

Advertising Link and Node Security Properties in OSPF/IS-IS

<https://datatracker.ietf.org/doc/html/draft-przygienda-lsr-ospf-security-states-00>

Tony P, Juniper

Problem Statement & Chosen Solution Space

- Routers are Being Attacked in More and More Sophisticated Ways, Also in Physical Locations
 - Crucial to Detect and Decommission AFAP
- Demand for Paths that Satisfy Security Concerns is Raising
- Security Monitoring Infrastructure Offers Many Attack Vectors
 - Transport
 - Loss of Monitoring Connection Semantics Unclear
- IGP Database is the Fastest, Safest Place to Advertise Security Properties Applied
 - No Additional Monitoring Infra Needed
 - Once IGP Database is Hacked then “Nothing Else Matters”

Short Introduction to *CIA*

- Simple Security Model Used More Often Than Not
 - Confidentiality
 - Prevents Snooping
 - Integrity
 - Prevents Changes in the Middle and Replays
 - Availability
 - Is the Service/Information Disponible When Expected/Needed
- Let's Call Those Things *sec-characteristics*
- They are Not Comparable
- Some Technologies Offer a Mix
- Technologies Used Differ in *strength*

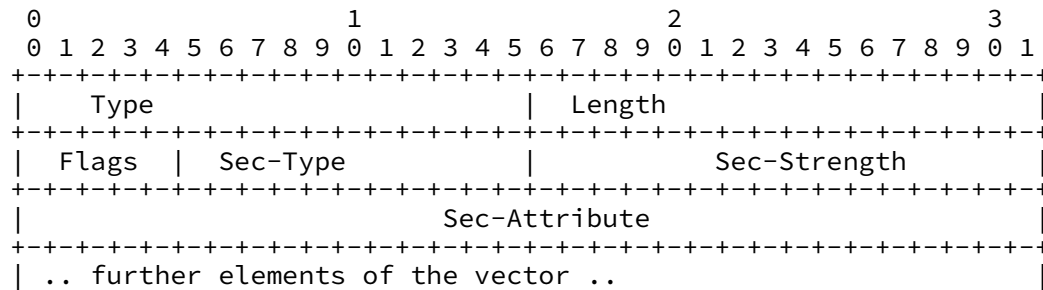
Security Property

- A **security property** is an instance of a security characteristic, e.g. Checksum is instance of Integrity (very weak one)
 - We add previously mentioned **strength** to each property
- Security properties are Comparable to Each Other by Their Strength so a Vector can be ordered so e.g. for a link
 - Integrity: [50-ipsec, 10-sha-2, 5-csum]
 - Confidentiality [50-ipsec]
- We add implied **null** to make different vectors easily comparable
 - [50-X, 30-Y, null] is comparable to [null, 30-Y, 10-Z] as [50-X] vs. [null]
- A security property has also a **security property attribute** (think key length for encryption)

Why the fuzz? Because This Allows to Compare Opaque Stuff, i.e. Deploy New Stuff

- Last Missing Piece are some *security property flags*
 - Is higher attribute better or worse or don't compare
 - Is default attribute value 0 or MAX if property is missing
- This Magically Allows to Flood a New
 - [strength, <whatever name>, attribute value, flags]
- And make it part of the solution without software updates

The Inevitable Encoding, Example OSPF



- Usual Opaque
- Type indicates *Characteristics*
- Both for Node and Link

Use Cases

- Obviously Computation, Distributed or Centralized
- Discovery of Compromised Routers By Changes in Security Properties
 - E.g. Availability Advertising Number 3-way Interfaces
- Discovery or Degradation of Routers (yes)
 - #flaps per Time Can Be Used as “Availability” and “Better” Routers Chosen

Where are the Attributes?

- None in Draft Now
- Framework for Clear Definition What to Include Initially and Discussion
- Arbitrarily Extensible Later