            Keying and Authentication for Routing Protocols (KARP)
                    Overview, Threats, and Requirements

Abstract

   Different routing protocols employ different mechanisms for securing
   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 does not contain
   protocol specifications. Instead, it defines the areas where
   protocol specification work is needed. This document is a companion
   document to RFC 6518, "Keying and Authentication for Routing
   Protocols (KARP) Design Guidelines"; together they form the guidance
   and instruction KARP design teams will use to review and overhaul
   routing protocol transport security.

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 "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:

   o Create secure mechanisms and practices for operating routers.

   o Clean up the Internet Routing Registry (IRR) repository, and
      secure both the database and the access to it, so that it can be
      used for routing verification.

   o Create specifications for cryptographic validation of routing
      message content.

   o Secure the routing protocols' packets on the wire

   The first bullet is being addressed in the OPSEC working group. The
   second bullet should be addressed through liaisons with those running
   the IRR's globally. The third bullet is being addressed in other
   efforts within the IETF. For example, BGP message content validity
   is being addressed in the SIDR working group.

   This document addresses the last item in the list above, securing the
   transmission of routing protocol packets on the wire. More
   precisely, it focuses on securing the transport systems employed by
   routing protocols, including any mechanisms built into the protocols
   themselves to authenticate packets. This effort is referred to as
   Keying and Authentication for Routing Protocols, or "KARP". KARP is
   concerned with issues and techniques for protecting the messages
   between directly communicating peers. This type of protection may
   overlap with, but is strongly distinct from, protection designed to
   ensure that routing information is properly authorized relative to
   the source of the information. Such assurances are provided by other
   mechanisms and are outside the scope of this document.

   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 [RFC6518].

   This document does not contain protocol specifications. Instead, its
   goal is to define the areas where protocol specification work is
   needed and to provide a set of requirements for KARP design teams to
   follow as they update a routing protocol's existing transport
   security (see Work Phase 1 in Section 4.1 of [RFC6518]).

   This document has three main parts. The first part, found in Section
   2, provides an overview of the KARP effort. The second part, in
   Section 3, lists the threats from "Generic Threats To Routing
   Protocols" [RFC4593] that are in scope for per-packet authentication
   for routing protocol transport systems. Therefore, this document
   does not contain a complete threat model; it simply points to the
   parts of the governing threat model that KARP design teams must
   address and explicitly states which parts are out of scope for KARP
   design teams. The third part, in Section 4, enumerates the
   requirements that routing protocol specifications must meet when
   addressing the threats related to KARP's Work Phase 1, the update to
   a routing protocol's existing transport security. ("Work Phase 2", a
   framework and usage of a Key Management Protocol (KMP), will be
   addressed in a future document[s]).

1.1. Terminology

   This document uses the terminology "on the wire" to refer to the
   information used by routing protocols' transport systems. This term
   is widely used in RFCs, but is used in several different ways. In
   this document, it is used to refer both to information exchanged
   between routing protocol instances and to underlying protocols that
   may also need to be protected in specific circumstances. Individual
   protocol analysis documents will need to be more specific in their
   use of this phrase.

   Additionally, within the scope of this document, the following words,
   when beginning with a capital letter, or spelled in all capital
   letters, hold the meanings described in this section. If the same
   word is used uncapitalized, then it is intended to have its common
   English definition.

   Identifier
      The type and value used by a peer of an authenticated message
      exchange to signify who it is to another peer. The Identifier is
      used by the receiver as an 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 Authentication
   Once the identity is verified, there must be a cryptographic proof
   of that identity, to ensure that the peer really is who it asserts
   to be. Proof of identity can be arranged among peers in a few
   ways, for example, symmetric and asymmetric pre-shared keys, or an
   asymmetric key contained in a certificate. Certificates can be
   used in ways that require no additional supporting systems
   external to the routers themselves. An example of this is using
   self-signed certificates and a flat file list of "approved
   thumbprints". The different identity verification mechanisms vary
   in ease of deployment, ease of ongoing management, startup effort,
   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 recover 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.

KDF (Key Derivation Function)
   A KDF is a function in which an input key and other input data are
   used to generate 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 (i) a random or pseudorandom seed value, or (ii)
   the result of the Diffie-Hellman exchange, or (iii) a non-uniform
   random source (e.g., from a non-deterministic random bit
   generator), or (iv) a pre-shared key that may or may not be
   memorable by a human.

KMP (Key Management Protocol)
   KMP is a protocol that establishes a shared symmetric key between
   a pair (or among a group) of users. It determines how secret keys
   are made available to the users, and in some cases also determines
   how the secret keys are generated. In some routing protocols, the
   routing protocol derives the traffic keys from a master key. In
   this case, KMP is responsible for the master-key generation and
   for determining when the master key should be renewed. In other
   cases, there are only traffic keys (and no master key); in such a
   case, KMP is responsible for the traffic key generation and
   renewal mechanism.

KMP Function
   Any KMP used in the general KARP solution framework.

Peer Key
   Peer keys are keys that are used among peers as a basis for
   identifying one another. These keys may or may not be connection
   specific, depending on how they were established, and what forms

of identity and identity authentication mechanism are used in the
system. A peer key generally would be provided by a KMP and would
later be used to derive fresh traffic keys.

PSK (Pre-Shared Key)
   A PSK is a key used to communicate with one or more peers in a
   secure configuration. It is always distributed out of band prior
   to a first connection.

Replayed Messages
   Replayed messages are genuine messages that have been re-sent by
   an attacker. Messages may be replayed within a session (i.e.,
   intra-session) or replayed from a different session (i.e., inter-
   session). For non-TCP-based protocols like OSPF [RFC2328] and
   IS-IS [RFC1195], two routers are said to have a session up if they
   are able to exchange protocol packets (i.e., the peers have an
   adjacency). Messages replayed during an adjacency are intra-
   session replays, while a message replayed between two peers who
   re-establish an adjacency after a reboot or loss of connectivity
   are inter-session replays.

Routing Protocol
   This term refers to a Routing Protocol on which a KARP team is
   working to improve the security of its packets on the wire.

SA (Security Association)
   An SA is a relationship established between two or more entities
   to enable them to protect the data they exchange. Examples of
   attributes that may be associated with an SA include Identifier,
   PSK, Traffic Key, cryptographic algorithms, and key lifetimes.

Threat Source
   A threat source is a motivated, capable adversary.

Traffic Key
   A Traffic Key is the key (or one of a set of keys) used for
   protecting the routing protocol traffic. A traffic key should not
   be a fixed value in a device configuration. A traffic key should
   be known only to the participants in a connection, so that a
   compromise of a stored key (possibly available to a terminated or
   turned employee) does not result in disclosure of traffic keys.
   If a server or other data store is stolen or compromised, the
   attackers gain no access to current traffic keys. They may gain
   access to key-derivation material, like a PSK, but not traffic
   keys currently in use.

Additional terminology specific to threats are listed and defined
below in Section 3.

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 RFC 2119 [RFC2119].

   When used in lower case, these words convey their typical use in
   common language, and are not to be interpreted as described in RFC
   2119.

2. KARP Effort Overview

2.1. KARP Scope

   Three basic principles can be used to secure any piece of data as it
   is transmitted over the wire: confidentiality, authenticity, and
   integrity. The focus for the KARP working group will be message
   authentication and message integrity only. At this time, this work
   explicitly excludes confidentiality. 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 are authentically identified and that no rogue peers or
   unauthenticated packets can compromise the stability of the routing
   environment are critical and thus in scope. Confidentiality and non-
   repudiation may be addressed in future work.

   OSPF [RFC5709], IS-IS [RFC5310], LDP [RFC5036], and RIP [RFC2453]
   [RFC4822] already incorporate mechanisms for cryptographically
   authenticating and integrity checking the messages on the wire.
   Products and code that incorporate these mechanisms have been
   produced and have been optimized for these existing security
   mechanisms. Rather than turn away from these mechanisms, this
   document aims to enhance them, updating them to modern and more
   secure levels.

   Therefore, the scope of KARP's roadmap of work includes:

   o Making use of existing routing protocol transport security
      mechanisms, where they have been specified, and enhancing or
      updating them as necessary for modern cryptographic best
      practices. [RFC6518], Section 4.1 labels this KARP's Work Phase 1.

   o 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. [RFC6518], Section 4.1 labels
      this KARP's Work Phase 2.

    o Specifying an automated key management protocol that may be
       combined with Routing Protocol mechanisms. [RFC6518], Section 4.1
       labels this KARP's Work Phase 2.

   Neither this document nor [RFC6518] contains protocol specifications.
   Instead, they define the areas in which protocol specification work
   is needed, and they set a direction, a set of requirements, and
   priorities for addressing that specification work.

   There are a set of threats to routing protocols that are considered
   in scope for KARP, and a set considered out of scope. These are
   described in detail in Section 3.

2.2. Incremental Approach

   This document serves as an agreement between the Routing Area and the
   Security Area about the priorities and work plan for incrementally
   delivering the work described in the KARP roadmap above. The
   principle of "crawl, walk, run" will be employed. Thus routing
   protocol authentication mechanisms may not go immediately from their
   current state to a state reflecting 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 security that is
   vastly improved over current security but that is admittedly not the
   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 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 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 a future release of the specification. This approach 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, which will take time.

   An example where these three steps were at play in an incremental
   improvement roadmap was the improvement of BGP's [RFC4271] security
   via the TCP Authentication Option (TCP-AO) [RFC5925] effort. It
   would have been ideal, and would have reflected best common security
   practice, to have a fully specified key management protocol for
   negotiating the TCP-AO keying material, e.g., using certificates for
   peer authentication. However, in the spirit of incremental
   deployment, the IETF first addressed issues like cryptographic
   algorithm agility, replay attacks, and the resetting of TCP sessions
   in the base TCP-AO protocol, and then later began work to layer key
   management on top of these.

2.3. Goals

   The goals and general guidance for the KARP work follow:

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

   2. Define a path to incrementally improve security of the routing
       infrastructure as explained in Section 2.2.

   3. Ensure that the improved security solutions are deployable on
       current routing infrastructure. This requires consideration of
       the current state of processing power available on routers in the
       network today.

   4. Operational deployability - A solution's acceptability also will
       be measured by how deployable the solution is by operator teams,
       with consideration for their deployment processes and
       infrastructures. Specifically, KARP design teams will try to
       make these solutions fit as well as possible into current
       operational practices and router deployment methodologies. Doing
       so will depend heavily on operator input during KARP design
       efforts. Hopefully, operator input will lead to a more
       deployable solution, which will, in turn, lead to more production
       deployments. Deployment of incrementally more secure routing
       infrastructure in the Internet is the final measure of success.
       We would like to see an increase in the number of respondents to
       surveys such as [ISR2008] to report deployment of the updated
       authentication and integrity mechanisms in their networks, as
       well as see a sharp rise in usage of these mechanisms across a
       greater percentage of their network's routers.

Interviews with operators show several points about routing
security. First, according to [ISR2008], over 70% of operators
have deployed transport connection protection via TCP MD5
[RFC3562] on their External Border Gateway Protocol (eBGP)
sessions. Over 55% also deploy TCP MD5 on their Internal Border
Gateway Protocol (iBGP) connections, and 50% make use of TCP MD5
offered on some other internal gateway protocol (IGP). The same
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 TCP 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,
which was a decline from the few that reported doing so in the
previous year's report. Anecdotal evidence from operators using
MD5 shows that almost all report using one manually distributed
key throughout the entire network. These same operators report
that the 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 protecting BGP sessions using TCP
MD5, the following reasons were often given:

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

B. For external peers, it is difficult to coordinate with the
   other organization, and in practice the coordination is very
   cumbersome and tedious to execute. Once the operator finds
   the correct contact at the other organization (not always so
   easy), the coordination function is serialized and performed
   on a per-peer or per-AS basis.

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 the duration of a connectivity outage. This is
   incredibly difficult to do, operationally, especially between
   different organizations.

D. Key change is perceived as a relatively low priority compared
   to other operational issues.

E. Staff levels are insufficient to implement the changes on a
   device-by-device basis.

      F. There are three use cases for operational peering at play:
         peers and interconnection with other operators, iBGP and other
         routing sessions within a single operator, and operator-to-
         customer devices. All three have very different properties,
         and all are reported as cumbersome to manage securely. One
         operator reported that the same key is used for all customer
         premise equipment (CPE). The same operator reported that if
         the customer mandated it, 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 here is that
         a terminated employee from such an operator who had access to
         the one (or several) keys used for authentication in these
         environments could wage an attack. Alternatively, the
         operator could offer the keys to others who would wage the
         attack. In either case, the attacker could then bring down
         many of the adjacencies, thus destabilizing the routing
         system.

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

   6. Address the threats enumerated below in "Threats" (Section 3) for
       each routing protocol. 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 reusable architecture, framework, and guidelines for
       various IETF working groups that will address these security
       improvements for various Routing Protocols. The crux of the KARP
       work is to reuse the architecture, framework, and guidelines as
       much as possible across relevant Routing Protocols. For example,
       designers should aim to reuse the key management protocol that
       will be defined for BGP, which will establish keys for TCP-AO,
       for as many other routing protocols with similar characteristics
       and properties as possible.

   8. Bridge any gaps between the IETF Routing and Security Areas by
       recording agreements on work items, roadmaps, and guidance from
       the cognizant Area Directors and the Internet Architecture Board
       (IAB).

2.4. Non-Goals

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

   o Confidentiality and non-repudiation of the packets on the wire.
      Once the goals of this roadmap are realized, work on
      confidentiality may be considered.

   o Non-repudiation of the packets on the wire.

   o Message content validity (routing database validity). This work
      is being addressed in other IETF efforts. For example, BGP
      message content validity is being addressed in the SIDR working
      group.

2.5. Audience

   The audience for this document includes:

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

   o Security Area reviewers of Routing Area documents - These people
      are tasked by the Security Area Directors to perform reviews on
      routing protocol specifications as they pass through working group
      last call or IESG review. Their particular attention to the use
      of cryptographic authentication and newly specified security
      mechanisms for the routing protocols is appreciated. They also
      help to ensure that incremental security improvements are being
      made, in line with this roadmap.

   o 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.

   o Operators - The operators are a key audience for this work, as the
      work is considered to have succeeded only if operators deploy the
      technology. It is anticipated that deployment will take place
      only if operators perceive that the improved security offered by
      the Routing Protocol updates warrants the complexity and cost of
      deployment and operation. Conversely, the work will be considered
      a failure if operators do not deploy it, either due to a lack of

perceived value or due to perceived operational complexity. As a
result, the GROW and OPSEC working groups should be kept squarely
in the loop as well.

3. Threats

This document uses the definition of "threat" from RFC 4949
[RFC4949]: "[a] potential for violation of security, which exists
when there is an entity, circumstance, capability, action, or event
that could cause harm."

This section defines the threats that are in scope for the KARP
effort. It also lists those threats that are explicitly out of scope
for the KARP effort. Threats are discussed assuming that no
protection (i.e., message authentication and message integrity) has
been applied to routing protocol messages.

This document leverages the model described in "Generic Threats to
Routing Protocols" [RFC4593]. Specifically, the threats listed below
were derived by reviewing [RFC4593], analyzing how the threats
applied to the KARP problem space, and listing the threats that are
applicable to the work for the KARP design team. This document
categorizes [RFC4593] threats into those in scope and those out of
scope for KARP. Each in-scope threat is discussed below, and its
applicability to the KARP problem space is described. As such, the
following text intentionally is not a comprehensive threat analysis.
Rather, it describes the applicability of the existing threat
analysis in [RFC4593] to KARP.

Note: terms from [RFC4593] appear capitalized below -- e.g.
OUTSIDERS -- so as to make explicit the term's origin, and to enable
rapid cross referencing to the source RFC.

For convenience, a terse definition of most [RFC4593] terms is
offered here. Those interested in a more thorough description of
routing protocol threat sources, motivations, consequences, and
actions will want to read [RFC4593] before continuing here.

3.1. Threat Sources

3.1.1. OUTSIDERS

One of the threats that will be addressed in this roadmap is the
situation in which the source is an OUTSIDER. An OUTSIDER attacker
may reside anywhere in the Internet, may 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.
OUTSIDERS are not legitimate participants in the routing protocol.

   The use of message authentication and integrity protection
   specifically aims to identify packets originating from OUTSIDERS.

   KARP design teams will consider two specific use cases of OUTSIDERS:
   those on path, and those off path.

   o On Path - These attackers have control of a network resource or a
      tap that sits along the path between two routing peers. A "Man in
      the Middle" (MitM) is an on-path attacker. From this vantage
      point, the attacker can conduct either active or passive attacks.
      An active attack occurs when the attacker places packets on the
      network as part of the attack. One active MitM attack relevant to
      KARP, an active wiretapping attack, occurs when the attacker
      tampers with packets moving between two legitimate router peers 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.
      Protocols conforming to this roadmap will use cryptographic
      mechanisms to detect MitM attacks and reject packets from such
      attacks (i.e., discard them as being not authentic). Passive on-
      path attacks occur when the attacker silently gathers data and
      analyzes it to gain advantage. Passive activity by an on-path
      attacker may lead to an active attack.

   o Off Path - These attackers sit on some network outside of that
      over which the packets between two routing peers run. The source
      may be one or several hops away. Off-path attackers can launch
      active attacks, such as SPOOFING or denial-of-service (DoS)
      attacks, to name a few.

3.1.2. Unauthorized Key Holder

   This threat source exists when an unauthorized entity somehow manages
   to gain access to keying material. Using this material, the attacker
   could send packets that pass the authenticity checks based on Message
   Authentication Codes (MACs). The resulting traffic might appear to
   come from router A and be destined for router B, and thus the
   attacker could impersonate an authorized peer. The attacker could
   then adversely affect network behavior by sending bogus messages that
   appear to be authentic. The attack source possessing the
   unauthorized keys could be on path, off path, or both.

   The obvious mitigation for an unauthorized key holder is to change
   the keys currently in use by the legitimate routing peers. This
   mitigation can be either reactive or proactive. Reactive mitigation
   occurs when keys are changed only after one has discovered that the
   previous keys have fallen into the possession of unauthorized users.
   The reactive mitigation case is highlighted here in order to explain
   a common operational situation where new keying material will need to

be put in place with little or no advanced warning. In such a case,
new keys must be able to be installed and put into use very quickly,
and with little operational expense. Proactive mitigation occurs
when an operator assumes that unauthorized possession will occur from
time to time without being discovered, and the operator moves to new
keying material in order to cut short an attacker's window of
opportunity to use the stolen keys effectively.

KARP design teams can address this type of attack by creating
specifications that make it practical for the operator to quickly
change keys without disruption to the routing system and with minimal
operational overhead. Operators can further mitigate threats from
unauthorized key holders by regularly changing keys.

3.1.2.1. Terminated Employee

A terminated employee is an important example of an unauthorized key
holder. Staff attrition is a reality in routing operations and is
therefore a potential threat source. The threat source risk arises
when a network operator who had been granted access to keys ceases to
be an employee. If new keys are deployed immediately, the situation
of a terminated employee can become an "unauthorized key holder,
proactive" case, as described above, rather than an "unauthorized key
holder, reactive mitigation" case. It behooves the operator to
change the keys, to enforce the revocation of authorization of the
old keys, in order to minimize the threat source's window of
opportunity.

A terminated employee is a valid unauthorized key holder threat
source for KARP, and designs should address the associated threats.
For example, new keys must be able to be installed and made
operational in the routing protocols very quickly, with zero impact
to the routing system, and with little operational expense. The
threat actions associated with a terminated employee also motivate
the need to change the keys quickly, also with little operational
expense.

3.1.3. BYZANTINE

According to [RFC4593], Section 3.1.1.2, BYZANTINE "attackers are
faulty, misconfigured, or subverted routers; i.e., legitimate
participants in the routing protocol", whose messages cause routing
to malfunction.

[RFC4593] goes on to say that "[s]ome adversaries can subvert
routers, or the management workstations used to control these
routers. These Byzantine failures represent the most serious form of

attack capability in that they result in emission of bogus traffic by
legitimate routers."

[RFC4593] explains that "[d]eliberate attacks are mimicked by
failures that are random and unintentional. In particular, a
Byzantine failure in a router may occur because the router is faulty
in hardware or software or is misconfigured", and thus routing
malfunctions unintentionally. Although not malicious, such
occurrences still disrupt network operation.

Whether faulty, misconfigured, or subverted, Byzantine routers have
an empowered position from which to provide believable yet bogus
routing messages that are damaging to the network.

3.2. Threat Actions In Scope

The following THREAT ACTIONS are in scope for KARP:

o SPOOFING - when an unauthorized device assumes the identity of an
   authorized one. Spoofing is special in that it can be used to
   carry out other threat actions that cause other threat
   consequences. 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 a legitimate router.

o DoS attacks

   A. At the transport layer - This occurs when an attacker sends
       packets aimed at halting or preventing the underlying protocol
       over which the routing protocol runs. The attacker could use
       SPOOFING, FALSIFICATION, or INTERFERENCE (see below) to
       produce the DoS attack. For example, BGP running over
       Transport Layer Security (TLS) will still not solve the
       problem of an attacker being able to send a spoofed TCP FIN or
       TCP RST and causing the BGP session to go down. Since these
       attacks depend on spoofing, operators are encouraged to deploy
       proper authentication mechanisms to prevent them.
       Specification work should ensure that Routing Protocols can
       operate over transport subsystems in a fashion that is
       resilient to such DoS attacks.

   B. Using the authentication mechanism - This includes an attacker
       causing INTERFERENCE, which inhibits exchanges of legitimate
       routers. The attack is often perpetrated by sending packets
       that confuse or overwhelm a security mechanism itself. An
       example is initiating an overwhelming load of spoofed routing

protocol packets that contain a MAC (i.e., INSERTING
MESSAGES), so that the receiver spends substantial CPU
resources on the processing cycles to check the MAC, only to
discard the spoofed packet. Other types of INTERFERENCE
include REPLAYING OUT-DATED PACKETS, CORRUPTING MESSAGES, and
BREAKING SYNCHRONIZATION.

o FALSIFICATION - An action whereby an attacker sends false routing
   information. This document targets only FALSIFICATION from
   OUTSIDERS that may occur from tampering with packets in flight or
   sending entirely false messages. FALSIFICATION from BYZANTINES
   (see Section 3.3) are not addressed by the KARP effort.

o Brute-Force Attacks Against Password/Keys - This includes either
   online or offline attacks in which 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 it much harder for such
   attacks to succeed. For example, current guidance for the
   security strength of an algorithm with a particular key length
   should be deemed acceptable for a period of 10 years. (Section 10
   of [SP.800-131A] is one source for guidance.) 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.

3.3. Threat Actions Out of Scope

   BYZANTINE sources -- be they faulty, misconfigured, or subverted --
   are out of scope for this roadmap. KARP works to cryptographically
   ensure that received routing messages originated from authorized
   peers and that the message was not altered in transit. Formation of
   a bogus message by a valid and authorized peer falls outside the KARP
   scope. Any of the attacks described in Section 3.2 that may be
   levied by a BYZANTINE source are therefore also out of scope, e.g.
   FALSIFICATION from BYZANTINE sources or unauthorized message content
   by a legitimate authorized peer.

   In addition, these other attack actions are out of scope for this
   work:

   o SNIFFING (passive wiretapping) - Passive observation of route
      message contents in flight. Data confidentiality, as achieved by
      data encryption, is the common mechanism for preventing SNIFFING.
      While useful, especially to prevent the gathering of data needed
      to perform an off-path packet injection attack, data encryption is
      out of scope for KARP.

   o INTERFERENCE due to:

      A. NOT FORWARDING PACKETS - Cannot be prevented with
          cryptographic authentication. Note: If sequence numbers with
          sliding windows are used in the solution (as is done, for
          example, in Bidirectional Forwarding Detection (BFD)
          [RFC5880]), a receiver can at least detect the occurrence of
          this attack.

      B. DELAYING MESSAGES - Cannot be prevented with cryptographic
          authentication. Note: Timestamps can be used to detect
          delays.

      C. DENIAL OF RECEIPT (non-repudiation) - Cannot be prevented with
          cryptographic authentication.

      D. UNAUTHORIZED MESSAGE CONTENT - Covered by the work of the
          IETF's SIDR working group
          (http://www.ietf.org/html.charters/sidr-charter.html).

      E. DoS attacks not involving the routing protocol. 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 KARP will address. Many such
          examples could be contrived.

4. Requirements for KARP Work Phase 1: Update to a Routing Protocol's
    Existing Transport Security

   Section 4.1 of the KARP Design Guide [RFC6518] describes two distinct
   work phases for the KARP effort. This section addresses requirements
   for the first work phase only, Work Phase 1, the update to a routing
   protocol's existing transport security. Work Phase 2, the framework
   and usage of a KMP, will be addressed in a future document(s).

   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 [RFC6518]document). IT IS RECOMMENDED
   that any Work Phase 1 security update to a Routing Protocol contain a
   section of the specification document that describes how each of the
   following requirements are met. It is further RECOMMENDED that
   justification be presented for any requirements that are NOT
   addressed.

   1.   Clear definitions of which elements of the transmitted data
        (frame, packet, segment, etc.) are protected by an
        authentication/integrity mechanism.

2.   Strong cryptographic algorithms, as defined and accepted by the
     IETF security community, MUST be specified. The use of non-
     standard or unpublished algorithms MUST be avoided.

3.   Algorithm agility for the cryptographic algorithms used in the
     authentication MUST be specified, and protocol specifications
     MUST be clear regarding how new algorithms are specified and
     used within the protocol. This requirement exists because
     research identifying weaknesses in cryptographic algorithms can
     cause the security community to reduce confidence in some
     algorithms. Breaking a cipher isn't a matter of if, but when it
     will occur. Having the ability to specify alternate algorithms
     (algorithm agility) within the protocol specification to support
     such an event is essential. Additionally, more than one
     algorithm MUST be specified. Mandating support for two
     algorithms (i.e., one mandatory to implement algorithm and one
     or more backup algorithms to guide transition) provides both
     redundancy, and a mechanism for enacting that redundancy.

4.   Secure use of PSKs, offering both operational convenience and a
     baseline level of security, MUST be specified.

5.   Routing Protocols (or the transport or network mechanism
     protecting routing protocols) SHOULD be able to detect and
     reject replayed intra-session and inter-session messages.
     Packets captured from one session MUST NOT be able to be resent
     and accepted during a later session (i.e., inter-session
     replay). Additionally, replay mechanisms MUST work correctly
     even in the presence of routing protocol packet prioritization
     by the router.

     There is a specific case of replay attack combined with spoofing
     that must be addressed. Several routing protocols (e.g., OSPF
     [RFC2328], IS-IS [RFC1195], BFD [RFC5880], RIP [RFC2453], etc.),
     require all speakers to share the same authentication and
     message association key on a broadcast segment. It is important
     that an integrity check associated with a message fail if an
     attacker has replayed the message with a different origin.

6.   A change of security parameters MUST force a change of session
     traffic keys. The specific security parameters for the various
     routing protocols will differ and will be defined by each
     protocol design team. Some examples may include master key, key
     lifetime, and cryptographic algorithm. If one of these
     configured parameters changes, then a new session traffic key
     MUST immediately be established using the updated parameters.
     The routing protocol security mechanisms MUST support this
     behavior.

7. Security mechanisms MUST specify a means to affect intra-session
    rekeying without disrupting a routing session. This should be
    accomplished without data loss, if possible. Keys may need to
    be changed periodically based on policy or when an administrator
    who had access to the keys leaves an organization. A rekeying
    mechanism enables the operators to execute the change without
    productivity loss.

8. Rekeying SHOULD be supported in such a way that it can occur
    during a session without the peer needing to use multiple keys
    to validate a given packet. The rare exception will occur if a
    routing protocol's design team can find no other way to rekey
    and still adhere to the other requirements in this section. The
    specification SHOULD include a key identifier, which allows
    receivers to choose the correct key (or determine that they are
    not in possession of the correct key).

9. New mechanisms MUST resist DoS attacks described as in scope in
    Section 3.2. Routers protect the control plane by implementing
    mechanisms to reject completely or rate-limit traffic not
    required at the control-plane level (i.e., unwanted traffic).
    Typically, line-rate packet-filtering capabilities look at
    information in the IP and transport (TCP or UDP) headers, but do
    not include higher-layer information. Therefore, the new
    mechanisms should neither hide nor encrypt the information
    carried in the IP and transport layers in control-plane packets.

10. Mandatory cryptographic algorithms and mechanisms MUST be
    specified for each routing protocol security mechanism.
    Further, the protocol specification MUST define default security
    mechanism settings for all implementations to use when no
    explicit configuration is provided. To understand the need for
    this requirement, consider the case where a routing protocol
    mandates three different cryptographic algorithms for a MAC
    operation. If company A implements algorithm 1 as the default
    for this protocol, while company B implements algorithm 2 as the
    default, then two operators who enable the security mechanism
    with no explicit configuration other than a PSK will experience
    a connection failure. It is not enough that each implementation
    implement the three mandatory algorithms; one default must
    further be specified in order to gain maximum out-of-the-box
    interoperability.

11. For backward-compatibility reasons, manual keying MUST be
    supported.

12. The specification MUST consider and allow for future use of a
    KMP.

13. The authentication mechanism in a Routing Protocol MUST be
    decoupled from the key management system used. The
    authentication protocol MUST include a specification for
    agreeing on keying material. This will accommodate both manual
    keying and the use of KMPs.

14. Convergence times of the Routing Protocols SHOULD NOT be
    materially affected. Changes in the convergence time will be
    immediately and independently verifiable by convergence
    performance test beds already in use (e.g. those maintained by
    router vendors, service providers, and researchers). An
    increase in convergence time in excess of 5% is likely to be
    considered to have materially affected convergence by network
    operators. A number of other factors can also change
    convergence over time (e.g., speed of processors used on
    individual routing peers, processing power increases due to
    Moore's law, and implementation specifics), and implementors
    will need to take into account the effect of an authentication
    mechanism on Routing Protocols. Protocol designers should
    consider the impact on convergence times as a function of both
    the total number of protocol packets that must be exchanged and
    the required computational processing of individual messages in
    the specification, understanding that the operator community's
    threshold for an increase in convergence times is very low, as
    stated above.

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

16. Router implementations provide prioritized treatment for certain
    protocol packets. For example, OSPF Hello and Acknowledgement
    packets are prioritized for processing above other OSPF packets.
    The security 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 protection mechanisms provided by the routing protocols
    MUST work even if certain protocol packets are offered
    prioritized treatment.

17. The Routing Protocol MUST send minimal information regarding the
    authentication mechanisms and associated parameters in its
    protocol packets. This keeps the Routing Protocols as clean and
    focused as possible, and loads security negotiations into the
    KMP as much as possible. This also avoids exposing any security
    negotiation information unnecessarily to possible attackers on
    the path.

18. Routing Protocols that rely on the IP header (or information
    separate from routing protocol payload) to identify the neighbor
    that originated the packet MUST either protect the IP header or
    provide some other means to authenticate the neighbor.
    [RFC6039] describes some attacks that motivate this requirement.

19. Every new KARP-developed security mechanisms MUST support
    incremental deployment. It will not be feasible to deploy a new
    Routing Protocol authentication mechanism throughout a network
    instantaneously. Indeed, it may not actually be feasible to
    deploy such a mechanism to all routers in a large autonomous
    system (AS) in a bounded timeframe. Proposed solutions MUST
    support an incremental deployment method that benefits 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 peer to peer
        (unicast).

    B. Every new KARP-developed security mechanism MUST provide
        backward compatibility with respect to message formatting,
        transmission, and processing of routing information carried
        through secure and non-secure security environments.
        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 that don't support the new
        format.

    C. In an environment where both secured and non-secured routers
        are interoperating, a mechanism MUST exist for secured
        systems to identify whether a peer intended the messages 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).

20. The introduction of mechanisms to improve routing 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 that either incurs
substantial capital expense or threatens to degrade router
performance.

21. New authentication and security mechanisms should not rely on
systems external to the routing system (the equipment that is
performing forwarding) in order for the routing system to be
secure. 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. 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 security associations.

If authentication and security mechanisms rely on systems
external to the routing system, then there MUST be one or more
options available to avoid circular dependencies. It is not
acceptable to have a routing protocol (e.g., unicast routing)
depend upon correct operation of a security protocol that, in
turn, depends upon correct operation of the same instance of
that routing protocol (i.e., the unicast routing). However, it
is acceptable to have operation of a routing protocol (e.g.,
multicast routing) depend upon operation of a security protocol,
which depends upon an independent routing protocol (e.g.,
unicast routing). Similarly, it would be okay to have the
operation of a routing protocol depend upon a security protocol,
which in turn uses an out-of-band network to exchange
information with remote systems.

5. Security Considerations

This document is mostly about security considerations for the KARP
efforts, both threats and the requirements for addressing those
threats. More detailed security considerations are provided in the
Security Considerations section of the KARP Design Guide
[RFC6518]document.

The use of a group key between a set of Routing Protocol peers has
special security considerations. Possession of the group key itself
is used for identity validation; no other identity check is used.
Under these conditions, an attack exists when one peer masquerades as
a neighbor by using the neighbor's source IP address. This type of
attack has been well documented in the group-keying problem space,
and it is non-trivial to solve. Solutions exist within the group-

keying realm, but they come with significant increases in complexity
and computational intensity.

6. Acknowledgements

The majority of the text for initial draft of this document was taken
from "Roadmap for Cryptographic Authentication of Routing Protocol
Packets on the Wire", authored by Gregory M. Lebovitz.

Brian Weis provided significant assistance in handling the many
comments that came back during IESG review, including making textual
edits directly to the XML. For his extensive efforts he was added as
an author.

We would like to thank the following people for their thorough
reviews and comments: Brian Weis, Yoshifumi Nishida, Stephen Kent,
Vishwas Manral, Barry Leiba, Sean Turner, and Uma Chunduri.

Author Gregory M. Lebovitz was employed at Juniper Networks, Inc. for
much of the time he worked on this document, though not at the time
of its publishing. Thus, Juniper sponsored much of this effort.

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

[ISR2008]   McPherson, D. and C. Labovitz, "Worldwide
               Infrastructure Security Report", October 2008,
               <http://pages.arbornetworks.com/rs/arbor/images/
               ISR2008_EN.pdf>.

[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., "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., Ed., Li, T., Ed., and S. Hares, Ed., "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.

   [RFC4822]   Atkinson, R. and M. Fanto, "RIPv2 Cryptographic
                      Authentication", RFC 4822, February 2007.

   [RFC4949]   Shirey, R., "Internet Security Glossary, Version 2",
                      FYI 36, RFC 4949, August 2007.

   [RFC5036]   Andersson, L., Ed., Minei, I., Ed., and B. Thomas,
                      Ed., "LDP Specification", RFC 5036, October 2007.

   [RFC5310]   Bhatia, M., Manral, V., Li, T., Atkinson, R., White,
                      R., and M. Fanto, "IS-IS Generic Cryptographic
                      Authentication", RFC 5310, February 2009.

   [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.

   [RFC5880]   Katz, D. and D. Ward, "Bidirectional Forwarding
                      Detection (BFD)", RFC 5880, June 2010.

   [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.

   [RFC6518]   Lebovitz, G. and M. Bhatia, "Keying and Authentication
                      for Routing Protocols (KARP) Design Guidelines",
                      RFC 6518, February 2012.

   [SP.800-131A] Barker, E. and A. Roginsky, "Transitions:
                  Recommendation for Transitioning the Use of
                  Cryptographic Algorithms and Key Lengths", United
                  States of America, National Institute of Science and
                  Technology, NIST Special Publication 800-131A,
                  January 2011.

Authors' Addresses

   Gregory Lebovitz
   Aptos, California 95003
   United States

   EMail: gregory.ietf@gmail.com

   Manav Bhatia
   Alcatel-Lucent
   Bangalore,
   India

   EMail: manav.bhatia@alcatel-lucent.com

   Brian Weis
   Cisco Systems
   170 W. Tasman Drive
   San Jose, California 95134-1706
   United States

   EMail: bew@cisco.com
   URI: http://www.cisco.com