Secure routing: State-of-the-art deployment and impact on network resilience

enisa
European Network and Information Security Agency

About ENISA: *The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors. Internet: http://www.enisa.europa.eu/*

Contact details:

To contact ENISA or for enquiries regarding this study, please communicate with:

Technical Department, Security Tools and Architectures Section
Email: sta@enisa.europa.eu
Web: http://www.enisa.europa.eu/act/res/technologies/tech/routing/

This report is the result of the collaboration between the European Network and Information Security Agency (ENISA), GNKS Consult http://www.gnksconsult.com/ and NLnet Labs http://www.nlnetlabs.nl/.

Acknowledgements:

The authors are grateful to all who contributed—in the first place to the people who helped us to make it possible to launch a survey in the community using existing mailing lists, thus targeting those who truly matter in the field; in Europe, Rob Evans and João Damas (RIPE Routing WG), Henk Steenman (AMS-IX), Mike Hughes (LINX), Wolfgang Tremmel (DE-CIX), Kurtis Lindqvist (Netnod) and Serge Radovcic (Euro-IX). We would also like to thank the people who volunteered their time for an interview, either during IETF 77 in Anaheim (March 2010), RIPE 60 in Prague (May 2010), or over the telephone at other times. Daniel Karrenberg (RIPE NCC) provided important feedback on the draft final version of this document.

Legal notice: Notice must be taken that this publication represents the views and interpretations of the editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of the-art in secure routing technologies deployment and it may be updated from time to time. Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

Table of contents

Executive summary

Reliable communications networks and services are now critical for public welfare and economic stability. Intentional attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human mistakes all affect the proper functioning of public communications networks. Such disruptions reveal the increased dependence of our society on these networks and their services. A vital part of reliable communication networks is the routing infrastructure.

Routing is enabled by the Border Gateway Protocol (BGP) whose purpose is to keep systems on the Internet up to date with the information needed to send and receive data between independent networks; therefore the name inter-domain routing is also used for the routing between the boundaries of network operators.

BGP is a flexible protocol that provides many ways to sustain the system and address network failures as well as changes in network topology. The main goal of the protocol is to maintain connectivity between domains so that traffic can be efficiently routed to its destination. Without BGP, inter-domain routing, email, Web browsing and other Internet communications would not reach their intended destinations. Securing inter-domain routing is critical to keeping the Internet running smoothly.

It is clear that there is no single common understanding on what the issues really are. For the sake of our study we define *routing security* as follows: ‘Routing security is the set of measures taken to ensure the protection of the routers, and the correct operation of the routing control and data plane according to the intended policies and business relations’.

The study used an online survey and a number of interviews with stakeholders. Concerns have been expressed about the current state of security of the routing infrastructure and the need to take action to improve security. There is a rough consensus on the first step to improve the quality of the techniques currently deployed. A next step involving resource public key infrastructure (RPKI) is mentioned by most interviewees; however there are differing opinions about its deployment, the policies involved, and how the RPKI will be used. The most outspoken concern is an apprehensive feeling concerning a loss of autonomy by the ISPs or even by nations.

At the same time a trend was identified, in that organisations involved in routing would tend to keep security breaches ‘under cover’ rather than share them with the wider community, in particular if a breach were the result of targeted attacks. The study did not investigate security incidents, but rather explored current practices and future perspectives in routing security technology.

The barriers to any improvement on routing security are the implementation and operational costs. However, while stability is the underlying doctrine in network management, increased complexity and consequently increased difficulty in configuration and fault mitigation are also consistently mentioned as hurdles hindering the successful deployment of routing security.

Autonomy in transit, customer, and peering agreements and the routing policies expressing these agreements are at the core of the business of an ISP. The sector seems to have low confidence in government involvement with routing policies or with a single authoritative trust anchor. At the same time it is clear to interviewees that governments may move towards defining security requirements (eg, in terms of compliance). A natural role for governments is seen in the stimulation of investment, support for public R&D, and the raising of awareness. Within this self-made, originally mainly technical, Internet community, it is not surprising that there is a preference for self-regulation above legislative measures.

To improve on the current state of routing security, a number of recommendations emerged from the analysis of the information received in the online survey and the interviews with participants in the field study.

- Stimulate investments in the development of routers and (validation) tools to increase the level and quality of routing security.
- Stimulate self-regulation and the development of compliance to routing security regulations.
- Facilitate and stimulate better research on monitoring and the availability of routing data.
- Ensure the exchange of information and monitor the evolution of existing and possible future threats.
- Increase awareness of RPKI among network architects and operators.
- Leverage tier 1 and large tier 2 networks with the introduction of routing security technology.
- Demand specific measures to ensure routing security in public tenders.

Introduction

Reliable communications networks and services are now critical to public welfare and economic stability. Intentional attacks on the Internet, disruptions due to physical phenomena, software and hardware failures and human mistakes all affect the proper functioning of public communications networks. Such disruptions reveal the increased dependence of our society on these networks and their services. Experience shows that neither single providers nor a country alone can effectively detect, prevent, and respond to such threats. A vital part of reliable communication networks is the routing infrastructure.

Communications[1] [2] [3] from the European Commission have already highlighted the importance of network and information security and resilience for the creation of a single European information space that will drive job creation, sustainability and social inclusion, and so contribute to the overall goals of the Europe 2020 strategy[4]. They have stressed the importance of dialogue, partnership and the empowerment of all stakeholders to properly address these threats. The updated Regulatory Framework Directives[5] [6] include certain regulatory provisions for the improvement of the security and resilience of public eCommunications.

[1] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *i2010 – A European Information Society for growth and employment* /* COM/2005/0229 final */ http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF

[2] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *A strategy for a Secure Information Society – Dialogue, partnership and empowerment* /* COM(2006) 251 */
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Digital Agenda for Europe* /* COM/2010/0245 final */
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT

[4] http://ec.europa.eu/eu2020/index_en.htm

[5] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

[6] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

Since 2008 ENISA has been running a programme with the objective of collectively evaluating and improving the resilience of public eCommunications in Europe. The programme is comprised of four distinct phases.

The first step undertaken was an analysis on how national authorities implement current regulatory measures. This involved assessing how network and service providers of public communication networks ensure the availability and integrity of their networks and services, and evaluating whether existing technologies satisfy the needs and requirements of these providers. In this light an assessment of three key technologies (namely IP version 6, Multiprotocol Label Switching and DNS Security Extensions) was undertaken regarding their potential to provide increased network resilience[7]. This analysis was carried out from two perspectives.

The first consisted of analysing the characteristics of the selected technologies and their public communication network's resilience enhancing features[8]. In parallel, the effectiveness of these technologies, as well as the problems and gaps that potentially could compromise the availability of networks and services, was assessed through interviews with twelve network operators in the EU Member States[9].

Routing infrastructure is a critical infrastructure that needs to be attended in order to secure public communication networks. ***ENISA aims to assess the impact of deploying secure routing technologies. In particular, a survey was conducted of network operators in the EU on the use of or (concrete) plans to use secure routing technologies. It is the intent of ENISA to use the assessment to produce guidelines and/or recommendations for the deployment of secure routing technologies, targeting policy makers.***

The Internet evolved from the interconnection of independent networks and, as of today, it is still constantly evolving; the number of networks, the relations between them, and their connectivity are changing all the time. With the interconnection of independent networks (domains), a mechanism is needed to route data between the various domains.

Routing is enabled by the Border Gateway Protocol (BGP) whose purpose is to keep systems on the Internet up to date with the information needed to send and receive data between independent networks; therefore the name inter-domain routing is also used for the routing between the

[7] http://www.enisa.europa.eu/act/it/inf/tech

[8] http://www.enisa.europa.eu/act/it/library/deliverables/res-feat/at_download/fullReport

[9] http://www.enisa.europa.eu/act/it/library/deliverables/stock-tech-res/at_download/fullReport

boundaries of network operators. BGP is a rich protocol that has many features that enable it to cope with network failures as well as changes in the network topology. The main goal of the protocol is to maintain connectivity between domains so that traffic can be efficiently routed to its destination.

Without BGP, inter-domain routing, email, Web browsing, and other Internet communications would not reach their intended destinations. Securing inter-domain routing is thus critical to keeping the Internet running smoothly. Given the security concerns relating to the inter-domain routing system, several initiatives have already been launched to study the risks and analyse the threats, to develop technological solutions, and to formulate policies. The most notable are contributions from the IETF working groups and regional internet registries (RIRs).

The main objective of this report was to assess the impact of deploying secure routing technologies by carrying out a survey of network operators in the EU on their use of, or plans to use, secure routing technologies, including their performance expectations and operating experiences.

The awareness, availability, and actual and expected deployment of enhanced routing security were assessed. The experiences network operators have with network insecurity and the measures they have already taken to increase the level of routing security were explored. As there is 'no such thing' as a secure routing technology directly available for deployment, network operators apply a number of strategies and methods to secure their routing infrastructures; each has its own merits. The technologies deployed and the operational practices available to make inter-domain routing more secure were assessed, as well as the extent to which operators are prepared to invest in these technologies.

The study used an online survey and a number of interviews with stakeholders. Invitations to participate in the survey went out to the Internet communities. The survey inquired into the perception of those who are considering taking measures and the experiences of those who have already taken certain measures regarding secure routing technology, both in terms of investment and the realized and expected impact of several alternative measures, the plans of operators, and the factors inhibiting the global or local deployment of this technology.

In this report, we first present the background against which the study was conducted. This is followed by a presentation of the results of the study arising from the survey are discussed, and the insights obtained from the interviews and a moderated discussion of the RIPE Routing Working Group on 5 May 2010 in Prague.

Background

Border Gateway Protocol (BGP) is a protocol used for maintaining routing information between network domains which, in BGP, are also called autonomous systems (ASs). Each AS is connected to a number of other ASs (called neighbours or peers) and exchanges its routes with them according to AS-specific policies. After receiving information, an AS may propagate it to its own neighbours; this is why BGP is also known as 'routing by rumour'. BGP is vector-path based, which implies that BGP routers do not have the full topological view of the network. Each router knows only how to reach its direct neighbours and through which neighbour particular destinations can be reached.

For each destination network, an AS can use only one path as its default path, which is generally the shortest path according to local AS policies. It can propagate this path to its neighbours, so that they can use the AS as a transit for their traffic routing. In addition to the default path, all alternative paths leading to a given destination network received from the other neighbours have to be stored. This allows the connectivity to be restored quickly when the default path becomes unavailable. An AS may then start to use another path to route data packets and maintain connectivity even when a link has failed or when network topology or reachability has changed.

The current inter-domain routing protocol BGP assumes that the routing data exchanged between routers is correct, that is, that it complies with its neighbours' routing policies and peering agreements. The assumption is not always valid, and this makes the inter-domain routing infrastructure vulnerable to both accidental misconfiguration and deliberate attacks. The most notable recent accidental faults are the black-holing of Google YouTube by the Pakistan Telecommunication Company (February 2008) and the global Internet meltdown (for about one hour) by SuproNet, a local Czech provider (February 2009). At the DEFCON 16 conference in August 2008, Pilosov and Kapela (2008) showed how an attacker could eavesdrop or change data streams by exploiting BGP. The attacker would reroute all the traffic[10] of the target through their own network and then send it to its destination without the owner's knowledge.

BGP assumes that the routing data exchanged between routers is correct. This makes it vulnerable to both accidental misconfiguration and attacks.

A number of efforts have been proposed to protect routing protocols against faults and attacks. These include: TCP MD5 protection of BGP sessions; Byzantine robustness in the routing protocol; securing the exchange of BGP routing updates through the encryption of communication channels;

[10] *A more effective attack is not to re-route all traffic but to do so selectively. Easiest: do it a few minutes at a time.*

authorization of origin information and authorization of AS path data; and using protocol and network properties to detect faults, eg, prefix filtering by comparing received routes against the information listed in the Internet routing registry (IRR) database.

Previous work

There are a number of documents that present an analysis of security and inter-domain routing. One such important document is IETF RFC 4593 *Generic Threats to Routing Protocols*, which provides a description and a summary of threats that affect routing protocols in general. This document describes a threat model, including a taxonomy of threat sources and the consequences of threats. Given the threat model, different attack scenarios are discussed, as well as their consequences and how they may be mitigated.

Nordstrom and Dovrolis (2004) identify several attack objects and mechanisms, assuming that one or more BGP routers have been compromised. They also review existing and proposed countermeasures, stating that some mechanisms are either ineffective or probably too heavyweight to deploy.

Pei, Zhang, and Massey (2004) present their threat model as a fault tree, where each node in the tree represents a potential cause of faults. With the fault tree, they associate a so-called multi-fence defence framework, covering various components that add resilience to Internet routing.

Butler *et al* (2010) survey BGP security by analysing the vulnerabilities of existing inter-domain routing and presenting projects relating to BGP security. The limitations and advantages of proposed solutions are explored, and the systemic and operational implications of their design considered. The authors arrive at the same conclusion as Pei, Zhang, and Massey.

The NIST Border Gateway Protocol Security report (Kuhn *et al*, 2007) presents a comprehensive overview of BGP threats. The generic attacks are similar to attacks against other networked devices. Routers can be subject to denial of service, unauthorised access, eavesdropping, packet manipulation, session hijacking, and other attacks. Attacks targeting BGP routers can be extensions or specific cases of these.

To complement this report, ENISA has published a report on *Secure routing technologies*. That report addresses the issue of vulnerabilities in the routing protocols and related threats; attack objectives, mechanisms and the extent of their effects; mitigation measures; the operation of proposed secure routing protocols and the threats they are addressing; and the hurdles hindering their deployment. It also provides recommendations on the implementation of secure routing technologies. The report is available at: https://www.enisa.europa.eu/act/res/technologies/tech/routing/

Threat analysis

Potential attacks on the BGP protocol include peer spoofing and TCP resets, either inserting false information into the routing tables or resetting a BGP session resulting in the withdrawal of routes previously learned from each other.

BGP session hijacking can achieve more than simply bringing down a session; for example, the objective may be to change routes used by the peer, in order to facilitate eavesdropping, black-holing, or traffic analysis.

An attacker who announces a more specific route would be able to divert traffic to its own network, as BGP gives preference to the most specific routes.

Route disaggregation occurs when more specific routes are advertised by BGP peers. In some cases this is a normal operation resulting from configuration changes, but it can occur as a result of error or malicious activity. Because BGP gives preference to the most specific routes, it is effectively announcing it has the optimal path to a destination, so routing tables are updated, and the new route is propagated to other peers.

With incorrect or malicious route injection a party could begin sending out updates with incorrect routing information. Unallocated route injection is a variety of malicious route injection of routes to unallocated IP addresses. As these IP addresses have not yet been assigned, no traffic should be routed to them.

Current practice to counter threats

The current practice of securing inter-domain routing is a combination of session security, the filtering of BGP messages, anomaly detection (monitoring) and mitigation. The resource public key infrastructure, used to validate BGP announcements, has just recently been proposed and will be deployed in the next few years.

A number of methods are available to implement session security, eg, TCP MD5, IPsec, or ingress filtering (IETF BCP 38). With TCP MD5 or IPsec, a cryptographic method is used to authenticate the neighbour and validate the peer according to routing policies. Ingress filtering protects the router against spoofing. These technologies mitigate peer spoofing, TCP resets, and BGP session hijacks. The BGP TTL hack prevents malicious attacks from systems more than one hop away from the router.

Defensive filtering of suspicious BPG announcements is used to filter bad and potentially malicious announcements. Routers commonly filter incoming and outgoing routes based on routing policies, and filter against known IP address allocations obtained from an Internet route registries (IRR) database. If a BGP announcement arrives at a network, the validity of the IP end destination is checked against the IRR allocation database. Invalid BGP announcements are discarded to prevent IP address hijacking.

This mitigates route disaggregation, incorrect or malicious route injection and unallocated route injection. In addition to filtering incoming prefixes, outgoing prefixes should also be filtered. That practice would protect one's neighbours from configuration mistakes one might make. Route disaggregation can also be countered by maximum prefix filtering, a simple and effective way to control how many prefixes can be received from a neighbour.

This BGP filtering scheme is voluntary and quite brittle, as is shown by the global black-holing of Google YouTube by the Pakistan Telecommunication Company, or by a single router misconfiguration in the Czech Republic that resulted in a major disruption to the Internet.

Currently the state-of-the-art in route filtering is based on the use of data that is voluntarily collected in one of the various Internet route registries. Since the quality of these registries can vary globally, this technique is not used as effectively as possible everywhere. The current methods for adding or updating Internet IRR data have weak security.

Available technologies and research & development

In response to the insecure and brittle solutions to prevent IP hijacking and to create a more reliable and secure inter-domain routing infrastructure, a number of solutions have been proposed. The most well-known proposals are S-BGP by Stephen Kent (2003) and soBGP (secure origin BGP) by Russ White (2003). S-BGP provides secure communication with neighbours, and generates and validates BGP updates relative to an authorization model and address attestations.

A PKI is used to represent the delegation of IP prefixes and AS numbers. Address attestations authorise an AS to originate routes to a prefix, and a route attestation authorises a neighbour to advertise prefixes. IPsec is used for point-to-point security of BGP traffic between routers. Secure origin BGP (soBGP) addresses four goals to secure BGP: AS origin authorisation, valid AS path verification, peer advertising authorisation, and whether the path advertised by a peer AS falls within the policies.

S-BGP and soBGP are conceptually different, namely in whether they are signing actual routing information passing through the system (included in but not limited to S-BGP), or describe the routing system dynamically and in real time, and in how they decide if the routing information you are receiving actually matches the description you have built (eg, soBGP, IRV, and even reverse DNS lookup solutions).

Besides the two secure BGP protocols described above, a number of academic papers have been published on secure inter-domain routing. Dan, Pei, and Massey (2004) present a framework for resilient Internet routing protocols, and review the various approaches to secure routing protocols. Important observations the authors make are:

- in large systems such as today's Internet, faults are the norm rather than the exception;
- cryptographic protection mechanisms can be effective against specific faults, but cannot detect or prevent all types of faults; and
- a number of detection mechanisms have been developed and, although each is limited, collectively they can provide a strong overall protection against faults.

Clark *et al* (2003) and Feamster *et al* (2004) address a number of problems and architectural responses to real-world demands on the Internet, including weak security in inter-domain routing.

In addition, regional internet registries (RIRs), such as RIPE NCC, APNIC, and ARIN, have started pilot studies to provide feedback to the IETF working groups RPSEC and SIDR[11] on protocol design.

Besides running pilot studies, a RIR can fulfil an enabling role for the deployment of technologies for secure routing while, at the same time, offering a platform for the development of policy proposals for its community, namely the members of the RIR. In particular the development of a resource public key infrastructure (RPKI) by various RIRs establishes an important foundation on which secure routing techniques can be built.

In addition to the inter-domain routing security techniques developed in IETF SIDR, there are a number of developments to secure the routing protocols themselves and to allow for secured authentication of neighbours in the routing infrastructure and verification of the integrity of routing message, the deployment of which allows for piecemeal introduction. The IETF KARP[12] working group is chartered to do work in this area. Currently this group is defining the framework and requirements, and documenting the best current practices for creating and using protocol message authentication integrity keys.

[11] See http://datatracker.ietf.org/wg/sidr/charter/

[12] See http://datatracker.ietf.org/wg/karp/charter/

Survey results

To provide a good overview of the impact of deploying secure routing technologies, a survey was carried out amongst network operators on their use of, or plans to use, secure routing technologies, including their performance expectations and operating experiences. Invitations to respond to the questionnaire, set up for this purpose, were sent out using the mailing lists of relevant working groups at RIPE and the Internet exchanges of Amsterdam (AMS-IX), London (LINX), Frankfurt (DE-CIX) and Stockholm (Netnod), and Euro-IX (covering the other exchanges in Europe).

About 120 respondents took the time to share their experiences and insights by responding to an online questionnaire (ANNEX 2: Questionnaire). The survey was conducted between February and March 2010. The results are presented in this chapter and are not traceable to individual respondents[13].

Profile of participants

More than 120 respondents from 34 countries participated in the survey, including a large contingent of Dutch (24%), Germans (20%), followed by Swedes and others at 5% or less. About 80% of the respondents originate from EU countries. 64% of all respondents are ISPs, while 11.5% are content providers. The other 24.5% is divided across many categories, as shown in Figure 1.

In terms of 'responsibilities', 44% of the respondents were from the technical or operational level, 44% were from the strategic or architectural level, and the remaining 12% indicated they were at the policy or managerial level.

Awareness of secure routing issues

Awareness of security routing amongst respondents is high. When asked: 'Are you aware of security risks in inter-domain routing, in particular of the (external) Border Gateway Protocol?', only 2% of respondents answered 'no', 78% said 'yes', and 20% said 'somewhat'. Obviously, people who are less aware might be less inclined to complete the survey. At the same time the answers indicate that knowledge of the issues is relatively high in this population.

[13] *Personal information gathered through this survey was processed and stored in compliance with regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.*

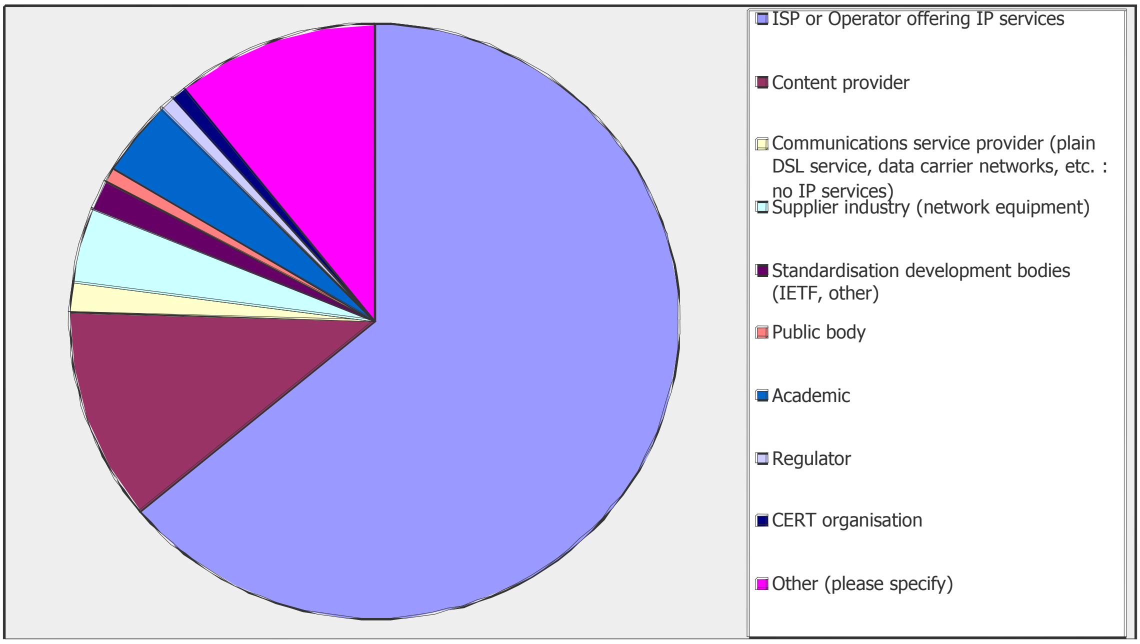


Figure 1: What type of organisation do you represent?

In terms of available technologies or methods to improve routing security, four clusters were distinguished. Awareness of session security methods (97%) and monitoring and filtering methods (87%) score high in awareness, but only 39% of respondents are somewhat aware of PKI based solutions, as is clear from Table 1.

Table 1: Which available technology/methods are you aware of?

Answer Options	Response Percent
Session security (TCP MD5, IPSec, BGP TTL Security Hack, Network Ingress Filtering (BCP 39), etc)	96.6%
Monitoring and filtering (IRR/RPSL based filtering, prefix filtering, AS-path filtering, Renesys Routing Intelligence, RIPE IS Alarms–MyASN project, etc)	87.1%
PKI-based solutions (cryptographic, certification/attestation)	38.8%
Don't know	1.7%

An important factor in awareness is experiencing routing related security incidents: 32% reports having suffered from this. From those who reported incidents, 18% said that it caused a ‘major disruption’, 30% reported a minor disruption, and 52% hardly noticed a disruption resulting from the incidents experienced. Examples of non-intentional incidents are full routing table re-announcements (attracting all traffic to your network), or route leakage and providing unintentional transit connectivity to a peer. Malicious IP prefix hijacks are fly-by spammers (announce prefix, spam, and withdraw), malicious denial-of-service or outage attacks (eg, to damage competitors), or target impersonation (hijack address space and setup impersonation service). Also, the incidents generated a strong positive, or positive, impact on awareness about routing security issues.

In terms of awareness of new initiatives, S-BGP, soBGP and RPKI score highest, yet more than 40% of the respondents are not aware of these. Highest expectations are with RPKI (25%), followed by S-BGP (12%).

Plans to deploy secure routing

Among those who responded to the survey, deploying routing security is seen as important, but not a priority (63%). 25% of respondents see it as top priority, 12% of respondents do not think it is important. Those who do not think it is important say that they are not aware of having experienced incidents yet.

It is generally estimated that improved routing security is valued by customers (58% of respondents think so), upstream providers (64%) and peers (69%). Today, the biggest risk for organizations should routing security be breached is damage to reputation (77%), followed by reduced performance (69%) and loss of money (43%). Session security methods and technologies are mostly deployed, followed by monitoring and filtering, as is clear from Figure 2.

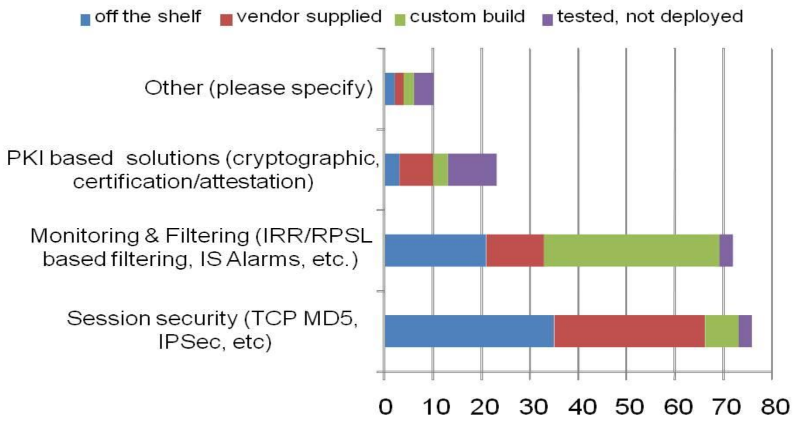


Figure 2: Which methods are deployed to improve security of inter-domain routing (absolute numbers)?

Monitoring and filtering are currently seen as the most effective solution by respondents (80% of respondents use monitoring and filtering), followed by session security (48%). As PKI is hardly deployed currently, it is not entirely clear what is meant by the score on ‘PKI based solutions’. With that, there are an equal number of respondents who consider PKI based solutions counterproductive, as there are those who find it effective (21%).

At the same time, 43% respondents indicate that the implementation of session security solutions is seen as easier to implement, and only 8% indicates this for PKI. 25% of the responders think that the risks of misconfiguration are increasing with the implementation of monitoring and filtering, whereas 12% of them or less foresee increasing risks when implementing other security measures.

Drivers and barriers

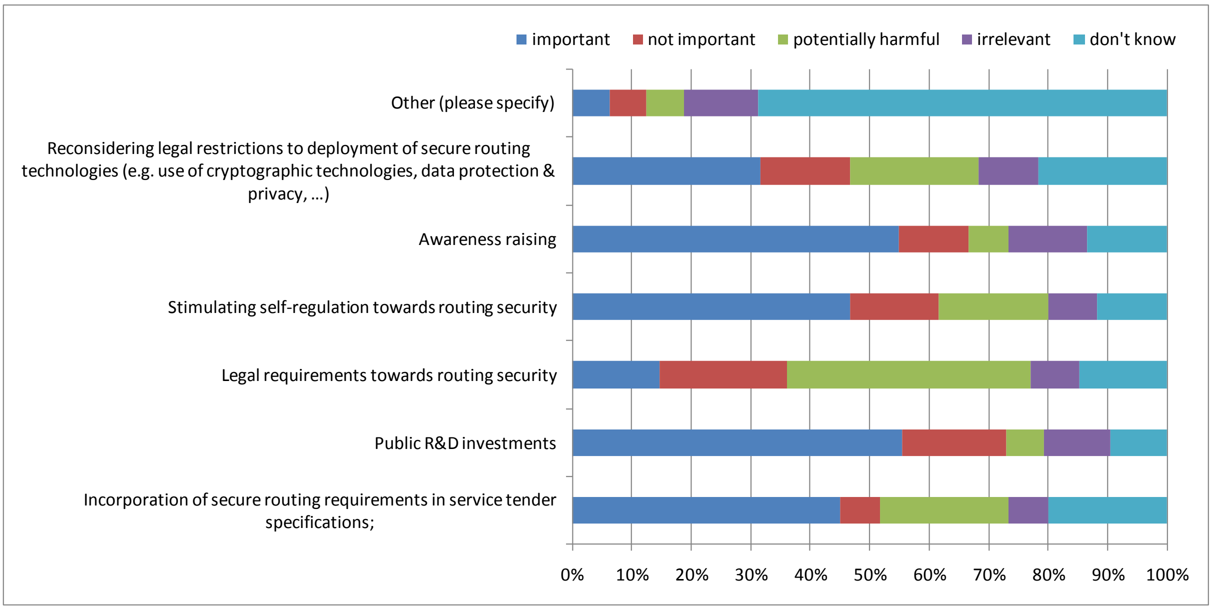
A reduction in operational risks is seen as the strongest driver (83%) towards securing the routing infrastructure; this is followed by an improvement in the image presented to customers (60%) and an expected reduction in operational costs (30%). The largest barrier is availability of knowledge (65%), and 45% of respondents expect an increase in costs, or find the implementation costs a hindrance. Just 32% have no confidence in their effectiveness.

Considering investments

About 38% of the respondents are considering investing in one or more areas of monitoring and filtering, session security, and PKI based solutions (each considered by about 30% of the respondents). A clear minority is considering investing considerable amounts, now or in the future (25% or less).

Role of government

With regards to the role of governments, respondents think the most positive effects could come from public R&D investments, followed by awareness-raising activities, and the stimulation of self-regulation and the incorporation of routing security requirements in tendering. Regulatory measures are considered possibly damaging by most of the respondents, as is clear from Figure 3.



Answer Options	important	not important	potentially harmful	irrelevant	don't know
Incorporation of secure routing requirements in service tender specifications;	27	4	13	4	12
Public R&D investments	35	11	4	7	6
Legal requirements towards routing security	9	13	25	5	9
Stimulating self-regulation towards routing security	28	9	11	5	7
Awareness raising	33	7	4	8	8
Reconsidering legal restrictions to deployment of secure routing technologies (e.g. use of cryptographic technologies, data protection & privacy, ...)	19	9	13	6	13
Other (please specify)	1	1	1	2	11

Figure 3: Should government facilitate by … (see first column)?

Conclusions and observations

The results show that session security and monitoring and filtering are both widely applied to protect the routing infrastructure. The deployment figures for session security and monitoring and filtering show almost identical values. For session security, deployed technology is almost exclusively off-the-shelve or vendor supplied. For monitoring and filtering, the deployed technology is mainly custom build. From discussions with experts, it became apparent that much consideration goes into the ‘art’ of filtering, where expertise is needed to implement policies that are both correct and effective. It is striking that, amongst respondents, the level of awareness of RPKI is at the time of the survey was still low.

From governments, it is expected that investments will be primarily in public R&D and that awareness should be raised on the threats to the routing infrastructure and on the available solutions. In this community, it is no surprise that there is a preference for self-regulation above legislative measures. Whilst the desire for continued high levels of autonomy is with no doubt an important driver in this, it is also true that the sector itself is much better aware of the challenges and possible solutions, so effective self-regulation is probably the most potent way forward.

Interview results: analysis based on the responses and debate

In order to be able to get beyond the responses to the survey questionnaire in understanding the real issues regarding routing security, 21 interviews were conducted between March and May 2010. Ten of the interviewees were network operators from European ISPs, while four were network operators from outside Europe (mainly from the USA). The others were academics involved in studying routing, non-profit organizations such as RIPE and APNIC that support routing, and product vendors. Prospective candidates for the interviews were approached through the RIPE and IETF community networks. Participants in the online survey who indicated their willingness to contribute to the study were also invited to the interviews.

The semi-structured interviews[14] were conducted either face-to-face or by telephone in the period March–April, and took 30 to 40 minutes each. The interviews were focused on specific insights relating to routing insecurity and how to improve security, in the full understanding that perfect security does not exist and that Internet routing is currently 'secure enough' to give many people and organizations around the world the confidence to rely on the Internet. The questions targeted on the specific area of knowledge of each interviewee and contributed to an increase in insight into the general state of awareness, the current state-of-the-art, expected future developments, and possible ways forward.

In addition, at the RIPE 60 Routing WG meeting in May 2010, a discussion session was scheduled on the subject of the survey. In this session, the RIPE community members were asked to discuss some of the outcomes of the online survey presented at the open plenary session the day before, and these discussions have been taken into account as well. Whereas the interviewees are not explicitly named, speakers during the public session are named where appropriate.

The following sections present the perceived level of awareness and current practices in securing networks. Next, expectations about future security threats are discussed, and ideas and approaches to counter these threats are put into perspective. The final sections describe the cost factors (both capital and operational expenditure), the expected benefits of routing security, and considerations for successful deployment.

[14] *As agreed with the interviewees and in compliance with Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000, all interviews are treated in confidence and the results are not attributed to individual persons.*

Routing security awareness and application, today

While the general awareness of routing security issues is quite high, as was also already apparent from the survey (78% aware, 20% 'somewhat aware' and only 2% not aware, see above) it became clear during the interviews that there is no single common understanding of what the issues are exactly. A high-level (functional) definition, given by one of the participants, specifies routing security as maintaining correct routing tables. Others definitions explicitly refer to IP-level security (session security) or the use of different networks (telco, data, ...), each with different security measures being taken.

From the interviews it became clear that there is no single common understanding of routing security.

For this study *routing security* is defined as follows:

Routing security is the set of measures taken to ensure the protection of the routers, and the correct operation of the routing control and data plane according to the intended policies and business relations.

Deploying routing security on the procedures and infrastructure of network operators will mitigate threats that can create incidents that have a great impact on the resilience of the networks.

From the interviews with the network operators, it became apparent that the first concern in operating a network is to ensure stability (availability) rather than security. Typically, people do not care about security as long as they do not have any problems with it. When taking security measures it is therefore important to understand the measures that would impede stability. Only if the stability of the network breaks down due to a lack of security will action be taken to secure the infrastructure and to restore stability. This understanding will be reiterated where necessary in the next sections discussing techniques to improve routing security.

For operators, the first concern in operating a network is to ensure stability (availability) rather than security.

The level of awareness in routing security issues clearly relates to the size and focus of network operators. Typically, tier 1 networks have a large, highly qualified security staff, and the awareness level on potential issues and solutions is very high (as it is also their daily business). For tier 2 network operators, the awareness level is already mediocre and/or more limited, and for tier 3 network operators and smaller operators, in general, the awareness level of issues arising and the potential ways of mitigating these is low.

These findings are in line with the results presented in Arbor Networks' *Network Infrastructure Security Report* (2010). Awareness did increase after the Pakistan YouTube incident (February 2008) and the *Stealing the Internet* DEF CON 16 presentation of Pilosov and Kapela (2008). But for most BGP incidents, there is no public news: routing is a handshake deal, and after an incident the issue is settled over a telephone call. As incidents are almost never made public, the level of awareness is relatively low in the community. The relatively high level of awareness apparent from the survey (in the previous section) can be explained by an obvious bias in the group of respondents, as the decision to invest time in completing in the survey can be explained by a specific interest in the topic rather than 'just having some spare time'.

Routing security in the core of the network is a shared responsibility of every ISP.

During the RIPE Routing WG session in Prague (May 2010), Rüdiger Volk (Deutsche Telekom) pointed out that routing security in the core of the network is a shared responsibility of every ISP. The routing infrastructure is fragile and attacks are easy. Most of the incidents have to do with 'fat fingering' and configuration errors and are thus non-intentional (non-malicious) security incidents. Fortunately only these incidents have received publicity.

The public perception of Internet security and reliability is quite positive but, according to Mr Volk, serious improvements need to be put in place before this public perception changes. A breach in this perception would damage the industry and it would be very hard to regain the positive judgement of the public.

Pilosov and Kapela (2008) presented, at DEF CON 16, a more sophisticated man-in-the-middle attack that is almost invisible except for a change in AS routing path. The AS path does eventually reveal the attacker, but changes in AS paths are a normal operation in a dynamic network such as the Internet and are currently mostly not double-checked. In addition, as Randy Bush (Internet Initiative Japan) pointed out during the RIPE Routing WG session, it is important to define the term 'attack'.

Actually it is important not to use the term 'attack' for 'fat fingers', but for the real routing attacks that are not talked about in public, just as banks do not like to talk about large frauds. The term attack should be used when there is a deliberate violation of the intended policy. While it is widely perceived that most attacks come from fat fingering, the non-malicious intent is not always clear. An additional problem is that the data plane does not follow the control plane; data packets are routed via different paths than announced by the routing protocol (Goldberg *et al*, 2008). Until this is fixed, no amount of security in the control plane will solve the problem.

To protect networks from both intentional attacks and non-intentional configuration errors, a number of techniques are currently deployed in combination to counter these incidents. Currently applied techniques can be classified into three categories:

1. session security: IP-level security (authentication and authorization);

2. filtering: correctness of routing tables;
3. monitoring: anomaly detection and alerting the responsible parties.

Whereas in the survey we talk about the categories of session security, filtering and monitoring, and encryption based techniques, it is clear that the use of encryption based techniques are not state-of-the-art yet, although activities are in preparation to develop (the application of) these techniques (see next section of this report). In addition, during the interviews it became clear that filtering and monitoring should be considered separately, as both have their own merits and challenges. Although many security measures are in place within the networks, the usage and quality of the tools are lagging behind, and a YouTube incident as in Pakistan can happen again.

Session security

Session security encompasses a number of methods to secure access to and interaction with the router. Widely applied methods include MD5 digests for authentication, TTL hack (based on Generalized TTL Security Mechanism) and ingress filtering (BCP 38) to counter spoofing (see also: Arbor Networks study). In the survey, 48% of the participants indicated that current session security methods are providing effective solutions. Although not considered the most effective method, the participants mentioned it as the most easily deployed method.

Session security is mentioned as the most easily deployed method.

From the interviews it appears that the use of MD5 authenticated sessions varies highly. Some operators require MD5 authentication from their peers, or from both peers and customers, and/or are required to use MD5 themselves by their transit providers. A weak point of MD5 is the ’password’ (shared secret) distribution (eg, broken and revealed password generation strategy). In addition, some routers have trouble booting and initializing 150+ BGP sessions with MD5 because of the high computational load related to the cryptography. Some operators have tested MD5, but the security risks in their operational environment did not justify its use. One operator noted that about 1/3 of BGP sessions are using MD5 authentication, and the absence of incidents makes further deployment not urgent. Recently, TCP Authentication Option (TCP-AO) has been accepted as an IETF RFC and might replace MD5 in the future, as it is easier to manage than MD5.

IPsec for session security is hardly deployed in practice. Routers are optimized towards current practices and protocols. When confronted with encapsulation systems (such as IPsec), the priority of a message cannot be determined directly from its header and/or contents: packets need to be decapsulated in order to be able to detect the message priority, which is a lot of extra effort in handling.

Routers are constantly under attack, eg, port scans, attempts to open SSL/SSH sessions, open ports, attempts to access the routers using the RADIUS protocol, etc. These threats are countered by firewalls that are activated when necessary.

Filtering

Filtering of BGP announcements is used to secure correct router tables that reflect the policies and intentions of the agreed BGP business relations between parties (the transit, customer, and peer agreements). Filtering is, with monitoring, the most effective solution according to 80% of the respondents to the online survey.

> Filtering is, with monitoring, the most effective solution according to 80% of the respondents to the online survey.

Three main filtering methods are distinguished by the interviewees, all with their own merits and challenges: IP prefix filtering, AS path filtering, and maximum prefix filtering.

IP prefix filtering: the challenge with prefix filtering is the generation of the prefix filter list. The so-called bogon filters are commonly installed to filter private and reserved address spaces (RFC 1918 and RFC 5735) as well as netblocks that have not been allocated. More specific filters could be constructed from the Internet routing registry (IRR) databases. The IRRs are databases where network operators publish their routing policies and routing announcements so that other network operators can use this data. Unfortunately, the quality of the IRRs varies, which makes it difficult to rely on them. For instance, the RIPE IRR is considered to be fairly consistent, as RIPE has strict policies regarding the IRR. RADb (a routing assets database run by Merit Networks) takes another perspective on its role as an IRR. RADb collects (aggregates) data from various sources and uses custom algorithms to create route objects. An interviewee indicated that within the APNIC region, only JPNIC has a consistent IRR.

The development of tools for the construction of filters based on IRRs can be based on the IRR toolset. The IRR toolset is complete but is also considered to be complex and not well documented. Many interviewees stated that they never came round to using the IRR toolset.

In the end, there is no single authoritative source that indicates how address space is allocated from IANA to the end-user. The RIRs, as stakeholders, have build the IRRs, but with the BGP protocol, routing is by rumour and it is up to the many independent players in the routing landscape to decide whether to trust specific information (announcements or IRR data) or not.

Confronted with poor data, filtering has become quite labour intensive for ISPs, and the processes are poorly documented. Some large ISPs have developed some internal policies and tooling to automate part of the process to construct customer filter lists. Most traffic via peering is traditionally not filtered, as peers trust each other to filter their customers. And with all prefix filtering lists installed, one has to ascertain that there are no configuration errors resulting in unreachable destinations, ie, customers can reach all other destinations and, vice versa, all other destinations can reach one's customers. Also, from the online survey, it can be seen that implementing filtering is considered a complex task.

During the RIPE Routing WG session, Rüdiger Volk described a very simple method of using the resource public key infrastructure (RPKI) that involves no change to the IRR, software that uses the IRR, or the RPKI. This proposal has been made in APNIC, RIPE, and ARIN.

AS path filtering gives fewer concerns about reachability, and adds to stability. It is an efficient alternative to listing hundreds of routes one-by-one, as might be required when filtering on a prefix basis is applied instead. According to one of the interviewees, it provides sufficient protection for reasonable effort. In particular for peers, route leaks (providing transit AS for other ASs) can be prevented.

Maximum prefix filtering is a simple and effective way to control how many prefixes can be received from a neighbour. Maximum prefix filtering is commonly used to counter configuration errors at the remote peering site, resulting in an increase in the number of received routes (ie, if remote peers announce the full routing table).

For some ISPs, full prefix and AS path filtering results in a critical loss of performance. These ISPs first accept an announcement and only then check whether the announcement is valid.

Finally, filtering only captures the most obvious errors and incidents. It is not suited to dealing with smart and sophisticated attacks, which are the ones we are most concerned with, but it does help in avoiding performance setbacks from obvious errors and attacks.

> Filtering only captures the most obvious errors and incidents. It is not suited to deal with smart and sophisticated attacks.

Monitoring

Network monitoring is a commonly used method to guard a network and check for anomalies. According to the online survey, this method is widely popular. Tools are available from commercial sources (eg, Arbor Networks and Renesys), open sources (eg, Cyclops and MyASN/IS Alarms), and/or are developed in-house.

To analyse and understand the global routing system, one needs to collect BGP data from various sites in different geographical locations. Oregon Route Views[15] and RIPE RIS[16] are two global routing

[15] See *University of Oregon Route Views Project*, http://www.routeviews.org/

[16] See *RIPE NCC Routing Information Service*, http://www.ripe.net/ris/

monitoring projects that are providing the necessary data for monitoring and alerting tools such as Cyclops, MyASN/IS Alarms, and others.

Although ISPs do make use of open source products for monitoring, according to the interviewees, they often prefer commercial products or in-house tools. They indicated that in-house tools, especially, are very important in monitoring network status. ISPs want service level agreements (SLAs) for the commercial tools or to run the tools themselves because of the liabilities they could incur, as their core business depends partially on these services.

To indicate how important monitoring is considered, some ISPs buy peering capacity from their competitors in order to be able to keep an eye on the performance of their own network and customers from the outside.

Potential routing security challenges, tomorrow, and potential responses

Routing outages are becoming more costly as the Internet is becoming even more essential as a critical infrastructure for businesses, governments, public organizations, media, etc. Therefore, the impact of both direct costs and damage to reputation resulting from outages are likely to increase. A damaged reputation, in particular, is serious and difficult to restore where a security incident has had a serious impact. Action is therefore needed and justified to improve the levels of routing security as otherwise incidents that cause damage will increase and networks will become less stable.

The imminent event of IPv4 depletion[17] and consequently the update of IPv6 are expected to incite an increased number of security incidents. For IPv4, these will primarily relate to the more efficient use of address space as space gets scarce, which will result in increased disaggregation and configuration errors. In addition, due to the scarcity of IPv4 address space, it is expected that prefix hijacks will occur more frequently. For IPv6, we note that there is less operational experience in the sector and therefore more configuration errors are expected, at least for a transitional period. In addition, an increase in multi-homing setups requires more skilled resources.

Overall, the lack of available knowledge and skills in routing security is recognised as a major barrier hindering further improvements in routing security, as became clear both from the online survey and the interviews. As Nick Hilliard (Netability) pointed out during the RIPE Routing WG session, a concern with the introduction of secure technology, such as RPKI or secure BGP, is that we are heading towards a state of increased complexity and increased difficulty in terms of the configuration of these systems. And this in itself will introduce a new class of outages. We will end up with hugely more complicated

[17] See *the projected date of IPv4 address space exhaustion*, *http://ipv4.potaroo.net/*

networks which fewer people will understand, and with problems that overall will probably be much worse that the single short outages which we actually deal with fairly quickly today. He calls for a risk analysis of the trade-off between increased complexity and increased routing security.

A risk analysis of the trade-off between increased complexity and increased routing security is needed.

Other factors will increase the pressure for more secure routing measures. Currently, botnets and viruses on the application level are the most important means to generate money or inflict damage by evil-doers. But when current challenges are adequately met, the routing infrastructure may well become the next easiest target. If no actions are taken to make the routing infrastructure more secure, there will be surgical routing attacks.

Besides the ‘greed and business’ kinds of attacks seen in the past, the potential danger that electronic warfare could bring down national infrastructures is becoming more prevalent. One interviewee formulates this threat as follows: ‘Infrastructure security is politics, not money’. Offenders are not afraid of leaving fingerprints, while the normal crooks stays with botnets and viruses.

In order to respond to those challenges, currently available and deployed technologies can be used as a first line of protection against routing security threats. Interviewees indicate that more sensible and strict filtering of customers and peers at all levels (from small to large ISPs) is possible and necessary. In particular, strict filtering (prefix and AS path) of customers and peers, bogon filtering (unallocated address space filtering) on the transit, authentication of peers, and monitoring to guarantee the stability of large ISPs are seen as essential.

A number of the interviewees mentioned that if the tier 1 and large tier 2 networks (eg, the top 1500 large networks) would pursue (more) strict filtering, many incidents would be averted or at least contained. The quality of filters should be improved and all routers should install increasingly better filtering systems. Obviously, a balance will need to be found in the trade-off between routing security and the network stability that facilitates end-to-end delivery.

Specific responses are being developed in the Internet community:

- In the IETF Keying and Authentication for Routing Protocols (KARP) working group, new methods and protocols are being defined to improve the communication security of protocols such as BGP for inter-domain routing, but also for protocols such as OSPF and ISIS for intra-domain routing, and to protect routers from unauthorized access and some DoS attacks. The KARP WG was established recently to work on these issues. It is expected to take two to four years before results from the KARP WG will be commonly available and used.

- The IETF Secure Inter-Domain Routing (SIDR) working group started in April 2006 to work on basic security questions regarding the validity of routing information, eg, prefix AS origination, accurate AS identification, and validating address prefixes and AS numbers. The scope of work of the SIDR WG is to formulate an extensible architecture for routing security. Given the complexity, both technical and policy-wise, the SIDR WG process is expected to take 10 to 15 years before there will be a general uptake of these technologies.

- In addition, the SIDR WG has been working with a number of stakeholders on the specification of the resource public key infrastructure (RPKI). The RPKI system can be used to certify resource allocations in order to improve the security of the routing system. For example, RPKI could be used to validate route origin attestations (ROAs) in the IRRs. In this way, the quality of data in the IRRs can be improved by signing and validating data in the IRRs, and some trust can be put in the correctness of the retrieved data. The validated IRR data can be used by (local) routing policies to select between validated and non-validated routes. The routing policies are defined by the network operators, and can include non-validated routes as a fall-back option, thus optimising network stability and end-to-end delivery.

Many of the interviewees made some critical comments about RPKI and its intended usage. The concerns with RPKI range from the PKI hierarchy and single authoritative trust anchor, through the costs of certificates, to the instability and vulnerability of the RPKI infrastructure. With RPKI, all well-known PKI problems, as formulated in the paper *Ten Risks of PKI* by Ellison and Schneier (2000), are introduced.

One of the interviewees suggested the use of information stored in the DNS reverse address tree (in-addr.arpa) for route origin validation as an alternative to RPKI. Another alternative proposal to RPKI was to use a security BGP overlay network with a direct connection to all content or AS nodes that are considered important. Although there is no direct AS path, a direct trust relation would be created by the overlay between the networks.

The main concerns related to RPKI are:

- the extra complexity of an RPKI and that the dependency on this infrastructure can also increase the instability of a network when put into practice;

- that the routing infrastructure can even become vulnerable to attacks through attacks on the RPKI infrastructure at the RIRs;

- that the costs of certificates provided by RIRs are not clear nor is the length of time for which they will be valid.

Operators are anxious about the incurred (increased) costs of address certification by the RIRs. The RIRs states that these costs are covered by the membership fees. Another dispute is the duration of the validity of a certificate: the RIRs prefer a period of two years (one year membership plus one year settlement in case of dispute), while operators prefer a period of three to five years (which will only be invalidated should address space be transferred to a new owner).

In addition, moving towards a single authoritative trust anchor is also a cause for anxiety among the interviewees. It would be hard to find an authority that would be widely trusted for that purpose. If it were IANA, there would be concern about the possible role of the US government, as they hold the contract. With RPKI in place and routing policies based on validated ROAs in the IRR, this would allow the trust anchor to bring down countries should they so wish, and that kind of ability should, in the eyes of many, not be in the hands of any one country.

Also, rumours that both the root CA used for routing, as well as the DNS root will be signed by the same company, has led to unrest, as this will place a huge amount of responsibility and power within one single organization, namely placing the management of the security of two of the most critical Internet infrastructures in one hand: DNS and inter-domain routing.

Cost factors in routing security, benefits, and considerations for successful deployment

An important factor determining the uptake and deployment of routing security methods is how the costs (capex and opex) are addressed. ISPs operate in a highly competitive and tough market with relatively small margins. ISPs invest their money in services such as VPN and content hosting, as these are services people expect to get charged for, rather than for inter-domain routing security, for which no direct charges are made. Investments in security are lagging behind as many ISPs are not able to justify business investments, as the costs of successful attacks are currently not measured. Should these costs be made clear, investments would be more easily justified.

Investments for deploying improved routing security are in new hardware (eg, for computationally intensive cryptographic operations), as well as in tooling and automation of operational processes. If ISPs have not made these investments during an early phase of developing their services, they will find that it is very expensive to incorporate security at a later phase, ie, there is no commercial pay-off. At the same time, the chances are they will lose out to newcomers in the market who do make these investments from the outset.

A complicating factor is that some of the investments only will pay off if all ISPs make the investment. For instance, when investing in routing security techniques based on RPKI, the added value is minimal, until *all* ISPs use validated ROAs. Up to that moment, those ISPs who have invested hardly get a return on their investment.

So far, the network sector has thrived in a market that regulated itself without control and direction from governments. In routing security, the sentiments are similar (this also materializes from the online survey), and there is no loud call for governments to step in, eg, by operating as trust brokers (where do governments get their information from and can it be trusted?). However, the domain is more and more subject to government oversight in ensuring the continuity of societal functions and critical networks. It is therefore conceivable that governments will define requirements for security levels, assurances, and the protection of citizens' interests. This could lead to compliance regulation comparable to PCI (credit card) or HIPAA (health).

The introduction of RPKI infrastructure incites a number of operational considerations and consequences. If RPKI or a similar security technology takes off, IP address blocks may be allocated and assigned in alignment with national jurisdictions, which would result in disaggregation of the IP address space as current networks cross national borders. Such a development is not inconceivable for RPKI systems, as trust is delegated to third parties, and nations may want to avoid having the ultimate trust anchor in some foreign organization in a foreign jurisdiction.

Please note that this is also at the heart of a discussion as to whether there should be one single ultimate trust anchor at IANA or a set of trust anchors at the RIRs. Interviewees indicate that they think a workable approach should be based on a trust model that follows the current business practice in routing (how money and the data packets flow).

A final consideration for deployment is that a solution needs to be found to resolve failure in the stability and security of the RPKI infrastructure. If something breaks at IANA or the RIRs, ISPs are in a bad position, as routes would no longer be validated. The autonomy of ISPs is seen as crucial by them, and therefore there is a need for clarity regarding possible address certificate revocation should there be conflicts with RIRs. This is reflected in the current debate where RIRs are proposing a certificate validity of two years, versus three to five years by ISPs. RPKI can solve a lot of the problems the sector is facing, if enough ISPs will adopt it. However, as today large ISPs do not filter each other, moving towards RPKI will be a major step and a huge investment.

However, as Rüdiger Volk stated at the end of the RIPE Routing WG session, 'Doing nothing on routing security will surely get us into the Wall Street Journal's headlines.'

Conclusions and recommendations

Amongst the respondents to the survey, routing security awareness is very high. This finding, however, represents a bias as the respondents are mostly those who have previously been confronted with routing security issues. The interviews and the RIPE Routing WG discussion confirm that, although at large ISPs (tier 1 and large tier 2 networks) the level of awareness of inter-domain routing security threats is high, on average the level of awareness is low, in particular among smaller ISPs. In a way this reflects the availability of skilled security staff at the NOCs of ISPs, as was also confirmed by the Arbor Networks report. The deployment and use of different security technologies varies widely between different ISPs who have differing requirements due to their operational environments and the availability of skilled staff.

Based on the results of the survey, it is clear that routing security currently is mostly accomplished by the implementation of session security, but that monitoring and filtering are becoming increasingly popular—despite the higher risks of misconfiguration. It is striking that, amongst the respondents, in which we expect a bias towards embracing secure routing measures, the level of awareness of RPKI is, at the time of the survey, still low.

According to the interviewees and the discussion at the RIPE Routing WG session, routing security must be aligned with the stability requirements for networks, mentioned earlier in the 'Routing Security Awareness' section. BGP announcement filtering is seen as an effective security measure, but it is difficult to generate good quality filter lists in the absence of trusted data and adequate tools. RPKI can help to improve quality and trust in IRR data, but discussions are ongoing as to how RPKI will be used and whether a single authoritative trust anchor is desired.

Autonomy in running the network is one of the most important concerns of ISP operators. Autonomy in transit, customer, and peering agreements, and the routing policies expressing these agreements are at the core of the business of an ISP. The sector seems to have low confidence in government involvement with routing policies, or with a single authoritative trust anchor. At the same time it is clear to interviewees that governments may move towards defining security requirements (eg, in terms of compliance). A natural role for governments is seen in stimulating investment, supporting public R&D, and raising awareness. Within this self-made, since its origin mainly technical, Internet community, it is no surprise that there is a preference for self-regulation above legislative measures.

'Weak signals'

From the interviews, a number of uncertain indications of security threats emerged, which may reach more substantive levels in the years to come, relating to:

- Surgical attacks to the routing system, which are difficult to detect and mitigate.
- Electronic warfare, bringing down national network infrastructures. And related to this, one single authoritative trust anchor residing at IANA is on the agenda.
- Moving towards (RKPI-based) filtering will be a major transition for large ISPs (large tier 1 and tier 2 providers).
- The Internet works because of savvy operators, and they need the means (knobs and dials) for configuring it to make it work, including the deployment of strict security. Autonomy in operating a network is essential to accommodate this quality.
- Shortages in skilled network operator staff can hinder the successful deployment of a routing security technology such as RPKI, as configuration and incident mitigation is expected to be more complex. In a competitive market with small revenues it is difficult to hire highly qualified and talented network engineers.

We recommend that these signals are further monitored and explored, as any of them may turn out to be crucial issues in the years to come.

Overall conclusions

This report presents an overview of the current modus operandi in routing security and the expectations for new technologies in routing security. About 120 network operators and architects participated in the online survey, and for the interviews 21 operators and experts were questioned. This sample is limited in size (a total of about 140 respondents versus 30,000 ASs) and has, of course, a strong bias towards participants and interviewees who are concerned about security and therefore decided to take part in the study. Still, with the selection of the interviewees, we see contributions from small, medium, large, and tier 1 network operators, with an accent on Europe. The experts interviewed are from companies as well as non-profit organizations from Europe, the USA, and Australia.

The participants in the survey and the interviewees responded to our questions on the basis of their personal perceptions and experiences. And, despite their differing views and backgrounds, several topics recurred. Concerns were expressed about the current state of security of the routing infrastructure and the need to take action to improve its security. There is a rough consensus on the first step to improve on the quality of the techniques currently deployed.

A next step involving RPKI is mentioned by most interviewees, though there are different opinions about its deployment, the policies involved, and how the RPKI will be used. The most outspoken concern is the apprehensive feeling about a loss of autonomy by the ISPs or even by nations.

With the proposals in the IETF SIDR working group, and the RIRs running the pilot studies to support a resource public key infrastructure (RPKI), the development of a more secure routing infrastructure is well underway. Building upon this, proposals have been put forth in ARIN, RIPE, and APNIC to introduce an overlay IRR with route objects generated using route origin authorisations (ROAs) from the RPKI. This data can be used by networks operators as a more trustworthy source as to who is authorised to originate what.

The main hurdles to overcome before secure routing can be deployed are choosing a technology that will be broadly supported by equipment suppliers and used by ISPs and operators. Most of the proposed solutions include cryptographic technology, which requires a public key infrastructure with all its technical, operational, and policy (political) complexities. The technology must be deployable incrementally, so that it provides some return on investment for the first organizations that begin implementing secure routing technology.

The barriers to any improvement on routing security are the implementation and operational costs. However, while stability is the underlying doctrine in network management, increased complexity and consequently increased difficulty in configuration and fault mitigation are also consistently mentioned as hurdles hindering the successful deployment of routing security.

Recommendations

A number of recommendations to improve on the current state of routing security emerged from the answers to the online survey and the interviews of participants in the field study.

- Stimulate investments in the development of routers and (validation) tools to increase the level and quality of routing security. The availability of support for routing security in hardware and software will also lower the implementation and operation costs of secure routing technologies and can facilitate their deployment.

- Stimulate self-regulation. Compliance regulation on routing security can move ISPs and content providers to take action and require it from the industry. It is conceivable that compliance requirements that will not include routing security policies could be defined.

- Facilitate monitoring research, eg, extend and improve Oregon Route Views and RIPE RIS, and include real-time collection of BGP routing information (see, for example, Yan *et al* (2009)). There is a lack of basic data on what is going on *right now* in the Internet. We can tell what planes are in the sky, what trains are on the tracks, but not what routes are being announced (and from where).

- Ensure the exchange of information and monitor the advance of existing and possible future threats (such as those indicated in the 'weak signals' list above). This can include the awareness of threats, but also the development of state-of-the-art and best practice guidelines. See, for example, Team Cymru, a group of experts that provide a (free) service for router configuration and the generation of a bogon filter list.

- Awareness of RPKI needs improvement to prepare network architects and operators as this technology is becoming available and will be deployed in the next few years.

- Leverage tier 1 and large tier 2 networks with the introduction of routing security technology (for example, based on RPKI). Tier 1 and tier 2 networks can require this from or sell this as a service to their customers (tier 3 networks). Convince tier 1 and large tier 2 networks of the necessity of routing security technology.

- Demand specific measures to ensure routing security in public tenders.

These recommendations are all in line with the results of the interviews, the survey and RIPE Routing Working Group session, but do not necessarily reflect the specific views of individuals who participated in the process. Nevertheless all of the recommendations may be worth further exploration, which is beyond the scope of this study.

Glossary of terms

APNIC A regional Internet registry (RIR) that allocates IP and AS numbers in the Asia Pacific region.

ARIN A regional Internet registry (RIR) that allocates IP and AS numbers in the North-American region and parts of the Caribbean.

AS An autonomous system is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet.

BGP The Border Gateway Protocol is the core routing protocol of the Internet. It maintains a table of IP networks or prefixes which designate network reachability among autonomous systems (AS).

Bogon address The term 'bogon' (hacker slang derived from 'bogus') refers to an IP address that is reserved but not yet allocated by IANA or some other Internet registry. Addresses that have not been allocated to legitimate users should never be routed, and packets that appear to come from these addresses are most likely forged.

Byzantine robustness See http://en.wikipedia.org/wiki/Byzantine_fault_tolerance for a comprehensive definition and explanation of robustness against Byzantine failures.

CA A certificate authority or certification authority (CA) is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

DNS/DNSSEC The Domain Name System is a hierarchical naming system for computers, services, or any resource connected to the Internet. Most importantly, it translates domain names that are meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. DNSSEC is a suite of specifications for securing certain kinds of information provided by the Domain Name System.

DoS/DDoS A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

IANA The Internet Assigned Numbers Authority (IANA) is the entity that oversees global IP address allocation, AS number allocation, root zone management for the Domain Name System (DNS), media types, and other Internet Protocol related assignments.

IETF The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standards bodies and dealing in particular with the standards of the TCP/IP and Internet protocol suite. It is an open standards organization, with no formal membership or membership requirements.

Internet exchange An Internet exchange point (IX or IXP) is a physical infrastructure through which Internet service providers (ISPs) exchange Internet traffic between their networks (autonomous systems).

IP hijack IP hijacking (sometimes referred to as BGP hijacking or prefix hijacking) is the illegitimate take over of groups of IP addresses by corrupting Internet routing tables.

IPsec Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

IRR The Internet routing registry consists of several databases where network operators publish their routing policies and routing announcements so that other network operators can use this data.

ISP An Internet service provider (ISP) is a company that offers its customers access to the Internet.

KARP The IETF Keying and Authentication for Routing Protocols working group is tasked with improving the communication security of the packets on the wire used by the routing protocols. This working group is concerned with message authentication, packet integrity, and denial of service (DoS) protection. See also https://datatracker.ietf.org/wg/karp/.

MD5 Message-Digest algorithm 5 is a widely used cryptographic hash function with a 128-bit hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files

PKI A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).

RADb The Routing Assets Database is an IRR run by Merit Network.

RFC A request for comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviours, research, or innovations applicable to the working of the Internet and Internet-connected systems. The IETF adopts some of the proposals published as RFCs as Internet standards.

RIR A regional Internet registry is an organization overseeing the allocation and registration of Internet number resources within a particular region of the world. Resources include IP addresses (both IPv4 and IPv6) and autonomous system numbers (for use in BGP routing)

RIPE NCC A regional Internet registry (RIR) that allocates IP and AS numbers in the European, Middle East, and Central Asian region.

ROA A route origin authorisation is a digitally signed object that provides a means of verifying that an IP address block holder has authorised an autonomous system (AS) to originate routes to one or more prefixes within the address block.

Route aggregation/disaggregation The Border Gateway Protocol allows the aggregation of specific routes into one route. Route aggregation can be used to decrease the size of the BGP routing tables. This helps in speeding up the convergence time and improves network performance. Route disaggregation is the reverse process, where a route is split into two or more specific routes, and hence increases the size of the BGP routing tables.

RPKI A resource public key infrastructure system can be used to certify autonomous system (AS) numbers and IP addresses allocations in order to substantially improve the security of the routing system.

SIDR The IETF Secure Inter-Domain Routing working group works on the formulation of an extensible architecture for an inter-domain routing security framework. This framework must be capable of supporting incremental additions of functional components. See also https://datatracker.ietf.org/wg/sidr/.

Tier 1/2/3 network A Tier 1 network is a transit-free network that does not pay settlements to any other network to reach any other portion of the Internet. Therefore, in order to be a Tier 1 network, a network must peer with every other Tier 1 network. A Tier 2 network peers with some networks, but still purchases IP transit or pays settlements to reach at least some portion of the Internet. A Tier 3 network solely purchases transit from other networks to reach the Internet.

References

Arbor Networks, Network Infrastructure Security Report, January 2010. http://www.arbornetworks.com/report

K. Butler, T. Farley, P. McDaniel, and J. Rexford, A Survey of BGP Security Issues and Solutions, Proceedings of the IEEE, vol. 98, no. 1, pp 100–122, January 2010.

D.D. Clark, K. Sollins, J. Wroclawski, and T. Faber, Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet, ACM SIGCOMM Computer Communication Review, vol. 33, no. 4, pp. 247–257, October 2003.

C. Ellison and B. Schneier, Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, Computer Security Journal, vol. 16, no. 1, pp. 1–7, 2000.

N. Feamster, H. Balakrishnan, and J. Rexford, Some Foundational Problems in Interdomain Routing, Proceedings of the 3rd Workshop on Hot Topics in Networks (HotNets-III), San Diego, CA, November 2004.

S. Goldberg, S. Halevi, A.D. Jaggard, V. Ramachandran, and R.N. Wright, Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP, Proceedings of the ACM Conference of the Special Interest Group on Data Communication (SIGCOMM'08), pp. 267-278, Seattle, WA, August 2008.

S.T. Kent, Securing the Border Gateway Protocol, The Internet Protocol Journal, vol. 6, no. 3, pp. 2–14, September 2003.

R. Kuhn, K. Sriram, and D. Montgomery, Border Gateway Protocol Security, NIST Special Publication 800-54, July 2007. http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

O. Nordstrom and C. Dovrolis, Beware of BGP attacks, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 1-8, April 2004.

D. Pei, L. Zhang, and D. Massey, A Framework for Resilient Internet Routing Protocols, IEEE Network, vol. 18, no. 2, pp. 5–12, March/April 2004.

A. Pilosov and T. Kapela, Stealing The Internet, DEF CON 16, August 2008. http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

R. White, Securing BGP Through Secure Origin BGP, The Internet Protocol Journal, vol. 6, no. 3, pp. 15–22, September 2003.

H. Yan, R. Oliveira, K. Burnett, D Matthews, L. Zhang, and D. Massey, BGPmon: A Real-Time, Scalable, Extensible Monitoring System, Cybersecurity Applications & Technology Conference for Homeland Security, pp.212–223, March 2009

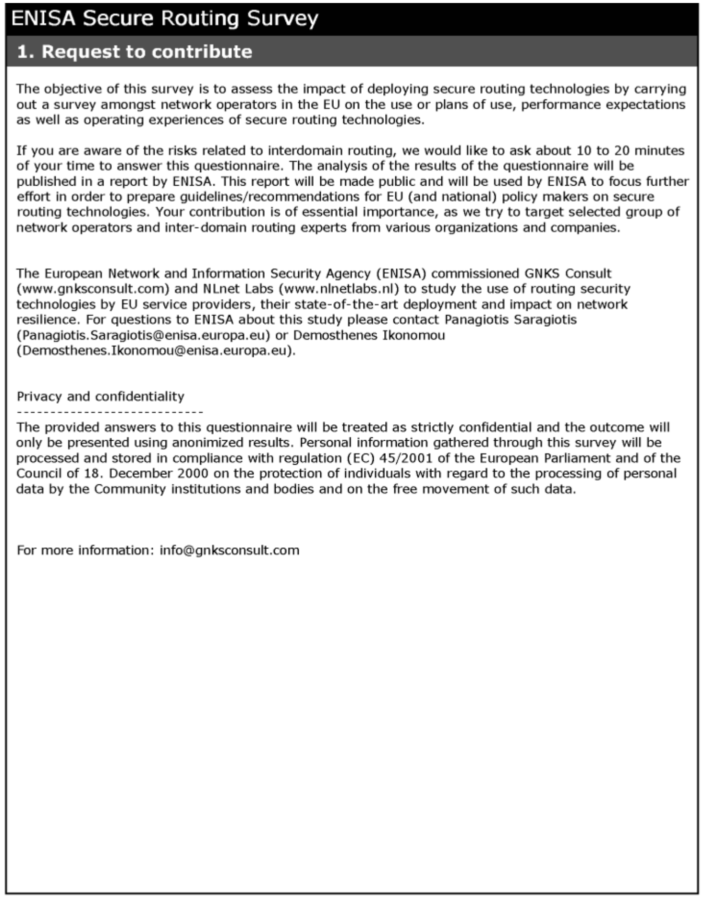
ANNEX 1: List of participants

The following people were interviewed. Although their affiliation is mentioned most participated on personal title:

Name		Organisation	Country
Marco	Hogewoning	XS4ALL	Netherlands
André	van Leeuwen	Ziggo	Netherlands
Rüdiger	Volk	Deutsche Telekom	Germany
Rob	Evans	Janet	UK
Bijal	Sanghani	Reliance Globalcom	UK
Chris	Morrow	Google	USA
Dan	Massey	Colorado State University	USA
Geoff	Huston	APNIC	Australia
Danny	McPherson	Arbor Networks	USA
Gregory	Lebovitz	Juniper	USA
Remco	van Mook	Equinix	Netherlands
Måns	Nilsson	Sveriges Radio	Sweden
Kurt	Lindqvist	NetNod	Sweden
Ted	Seely	Sprint	USA
Bill	Woodcock	Packet Clearing House	USA
Robert	Kisteleki	RIPE NCC	Netherlands
Jared	Mauch	NTT America	USA
Nina	Hjort Bargisen	TDC	Denmark
Gert	Doering	SpaceNet	Germany
Pekka	Savola	CSC/FUNET	Finland
Athanasio	Liakopoulos	GRNET	Greece

In addition, the input from members of the RIPE community that spoke up during the working session of the IP Routing Workgroup meeting that took place on 5 May 2010 in Prague was incorporated in the report.

ANNEX 2: Questionnaire



ENISA Secure Routing Survey

1. Request to contribute

The objective of this survey is to assess the impact of deploying secure routing technologies by carrying out a survey amongst network operators in the EU on the use or plans of use, performance expectations as well as operating experiences of secure routing technologies.

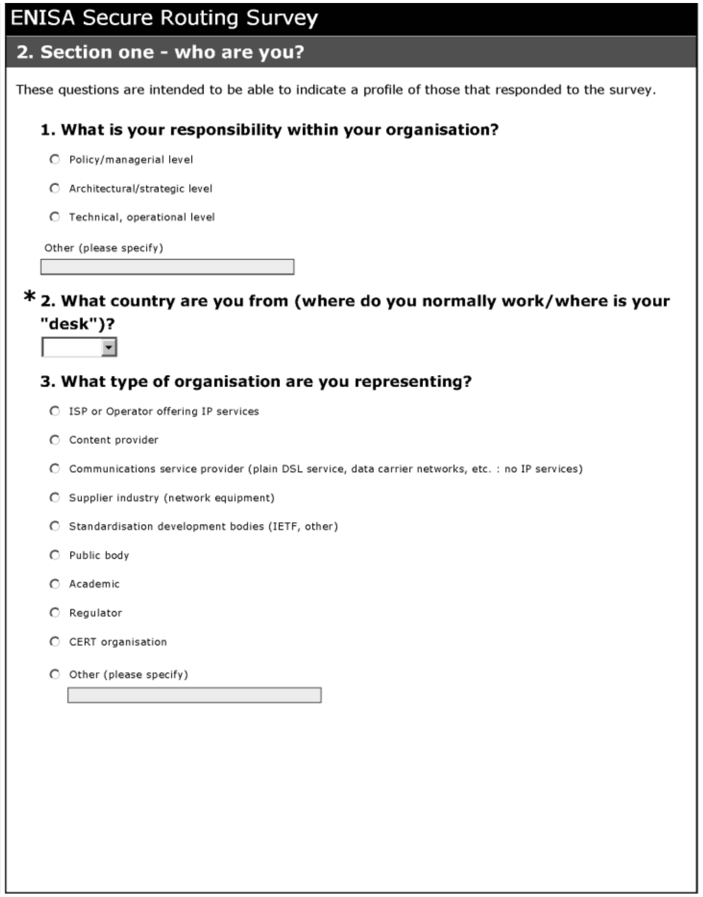
If you are aware of the risks related to interdomain routing, we would like to ask about 10 to 20 minutes of your time to answer this questionnaire. The analysis of the results of the questionnaire will be published in a report by ENISA. This report will be made public and will be used by ENISA to focus further effort in order to prepare guidelines/recommendations for EU (and national) policy makers on secure routing technologies. Your contribution is of essential importance, as we try to target selected group of network operators and inter-domain routing experts from various organizations and companies.

The European Network and Information Security Agency (ENISA) commissioned GNKS Consult (www.gnksconsult.com) and NLnet Labs (www.nlnetlabs.nl) to study the use of routing security technologies by EU service providers, their state-of-the-art deployment and impact on network resilience. For questions to ENISA about this study please contact Panagiotis Saragiotis (Panagiotis.Saragiotis@enisa.europa.eu) or Demosthenes Ikonomou (Demosthenes.Ikonomou@enisa.europa.eu).

Privacy and confidentiality

The provided answers to this questionnaire will be treated as strictly confidential and the outcome will only be presented using anonimized results. Personal information gathered through this survey will be processed and stored in compliance with regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

For more information: info@gnksconsult.com



ENISA Secure Routing Survey

2. Section one - who are you?

These questions are intended to be able to indicate a profile of those that responded to the survey.

1. What is your responsibility within your organisation?

○ Policy/managerial level

○ Architectural/strategic level

○ Technical, operational level

Other (please specify)

* 2. What country are you from (where do you normally work/where is your "desk")?

3. What type of organisation are you representing?

○ ISP or Operator offering IP services

○ Content provider

○ Communications service provider (plain DSL service, data carrier networks, etc. : no IP services)

○ Supplier industry (network equipment)

○ Standardisation development bodies (IETF, other)

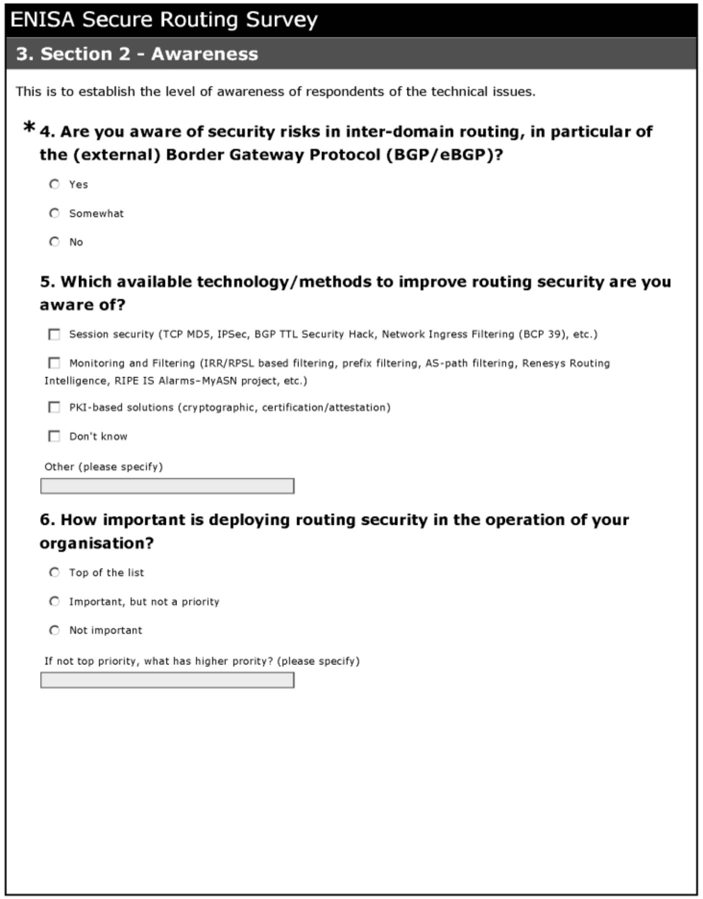
○ Public body

○ Academic

○ Regulator

○ CERT organisation

○ Other (please specify)



ENISA Secure Routing Survey

3. Section 2 - Awareness

This is to establish the level of awareness of respondents of the technical issues.

* 4. Are you aware of security risks in inter-domain routing, in particular of the (external) Border Gateway Protocol (BGP/eBGP)?

○ Yes

○ Somewhat

○ No

5. Which available technology/methods to improve routing security are you aware of?

□ Session security (TCP MD5, IPSec, BGP TTL Security Hack, Network Ingress Filtering (BCP 39), etc.)

□ Monitoring and Filtering (IRR/RPSL based filtering, prefix filtering, AS-path filtering, Renesys Routing Intelligence, RIPE IS Alarms-MyASN project, etc.)

□ PKI-based solutions (cryptographic, certification/attestation)

□ Don't know

Other (please specify)

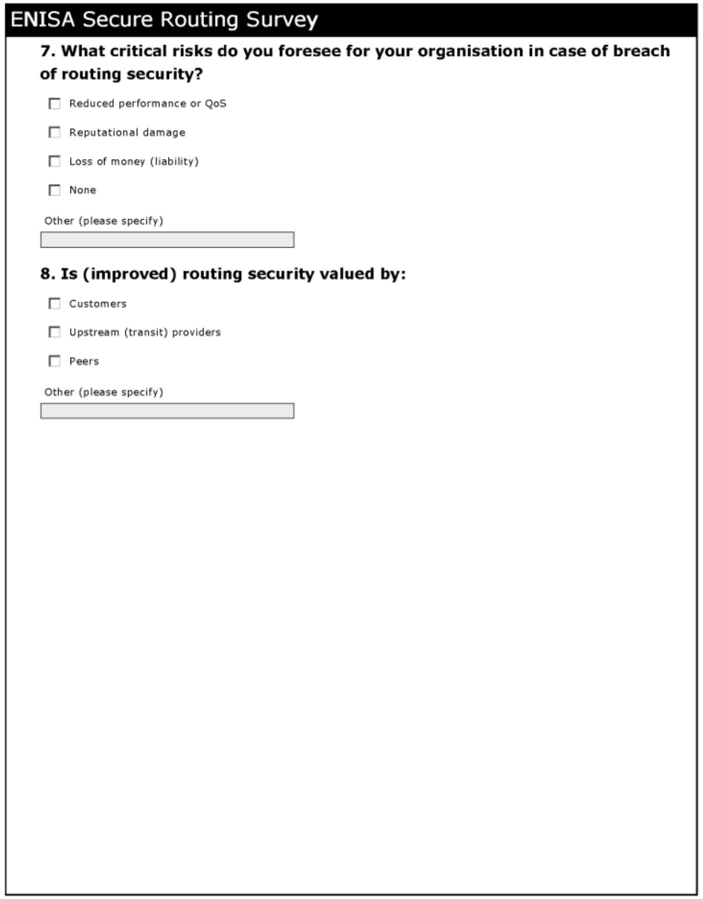
6. How important is deploying routing security in the operation of your organisation?

○ Top of the list

○ Important, but not a priority

○ Not important

If not top priority, what has higher prority? (please specify)



ENISA Secure Routing Survey

7. What critical risks do you foresee for your organisation in case of breach of routing security?

□ Reduced performance or QoS

□ Reputational damage

□ Loss of money (liability)

□ None

Other (please specify)

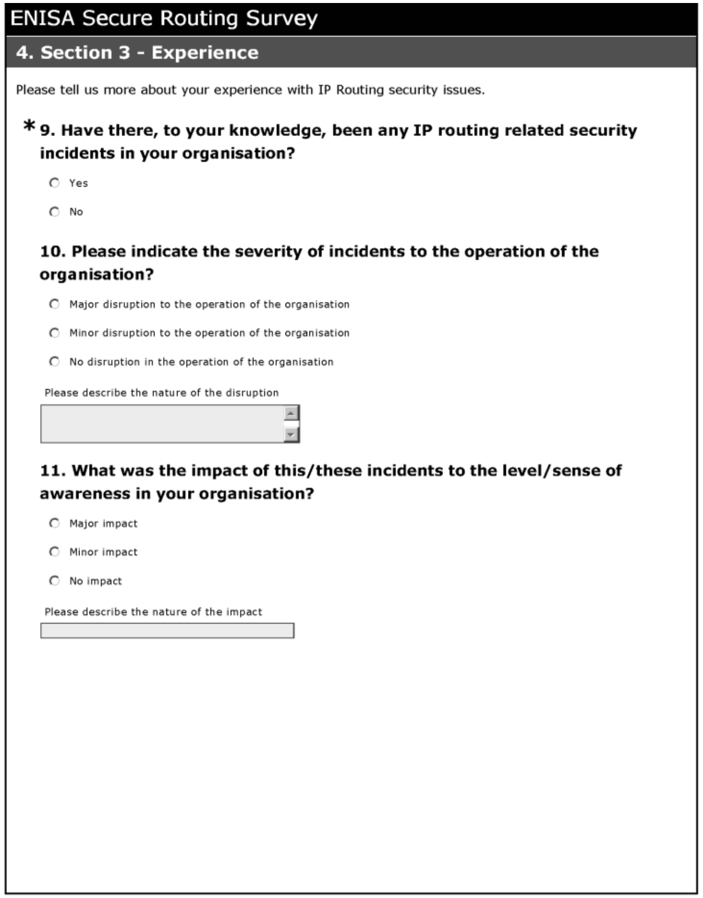
8. Is (improved) routing security valued by:

□ Customers

□ Upstream (transit) providers

□ Peers

Other (please specify)



ENISA Secure Routing Survey

4. Section 3 - Experience

Please tell us more about your experience with IP Routing security issues.

*9. Have there, to your knowledge, been any IP routing related security incidents in your organisation?

○ Yes

○ No

10. Please indicate the severity of incidents to the operation of the organisation?

○ Major disruption to the operation of the organisation

○ Minor disruption to the operation of the organisation

○ No disruption in the operation of the organisation

Please describe the nature of the disruption

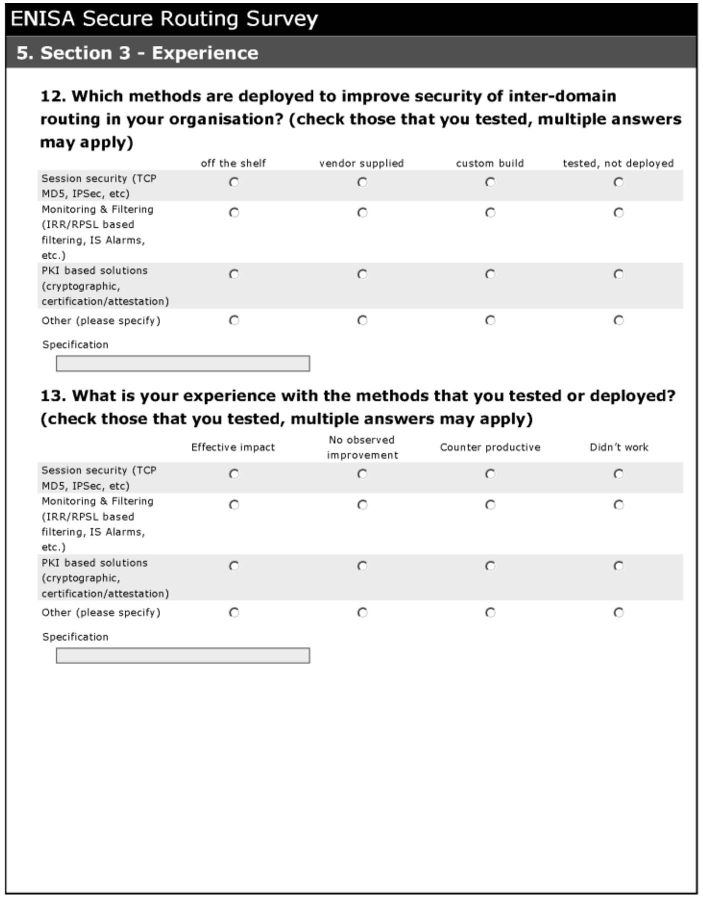
11. What was the impact of this/these incidents to the level/sense of awareness in your organisation?

○ Major impact

○ Minor impact

○ No impact

Please describe the nature of the impact



ENISA Secure Routing Survey

5. Section 3 - Experience

12. Which methods are deployed to improve security of inter-domain routing in your organisation? (check those that you tested, multiple answers may apply)

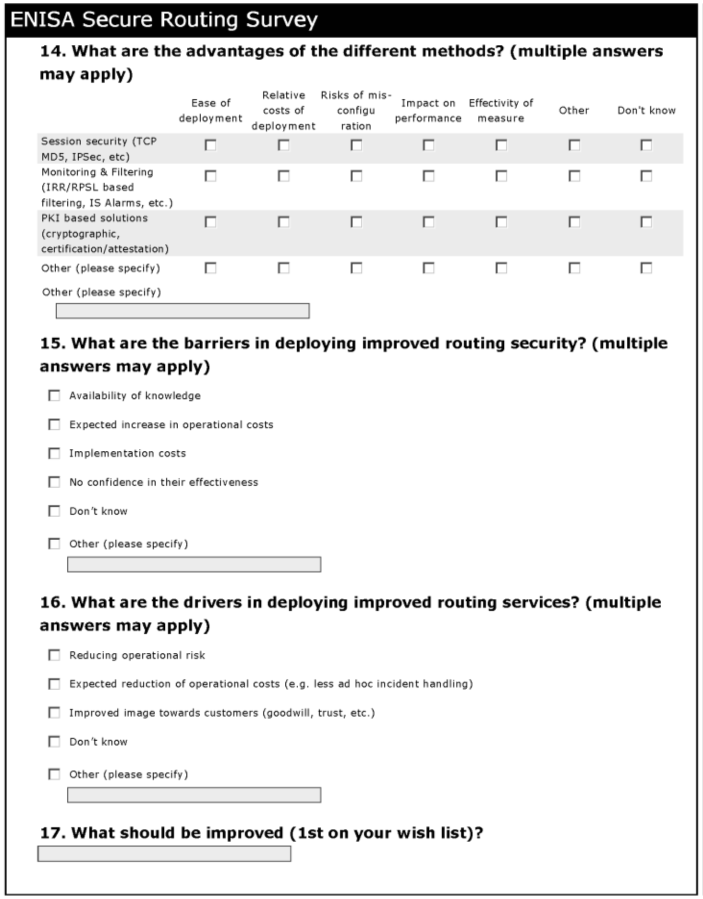
	off the shelf	vendor supplied	custom build	tested, not deployed
Session security (TCP MD5, IPSec, etc)	○	○	○	○
Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc.)	○	○	○	○
PKI based solutions (cryptographic, certification/attestation)	○	○	○	○
Other (please specify)	○	○	○	○

Specification

13. What is your experience with the methods that you tested or deployed? (check those that you tested, multiple answers may apply)

	Effective impact	No observed improvement	Counter productive	Didn't work
Session security (TCP MD5, IPSec, etc)	○	○	○	○
Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc.)	○	○	○	○
PKI based solutions (cryptographic, certification/attestation)	○	○	○	○
Other (please specify)	○	○	○	○

Specification



ENISA Secure Routing Survey

14. What are the advantages of the different methods? (multiple answers may apply)

	Ease of deployment	Relative costs of deployment	Risks of mis-configu ration	Impact on performance	Effectivity of measure	Other	Don't know
Session security (TCP MD5, IPSec, etc)	□	□	□	□	□	□	□
Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc.)	□	□	□	□	□	□	□
PKI based solutions (cryptographic, certification/attestation)	□	□	□	□	□	□	□
Other (please specify)	□	□	□	□	□	□	□

Other (please specify)

15. What are the barriers in deploying improved routing security? (multiple answers may apply)

□ Availability of knowledge

□ Expected increase in operational costs

□ Implementation costs

□ No confidence in their effectiveness

□ Don't know

□ Other (please specify)

16. What are the drivers in deploying improved routing services? (multiple answers may apply)

□ Reducing operational risk

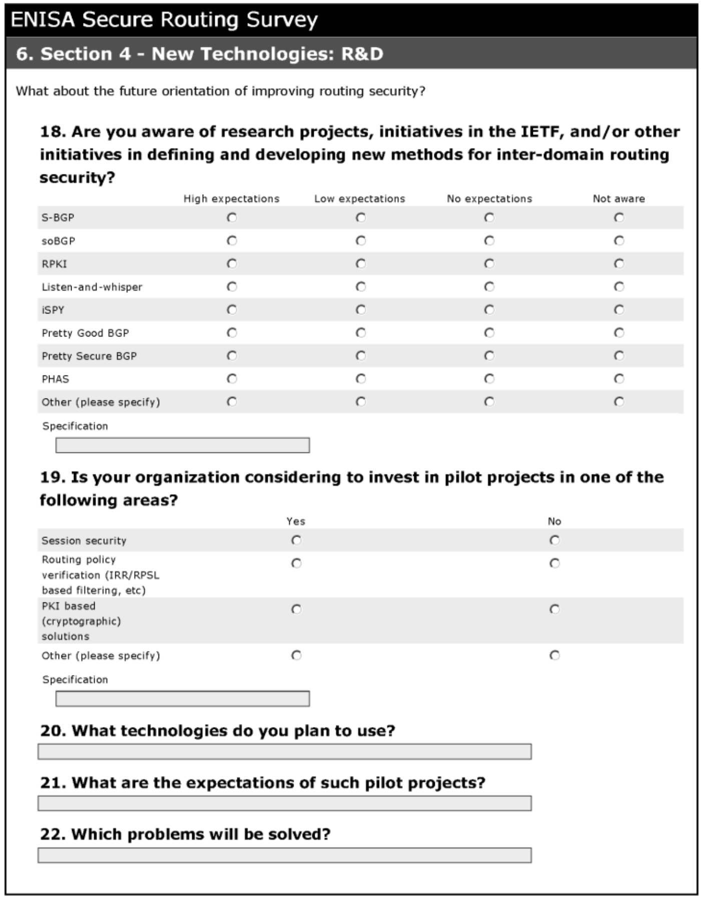
□ Expected reduction of operational costs (e.g. less ad hoc incident handling)

□ Improved image towards customers (goodwill, trust, etc.)

□ Don't know

□ Other (please specify)

17. What should be improved (1st on your wish list)?



ENISA Secure Routing Survey

6. Section 4 - New Technologies: R&D

What about the future orientation of improving routing security?

18. Are you aware of research projects, initiatives in the IETF, and/or other initiatives in defining and developing new methods for inter-domain routing security?

	High expectations	Low expectations	No expectations	Not aware
S-BGP	○	○	○	○
soBGP	○	○	○	○
RPKI	○	○	○	○
Listen-and-whisper	○	○	○	○
iSPY	○	○	○	○
Pretty Good BGP	○	○	○	○
Pretty Secure BGP	○	○	○	○
PHAS	○	○	○	○
Other (please specify)	○	○	○	○

Specification

19. Is your organization considering to invest in pilot projects in one of the following areas?

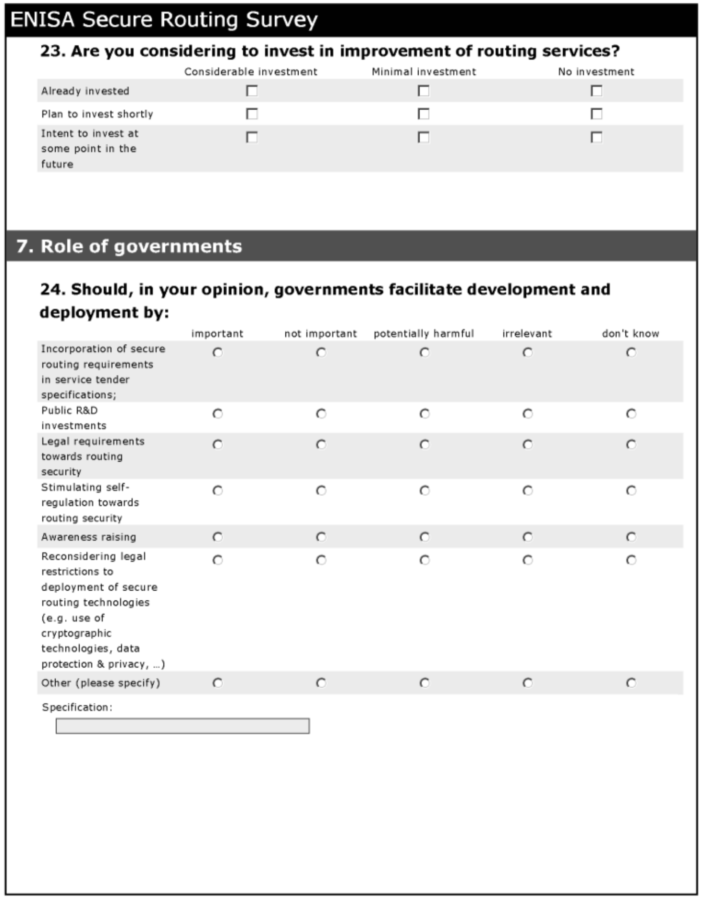
	Yes	No
Session security	○	○
Routing policy verification (IRR/RPSL based filtering, etc)	○	○
PKI based (cryptographic) solutions	○	○
Other (please specify)	○	○

Specification

20. What technologies do you plan to use?

21. What are the expectations of such pilot projects?

22. Which problems will be solved?



ENISA Secure Routing Survey

23. Are you considering to invest in improvement of routing services?

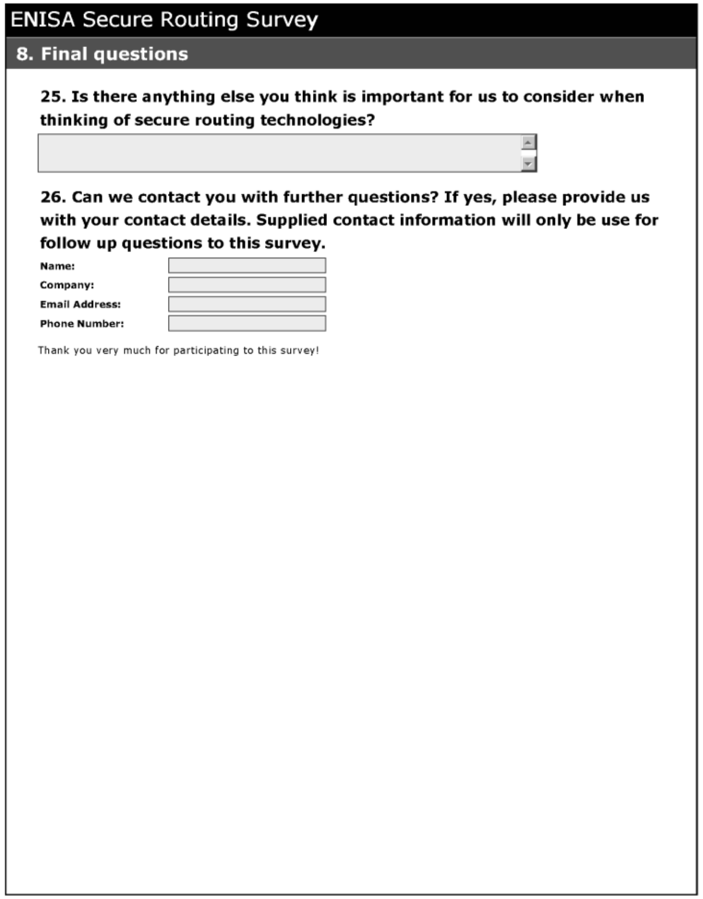
	Considerable investment	Minimal investment	No investment
Already invested	□	□	□
Plan to invest shortly	□	□	□
Intent to invest at some point in the future	□	□	□

7. Role of governments

24. Should, in your opinion, governments facilitate development and deployment by:

	important	not important	potentially harmful	irrelevant	don't know
Incorporation of secure routing requirements in service tender specifications;	○	○	○	○	○
Public R&D investments	○	○	○	○	○
Legal requirements towards routing security	○	○	○	○	○
Stimulating self-regulation towards routing security	○	○	○	○	○
Awareness raising	○	○	○	○	○
Reconsidering legal restrictions to deployment of secure routing technologies (e.g. use of cryptographic technologies, data protection & privacy, …)	○	○	○	○	○
Other (please specify)	○	○	○	○	○

Specification:



ENISA Secure Routing Survey

8. Final questions

25. Is there anything else you think is important for us to consider when thinking of secure routing technologies?

26. Can we contact you with further questions? If yes, please provide us with your contact details. Supplied contact information will only be use for follow up questions to this survey.

Name:
Company:
Email Address:
Phone Number:

Thank you very much for participating to this survey!