The Threat Analysis and Requirements for Cryptographic Authentication
of Routing Protocols' Transports
draft-ietf-karp-threats-reqs-03

Abstract

Different routing protocols exist and each employs its own mechanism
for securing the protocol packets on the wire. While most already have
some method for accomplishing cryptographic message authentication, in
many cases the existing methods are dated, vulnerable to attack, and
employ cryptographic algorithms that have been deprecated. The "Keying
and Authentication for Routing Protocols" (KARP) effort aims to
overhaul and improve these mechanisms.
This document has two main parts - the first describes the threat
analysis for attacks against routing protocols' transports and the
second enumerates the requirements for addressing the described
threats. This document, along with the KARP design guide will be used
by KARP design teams for specific protocol review and overhaul. This
document reflects the input of both the IETF's Security Area and
Routing Area in order to form a jointly agreed upon guidance.

Status of this Memo

Copyright Notice

Table of Contents

1. **Introduction**

In March 2006 the Internet Architecture Board (IAB) held a workshop on
the topic of "Unwanted Internet Traffic". The report from that workshop
is documented in [RFC4948]. Section 8.1 of that document states "A
simple risk analysis would suggest that an ideal attack target of
minimal cost but maximal disruption is the core routing
infrastructure." Section 8.2 calls for "[t]ightening the security of
the core routing infrastructure." Four main steps were identified for
that tightening:

> *More secure mechanisms and practices for operating routers. This
> work is being addressed in the OPSEC Working Group.
>
> *Cleaning up the Internet Routing Registry repository (IRR), and
> securing both the database and the access, so that it can be used
> for routing verifications. This work should be addressed through
> liaisons with those running the IRR's globally.
>
> *Specifications for cryptographic validation of routing message
> content. This work will likely be addressed in the SIDR Working
> Group.
>
> *Securing the routing protocols' packets on the wire

This document addresses the last item in the list above, securing the
the transmission of routing protocol packets on the wire, or rather
securing routing protocol transport. This effort is referred to as
Keying and Authentication for Routing Protocols, or "KARP". This
document specifically addresses the threat analysis for per packet
routing protocol transport authentication, and the requirements for
protocols to mitigate those threats.
This document is one of two that together form the guidance and
instructions for KARP design teams working to overhaul routing protocol
transport security. The other document is the KARP Design Guide [I-
D.ietf-karp-design-guide].

1.1. **Terminology**

Within the scope of this document, the following words, when beginning
with a capital letter, or spelled in all capitals, hold the meanings
described to the right of each term. If the same word is used
uncapitalized, then it is intended to have its common english
definition.

PSK (Pre-Shared Key)

A key used by both peers in a secure configuration. Usually
exchanged out-of-band prior to a first connection.

Routing Protocol

When used with capital "R" and "P" in this document the term refers
the Routing Protocol for which work is being done to provide or
enhance its peer authentication mechanisms.

PRF

In cryptography, a pseudorandom function family, abbreviated PRF, is
a collection of efficiently-computable functions which emulate a
random oracle in the following way: No efficient algorithm can
distinguish (with significant advantage) between a function chosen
randomly from the PRF family and a random oracle (a function whose
outputs are fixed completely at random). Informally, a PRF takes a
secret key and a set of input values and produces random-seeming
output values for each input value.

KDF (Key derivation function)

A KDF is a function in which an input key and other input data is
used to generate (or derive) keying material that can be employed by
cryptographic algorithms. The key that is input to a KDF is called a
key derivation key. KDFs can be used to generate one or more keys
from either (i) a uniformly random or pseudorandom seed value or
(ii) a Diffie-Hellman shared secret or (iii) a non-uniform random
source or (iv) a passphrase.

Identifier

The type and value used by one peer of an authenticated message
exchange to signify to the other peer who they are. The Identifier
is used by the receiver as a lookup index into a table containing
further information about the peer that is required to continue
processing the message, for example a Security Association (SA) or
keys.

Identity Proof

Once the form of identity is decided, then there must be a
cryptographic proof of that identity, that the peer really is who
they assert themselves to be. Proof of identity can be arranged
between the peers in a few ways, for example pre-shared keys, raw
assymetric keys, or a more user-friendly representation of
assymetric keys, such as a certificate. Certificates can be used in

a way requiring no additional supporting systems -- e.g. public keys
for each peer can be maintained locally for verification upon
contact. Certificate management can be made more simple and scalable
with the use of minor additional supporting systems, as is the case
with self-signed certificates and a flat file list of "approved
thumbprints". Self-signed certificates will have somewhat lower
security properties than Certificate Authority signed certificates .
The use of these different identity proofs vary in ease of
deployment, ease of ongoing management, startup effort, ongoing
effort and management, security strength, and consequences from loss
of secrets from one part of the system to the rest of the system.
For example, they differ in resistance to a security breach, and the
effort required to remediate the whole system in the event of such a
breach. The point here is that there are options, many of which are
quite simple to employ and deploy.

SA (Security Association)

The parameters and keys that together form the required information
for processing secure sessions between peers. Examples of items that
may exist in an SA include: Identifier, PSK, Traffic Key,
cryptographic algorithms, key lifetimes.

KMP (Key Management Protocol)

A protocol used between peers for creation, distribution and
maintenance of secret keys. It determines how secret keys are
generated and made available to both the parties. If session or
traffic keys are being used, KMP is responsible for generating them
and determining when they should be renewed.

A KMP is helpful because it negotiates unique, pair wise, random
keys without administrator involvement. It also negotiates as
mentioned earlier several of the SA parameters required for the
secure connection, including key life times. It keeps track of those
lifetimes using counters, and negotiates new keys and parameters
before they expire, again, without administrator interaction.
Additionally, in the event of a breach, changing the KMP key will
immediately cause a rekey to occur for the Traffic Key, and those
new Traffic Keys will be installed and used in the current
connection.

KMP Function

Any actual KMP used in the general KARP solution framework

Peer Key

Keys that are used between peers as the identity proof. These keys
may or may not be connection specific, depending on how they were

established, and what form of identity and identity proof is being
used in the system. This would generally be given by the KMP that
would later be used to derive fresh traffic keys.

Traffic Key

The actual key (or set of keys) used for protecting the routing
protocol traffic. Since the traffic keys used in a particular
connection are not a fixed part of a device configuration no data
exists anywhere else in the operator's systems which can be stolen,
e.g. in the case of a terminated or turned employee. If a server or
other data store is stolen or compromised, the thieves gain no
access to current traffic keys. They may gain access to key
derivation material, like a PSK, but not current traffic keys in
use.

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC2119 [RFC2119].
When used in lower case, these words convey their typical use in common
language, and are not to be interpreted as described in RFC2119
[RFC2119].

1.3. Scope

Three basic services (or techniques) may be employed in order to secure
any piece of data as it is transmitted over the wire: privacy,
authentication, and message integrity. The focus for this effort, and
the scope for this roadmap document, will be message authentication and
packet integrity only. This work explicitly excludes, at this point in
time, privacy services. Non-repudiation is also excluded as a goal at
this time. Since the objective of most routing protocols is to broadly
advertise the routing topology, routing protocol packets are commonly
sent in the clear; confidentiality is not normally required for routing
protocols. However, ensuring that routing peers truly are the trusted
peers expected, and that no rogue peers or packets can compromise the
stability of the routing environment is critical, and thus our focus.
Privacy and non-repudiation may be addressed in future work.
OSPF [RFC5709], IS-IS [RFC5310], LDP [RFC5036], and RIP already have
existing mechanisms for cryptographically authenticating and integrity
checking the packets on the wire. Products with these mechanisms have
already been produced, code has already been written and both have been
optimized for the existing mechanisms. Rather than turn away from these
mechanisms, this document aims to enhance them, updating them to modern
and secure levels.
Therefore, the scope of this roadmap of work includes:

*Making use of existing routing protocol transport security
 mechanisms, where they exist, and enhancing or updating them as
 necessary for modern cryptographic best practices

*Developing a framework for using automatic key management in
 order to ease deployment, lower cost of operation, and allow for
 rapid responses to security breaches

*Specifying the automated key management protocol that may be
 combined with the bits-on-the-wire mechanisms.

This document does not contain protocol specifications. Instead, it
defines the areas where protocol specification work is needed and sets
a direction, a set of requirements, and a relative priority for
addressing that specification work.
There are a set of threats to routing protocols that are considered in-
scope for this document, and a set considered out-of- scope. These are
described in detail in the Threats (Section 2) section below.

1.4. Incremental Approach

The work also serves as an agreement between the Routing Area and the
Security Area about the priorities and work plan for incrementally
delivering the above work. The principle of crawl, walk, run will be in
place and routing protocol authentication mechanisms may not go
immediately from their current state to a state containing the best
possible, most modern security practices. This point is important as
there will be times when the best-security-possible will give way to
vastly- improved-over-current-security-but-admittedly-not-yet-best-
security- possible, in order that incremental progress toward a more
secure Internet may be achieved. As such, this document will call out
places where agreement has been reached on such trade offs.
Incremental steps will need to be taken for a few very practical
reasons. First, there are a considerable number of deployed routing
devices in operating networks that will not be able to run the most
modern cryptographic mechanisms without significant and unacceptable
performance penalties. The roadmap for any one routing protocol MUST
allow for incremental improvements on existing operational devices.
Second, current routing protocol performance on deployed devices has
been achieved over the last 20 years through extensive tuning of
software and hardware elements, and is a constant focus for improvement
by vendors and operators alike. The introduction of new security
mechanisms affects this performance balance. The performance impact of
any incremental step of security improvement will need to be weighed by
the community, and introduced in such a way that allows the vendor and
operator community a path to adoption that upholds reasonable
performance metrics. Therefore, certain specification elements may be
introduced carrying the "SHOULD" guidance, with the intention that the

same mechanism will carry a "MUST" in the next release of the specification.
This gives the vendors and implementors the guidance they need to tune their software and hardware appropriately over time. Last, some security mechanisms require the build out of other operational support systems, and this will take time. An example where these three reasons are at play in an incremental improvement roadmap is seen in the improvement of BGP's [RFC4271] security via the update of the TCP Authentication Option (TCP-AO) [RFC5925] effort. It would be ideal, and reflect best common security practice, to have a fully specified key management protocol for negotiating TCP-AO's authentication material, using certificates for peer authentication in the keying.
However, in the spirit of incremental deployment, we will first address issues like cryptographic algorithm agility, replay attacks, TCP session resetting in the base TCP-AO protocol before we layer key management on top of it.

1.5. Goals

The goals and general guidance for the KARP work follow:

1. Provide authentication and integrity protection for packets on the wire of existing routing protocols

2. Deliver a path to incrementally improve security of the routing infrastructure as explained in the earlier sections.

3. The deployability of the improved security solutions on currently running routing infrastructure equipment. This begs the consideration of the current state of processing power available on routers in the network today.

4. Operational deployability - A solutions acceptability will also be measured by how deployable the solution is by common operator teams using common deployment processes and infrastructures. I.e. We will try to make these solutions fit as well as possible into current operational practices or router deployment. This will be heavily influenced by operator input, to ensure that what we specify can -- and, more importantly, will -- be deployed once specified and implemented by vendors. Deployment of incrementally more secure routing infrastructure in the Internet is the final measure of success. Measurably, we would like to see an increase in the number of surveyed respondents who report deploying the updated authentication mechanisms anywhere across their network, as well as a sharp rise in usage for the total percentage of their network's routers.

   Interviews with operators show several points about routing

security. First, over 70% of operators have deployed transport connection protection via TCP-MD5 [RFC3562] on their EBGP [ISR2008]. Over 55% also deploy MD5 on their IBGP connections, and 50% deploy MD5 on some other IGP. The survey states that "a considerable increase was observed over previous editions of the survey for use of TCP MD5 with external peers (eBGP), internal peers (iBGP) and MD5 extensions for IGPs." Though the data is not captured in the report, the authors believe anecdotally that of those who have deployed MD5 somewhere in their network, only about 25-30% of the routers in their network are deployed with the authentication enabled. None report using IPsec [RFC4301] to protect the routing protocol, and this was a decline from the few that reported doing so in the previous year's report. From my personal conversations with operators, of those using MD5, almost all report deploying with one single manual key throughout the entire network. These same operators report that the one single key has not been changed since it was originally installed, sometimes five or more years ago. When asked why, particularly for the case of BGP using TCP MD5, the following reasons are often given:

A. Changing the keys triggers a TCP reset, and thus bounces the links/adjacencies, undermining Service Level Agreements (SLAs).

B. For external peers, difficulty of coordination with the other organization is an issue. Once they find the correct contact at the other organization (not always so easy), the coordination function is serialized and on a per peer/AS basis. The coordination is very cumbersome and tedious to execute in practice.

C. Keys must be changed at precisely the same time, or at least within 60 seconds (as supported by two major vendors) in order to limit connectivity outage duration. This is incredibly difficult to do, operationally, especially between different organizations.

D. Relatively low priority compared to other operational issues.

E. Lack of staff to implement the changes device by device.

F. There are three use cases for operational peering at play here: peers and interconnection with other operators, Internal BGP and other routing sessions within a single operator, and operator-to-customer-CPE devices. All three have very different properties, and all are reported as cumbersome. One operator reported that the same key is used

for all customer premise equipment. The same operator
reported that if the customer mandated, a unique key could
be created, although the last time this occurred it created
such an operational headache that the administrators now
usually tell customers that the option doesn't even exist,
to avoid the difficulties. These customer-unique keys are
never changed, unless the customer demands so. The main
threat at play here is that a terminated employee from such
an operator who had access to the one (or few) keys used for
authentication in these environments could easily wage an
attack -- or offer the keys to others who would wage the
attack -- and bring down many of the adjacencies, causing
destabilization to the routing system.

5. Whatever mechanisms we specify need to be easier than the
   current methods to deploy, and should provide obvious
   operational efficiency gains along with significantly better
   security and threat protection. This combination of value may
   be enough to drive much broader adoption.

6. Address the threats enumerated above in the "Threats" section
   (Section 2) for each routing protocol, along a roadmap. Not all
   threats may be able to be addressed in the first specification
   update for any one protocol. Roadmaps will be defined so that
   both the security area and the routing area agree on how the
   threats will be addressed completely over time.

7. Create a re-usable architecture, framework, and guidelines for
   various IETF working teams who will address these security
   improvements for various Routing Protocols. The crux of the
   KARP work is to re-use that framework as much as possible
   across relevant Routing Protocols. For example, designers
   should aim to re-use the key management protocol that will be
   defined for BGP's TCP-AO key establishment for as many other
   routing protocols as possible. This is but one example.

8. Bridge any gaps between IETF's Routing and Security Areas by
   recording agreements on work items, roadmaps, and guidance from
   the Area leads and Internet Architecture Board (IAB, http://
   www.iab.org).

1.6. Non-Goals

The following two goals are considered out-of-scope for this effort:

*Privacy of the packets on the wire. Once this roadmap is
 realized, we may revisit work on privacy.

*Message content validity (routing database validity). This work
 is being addressed in other IETF efforts, like SIDR.

Audience

The audience for this document includes:

   *Routing Area working group chairs and participants - These people
    are charged with updates to the Routing Protocol specifications.
    Any and all cryptographic authentication work on these
    specifications will occur in Routing Area working groups, with
    close partnership with the Security Area. Co- advisors from
    Security Area may often be named for these partnership efforts.

   *Security Area reviewers of routing area documents - These people
    are delegated by the Security Area Directors to perform reviews
    on routing protocol specifications as they pass through working
    group last call or IESG review. They will pay particular
    attention to the use of cryptographic authentication and
    corresponding security mechanisms for the routing protocols. They
    will ensure that incremental security improvements are being
    made, in line with this roadmap.

   *Security Area engineers - These people partner with routing area
    authors/designers on the security mechanisms in routing protocol
    specifications. Some of these security area engineers will be
    assigned by the Security Area Directors, while others will be
    interested parties in the relevant working groups.

   *Operators - The operators are a key audience for this work, as
    the work is considered to have succeeded if the operators deploy
    the technology, presumably due to a perception of significantly
    improved security value coupled with relative similarity to
    deployment complexity and cost. Conversely, the work will be
    considered a failure if the operators do not care to deploy it,
    either due to lack of value or perceived (or real) over-
    complexity of operations. And as such, the GROW and OPSEC WGs
    should be kept squarely in the loop as well.

Threats

In RFC4949 [RFC4949], a threat is defined as a potential for violation
of security, which exists when there is a circumstance, capability,
action, or event that could breach security and cause harm. This
section defines the threats that are in scope for this roadmap, and
those that are explicitly out of scope. This document leverages the
"Generic Threats to Routing Protocols" model, RFC 4593 [RFC4593],
capitalizes terms from that document, and offers a terse definition of
those terms. (More thorough description of routing protocol threats
sources, motivations, consequences and actions can be found in RFC 4593
[RFC4593] itself). The threat listings below expand upon these threat
definitions.

Threats In Scope

The threats that will be addressed in this roadmap are those from
OUTSIDERS, attackers that 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.
Message authentication and integrity protection specifically aims to
identify packets originating from OUTSIDERS.
The concept of OUTSIDERS can be further refined to include attackers
who are terminated employees, and those sitting on-path.

   *On-Path - attackers with control of a network resource or a tap
    along the path of packets between two routers. An on-path
    outsider can attempt a man-in-the-middle attack, in addition to
    several other attack classes. A man-in-the-middle (MitM) attack
    occurs when an attacker who has access to packets flowing between
    two peers tampers with those packets in such a way that both
    peers think they are talking to each other directly, when in fact
    they are actually talking to the attacker only. Protocols
    conforming to this roadmap will use cryptographic mechanisms to
    prevent a man-in-the-middle attacker from situating himself
    undetected.

   *Terminated Employees - in this context, those who had access
    router configuration that included keys or keying material like
    pre-shared keys used in securing the routing protocol. Using this
    material, the attacker could send properly MAC'd spoofed packets
    appearing to come from router A to router B, and thus impersonate
    an authorized peer. The attacker could then send false traffic
    that changes the network behavior from its operator's design. The
    goal of addressing this source specifically is to call out the
    case where new keys or keying material becomes necessary very
    quickly, with little operational expense, upon the termination of
    such an employee. This grouping could also refer to any attacker
    who somehow managed to gain access to keying material, and said
    access had been detected by the operators such that the operators
    have an opportunity to move to new keys in order to prevent an
    attack.

These attack actions are in scope for this roadmap:

   *Spoofing - when an unauthorized device assumes the identity of an
    authorized one. Spoofing can be used, for example, to inject
    malicious routing information that causes the disruption of
    network services. Spoofing can also be used to cause a neighbor
    relationship to form that subsequently denies the formation of
    the relationship with the legitimate router.

*Falsification - an action whereby an attacker sends false routing
 information. To falsify the routing information, an attacker has
 to be either the originator or a forwarder of the routing
 information. Falsification may occur by an originator, or a
 forwarder, and may involve overclaiming, misclaiming, or
 mistatement of network resource reachability. We must be careful
 to remember that in this work we are only targeting falsification
 from outsiders as may occur from tampering with packets in
 flight. Falsification from BYZANTINES (see the Threats Out of
 Scope section (Section 2.2) below) are not addressed by the KARP
 effort.

*Interference - when an attacker inhibits the exchanges by
 legitimate routers. The types of interference addressed by this
 work include:

   a. Adding noise

   b. Replaying out-dated packets

   c. Inserting protocol packets

   d. Corrupting protocol packets

   e. Breaking synchronization

   f. Changing message content

*DoS attacks on transport sub-systems - This includes any other
 DoS attacks specifically based on the above attack types. This is
 when an attacker sends spoofed packets aimed at halting or
 preventing the underlying protocol over which the routing
 protocol runs. For example, BGP running over TLS will still not
 solve the problem of being able to send a TCP FIN or TCP RST and
 causing the peer session to go down. Since this attack depends on
 spoofing, operators are encouraged to deploy proper
 authentication mechanisms to prevent such attacks. Routing
 Protocols should thus be made resilient to potential attacks on
 the layers above which they run.

*DoS attacks using the authentication mechanism - This includes an
 attacker sending packets which confuse or overwhelm a security
 mechanism itself. An example is initiating an overwhelming load
 of spoofed authenticated routing protocol packets so that the
 receiver needs to process the MAC check, only to discard the
 packet, sending CPU levels rising. Another example is when an
 attacker sends an overwhelming load of keying protocol
 initiations from bogus sources. All other possible DoS attacks
 are out of scope (see next section).

*Brute Force Attacks Against Password/Keys - This includes either
 online or offline attacks where attempts are made repeatedly
 using different keys/passwords until a match is found. While it
 is impossible to make brute force attacks on keys completely
 unsuccessful, proper design can make such attacks much harder to
 succeed. For example, the key length should be sufficiently long
 so that covering the entire space of possible keys is improbable
 using computational power expected to be available 10 years out
 or more. Using per session keys is another widely used method for
 reducing the number of brute force attacks as this would make it
 difficult to guess the keys.

2.2. Threats Out of Scope

Threats from BYZANTINE sources -- faulty, misconfigured, or subverted
routers, i.e., legitimate participants in the routing protocol -- are
out of scope for this roadmap. Any of the attacks described in the
above section (Section 2.1) that may be levied by a BYZANTINE source
are therefore also out of scope.
In addition, these other attack actions are out of scope for this work:

*Sniffing - passive observation of route message contents in
 flight

*Falsification by Byzantine sources - unauthorized message content
 by a legitimate authorized source.

*Interference due to:

   a. Not forwarding packets - cannot be prevented with
      cryptographic authentication

   b. Delaying protocol packets - cannot be prevented with
      cryptographic authentication

   c. Denial of receipt - cannot be prevented with cryptographic
      authentication

   d. Unauthorized message content - the work of the IETF's SIDR
      working group (http://www.ietf.org/html.charters/sidr-
      charter.html).

   e. Any other type of DoS attack. For example, a flood of
      traffic that fills the link ahead of the router, so that the
      router is rendered unusable and unreachable by valid packets
      is NOT an attack that this work will address. Many other
      such examples could be contrived.

Requirements for Phase 1 of a Routing Protocol Transport's Security Update

The following list of requirements SHOULD be addressed by a KARP Work Phase 1 security update to any Routing Protocol (according to section 4.1 of the KARP Design Guide [I-D.ietf-karp-design-guide] document). IT IS RECOMMENDED that any Phase 1 security update to a Rouing Protocol contain a section of the specification document that describes how each of these requirements are met. It is further RECOMMENDED that textual justification be presented for any requirements that are NOT addressed.

1. Clear definitions of which elements of the transmission (frame, packet, segment, etc.) are protected by the authentication mechanism

2. Strong algorithms, and defined and accepted by the security community, MUST be specified. The option should use algorithms considered accepted by the IETF's Security community, which are considered appropriately safe. The use of non-standard or unpublished algorithms SHOULD BE avoided.

3. Algorithm agility for the cryptographic algorithms used in the authentication MUST be specified, i.e. more than one algorithm MUST be specified and it MUST be clear how new algorithms MAY be specified and used within the protocol. This requirement exists in case one algorithm gets broken suddenly. Research to identify weakness in algorithms is constant. Breaking a cipher isn't a matter of if, but when it will occur. It's highly unlikely that two different algorithms will be broken simultaneously. So, if two are supported, and one gets broken, we can use the other until we get a new one in place. Having the ability within the protocol specification to support such an event, having algorithm agility, is essential. Mandating two algorithms provides both a redundancy, and a mechanism for enacting that redundancy when needed. Further, the mechanism MUST describe the generic interface for new cryptographic algorithms to be used, so that implementers can use algorithms other than those specified, and so that new algorithms may be specified and supported in the future.

4. Secure use of simple PSKs, offering both operational convenience as well as building something of a fence around stupidity, MUST be specified.

5. Routing protocol packets replay shouldnt affect the routing system. For non TCP based protocols like OSPF [RFC2328], IS-IS [RFC1195] , etc., two routers are said to have a session up if they are able to exchange protocol packets. Packets captured from one session must not be able to be re-sent and accepted

during a later session. Additionally, replay mechanisms must work correctly even in the presence of routing protocol packet prioritization by the router.

6. A change of security parameters REQUIRES, and even forces, a change of session traffic keys

7. Intra-connection re-keying which occurs without a break or interruption to the current peering session, and, if possible, without data loss, MUST be specified. Keys need to be changed periodically, for operational privacey (e.g. when an administrator who had access to the keys leaves an organization) and for entropy purposes, and a re-keying mechanism enables the deployers to execute the change without productivity loss.

8. Efficient re-keying SHOULD be provided. The specificaion SHOULD support rekeying during a connection without the need to expend undue computational resources. In particular, the specification SHOULD avoid the need to try/compute multiple keys on a given packet.

9. Prevent DoS attacks as those described as in-scope in the threats section Section 2.1 above.

10. Default mechanisms and algorithms specified and defined are REQUIRED for all implementations.

11. For backward compatibilty reasons manual keying MUST be supported.

12. Architecture of the specification SHOULD consider and allow for future use of a KMP.

13. The authentication mechanism in the Routing Protocol MUST be decoupled from the key management system used. It MUST be obvious how the keying material was obtained, and the process for obtaining the keying material MUST exist outside of the Routing Protocol. This will allow for the various key generation methods, like manual keys and KMPs, to be used with the same Routing Protocol mechanism.

14. Convergence times of the Routing Protocols SHOULD NOT be materially affected. Materially here is defined as anything greater than a 5% convergence time increase. Note that convergence is different than boot time. Also note that convergence time has a lot to do with the speed of processors used on individual routing peers, and this processing power increases by Moore's law over time, meaning that the same route calculations and table population routines will decrease in

duration over time. Therefore, this requirement should be considered only in terms of total number of protocol packets that must be exchanged, and less for the computational intensity of processing any one message. Alternatively this can be simplified by saying that the new mechanisms should only result in a minimal increase in the number of routing protocol packets passed between the peers.

15. The changes or addition of security mechanisms SHOULD NOT cause a refresh of route updates or cause additional route updates to be generated.

16. Router implementations provide prioritized treatment to certain protocol packets. For example, OSPF HELLO packets and ACKs are prioritized for processing above other OSPF packets. The authentication mechanism SHOULD NOT interfere with the ability to observe and enforce such prioritization. Any effect on such priority mechanisms MUST be explicitly documented and justified.Replay mechanisms provided by the routing protocols MUST work even if certain protocol packets are offered prioritized treatment.

17. The authentication mechanism does not provide message confidentiality, but SHOULD NOT preclude the possibility of confidentiality support being added in the future.

18. Routing protocols MUST only send minimal information regarding the authentication mechanisms and the parameters in its protocol packets to avoid exposing the information to parties on the path.

19. In most routing protocols (OSPF [RFC2328], IS-IS [RFC1195], BFD [RFC5880], RIP [RFC2453], etc), all speakers share the same key on a broadcast segment. Possession of the key itself is used for identity validation and no other identity check is used. This opens a window for an attack where the sender can masquerade as some other neighbor. Routing protocols SHOULD thus use some other information besides the key to validate a neighbor. One could look at [RFC6039] for details on such attacks.

20. Routing protocols that rely on the IP header (or information beyond the routing protocol payload) to identify the neighbor which originated the packet must either protect the IP header or provide some other means to identify the neighbor. [RFC6039] describes some attacks that are based on this.

21. The new security and authentication mechanisms MUST support incremental deployment. It will not be feasible to deploy a new

Routing Protocol authentication mechanism throughout the
network instantaneously. It also may not be possible to deploy
such a mechanism to all routers in a large autonomous system
(AS) at one time. Proposed solutions SHOULD support an
incremental deployment method that provides some benefit for
those who participate. Because of this, there are several
requirements that any proposed KARP mechanism should consider.

   a. The Routing Protocol security mechanism MUST enable each
      router to configure use of the security mechanism on a
      per- peer basis where the communication is one-on-one.

   b. The new KARP mechanism MUST provide backward compatibility
      in the message formatting, transmission, and processing of
      routing information carried through a mixed security
      environment. Message formatting in a fully secured
      environment MAY be handled in a non-backward compatible
      fashion though care must be taken to ensure that routing
      protocol packets can traverse intermediate routers which
      don't support the new format.

   c. In an environment where both secured and non-secured
      systems are interoperating a mechanism MUST exist for
      secured systems to identify whether an originator intended
      the information to be secured.

   d. In an environment where secured service is in the process
      of being deployed a mechanism MUST exist to support a
      transition free of service interruption (caused by the
      deployment per se).

22. The introduction of mechanisms to improve routing
    authentication and security may increase the processing
    performed by a router. Since most of the currently deployed
    routers do not have hardware to accelerate cryptographic
    operations, these operations could impose a significant
    processing burden under some circumstances. Thus proposed
    solutions should be evaluated carefully with regard to the
    processing burden they may impose, since deployment may be
    impeded if network operators perceive that a solution will
    impose a processing burden which either provokes substantial
    capital expense, or threatens to destabilize routers.

23. Given the high number of routers that would require the new
    authentication mechanisms in a typical ISP deployment,
    solutions can increase their appeal by minimizing the burden
    imposed on all routers in favor of confining significant work
    loads to a relatively small number of devices. Optional
    features or increased assurance that provokes more pervasive

processing load MAY be made available for deployments where the additional resources are economically justifiable.

24. The new authentication and security mechanisms should not rely on systems external to the routing system (the equipment that is performing forwarding). In order to ensure the rapid initialization and/or return to service of failed nodes it is important to reduce reliance on these external systems to the greatest extent possible. Therefore, proposed solutions SHOULD NOT require connections to external systems, beyond those directly involved in peering relationships, in order to return to full service. It is however acceptable for the proposed solutions to require post initialization synchronization with external systems in order to fully synchronize the security information.

4. Security Considerations

This document is mostly about security considerations for the KARP efforts, both threats and requirements for solving those threats. More detailed security considerations were placed in the Security Considerations section of the KARP Design Guide [I-D.ietf-karp-design-guide] document.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgements

The majority of the text for version -00 of this document was taken from draft-lebovitz-karp-roadmap, authored by Gregory Lebovitz.

7. References

7.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC4593]	Barbir, A., Murphy, S. and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.
[RFC4948]	Andersson, L., Davies, E. and L. Zhang, "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006", RFC 4948, August 2007.

7.2. Informative References

[RFC1195]	Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.
[RFC2328]	

	Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.
[RFC2453]	Malkin, G.S., "RIP Version 2", STD 56, RFC 2453, November 1998.
[RFC3562]	Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.
[RFC4271]	Rekhter, Y., Li, T. and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.
[RFC4301]	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
[RFC4949]	Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.
[RFC5036]	Andersson, L., Minei, I. and B. Thomas, "LDP Specification", RFC 5036, October 2007.
[RFC5925]	Touch, J., Mankin, A. and R. Bonica, "The TCP Authentication Option", RFC 5925, June 2010.
[RFC6039]	Manral, V., Bhatia, M., Jaeggli, J. and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols", RFC 6039, October 2010.
[RFC5880]	Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, June 2010.
[RFC5709]	Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T. and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009.
[RFC5310]	Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R. and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.
[I-D.ietf-karp-design-guide]	Lebovitz, G and M Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", Internet-Draft draft-ietf-karp-design-guide-08, November 2011.
[ISR2008]	McPherson, D and C Labovitz, "Worldwide Infrastructure Security Report", October 2008.

Authors' Addresses

Gregory Lebovitz Lebovitz Juniper Networks, Inc. 1194 North Mathilda Ave. Sunnyvale, California 94089-1206 USA EMail: gregory.ietf@gmail.com

Manav Bhatia Bhatia Alcatel-Lucent Bangalore, India EMail: manav.bhatia@alcatel-lucent.com

Russ White White Cisco Systems USA EMail: russ@cisco.com