Secure communication and digital sovereignty in Europe

Norbert Pohlmann · Michael Sparenberg · Illya Siromaschenko · Kilian Kilden

Institute for Internet Security – if(is)
Westfälische Hochschule, Gelsenkirchen
University of Applied Sciences
{pohlmann | sparenberg | siromaschenko | kilden}@internet-sicherheit.de

Abstract

Recent discussions about the weakening of Europe's digital sovereignty have highlighted the fundamental importance of integrity and trustworthiness of Internet communication and services.

This work introduces a scientific approach to simulate the effects of routing regulation concepts that limit data traffic to specific regions, which are supposed to be covered by a common data protection act. This concept was proposed as a potential countermeasure against the violation of European data protection and privacy policies by US intelligence services and other international governmental organizations. The objective is to analyze the current landscape of European Internet interconnections, illustrated by technical key figures and focusing on security implications of data traffic routing.

By simulating a virtual "Schengen Net", where data routing between member states is limited to autonomous systems located in countries covered by the Schengen agreement, an estimation of resulting effects is presented, including technical, economical and security-related aspects.

Based on these analytical findings, the concept of routing restriction is matched against the alternative approach of data encryption to compare the fitness for purpose of both technical concepts for security improvements.

1 The Internet from an infrastructure point of view

For a typical end user, it is hard to appreciate the complex infrastructure that we colloquially call "the Internet". Behind that term lies a non-homogeneous, decentralized and geographically asymmetrical distributed network of managed sub-nets, called "autonomous systems" (AS). Being a network of networks, the Internet can be measured by its infrastructure components.

Key indicators of current Internet infrastructure:

- 50.000 autonomous systems worldwide, e.g. 1.500 in Germany, 15.000 in the USA
- 234 country signifiers
- 500.000 logical connections between AS
- 50% of all connections are attributed to G20 member states
- 50+% average rate of domestic connections

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2014), 1-15

To gain further insights into the underlying structure, development and scale of the Internet, the Institute for Internet Security – if(is) has developed the Internet Key Figure System, an integrated monitoring and evaluation system of critical Internet infrastructure. The IKS enables us to generate and review a large number of key statistical information, including everything shown in the table above.

In the light of recent discussions about possible ways of achieving a higher state of informational integrity and security, we feel it is of importance to analyze and discuss the inner workings of this global network and the possible impacts on this structure that some of the proposed solutions might have. Going back to the summer of 2013, shortly after the initial publication of the Snowden Leaks, prominent voices inside the Internet-provider industry have argued for geographically/locally based routing restrictions, discussed under the terms such as "Schengen Net". The idea was to restrict the routing of data between two systems located in country A to systems that are also located in country A. By never crossing into a second judicial territory, your information will be protected by the same privacy laws for its entire journey, bypassing possible snooping attempts from the outside. This concept can be easily expanded from a country to a number of countries protected by either the same privacy laws, or those who are equal in spirit.

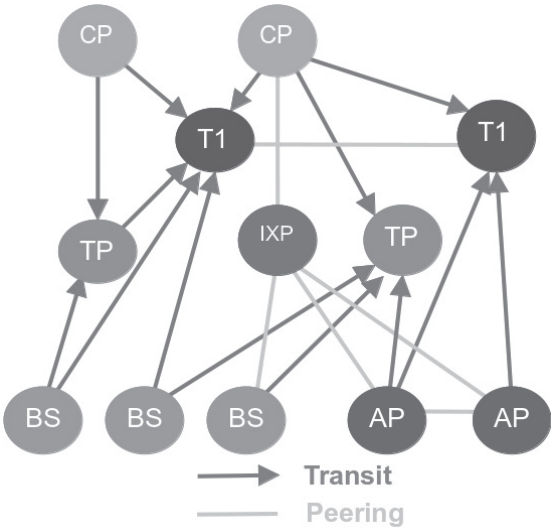

Fig. 1: Data traffic routing scheme

Now many people have largely considered this to be already working in practice – Why would Internet service providers use a route that, in most cases, would be longer, at least in geographical terms, and how substantial is the amount of traffic in practice that bypasses local routes? After all, longer routes mean more systems being involved into the routing process, which usually results in higher cost. To understand the logic behind traffic routing in a global network, we need to understand the underlying economics that guide the organization and expansion of ISPs and transit providers. In order to provide access to the rest of the network, an autonomous system has to be physically connected to other AS in the system, either directly or indirectly by using a connection a third-party AS has already established. Indirect connections rely on using bandwidth of the third-party AS to direct traffic from and to your AS. To secure access, an AS has to either be big enough and/or serve data that is important enough to establish a peering

contract, which enabled both contract partners to use each other's infrastructure to route data – a mutually beneficial agreement. Transit agreements are a paid-for service, allowing the operator of one AS to use a certain amount of bandwidth or capped transit volume of a third party AS to gain access. Conditions vary throughout the industry, but using transit routes always comes at a variable cost to the operator in contrast to peering agreements, where only a fixed connection cost is incurred. In order to improve reliability of the network, operators will want to have several different routes prepared, choosing the least expensive option for as long as it is available and switching to the next cheapest stored route when it is not.

2 Focusing on Internet security: trends, threats and countermeasures

The early paradigm of Internet development was clearly focused on technological improvement and economies of scale: faster upgrades circles, better equipment, deployment and expansion of infrastructure to expand the network and to offer better digital services for lower prices. Following the simple principles of unsaturated markets, the growth of the Internet gained a tremendous speed, making it the most powerful communication system. With price and performance being the main driving forces, security features were not on the list of high priority objectives, neither for supply nor demand. This changed gradually when the Internet spread with an exponentially growing user base, evolving from a simple vehicle for data transport to an integral part of the global value chain.

Today it is regarded as one of the most versatile tools for everyday tasks, and utilization of this global medium became a widespread standard in both business and private use. With more and more data moving to the "cloud", digital services became an attractive target for espionage, data theft and intelligence investigation.

Especially the latter one was recently raising concerns about security and trustworthiness of Internet services. Information leaked by whistleblower Edward Snowden revealed that US intelligence services put an immense effort in technical measures to acquire any kind of digital information from the Internet, including actions that do not comply with national and international law in many regions of the world, including Europe.

As a result of this new dimension of security threats, several proposed solutions emerged from controversial discussions on how to increase the level of integrity and privacy protection on a technical, organizational and policy level. One of these approaches is based on the idea of routing restrictions, aiming to reclaim European digital sovereignty by avoiding external network interconnections for inner-European data traffic. The following chapter illustrates the technical characteristics of this concept.

2.1 "Schengen Net": Simulation of a restricted routing model for Europe

The terms "Schengen Net" and "Schengen routing", which were recently introduced refer to a policy concept that regulates data communication within European countries, deliberately excluding UK (due to close cooperation with US intelligence). According to this proposal, In-

ternet traffic must not be routed via autonomous systems located outside the Schengen area, whenever both start and end point of the communication are located in the respective region.

While there are pending extensions and associated (collaborating) countries, the list of member states covered by the Schengen agreement currently comprises of Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland.

In case of corresponding legal requirements, this will effectively prevent Internet service providers to route data between European countries via e.g. US-based systems.

Since this approach has implications way beyond technological aspects, changing the rules for competition and market balance, it is accompanied by an ongoing controversial discussion about its fitness for purpose, and the pros and cons of Internet regulation in general.

2.2 Building a data model for routing analysis

For the purpose of evaluating the concept of routing restrictions, we opted for a quantitative analytical approach, aiming to simulate the overall technical impact to expect in case that mandatory data traffic routing regulations will be in effect.

IKS Internet Key figure System, a research project of the **Institute for Internet Security**, serves as the technical foundation of our analysis, providing the necessary tools and data.

The data set used here contains an aggregated listing of more than 50.000 publicly visible autonomous systems and about 500.000 links between these systems (based upon publicly announced BGP routing information). Following a standard data preparation procedure, which removes redundant links and local loops to ensure data quality, a directed graph model is build, representing the observed infrastructure elements of the Internet.

Country Internet

To determine a mapping from autonomous systems to countries, geo-localization of allocated IPv4 addresses is performed, using a simple major share for voting. According to that rule, e.g. AS which have a major share of allocated IP addresses resolving to locations in Germany are referred to as "DE-AS". With this basic form of localization, any AS can be mapped to a single country, using the full range of 234 ISO codes currently available.

Different types of AS

To further break down the set of autonomous systems in addition to regional classification, a heuristic categorization scheme is applied, based on the role of individual AS within the infrastructure. This facilitates a refinement of statistics by distinguishing **business systems AS (BS)** from **access provider (AP)**, **transit provider (TP)** and **content provider (CP)**, which has a significant influence on the extent to which autonomous systems will be affected by routing restrictions.

The following table shows the current number of Schengen-AS according to the type of services they offer [FPSW12].

Tab. 1: Categorization of autonomous systems (Schengen area)

	ISO	Country	Access	Transit	Content	Business
1	AT	Austria	44	88	40	344
2	BE	Belgium	11	41	35	143
3	CH	Switzerland	33	110	50	438
4	CZ	CzechRepublic	22	108	55	294
5	DE	Germany	126	315	253	1048
6	DK	Denmark	25	34	37	180
7	EE	Estonia	6	17	12	36
8	ES	Spain	30	52	88	402
9	FI	Finland	28	22	35	156
10	FR	France	76	176	142	651
11	GR	Greece	20	12	15	129
12	HU	Hungary	19	34	34	139
13	IS	Iceland	3	20	12	24
14	IT	Italy	45	127	95	510
15	LI	Liechtenstein	0	6	0	9
16	LT	Lithuania	9	25	17	77
17	LU	Luxembourg	4	20	7	26
18	LV	Latvia	5	30	23	171
19	MT	Malta	2	6	3	19
20	NL	Netherlands	67	233	147	356
21	NO	Norway	30	62	30	119
22	PL	Poland	41	148	88	1347
23	PT	Portugal	15	17	15	52
24	SE	Sweden	47	103	58	365
25	SI	Slovenia	11	21	17	236
26	SK	Slovakia	7	43	13	77

To mimic the effect of routing restrictions, a filter mechanism is applied to the global data set, based on the results of previous geo-mapping. To provide more flexibility for future applications, the filter mechanism can be easily modified to contain multiple data sets and analysis is based on a generalized data model that works with arbitrary filter settings, so the given example may be replaced by virtually any regional grouping scheme. The Schengen filter definition applied for analysis results in a subset of 10,000+ AS, representing a share of 20% of the global amount of autonomous systems.

By transforming the resulting subset to an interconnection matrix, the latter is analyzed for pair-wise shortest paths between all autonomous systems. This step leaves the graph model of routing information unmodified, avoiding any loss of information due to sub setting.

At the core of network analysis is a classification function which allows to assign one of three distinct types to all routes in the network graph model:

a) Domestic route (national)

All AS in the respective path are located in the same country, including source and destination systems.

b) Internal route (Schengen)

All AS in the respective path are located within Schengen area, including source and destination systems.

c) External route (non-Schengen)

One or more AS in the respective path are located outside the Schengen area, whereas both source and destination AS are located within Schengen area.

Frequency counts are saved according to these classification results, counting each type of connection for all shortest routes between two AS for all systems within the respective country of the Schengen area. Each respective indicator is statistically aggregated and averaged from AS level to country level, providing key figures for effect estimation of local routing restrictions.

The current version of the data model does not support edge weighting, meaning that utilization of routes is assumed to be equally distributed. Future improvements of the model will include a functional estimation for effective route selection based on piecewise (theoretical) frequency counts and parameters derived from an extended network graph with additional attributes like e.g. bandwidth, cost and capacity of connections.

2.3 Key results of analysis

The map and table below show the estimated effect of Schengen routing restrictions per country, where darker color means higher impact.

Color coded score values per country (ranging from 0 to 37.5) represent the percentage of routes that are marked as non-Schengen according to the classification mechanism previously described, meaning that these routes will have to be excluded for inner-Schengen data traffic, since routing paths contains autonomous systems which are located outside the Schengen area.

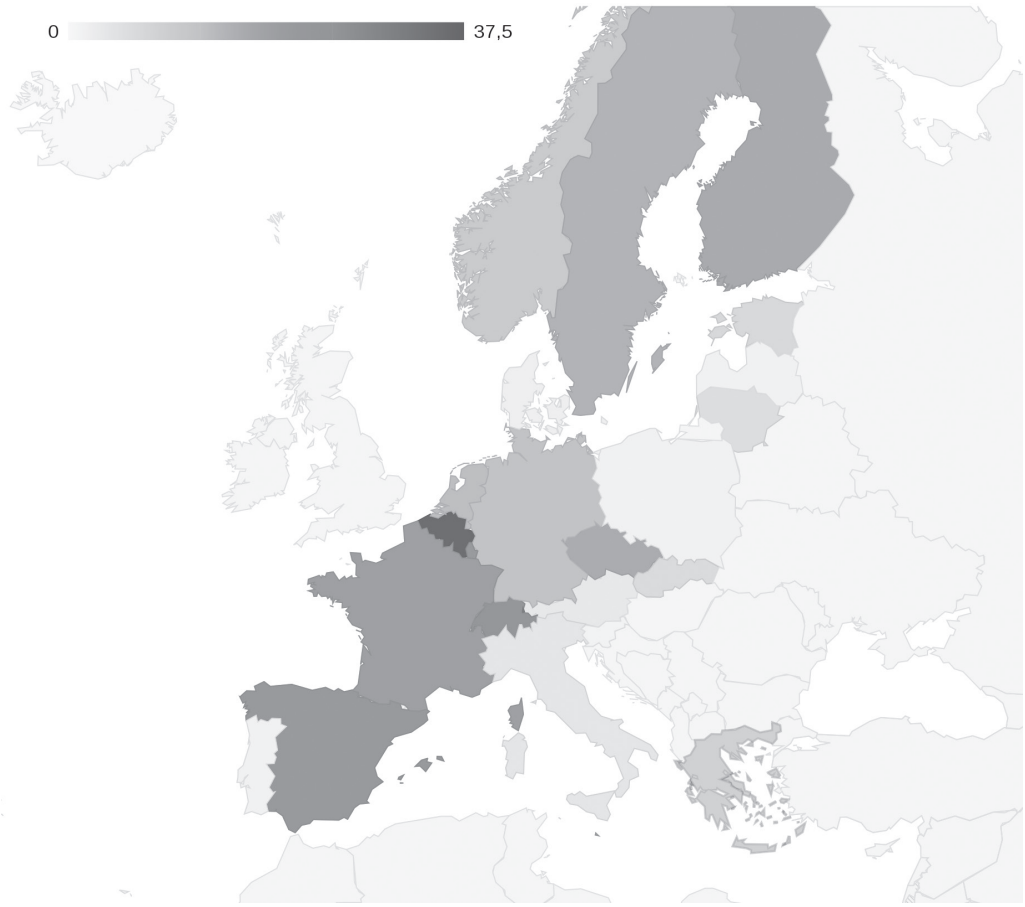

Fig. 2: Simulated effects of Schengen routing restrictions
(Score=average percentage of non-Schengen routes per country)

According to the range of values displayed in the map, it becomes obvious that the concept of regional routing restrictions affects Schengen countries to a very different extent, with Belgium, Spain and France in the group of countries accounting for the highest impact.

Tab. 2: Estimated impact of Schengen routing restrictions per country

	ISO	Country	Score	AS
1	BE	Belgium	35,38	195
2	LI	Liechtenstein	29,41	17
3	CH	Switzerland	23,48	578
4	ES	Spain	21,27	489
5	LU	Luxembourg	21,15	52
6	FR	France	19,13	915
7	MT	Malta	17,86	28

	ISO	Country	Score	AS
8	FI	Finland	16,58	193
9	CZ	CzechRepublic	16,31	424
10	SE	Sweden	14,92	517
11	NL	Netherlands	13,07	659
12	DE	Germany	12,26	1494
13	NO	Norway	10,31	195
14	GR	Greece	8,67	150
15	EE	Estonia	6,78	59
16	SK	Slovakia	6,25	128
17	LT	Lithuania	5,50	109
18	IT	Italy	3,70	703
19	AT	Austria	3,23	465
20	DK	Denmark	1,75	229
21	PL	Poland	1,43	1754
22	PT	Portugal	1,39	72
23	LV	Latvia	1,34	224
24	SI	Slovenia	1,15	260
25	HU	Hungary	0,49	203
26	IS	Iceland	0,00	47

Since indicators shown in the table represent a national average, the spread of values on AS level is even higher, meaning that the individual impact on the operator level of autonomous systems varies a lot more. A modified analysis simulating a restriction to national (domestic) routes for data traffic shows greater impact scores, ranging from 0 to 50%.

This means that e.g. in Belgium, Switzerland and Spain, more than one third of available routes are operating via autonomous systems located outside the respective country.

Despite the fact that absolute results have to be interpreted with caution and taking into account that the overall effect of mandatory routing restrictions may only be estimated qualitatively, it becomes evident that this concept will have an impact beyond purely technical aspects including economic implications. It is likely that this will at least temporarily increase dissimilarities within and between countries instead of fostering harmonization of the European Internet market.

Taking into account that an approach based on the intentional exclusion of relevant players will likely be facing countermeasures on the corresponding side, a protective concept like Schengen routing will presumably lead to fragmentation and Balkanization of the Internet, contradicting the objective of unified regulation.

2.4 Evaluating the concept of routing restrictions

As seen from the national effect estimation indicators, a mandatory Schengen routing model will affect autonomous systems unequally, ranging from "no change" to "high impact" levels.

From an economical perspective, this corresponds to varying degrees of business reorganization requirements, depending on the relevance of non-Schengen routing for individual business models of AS operators.

In saturated markets, facing intense competition, this may have a non-negligible impact on the overall competitive strength of the European Internet economy, at least for the market of Internet services, which is regarded as a critical infrastructure these days. Given the fact that broadband services became a low profit business and most end users nowadays prefer flat rate pricing models, it can be assumed that the necessary effort to implement and operate the Schengen routing model will result in increased prices, at least for some market segments, products and services.

But even if economical disadvantages are accepted as an inevitable side effect of the Schengen routing concept, which may be expected given the results of our analysis, it seems questionable if regional routing restrictions will prove to be beneficial for the purpose of strengthening security. Without a strict unification of European data protection policies in effect, security enhancements may only be achieved based on voluntary agreements between policy makers and the Internet economy of the respective member states.

As a result, a realistic implementation of this concept is merely build on trust and thus lacks a technical proof of security from the Internet user's point of view, who rather demands for a reliable solution to protect privacy, integrity and sovereignty of digital communication for business and private use.

The following chapter will introduce an alternative approach to meet those requirements, based on solutions and technologies that are already available and in use, but to an extent that allows for improvements. While future security enhancements obviously require extensive research and new technologies, deployment of available solutions is always key to success.

3 Cryptography as an alternative approach to security improvements

While geographically restricted routing zones do not seem to achieve the desired results, the main impetus behind the proposal is still very much in force. Businesses, private citizens and government entities are actively looking for solutions to protect their data in global networks from outside attacks, regardless of their origin. The logical conclusion, therefore, is that if we can't guarantee a secure line between communicating entities, we have to build systems to reduce or eliminate the threat even when our communications have been siphoned off. Our suggestions is in no way revolutionary, but focuses on an evolutionary approach to implementation and further development of current technologies, namely comprehensive encryption at the enterprise and user level.

Active Encryption

An important aspect for a security communication and digital sovereignty in Europe is the need of much more encryption in the Schengen area to protect us appropriately. We need substantial encryption for a sustainable protection of our data during the communication, wherever it is possible. From the Internet point of view the communication channel encryption in the Schengen area will be very helpful. IPSec and SSL/TLS encryption are the standards in the field of communication channel encryption which we should use much more in the future.

3.1 IPSec encryption

The IPSec standard is for the encrypted communication between companies or parts of companies. The normal implementation for the communication infrastructure is the use of IPSec gateways at the endpoint of the companies. In the Institute for Internet Security we measure that every 125th IP packed in the Internet is IPSec encrypted at the moment. Since Snowden the growth rate of IPSec encryption is 60%.

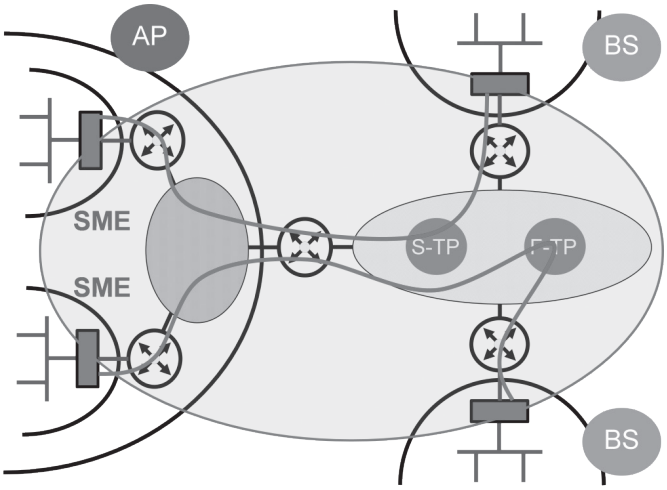

Fig. 3: IPSec encryption scheme

Application cases

If the companies in the Schengen area use IPSec gateways the communication encryption will be easily implemented. SME will integrate the gateways into the communication line to the Access Provider (AP) and the bigger companies with own Business Customers Autonomous Systems (BP) integrate the gateways into the communication line to the Transit Provider (TP).

Benefits

All the communication between companies and parts of companies could be easily encrypted and the quality of the protection will be independent if the Transit Provider is from the Schengen area (S-TP) or from a foreign country (F-TP) like the US, China or Russia. It is also independent where the router technology comes from, because all IP packets are encrypted.

Tasks to do

Because of the key management we should organize an IPSec center which helps realize the common key management in the Schengen area. This IPSec center should be responsible for the interoperability of gateways, the key management for all the companies and governments which would like to participate and also the trustworthiness of the gateways and the producer of the gateways.

3.2 SSL/TLS encryption

SSL/TLS is for example the standard for the encrypted communication between the browser and the web servers. In the field of SSL/TLS encryption the Institute for Internet Security measure that every 7th IP packed in the Internet is SSL/TLS encrypted. Since Snowden the growth rate of SSL encryption is 90%. The reason for that is that big companies like Google, Facebook, Deutsche Telekom and so on started to offer SSL/TLS as default.

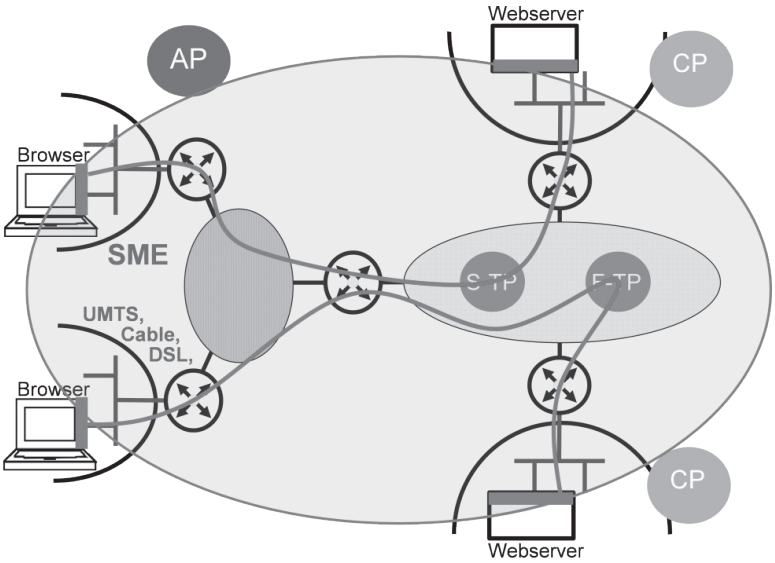

Fig. 4: SSL encryption scheme

Application cases

Every browser and web server is able to build up a communication channel between the client and the server. The PKI infrastructure is in principle established. The browsers have already the root certificates of about 200 different PKI service providers which offer the domain certificates for the web server. It is also possible to use SSL/TLS for other application protocols. One important application is email transfer protocol SMTP. If all email gateways are using SMTPS (SMTP with SSL) the communication would be protected during the communication between the email gateways. But the email is in plain text in the email gateway itself.

Benefits

All the communication between clients and servers could be easily encrypted.

Tasks to do

We need more trustworthy PKI infrastructure from Europe, because of the potential risk of manipulations of the technologies and the provider itself.

3.3 General discussion about encryption

We have to put much more effort in the encryption to be better protected. We also need to catch up with email end-to-end encryption, disc-, file encryption etc.

S/MIME or PGP

S/MIME or PGP are the standards for email end-to-end encryption. According to our measurements, more than 5% of the business emails are encrypted. But we also know from studies that 43% of the transmitted business email need to be encrypted.

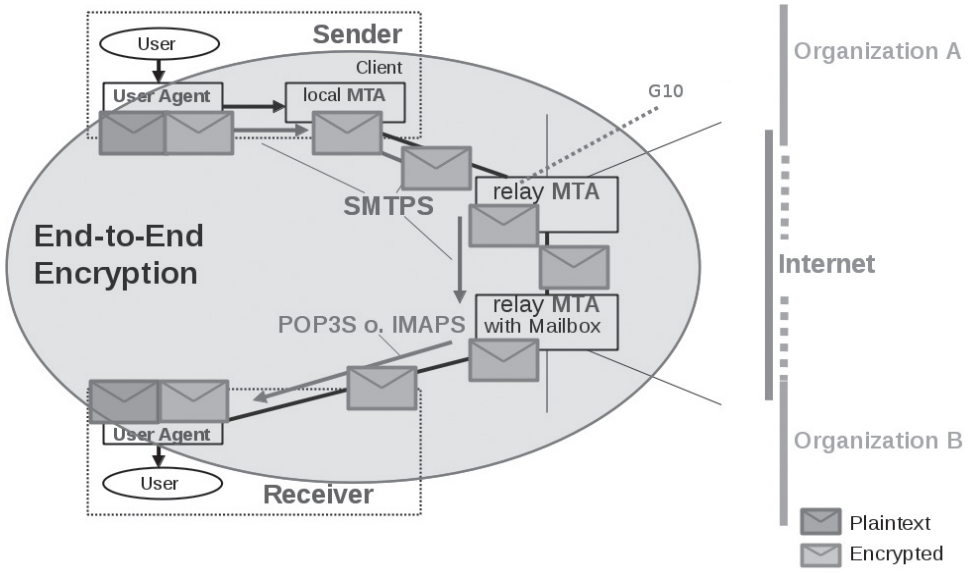

Fig. 5: Email encryption scheme

Application cases

The emails and the annex can be encrypted in the user agent of the sender and then transmitted in encrypted form via the Internet. Only the receiver is able to decrypt the email again in the user agent. Nearly every email user agent offers extension for email end-to-end encryption.

Benefits

All email user agents are able to encrypt easily the needed emails.

Tasks to do

We need a trustworthy PKI infrastructure originating from Europe, because of the potential risk of manipulations of the technologies and the provider itself. But we also need much better integration of email user agents in PCs, notebook, smartphones etc.

3.4 Trustworthy IT security technologies and services

It is very important that we take some key requirements for the use of the different kinds of encryption possibilities into account. One important requirement is trustworthy encryption technology that means no backdoors, strong random number generators, correct implementation and so on. The recent severe implementation error in the OpenSSL library (Heartbleed Bug) shows that also open source software will only be secure if real effort is put into the evaluation. So we have to take responsibility to support the European IT security industry to develop really trusted technologies and to make evaluations according to international standards.

In Europe we have a very powerful IT security industry. That could be a good reason to take more responsibility for a secure and trustworthy Internet. But we also need trustworthy IT security infrastructure. Public Key Infrastructure (PKI) services with Registration Authority (RA) and Certification Authority (CA) components. Also here we have to support the European IT security industry to build up successful solutions.

4 Conclusion

With the objective of evaluating alternative approaches for security enhancement, reclaiming integrity and trustworthiness of Internet communication and thus digital sovereignty, two basic concepts were discussed in this paper.

The concept of local routing restrictions aims to avoid problems like eavesdropping by regionally limiting data traffic to an area of common data protection regulation in order to ensure consistent policies within the respective region. This comes with an additional side effect of further standardization of some technical components.

On the other hand, these protective measures are at the same time a potential source of conflict, discriminating vendors and solution providers who are not able to fulfil corresponding requirements with a reasonable effort. Depending on the degree of dependency from external providers, this might even imply a decreased level of robustness on the supply side of infrastructure services.

But the weakest point of this approach is the fact that security enhancements completely rely on policies and the routing of data, protecting neither the content of communication nor the physical communication layer. Applying routing manipulations also fails to improve security in communication with external parties outside the Schengen area.

While users demand for solutions that provide a proven technical level of security, the Schengen routing concept requires people to trust in the functional suitability of measures taken by policy makers, Internet services providers and system operators. In this sense, provable security enhancements may only be feasible by deploying technologies that protect the content of communication, which is regularly achieved by applying cryptography to data traffic. This paper illustrates the key technical characteristics of two essential technologies for this purpose, IPSec and SSL/TLS.

Additionally, we have briefly described two specific encryption mechanisms exemplary with email communication. They can be implemented either for end-to-end encryption between parties or as transparent gateway solution at email provider site.

Combining these existing technologies helps to ensure comprehensive transport security with an improved balance of usability and security for end users. The proposed solutions are in a mature state of development, available to the general public and supported by a broad range of products and services for business and private use. Nevertheless, there is still room for improvements, since - from a global point of view - deployment and utilization of strong cryptographic data protection is far from being widespread and a trade-off between security and usability still seems inevitable for many users, while businesses struggle with the perceived gain in security contrasted by higher cost.

Regarding the long-term perspective, paving the way to end point security appears to be the most sustainable approach, effectively putting the power to control in the hand of the user. Furthermore, this will eliminate the need to secure data routing, since digital content is seamlessly protected on its way from source to destination, effectively rendering eavesdropping and similar techniques useless.

Furthermore, a migration to seamlessly encrypted traffic eliminates the need to trust in the technical integrity of routing equipment, since bypassing mechanisms that replicate data in a non-transparent manner will be ineffective as well.

To summarize the key findings of this work, moving towards complete encryption of data traffic seems to be the most sensible approach, given the fact that technological, organizational and financial efforts have to be take in any case to enhance the level of security. Instead of simple protective measures which imply the risk of technological isolation of Europe, an open approach based on strong cryptographic protection aligns much better to the spirit of harmonization, open markets and sustainable digital sovereignty in Europe.

References

[FPSW12] Feld, Pohlmann, Sparenberg, Wichmann:Analyzing G-20's key autonomous systems and their intermeshing using AS-Analyzer. In: ISSE 2012 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2012 Conference, Springer Vieweg, 2012.

[CaRe05] Matthew Caesar, Jennifer Rexford: "BGP routing policies in ISP networks ", 2005 http://www.cs.princeton.edu/~jrex/papers/policies.pdf Last access: 22.07.2014

[KaFR09] Josh Karlin, Stephanie Forrest, and Jennifer Rexford : "Nation-State Routing: Censorship, Wiretapping, and BGP ", 2009 http://arxiv.org/pdf/0903.3218v1.pdf Last access: 22.07.2014

[FPS+02] Joan Feigenbaum, Christos Papadimitriou, Rahul Sami, Scott Shenker: "A BGP-based Mechanism for Lowest-Cost Routing", 2002 http://www.cs.yale.edu/homes/jf/PODC02.pdf Last access: 22.07.2014

[MuFe06] Wolfgang Mühlbauer , Anja Feldmann, Olaf Maennel , Matthew Roughan, Steve Uhlig „Building an AS-Topology Model that Captures Route Diversity", 2006 http://dl.acm.org/ft_gateway.cfm?id=1159937 Last access: 22.07.2014

[YoJB02] Soon-Hyung Yook, Hawoong Jeong, and Albert-László Barabási "Modeling the Internet's large-scale topology", 2002 http://www.pnas.org/content/99/21/13382.abstract Last access: 22.07.2014

[ACF+12] Ager, Bernhard; Chatzis, Nikolaos; Feldmann, Anja; Sarrar, Nadi; Uhlig, Steve; Willinger, Walter: Anatomy of a Large European IXP. In: ACM SIGCOMM '12. 2012.

[COMM09] Commission of the European Communities: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. 2009.

[FPPS11a] Feld, Sebastian; Perrei, Tim; Pohlmann, Norbert; Schupp, Matthias: Objectives and added value of an Internet Key Figure System for Germany. In: ISSE 2011 Securing Electronic Business Processes. Vieweg+Teubner Verlag, 2011.

[FPPS11b] Feld, Sebastian; Perrei, Tim; Pohlmann, Norbert; Schupp, Matthias: Ein Internet-Kennzahlensystem für Deutschland: Anforderungen und technische Maßnahmen. In: D-A-CH Security 2011. IT-Quartier Oldenburg, 2011.

[GOOG12] Google.com: Google Safe Browsing diagnostic page for AS680 (DFN). http://www.google.com/safebrowsing/diagnostic?site=AS:680. Last access: 16.07.2012.

[MAXM12a] Maxmind.com. http://www.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz. Last access: 16.07.2012.

[MAXM12b] Maxmind.com. http://www.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz. Last access: 16.07.2012.

[PMAM08] Provos, Niels; Mavrommatis, Panayiotis; Abu Rajab, Moheeb; Monrose, Fabian: All Your iFRAMEs Point To Us. Google Technical Report. 2008.

[POTA12] potaroo.net. http://bgp.potaroo.net/cidr/autnums.html. Last access: 16.07.2012.

[RIPE12a] RIPE NCC: Routing Information Service (RIS) - RIPE Network Coordination Centre. http://www.ripe.net/data-tools/stats/ris/routing-information-service. Last access: 16.07.2012.

[RIPE12b] RIPE NCC. ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest. Last access: 16.07.2012.

[ROUT12] Routeviews.org. http://archive.routeviews.org/oix-route-views/. Last access: 16.07.2012.

[SITE12a] Sitevet.com: SiteVet Autonomous System Repor t AS680 - DFN. http://sitevet.com/pdf/asn/AS680. Last access: 16.07.2012.

[SITE12b] Sitevet.com: HE Index. http://sitevet.com/info/he_index.php. Last access: 16.07.2012.

[SITE12c] Sitevet.com: HE Rank. http://sitevet.com/info/he_rank.php. Last access: 16.07.2012.

[TECH11] Technorati: Egypt Counts Cost of Protests, Internet Down-Time. http://technorati.com/politics/article/egypt-counts-cost-of-protests-internet/. Last access: 16.07.2012.