SECURE PROTOCOLS FOR THE ROUTING INFRASTRUCTURE (SPRI) INITIATIVE

A ROAD MAP

(First Draft)

SPARTA, INC

SEPTEMBER 2006

Table of Contents

List of Figures

1 Executive Summary

The Internet consists of a large number of interconnected autonomous systems (ASs) each of which constitutes a distinct routing domain. Such autonomous systems are usually run by a single organization such as a company or university. Within an AS, routers communicate with each other using one of several possible intra-domain routing protocols also known as interior gateway protocols. ASs are connected via gateways, these exchange information using inter domain routing protocol also known as exterior gateway protocols.

Routing in the Internet is very complex task involving operations like physical address determination, selection of inter-network gateways, and forwarding messages to the correct destination. In order for these tasks to be achieved many infrastructure protocols such as RIP, OSPF, IS-IS, BGP have been developed and put into place. Securing routing protocols for reliable, persistent communication has been widely acknowledged as an important problem, yet there is a lack of consensus and motivation to derive common and widely deployable standard techniques to mitigate these problems. Through this roadmap, we aim to bring together the various facets of creating secure protocols for the routing infrastructure, namely,

- Highlight important problems
- Examine existing approaches to mitigate or “work around” these problems.
- Facilitating development of approaches that address the larger problem of routing security.
- Identify barriers to deployment.
- Identify key players in each realm, Targeted Adopters and Early Adopters.
- Develop robust transitioning mechanisms.
- Identify useful metrics and measurements for validation.
- Identify and create opportunities for education and awareness programs tailored for each problem.
- Identify tools and resources for the operator, vendor and ISP community.
- Develop a timeline to achieve these goals.

2 Introduction

2.1 Threats to the Routing Infrastructure

The readers are referred to [draft-ietf-rpsec-routing-threats] for a detailed exposition of the generic threats to routing security. Some of the threat sources, threat actions and threat consequences from that document are excerpted in this section for reference.

Threat source

Outsiders: These attackers may reside anywhere in the Internet, have the ability to send IP traffic to the router, may be able to observe the router's replies and may even control the path for a legitimate peer's traffic. These are not legitimate participants in the routing protocol.

Byzantine: These attackers are faulty, misconfigured or subverted routers, i.e., legitimate participants in the routing protocol.

Threat Actions

Spoofing: occurs when an illegitimate device assumes the identity of a legitimate one.

Falsification: is an action whereby a router (as the originator or a forwarder) sends false routing information.

Interference: is a threat action where an attacker inhibits the exchanges by legitimate routers. The attacker can do this by adding noise, by not forwarding packets, by replaying out-dated packets, by inserting or corrupting messages, by delaying responses, by denial of receipts, or by breaking synchronization.

Overload: is defined as a threat action whereby attackers place excess burden on legitimate routers.

Threat Consequence

Deception: This consequence happens when a legitimate router receives a forged routing message and believes it to be authentic. Both outsiders and Byzantine routers can cause this consequence if the receiving router lacks the ability to check routing message integrity or origin authentication.

Disruption: This consequence occurs when a legitimate router's operation is being interrupted or prevented. Outsiders can cause this by inserting, corrupting, replaying, delaying, or dropping routing messages, or breaking routing sessions between legitimate routers. Byzantine routers can cause this consequence by sending false routing messages, interfering with normal routing exchanges, or flooding unnecessary routing protocol messages. (DoS is a common threat action causing disruption.)

Usurpation: This consequence happens when an attacker gains control over the services/functions a legitimate router is providing to others. Outsiders can cause this by delaying or dropping routing exchanges, fabricating or replaying routing information. Byzantine routers can cause this consequence by sending false routing information or interfering with routing exchanges.

Since data confidentiality is not a design goal for routing protocols, “disclosure” of routing information is not seen as a threat to the routing infrastructure.

This document outlines a roadmap for developing countermeasures against most of the above threats, for the given threat sources.

3 Road Map

3.1 Organization of the Roadmap

Components in this roadmap are organized in a manner that allows them to be roughly represented within a timeline. Different components within the roadmap framework represent well-defined problem spaces that have their own sets of tools, techniques, entities and action plan required to drive the specification and deployment of their relevant solutions. This organization is useful since the solution space within the routing security area ranges from security mechanisms that can be immediately deployed as incremental security measures within the infrastructure, to mechanisms that will be eventually developed through further research in the field of routing security. Maintaining a time-ordered set of functionally separate components helps in tracking forward momentum of the deployment effort and ensures that all essential tasks, issues and their dependencies have the adequate level of visibility.

Deployment and research form the two broad tracks in this roadmap.

The deployment track is comprised of those components that deal with driving the adoption of incremental improvements to the routing infrastructure using existing, well-known approaches for routing security. Research problems can themselves be segmented into two branches: one that deals with problems that are near-term and apply to improving existing security mechanisms, and the other that deals with secure mechanisms that are still under active investigation by the research community and are hence long-term.

The organization of components in this roadmap is "live" in that research problems are expected to transform into deployment problems as and when solutions to such research problems are devised and agreed upon. Deployment issues, when such are identified, may similarly be transformed into new near-term or long-term research problems.

The current roadmap is an expression of the current status quo within the routing security arena.

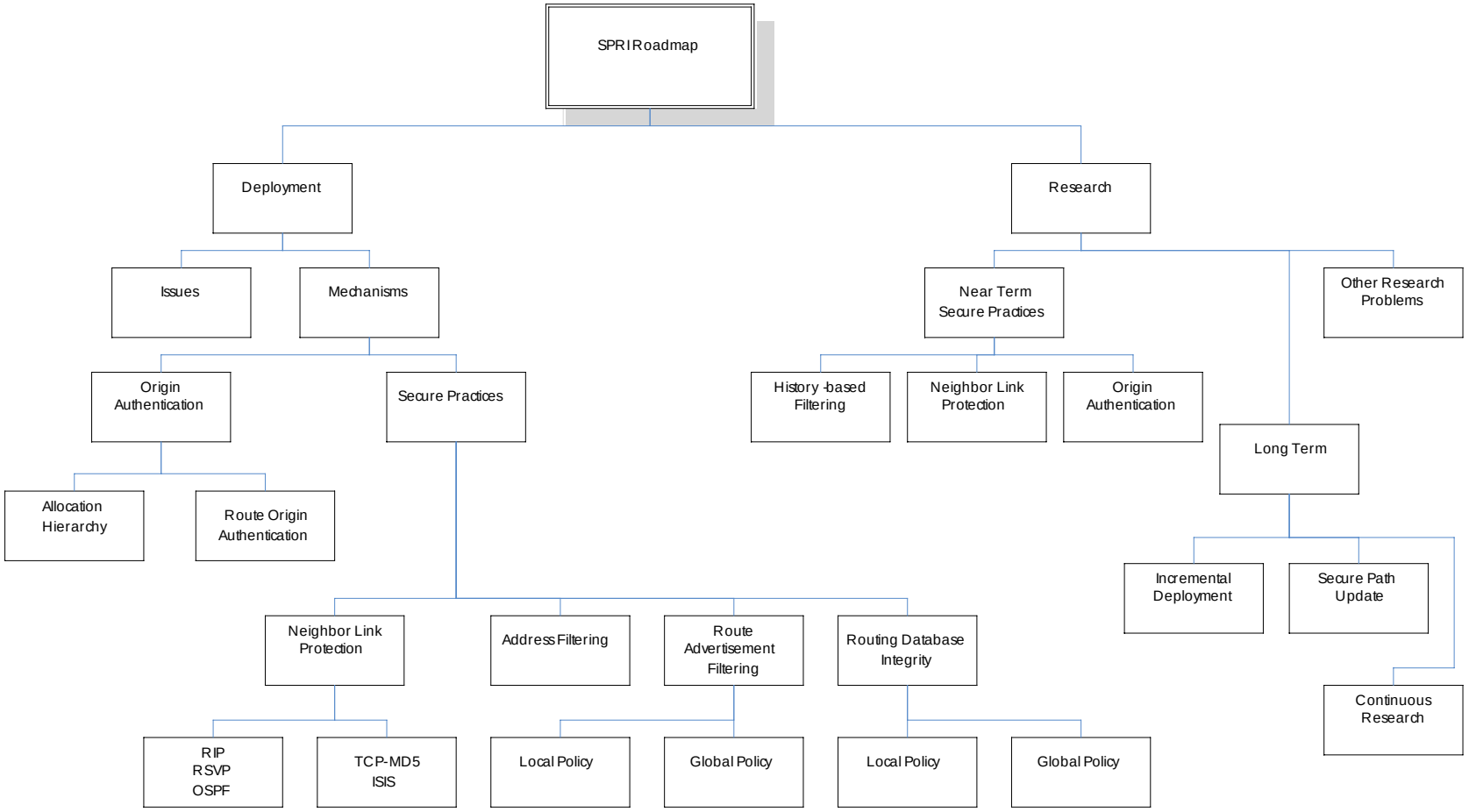

Figure 1: High-level Roadmap

3.2 Deployment Roadmap

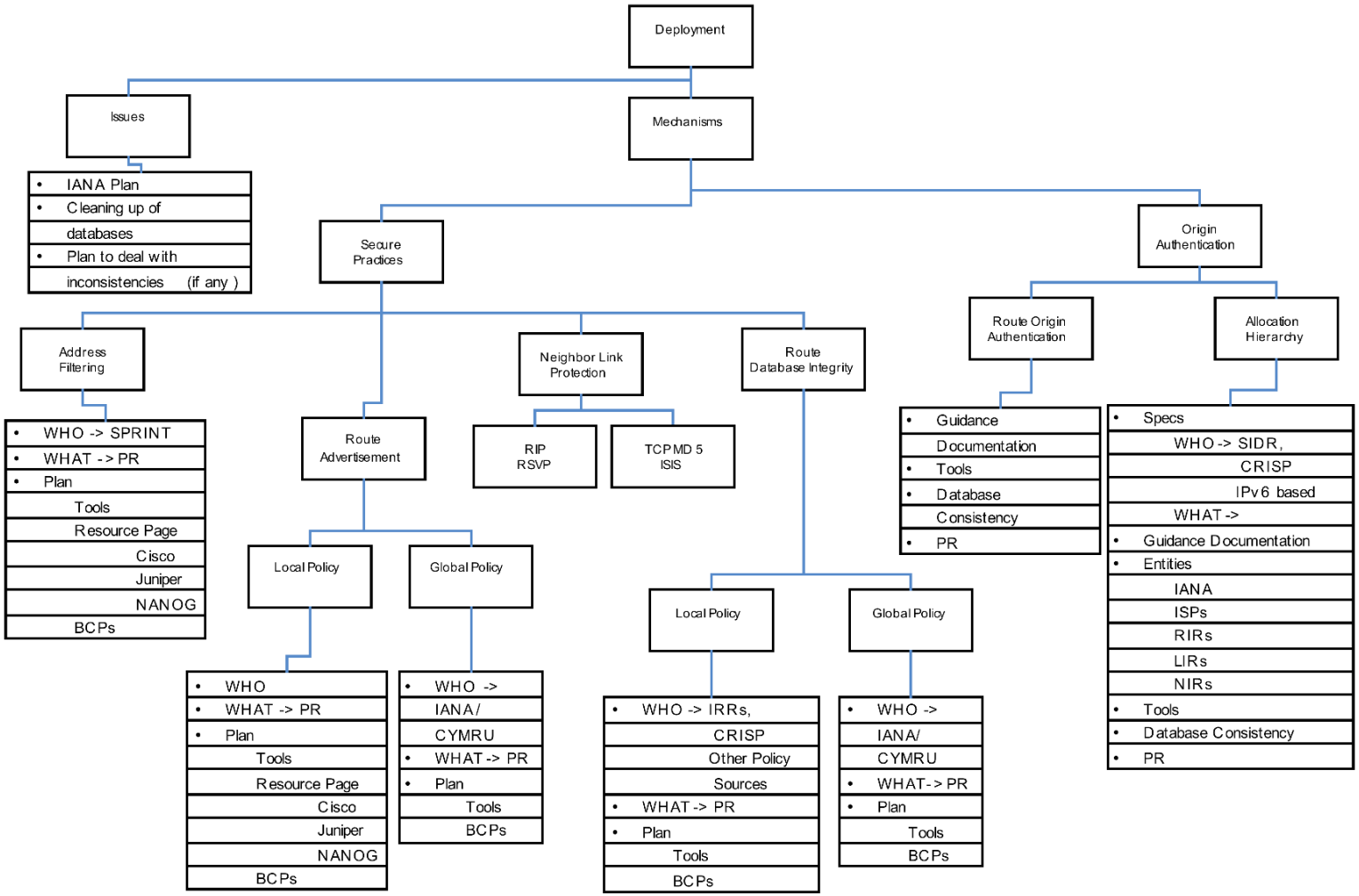

Figure 2: Deployment Roadmap

Deployment Roadmap

3.2.1 Mechanisms

3.2.1.1 Secure Practices

Simple changes to router configurations can sometimes contribute significantly towards improving routing security. The guidelines for making these configurations changes are codified in various Best Current Practices (BCP) documents but they are still far from being ubiquitously deployed. There are legitimate reasons for not making these changes in some cases; however the reason for this inertia may also be explained by a lack of education and outreach, and in some cases, even a matter of the operators not knowing that a problem exists.

NIST is presently drafting a publication (http://csrc.nist.gov/publications/drafts/800-54/Draft-SP800-54.pdf) which contains recommendations for BGP security. The publication covers threats and attacks on BGP, common practices that can counter or ameliorate the attacks, and recommendations of the practices to use. Many of the following practices are covered in the NIST document. (Future versions of this document will do a better job of integrating the NIST recommendations into the discussion.)

The approaches stated in this section are all countermeasures against the outsider threat source and are geared towards limiting the effectiveness of trivial spoofing, falsification, interference and overload attacks in the network [draft-ietf-rpsec-routing-threats].

The discussion for each practice following includes a list of characteristics:

a) **Synopsis**: Summary of the practice

b) **Barriers to Deployment:** What is currently hampering the deployment and use of this practice? This can be technical problems, management problems, perceptual problems, etc.

c) **Targeted Adopters:** Which entities would it be important to get to adopt the practice? These entities could be important either from influence or from a crucial part in the design?

d) **Early Adopters:** Who is ready, willing and able to deploy and use the practice? Such partners are important for working out issues initially and can provide experience to help others.

e) **Transitioning Mechanisms:** What steps or tools or plan is there for moving from the current state to deployment and use?

f) **Drivers:** Are there external events that could help move to deployment and use?

g) **Metrics and Reporting for Measuring Effectiveness:** What measurements can prove to ourselves that deployment and use efforts are succeeding or reassure others that deployment and use is possible?

h) **Tools and Resources – Required/Available:** Anything that could help, whether needing development or needing proselytizing.

i) **Educational Awareness (If applicable)**

3.2.1.1.1 Ingress and Egress Address Filtering in Symmetric Routing Environments

a) **Synopsis**

Ingress and egress data filtering can be employed in several positions in the Internet.

Firstly, filtering can be employed at the periphery of the Internet: by the ISPs to ensure that source address in incoming traffic is within some legitimate network prefix range, and by corporate networks to ensure that they are not the source of such spoofing attacks [BCP 38]. This also includes approaches such as strict and feasible Reverse Path Forwarding.

Secondly, filtering can be employed on peering links where routing is reasonably symmetric.

Finally, ingress filtering can be employed at multiple levels: at routers connecting LANs to the enterprise network and within service provider networks so that packets that arrive with the source address of an infrastructure node are dropped [draft-savola-rtgwf-backbone-attacks].

b) Barriers to Deployment

- Legacy equipment that is not capable of line-rate filtering
- Extremely large networks that are not amenable to using this technique.
- Management versus risk trade-off; operator arguments that this is rarely a problem at the current time.
- Requirement to always keep filters current; inadvertent multi-homing can (and will) cause problems
- PMTUD and Private/Non-routed Addresses (as described and in draft-savola-bcp84-urpf-experiences).

c) Targeted Adopters

- Large ISPs (ingress filtering)
- Corporate networks (egress filtering)
- ISPs with a peering relationship and where routing is symmetric.

d) Early Adopters

- Examples of the above

e) Transitioning Mechanisms

- Education and Outreach at various Network Operator Group venues
- Router vendors carrying this message

f) Drivers

- Quantifying the actual number of spoofed messages that exist in a typical network during steady state and highlighting the reduction in this number following usage of the filtering techniques.

g) Metrics and Reporting for Measuring Effectiveness

- Number of packets dropped.
- Address range that such packets originated from.
- False positives observed/noted.

h) Tools and Resources – Required/Available

- BCP 38
- BCP 84
- ietf-opsec-current-practices
- ietf-opsec-filter-caps
- RFC 3871
- Tools for detecting spoofed addresses
- Tool that can help identify when filtering is not being done or is done improperly. . For example, Obgp which can download data from monitoring points such as RouteViews and

RIPE RIS, organize data into a common format, add labeling information into the updates, and compare the update logs with the routing table snapshots

- NANOG resource pages containing step-by-step instructions for different classes of targeted adopters.
- Routing Working Group discussion on detecting spoofed addresses
- NSA Router Security Configuration Guide
- NRIC Best Practices
- NSTAC ISP-BGPDNS Working Group
- Cisco's BGPv4 Security Essentials
- Cisco Router Security Guide

3.2.1.1.2 Ingress and Egress Address Filtering in Multi-homed Sites

a) Synopsis

Ingress filtering as applied to multi-homed networks [BCP 84].

b) Barriers to Deployment

- Only works well if routing information at all ingress routers is consistent and accurate.
- The argument that perceived benefit of knowing that spoofed traffic comes from legitimate addresses is not worth the operational complexity of unicast RPF.
- Inconsistent/lack of support for unicast RPF at high link speeds [ietf-opsec-current-practices]

c) Targeted Adopters

- Large Transit networks.
- Small edge networks that are multi-homed

d) Early Adopters

- Examples of Tier-1 and Tier-2 ISPs that have deployed this mechanism
- Examples of sites that are multi-homed and have deployed BCP84

e) Transitioning Mechanisms

- Education and Outreach at various NOG venues.
- Router vendors carrying this message

f) Drivers

- Quantifying the actual number of spoofed messages that exist in a typical network during steady state and highlighting the reduction in this number following usage of the filtering techniques

g) Metrics and Reporting for Measuring Effectiveness

- Number of packets dropped.
- Address range that such packets originated from.
- False positives observed/noted.

h) Tools and Resources – Required/Available

- BCP 84
- draft-savola-bcp84-urpf-experiences

- ietf-opsec-current-practices
- ietf-opsec-filter-caps
- NANOG discussion of rpf and spoofed addresses
- Tools for detecting spoofed addresses
- Tool that can help identify when filtering is not being done or is done improperly.
- Operator Resource pages for different classes of ISPs and multi-homed sites.

3.2.1.1.3 Local Policy-based Route Advertisement Filtering

a) Synopsis

Use peering and route policy information being maintained by IRRs as well as internal data to automatically create filters for route origination information in updates.

b) Barriers to Deployment

- Data in IRRs may neither be reliable nor up-to-date.
- Complexity of IRR data
- Disinclination towards making the list of customers and peers public

c) Targeted Adopters

- SPRINT

d) Early Adopters

- NTT/Verio
- Level(3)
- SAVVIS

e) Transitioning Mechanisms

- Pilot approaches to ensure that the results based on filtering using the IRR database do not deviate from expected behavior.
- Automated creation of router configuration using IRR toolset/powertools
- Using MyASN, to monitor route advertisements out of own network
- Presentation of tools and techniques at various Network Operator Group venues.
- Hands-on workshops

f) Drivers

- Creation of an IRR/repository having reliable and up-to-date routing policy information.[See Section 3.2.1.1.6.a]
- Incentives for ISPs to maintain up-to-date information in the IRRs

g) Metrics and Reporting for Measuring Effectiveness

- Number of route advertisements dropped
- Prefixes in such route advertisements
- Number of false positives observed/noted.

h) Tools and Resources – Required/Available

- IRR toolset/powertools

- MyASN
- Resource pages for operators
- Results from various pilot projects
- Tools available as part of the RIPE Routing Registry Consistency Check project and those envisioned, such as the IRR Correction Wizard

3.2.1.1.4 Global Policy-based Route Advertisement Filtering

a) Synopsis:

Filter out advertisements for unallocated and non-routable address spaces based on publicly available information. These are filters that should be the same everywhere and applied globally.

b) Barriers to Deployment:

- Information on allocated address space may not be up-to-date.
- IANA database inconsistencies with respect to ownership of legacy prefixes.
- Identifying the authority that can publish information about martians
- Identifying the authority that can publish information about what the other important addresses are (such as DNS root servers)
- Identifying the authority from where bogon information can be obtained
- Publication mechanism for allocated and martian prefixes

c) Targeted Adopters

- IANA
- RIRs
- CYMRU

d) Early Adopters

- CYMRU
- Examples of sites that peer with the Cymru bogon route-server.

e) Transitioning Mechanisms

- Pilot approaches to ensure that the results based on filtering using the public databases do not deviate from expected behavior.
- Checking leakage of bogons using tools such as the Cymru Bogus ASN monitoring tool
- Presentation of tools and techniques at various Network Operator Group meetings.
- Hands-on workshops

f) Drivers

- Creation of a repository having reliable and up-to-date information on allocated (and allocated) address space and martians [see section 3.2.1.1.6.b3.2.1.1.6.b]
- Incentives for registries to maintain up-to-date information on allocated prefixes in these repositories.

g) Metrics and Reporting for Measuring Effectiveness

- Number of route advertisements dropped
- Prefixes in such route advertisements

- Number of false positives observed/noted.
- Measurements for how often the repository is updated and the bandwidth of downloads.

h) Tools and Resources – Required/Available

- Cymru Bogus ASN monitoring tool
- Cisco's BGPv4 Security Essentials
- NRIC Best Practices
- NISCC Border Gateway Protocol Filtering Guidelines
- Operator Resource pages
- Presentation of tools and techniques at various Network Operator Group meetings.
- Results from various pilot projects

3.2.1.1.5 Neighbor Link Protection

ISPs employ several different types of mechanisms to protect the router-router links in routing protocols. Some of these are operational: network design to limit access to the router-router links, routing design to prohibit access to internal addresses from external hosts, use of the TTL field to ensure that a packet must have been sent from the immediate neighbor. However, there are network topologies and environments where these mechanisms cannot be employed and cryptographic mechanisms must be used.

Currently, BGP, OSPF, ISIS, and RSVP have specifications for cryptographic protections. Even in environments where cryptographic mechanisms would be advisable, ISPs are not using the existing mechanisms.

a) Synopsis

The link to neighbors must be protected against flooding and clogging and against spoofed messages. Cryptographic mechanisms are used in some network environments to provide that protection.

b) Barriers to Deployment

- Hardware platform resource limitations
- Complexity of cryptographic key management; limitations of existing management tools
- Personnel training costs
- Potential for cryptographic mis-management to create another failure path

c) Targeted Adopters

- all tier-1 ISPs

d) Early Adopters

- Many ISPs are currently using various techniques; reports of experienced users should not be difficult to obtain.

e) Transitioning Mechanisms and Steps

- Perform risk assessment: identify potential link protection technologies and the network topologies, environments, and scenarios where each is appropriate
- Provide better cryptographic management tools
- Assist the operators in education and training in the use of the cryptography and the management tools.

f) Drivers

- The better management tools would be of great benefit.

g) Metrics and Reporting for Measuring Effectiveness

- Percentage of prefixes in routing table that have associated certificates (increase is good)
- Percentage of ASs in routing table that have associated certificates (increase is good)
- Number and percentage of suspected mis-originations, based on routing history (decrease is good)

h) Tools and Resources – Required/Available

- Cryptographic management tools

3.2.1.1.6 Routing Policy Database Integrity

Route filters are built using information contained in various repositories. Route policies published at the IRRs form the basis for the creation of local, ISP-specific filtering rules, while information on the current list of bogon addresses forms the basis for the creation of global rules, or rules that are consistent across ISPs. In both these cases, the repository that contains the relevant information must be trusted, current, and accurate.

3.2.1.1.6.a Local Policy Database Integrity

a) Synopsis

Maintaining the integrity and freshness of data in the IRR databases.

b) Barriers to Deployment

- Non-willingness of ISPs to update or register policy in the database due to concerns of policy exposure.
- Maintaining integrity of data contained in policy mirrors.
- Asserting who is authorized to say which routes are important and which ones should be the priority routes.
- Information from *rwhois* servers is not uploaded to the ARIN database.

c) Targeted Adopters

- IRRs, CRISP, Other Policy sources

d) Early Adopters

- All RIRs currently work to maintain their database integrity. However, some have legacy data that is slowly being cleaned up.

e) Transitioning Mechanisms

- Creating and exposing useful tools like database comparison tools, searching for anomalies and expired entries, creation of best current practices etc
- Running pilot programs to demonstrate successes on limited but real databases and requests.

f) Drivers

- Successful demonstration of pilot programs will encourage ISPs to register policies in the database.

g) Metrics and Reporting

- Metrics on quality of RIR data will be difficult to collect other than from the RIRs themselves. It will be difficult to measure increase in quality for those RIRs that are reluctant to provide measures.

h) Tools and Resources

- Route Configuration Checker (rcc) is an under-development tool created by M.I.T Labs that allows network operators to verify that their networks router configurations satisfy high-level properties
- RIPE has a project "Routing Registry Consistency Check" (rrcc) which compares routing data advertised in BGP with routing policies advertised in the RIPE IRR. The Nemecis project also compares advertised routing data to IRR data.
- The volunteer web site www.cidr-report.org occasionally reports on the conflicts between RIR "stat files" and their whois databases, under the title "RIR Resource Allocation Data Inconsistencies".
- Such comparisons for routing data consistency are important. However, these comparisons capture inconsistencies with routing information, not contact info. The contact data is exactly the data that is most problematic to keep current.

i) Education and Awareness

- Hold Hands-on workshops and presentations of various pilot tested tools and techniques at various Network Operator Group meetings, RIPE, etc.

3.2.1.1.6.b Global Policy Database Integrity

a) Synopsis

Maintaining the integrity and freshness of the bogon and bogus ASN listing.

b) Barriers to Deployment

- Policy information not correctly updated in the database.

c) Targeted Adopters

- IANA, CYMRU

d) Early Adopters

e) Transitioning Mechanisms

- Creating and exposing useful tools like database comparison tools, searching for anomalies and expired entries, creation of best current practices etc
- Running pilot programs to demonstrate successes on limited but real databases and requests.

f) Drivers

- Successful demonstration of pilot programs.

g) Metrics and Reporting

h) Tools and Resources

- Best Current Practices Resource pages
- Presentation of tools and techniques at various Network Operator Group meetings.
- Results from various pilot projects

3.2.1.2 Origin Authentication

The most obvious vulnerability in BGP is the unauthorized origination of routes to prefixes. When an AS originates a prefix, routes for traffic to that prefix are influenced. Some or all of the Internet may be sending traffic to the unauthorized AS, who may or may not be able to deliver the traffic. Certainly the unauthorized AS would have unauthorized access to the traffic.

This has been an operational problem in BGP for a decade or more. The operational solution has been to configure route filters on border routers to reject routes with improper originations. The burning question then becomes how to distinguish the improper originations from the proper originations. Some ISPs base this on their knowledge of their customers' addresses. A richly connected ISP may have as clear a vision as needed to the addresses advertised by their customers and peers to produce these filters. In some cases, the ISP will rely on an Internet Routing Registry to produce their route filters. Unfortunately, the IRRs are known to be inaccurate and incomplete and insecure, so this is not the best solution. For ISPs that provide transit and are close to the core of the Internet, these route filters can be so large as to stress the capacity of many router platforms.

There is work in the IETF, NOG, and RIR communities to produce a cryptographically based route origination authorization. This authorization must be based on a secure identification of the prefix holder, because the prefix holder is the only authority for origination of a route to that prefix. The IETF is currently working to define a PKI that will represent the identification of the prefix holder, based on the RIR address allocation process.

a) Synopsis

ISPs would find an authenticated list of authorized prefix originations useful. A cryptographically basis for such a list would lend itself to the assurance of the "authenticated" and "authorized" parts of this description.

b) Barriers to Deployment

- ISP distaste for centralized authorities
- Cost to ISPs to integrate certificate system within their current internal operations
- RIR unwillingness to undertake cost and risk to participate in the certificate system
- Hardware platform resource limitations

c) Targeted Adopters

- RIRs
- IRR/NRO
- all tier-1 ISPs

d) Early Adopters

- IIJ is rumored to be committed to deploying internally
- Other ISPs with a willingness to experiment (Internet 2 is an example of a contained network that might be good to ask)

e) Transitioning Mechanisms

There are several actions to be undertaken to further this work

- Progress the address and AS allocation PKI specifications through the IETF process
- Design an architecture for the distribution of the address and AS certificates, identify acceptable and willing entities for the roles of any data repositories in the distribution architecture, and implement distribution tools
- Based on that PKI, define a specification for a route origination object, decide on its distribution and authorization, and progress the specification through the IETF
- Identify acceptable and willing trust anchors for this PKI. The certificate specification is based on the address allocation process of the RIRs, but the RIRs may or may not be the acceptable trust anchors and may or may not agree to take on that role.
- Initiate pilot programs for production of certificates, to include producing and verifying certificates, distribution and retrieval of certificates.

- Initiate pilot programs for use of certificates, i.e., injecting certificates into ISP operations (into both business practices, i.e., communication with RIR, provider, and customer, and routing operations, i.e., routing anomaly debugging, filter building, router configuration generation, etc.)
- Initiate confidence building activities, e.g., comparison of routing information derived from certificate system to routing information derived from routing history or from an ISP's existing tools.
- Address the consistency between RIR allocation databases and the PKI - will the PKI design be intended to be parallel to the RIR database? Will there be mechanisms to ensure their consistency? How will inconsistencies impact the routing infrastructure? How will they be addressed? etc.
- Plan for incremental deployment - establishing operational guidelines for judging the security of routing information when not all routing information is secured.

f) Drivers

- Publication of prefixes that appear to have been mis-originated on a periodic basis (daily, weekly as in routing table reports to *NOG mailing lists, *NOG and RIR public meetings), with a "if your prefix had been protected, you might not be in this mess" message

g) Metrics and Reporting for Measuring Effectiveness

- Percentage of prefixes in routing table that have associated certificates (increase)
- Percentage of ASs in routing table that have associated certificates (increase)
- Number and percentage of suspected mis-originations, based on routing history (decrease)

h) Tools and Resources – Required/Available

- Certificate authority tools (signing, verifying certificates)
- Distributed repository tools - discovery, retrieval and upload, etc.
- ISP tools - communication with certificate authorities, verifying signed objects, retrieving verified lists, injection into router configuration, etc.

3.2.2 Issues

A few operational and deployment related issues came up during the creation of this roadmap that were deemed very important, and needed to be addressed to ensure the correct and secure working of most deployment mechanisms. A few of these issues have been summarized below. While this list is not complete, it may help increase awareness and bring up other related and non-related issues that may be important to the ISP operator community.

- IANA Plan
- Cleaning up of databases
- Plan to deal with inconsistencies if any.

3.3 Research Roadmap

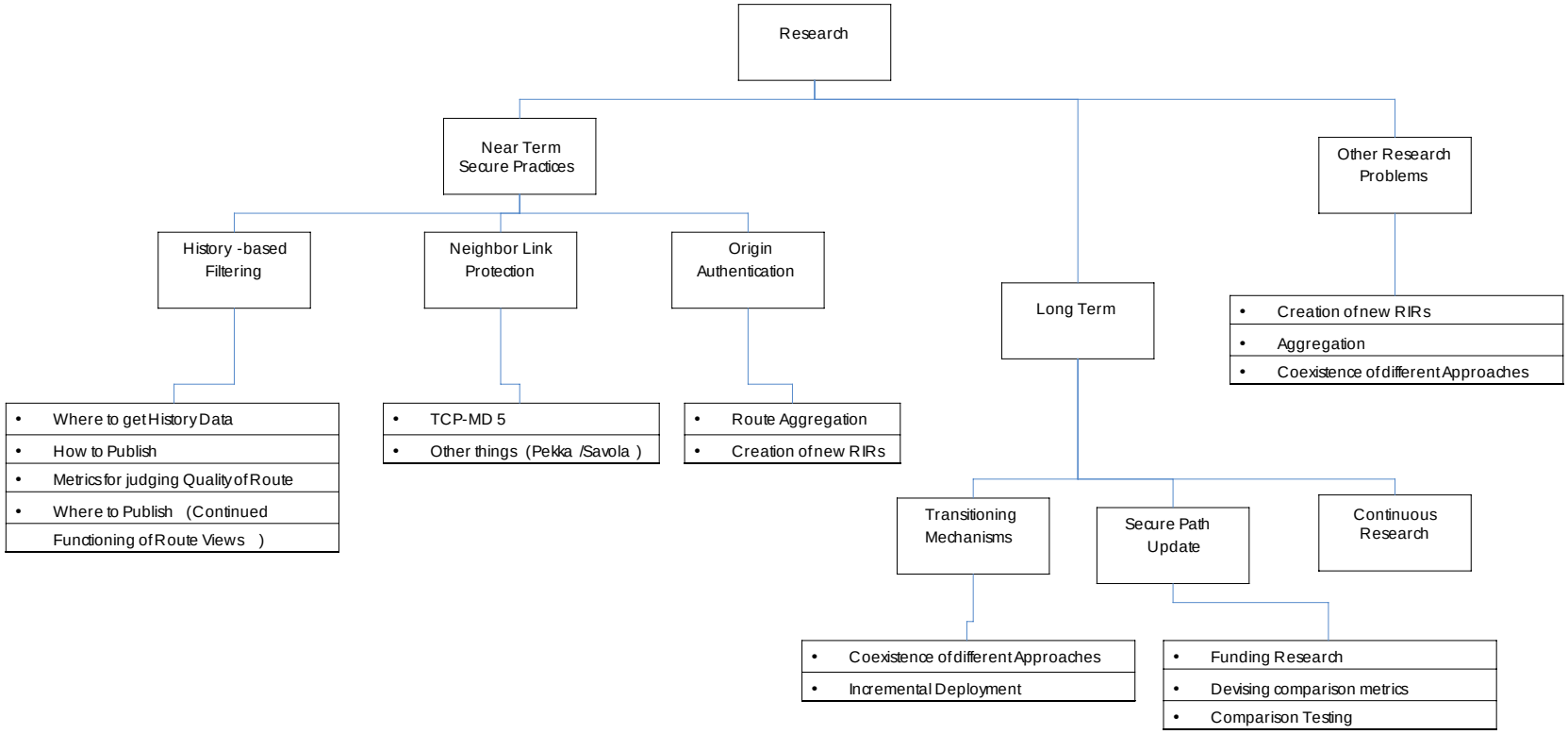

Figure 3: Research Roadmap.

Research Roadmap

As mentioned earlier, the Research track comprises of a near-term and a long term sub-tracks. The near-term sub-track examines various aspects of current routing security practices for their effectiveness and suggests enhancements where necessary on an immediate basis. The long-term sub-track, on the other hand, examines conceptual problems, security implications of current approaches, and new recommendations as newer technologies are phased-in. These may require a significant amount of research as well as consensus among both the research as well as the deployment community.

3.3.1 Near term Research

The research problems focused on in this sub category are issues that have critical importance in the main scheme of things, and will have a direct impact on day-to-day operations of the Internet. The problems identified in this category thus far are History-based filtering, Neighbor-link protection and Origin authentication; the prime focus being the creation of secure routing practices for each of these problems.

3.3.1.1 History-based filtering

Prefix filters are commonly used in an attempt to add some security to the BGP routing protocol advocates the use of aggressive filtering to ensure that malicious routing events are identified and eliminated. Ensuring that routing updates and messages are only obtained from trusted peers provides some security in the Internet. History-based filtering is an additional step to ensure that only trusted and previously known routes are accepted from peers. This technique utilizes previous network connection history that ensures BGP routers accept advertisements from peers that have traditionally advertised these prefixes, which is the predominant case. History based filtering has the advantage that may enable BGP nodes to detect anomalies, reject incorrect advertisements, and avoid inserting incorrect entries into their tables. In order to promote this approach as a recommended approach however, more research is needed to understand its side effects, additional requirements it may impose, new vulnerabilities it may introduce, how best it be deployed incrementally, what changes are required from the vendor and operator community and how to convince current ISPs, operators and vendors to transition to this technology.

3.3.1.2 Neighbor Link Protection

Some secure routing techniques like Secure Origin BGP rely on peer information. Thus if the neighbor links are not protected, a corrupt or even misconfigured router might be able to mislead other neighboring routers into inserting and propagating incorrect information throughout the infrastructure with a profoundly negative global effect. Various approaches exist to provide neighbor link protection, and in order to arrive at an agreement an in depth study should be performed similar to the history based filtering problem mentioned above.

Cryptographic protections are currently defined for BGP, ISIS, OSPF, RSVP, and LDP. All the current specifications are based on MD5, which is recognized to be weak. Furthermore, some of the designs are not suited for algorithms agility, so they cannot easily move to a new hash algorithm, and some have no provision for key rollover. There is a near term need for research into better protocol designs for cryptographic protections that would permit more dynamism in algorithm and keys. The action items would be:

- Assist the IETF process to design replacements for existing weak cryptographic protections in current protocols
- Work with vendors to get new cryptographic protections implemented and deployed
- Create guidelines for use of existing and new cryptographic protections (key sizes, roll-over, etc)
- Create guidelines for acceptance or rejection of existing cryptographic protections in mixed new crypto/old crypto environments

3.3.1.3 Origin Authentication

There is current work to produce a cryptographically based authorization of prefix originations. This work is based on established research, but there are a few areas where work still needs to be done:

- Aggregation: the BGP spec allows ISPs to aggregate announcements into announcements of shorter prefixes. When an aggregating ISP is the holder of the aggregate prefix and the aggregated prefixes, the existing approach works well. When the aggregating ISP is not the holder of some of the aggregated prefixes (proxy aggregation), the existing approach does not work well. Possible solutions to this need to be studied.
- Incremental deployment: because immediate deployment and use of any new technique throughout the Internet is not possible, there must be consideration of incremental deployment. Should secure information be communicated from one security aware area over a gap to another security aware area? If so, how is the recipient to judge routing information which is partially secured and partially not secured.

3.3.2 Long Term Research

Over time, it is expected that there will be many improvements, and many approaches to solving the same issues in the secure internet routing area that may be guided by the policies of individual organizations, governments, government agencies and academic entities. Such issues have been absorbed into the long-term research category, which not only absorbs the problem, but also issues related to the defining, solving and transitioning of the solutions into the *mainstream*. Continuous research may be needed to discover new vulnerabilities as newer technologies are phased-in, faster and cheaper computing resources become the norm and maintain scalability as more nations move towards internet culture. Thus, the main issues identified thus far in this sub-category are solving the problem of securely updating the path itself, and envisioning various transitioning mechanisms for incremental deployment and ensuring coexistence with other approaches. We elaborate on these below.

3.3.2.1 Transitioning Mechanisms

Coexistence of different Approaches

As routing in the Internet conceptually undergoes improvements, situations may arise where different organizations have employed different approaches. For the sake of a meaningful improvement to Internet routing as a whole, it becomes imperative to ensure that routers employing different approaches can coexist with each other without breaking the system.

Incremental Deployment

Similarly, as new approaches are researched and developed for deployment, a plan must be created to deploy this technology in an incremental fashion, so as to ensure nil-to-minimum down time for critical systems, avoid system overloads, and to iron out kinks in the newly deployed systems.

3.3.2.2 Secure Path Update

Secure Path Update is largely acknowledged as a *real* problem in routing security, yet little progress has been made in comparison with other problems in the same league.

Origin authentication and authorization is widely recognized as the necessary first step of protecting the routing information contained in a BGP Update. But the origination of a route to a prefix represents just the first step of protection of the information in the Update's AS_PATH. Many different techniques for AS_PATH protection have been suggested ((S-BGP, SoBGP, psBGP, SRV, IRV, etc.), but none have gained wide acceptance. Other attributes carried in the BGP Update, like communities, may also need protection. New attributes added to the BGP specification may also require protection.

Providing more funding for research in this area, devising comparison metrics to evaluate improvements and comparison testing are few ways to accelerate and make sizeable progress in this area.

- Examine the problem space

- Study existing solutions
- Weigh their merits, dependencies and drawbacks,
- Evaluate their benefits and cost
- Spread awareness in the research, vendor and operator community and
- Generate consensus that can lead to standardized deployment plans.

3.3.2.3 Continuous Research

As newer technologies are phased-in, improvements in Operating Systems and communication channels occur, faster and cheaper computing resources become the norm and maintain scalability as more nations move towards internet culture, there arises a need to revisit and refine older solutions and approaches, possibly create new ones in response to newer challenges.

3.3.3 Other research problems

This is a high visibility punch-out list of salient issues that may have arisen during research, from operators, deployment organizations, at IETF meetings, common workshops, etc that require some amount of investigation on how best to solve. Issues that have been realized so far are summarized below:

- Creation of new RIRs
- Prefix Aggregation
- Ensuring co-existence of different approaches for securing path updates

Each of these issues can be found elsewhere in the roadmap in their respective logical categories where they may have arisen.

4 Timeline

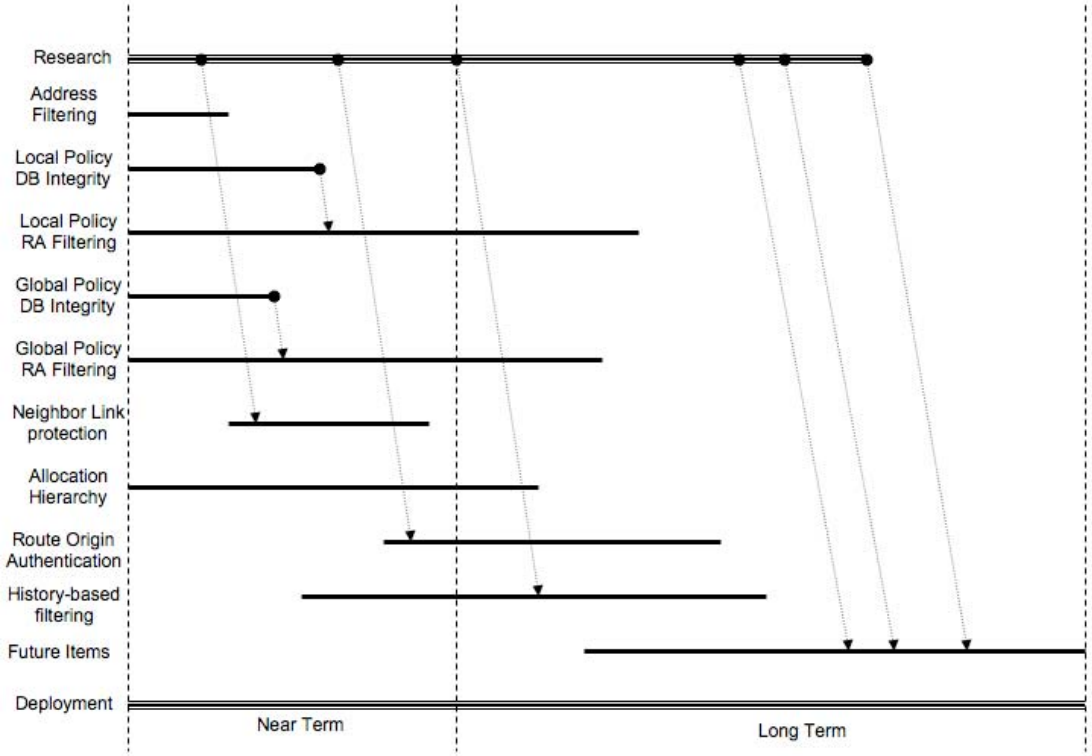

Figure 4: Timeline