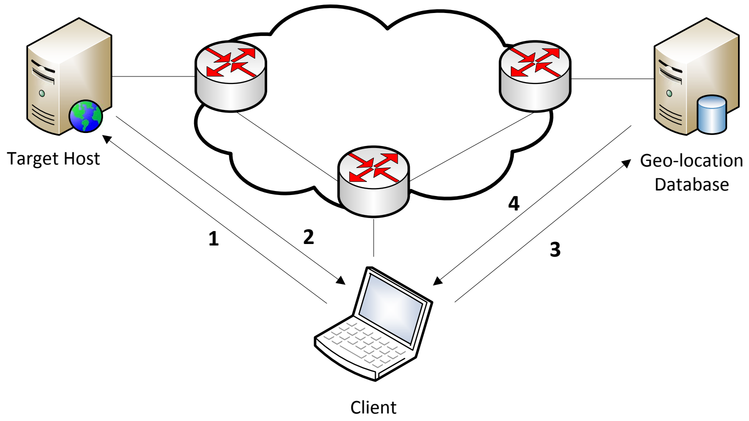


Fig. 2. The chkroute architecture

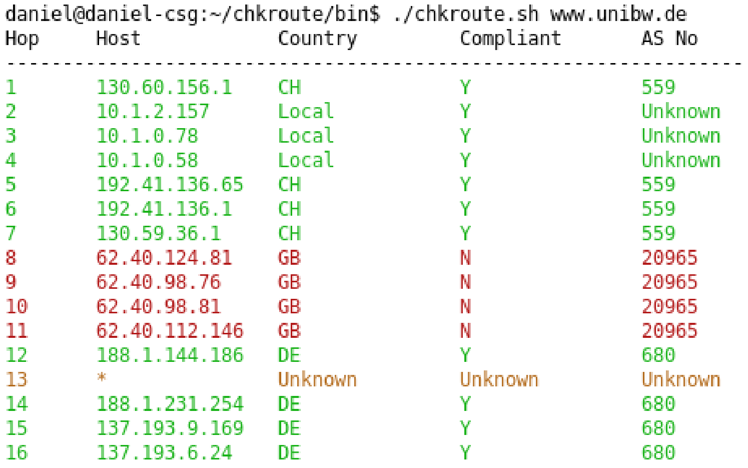
The sample output shows that this network traffic remains inside the Schengen Area until hop 7, leaves the Schengen Area for hops 8 to 11, and it returns at hop 12. Hop 13 is unknown. To ease the readability of this result, all hops are color-coded: green is for compliant, red for non-compliant, and yellow for unknown.

6 Summary, Conclusion, and Future Work

This paper presented key results of a larger-scale measurement conducted to determine the extent to which current routing is Schengen-compliant in Schengen countries. Based on 3388 TCP, UDP, and ICMP traceroute measurements run from RIPE Atlas probes located in over 1100 ASes in the Schengen Area it was found that compliance levels vary substantially among countries and range from 0% (TCP), 0% (UDP) and 0% (ICMP) in the case of Malta to 80% (TCP), 75% (UDP), and 80% (ICMP) in the case of Liechtenstein. The overall compliance levels range from 34.5% (TCP) to 37.4% (UDP) and 39.7% (ICMP).

Based on these measurements performed, this paper concludes that Schengen Routing compliance is not achieved in any of the Schengen countries, contradicting the claim that Schengen routing already was a factual reality today, as it has been stated by the Association of the German Internet Industry [4]. Therefore, intelligence agencies still can perform potential wiretapping activities outside the Schengen jurisdiction on traffic originating within and destined to the Schengen Area.

This work and chkroute especially with the data set collected only analyze traffic in the forward direction. The reverse path may not necessarily be the same [11]. Hence, future work will address the reverse path, too. Furthermore, as only routes originating in Schengen countries targeted at a single node in Switzerland have been analyzed, results may differ, if a target node in another



```
daniel@daniel-csg:~/chkroute/bin$ ./chkroute.sh www.unibw.de
Hop     Host            Country         Compliant       AS No
-----------------------------------------------------------------
1       130.60.156.1    CH              Y               559
2       10.1.2.157      Local           Y               Unknown
3       10.1.0.78       Local           Y               Unknown
4       10.1.0.58       Local           Y               Unknown
5       192.41.136.65   CH              Y               559
6       192.41.136.1    CH              Y               559
7       130.59.36.1     CH              Y               559
8       62.40.124.81    GB              N               20965
9       62.40.98.76     GB              N               20965
10      62.40.98.81     GB              N               20965
11      62.40.112.146   GB              N               20965
12      188.1.144.186   DE              Y               680
13      *               Unknown         Unknown         Unknown
14      188.1.231.254   DE              Y               680
15      137.193.9.169   DE              Y               680
16      137.193.6.24    DE              Y               680
```

Fig. 3. chkroute output

country was chosen. In particular, routes originating in a Schengen country A may be more or less likely than those originating in another Schengen country B to traverse a non-Schengen country depending on the location of the target node. Finally, an additional extension to this work is to analyze traffic for individual countries in more detail as well as to provide details with respect to countries that cause routes to be non-compliant with Schengen routing. It is also essential to identify those Schengen countries that are exit and entry points for traffic out of the Schengen Area and to examine the reason why this is the case.

7 Acknowledgments

This work was partially supported by the SmartenIT and the FLAMINGO projects, funded by the EU FP7 Program under Contract No. FP7-2012-ICT-317846 and No. FP7-2012-ICT-318488, respectively.

References

1. B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira: Avoiding Traceroute Anomalies with Paris Traceroute, 6th ACM SIGCOMM Conference on Internet Measurement (IMC 2006), Rio de Janeiro, Brazil, 2006, pp. 153–158
2. J. Blau: NSA Surveillance Sparks Talk of National Internets, IEEE Spectrum 51, February 2014, pp. 14–16
3. T. Bourgeau: Monitoring Network Topology Dynamism of Large-scale Traceroute-based Measurements, 7th IEEE International Conference on Network and Service Management, Paris, France, October 2011, pp. 489–493

4. Computerwoche: Internet-Verband ECO Beklagt Scheindiskussion um “Schengen-Routing”, http://www.computerwoche.de/a/internet-verband-eco-beklagt-scheindiskussion-um-schengen-routing,2556658, Last Accessed: Feburary 2015
5. Daniel Dönni, Guilherme Sperb Machado: Traceroute Measurements in Schengen Area, http://www.csg.uzh.ch/publications/data/traceroute-schengen/, Last Accessed: February 2015
6. Daniel Dönni: chkroute utility, https://cms.uzh.ch/lenya/csg/authoring/publications/software/chkroute.html, Last Accessed: March 2015
7. Suman Banerjee, Timothy G. Griffin, Marcelo Pias: The Interdomain Connectivity of PlanetLab Nodes, 5th Passive and Active Network Measurement Conference (PAM 2004), Lecture Notes in Computer Science, Volume 3015, Antibes Juan-les-Pins, France, April 2004, pp. 73 – 82
8. EMANICSLab, http://www.emanicslab.org, Last Accessed: December 2014
9. European Commission: The Schengen Area, http://biblio.ucv.ro/bib_web/bib_pdf/EU_books/0056.pdf, Last Accessed: February 2015
10. Maxmind: GeoLite Legacy Downloadable Databases, http://dev.maxmind.com/geoip/legacy/geolite, Last Accessed: December 2014
11. Y. He, M. Faloutsos, S. Krishnamurthy, and B. Huffaker: On Routing Asymmetry in the Internet, Global Telecommunications Conference (GLOBECOM 2005), Volume 2, St. Louis, USA, 2005, pp. 6 pp
12. Y. Hyun, A. Broido, and K.C. Claffy: Traceroute and BGP AS Path Incongruities, Cooperative Association for Internet Data Analysis (CAIDA), Technical Report, March 2003. Available at: http://www.caida.org/publications/papers/2003/ASP/asp-incon.pdf. Last Accessed: February 2015
13. S. Landau: Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations, Journal of Security Privacy, Vol. 11, No. 4, July 2013, pp. 54–63
14. OpenWRT, https://openwrt.org, Last Accessed: January 2015
15. Planet-Lab, https://www.planet-lab.org, Last Accessed: December 2014
16. N. Pohlmann, M. Sparenberg, I. Siromaschenko, and K. Kilden: Secure Communications and Digital Sovereignty in Europe, ISSE 2014 Securing Electronic Business Processes, Brussels, Belgium, 2014, pp. 155–169
17. RIPE NCC: RIPE ATLAS, atlas.ripe.net, Last Accessed: December 2014
18. S. Sundaresan, S. Burnett, N. Feamster, and W. De Donato: BISmark: A Testbed for Deploying Measurements and Applications in Broadband Access Networks, 2014 USENIX Conference, San Diego, USA, August 2014, pp. 383 – 394
19. Y. Zhang, R. Oliveira, H. Zhang, L. Zhang: Quantifying the Pitfalls of Traceroute in AS Connectivity Inference, 11th Passive and Active Measurement Conference (PAM 2010), Lecture Notes in Computer Science, Vol. 6032, Zurich, Switzerland, April 2010, pp. 91–100