

Update on draft-ietf-opsec-v6-13

Kiran Kumar Chittimaneni
Merike Kaeo
Enno Rey
Eric Vyncke

IETF-101, London, March 2018

The Fourth Musketeers



Enno Rey

@Enno_insinuator

Security practitioner (esp IPv6)

Founder of ERNW.de and

of the conference Troopers.de



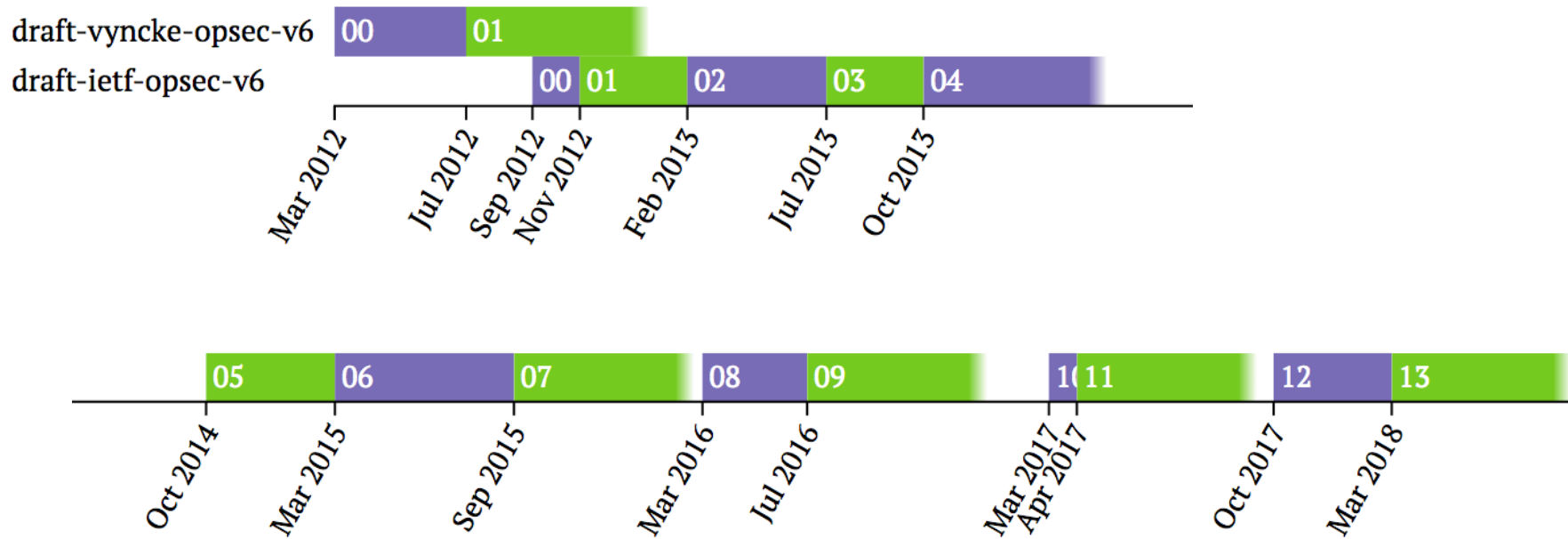
Source: <https://insinuator.net>

And Many Many Expertise

7. Acknowledgements

The authors would like to thank the following people for their useful comments: Mikael Abrahamsson, Fred Baker, Brian Carpenter, Tim Chown, Markus deBruen, Tobias Fiebig, Fernando Gont, Jeffry Handal, Panos Kampanakis, Erik Kline, Jouni Korhonen, Mark Lentczner, Bob Sleigh, Tarko Tikan, Ole Troan, Bernie Volz (by alphabetical order).

(Pre)-History



Changes Since -12

- About 100 changes (thank you to Enno, Ron Bonica, Bernie Voltz, Ole Troan)
- There remain 2 open issues (see later)

Structure of the Document /1

- Generic Security Considerations
 - Many subsections... See later
- Enterprises Specific Security Considerations
 - External security
 - Internal security
- Service Providers Security Considerations
 - BGP
 - Transition mechanism
 - Lawful Intercept
- Residential Users Security Considerations

Structure of the Document /2

- Generic Security Considerations
 - Addressing Architecture
 - Extension Headers
 - Link-Layer Security
 - Control-Plane Security
 - Routing Security
 - Logging/Monitoring
 - Transition/Coexistence Technologies
 - General Device Hardening

Structure of the Document /2

- Generic Security Considerations
 - Addressing Architecture
 - Extension Headers
 - Link-Layer Security
 - Control-Plane Security
 - Routing Security
 - Logging/Monitoring
 - Transition/Coexistence Technologies
 - General Device Hardening



ULA



Tunnels

Text on ULA (Section 2.1.2 page 5)

Unique Local Addresses (ULAs) [RFC4193](#) are intended for scenarios where IP addresses are not globally reachable, despite formally having global scope. They must not appear in the routing system outside the administrative domain where they are considered valid. **Therefore, packets with ULA source and/or destination addresses MUST be filtered at the domain boundary.**

ULAs are assigned within pseudo-random /48 prefixes created as specified in [RFC4193](#). **They could be useful for infrastructure hiding as described in [RFC4864](#).**

ULAs may be used for internal communication, in conjunction with globally reachable unicast addresses (GUAs) for hosts that also require external connectivity through a firewall. For this reason, **no form of address translation is required in conjunction with ULAs.**

Using ULAs as described here might simplify the filtering rules needed at the domain boundary, by allowing a regime in which only hosts that require external connectivity possess a globally reachable address. **However, this does not remove the need for careful design of the filtering rules. Routers with ULA on their interfaces may also leak their address to the Internet when generating ICMP messages or ICMP error messages can also include ULA address as they contain a copy of the offending packet.**

Text on Tunnels

- All tunnels are analyzed from a security angle
- Even nearly obsolete tunnels such as 6to4 and Teredo
- Authors believe that being exhaustive is important and would like to keep text on 6to4 and Teredo

Next Steps

- We feel ready to push our baby into WGLC