LABELED IPSEC
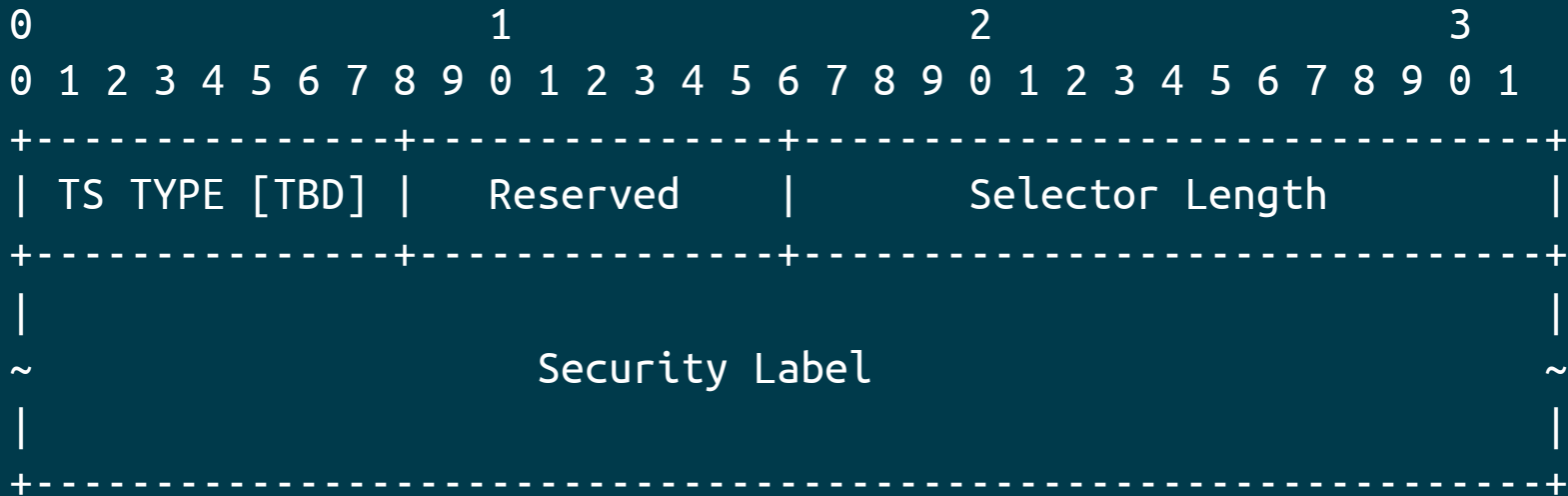
IPsec, IETF 105
July, 2019

Sahana Prasad, Technical University of Munich
Paul Wouters, RHEL Security

redhat. | libreswan

draft-ietf-ipsecme-labeled-ipsec-01

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+-------------------------------+
| TS TYPE [TBD] |   Reserved    |       Selector Length         |
+---------------+---------------+-------------------------------+
|                                                               |
~                       Security Label                          ~
|                                                               |
+---------------------------------------------------------------+
```

o TS TYPE (one octet) - Specifies the type of Traffic Selector.
o Selector Length (2 octets, network byte order) - Specifies the
   length of Security Label including the header.
o Security Label - This field contains the opaque payload.

Changes in -01 revision

- Remove "documentation" of how Traffic Selectors work (read RFC 7296)
- Clearly split "security label" part from "updates to processing TS" part
- Allow multiple seclabels, just in case a non-MLS based system could use.
- Be explicit about not allowing zero length seclabels.
- Clarify handling of multiple of one TS_TYPE and combinations.
- Clarify all TSi/TSr MUST include at least one TS_IPV4_ADDR_RANGE or TS_IPV6_ADDR_RANGE.

- Inserted nonsense into the document shortly before the deadline, so my co-author couldn't correct me in time