Charter Discussion

Charter Discussion
Description of WG (1)

The KARP working group is tasked to work with the routing protocol working groups in order to improve the communication security of the packets on the wire used by the routing protocols. Of the five basic goals that may sought relative to securing any piece of data as it is transmitted over the wire: privacy (or encryption), message authentication, message integrity, non-repudiation, and denial of service protection, three are considered relevant for this working group. This working group is concerned with message authentication, packet integrity, and denial of service (DoS) protection. At present, this charter explicitly excludes privacy and non-repudiation concerns.

Authenticating the routing peer sending a message, and message integrity protection will be provided through the use of per-packet cryptographic message authentication. Peer authentication will protect against unrecognized peers, imposter peers, and some DoS attacks aimed at routers. Protecting against misbehavior of an otherwise allowed peer router is outside the scope of this working group.

Charter Discussion
Description of WG (2)

Many routing protocols (or groups of protocols) already have some method for accomplishing cryptographic message authentication. In most cases the existing methods are vulnerable to known attack, and/or employ cryptographic algorithms that have been deprecated. Internet security practices have progressed in the last 10 years when many of the first generation routing authentication mechanisms were created. It is time to review and update those mechanisms to use modern security practices. Ensuring algorithm agility within routing protocols is of particular importance. A goal of the working group is to add incremental security to existing mechanisms rather than replacing them. Better deployable solutions that vendors and operators can migrate to is more important than getting a perfect security solution.

The working group will coordinate very closely with the protocol development working groups for any routing protocol being evaluated. This coordination will include cooperatively determining the current or already planned state of the security work in the protocol. It will also include ensuring that any proposed mechanisms are consistent with with architecture and use of the protocol. And any specific proposal will be developed in cooperation with the concerned protocol working group.

Charter Discussion
Description of WG (3)

Many different routing protocols exist. These protocols use a range of transport mechanisms and communication relationships. There are also differences in details among the various protocols. Clearly, no one solution will work for all protocols, and even general solutions that are applicable across protocols will need tailoring for each case. The working group will attempt to describe the security relevant characteristics of routings protocols, such as the use or non-use of TCP, or the frequent use of group communication versus purely pairwise communication. Using these characteristics, the working group will then provide suitable common frameworks that can be applied, and tailored, to improve the communication security of the routing protocols. In later phases, it is expected that the working group will investigate the suitably of defining conceptual structures and APIs, so as to enable further work to be more effective.

Charter Discussion
Description of WG (4)

One area for study is the applicability of automated key management to these environments. It is anticipated that at least the techniques for separating session keys from key established keys will be applicable. This charter provides for preliminary work in this space, although it is expected that detailed work items will be added to the charter when the problem has been better analyzed.

Routing protocols in scope include BGP, OSPF, OSPFv3, ISIS, RIPv2, RIPng, MSDP, PCE, PIM (SM and DM), LDP, RSVP-TE, and BFD. The working group will not be working on emerging routing protocols such as ROLL or MANET. The WG will not work on control protocol such as GSMP or ForCES, nor on Network Management protocols such as SNMP or NETCONF.

Charter Discussion
WG Work Items

- Determine current threats to the routing protocol operation, and define general requirements for cryptographic authentication of routing protocols
- Identify deficiencies of each routing protocol in scope, and specify mechanisms that bring them in line with the general requirements
- Define one or more frameworks describing the common elements for modern authentication in routing protocols
- Specify automated key management needs for routing protocols

Charter Discussion

Goals and Milestones

- TBD - Separate current roadmap document (a place holder document) into General Framework, General Requirements, Priorities/Work-Plan documents
- TBD - Specification document for each protocol
- TBD - Framework document on protocol groups and the common techniques and interfaces that apply to them.