IPsec workshop 2022
November 3th – 4th

Report

Steffen Klassert

Some background about the event

- Funded by IPsec and Network Security Association
- Yearly event
- Held first time in 2018
- Semi public (< 20 attendees)
- Topics: IPsec Implementation + Protocol

FIPS requirements for AES-GCM
(Paul Wouters)

- Question: Can we use the same key for more than 2^32 packets?
- Yes: Can use 2^64 packets even in FIPS mode
- Limitation: 8 octets ICV is limited to 2^32 packets in FIPS mode

Decorrelated policies – avoid overlapping policies
(Tero Kivinen)

- Overview of decorrelated policies with examples
- Gives a flat SPD structure without priorities
- Makes lookups more efficient

Full IPsec datapath HW offload
(Leon Romanovsky)

- Offload lookups, encapsulation and crypto operations to HW
- Offloading API for Linux exists
- Nvidia/Mellanox CX-7 supports this offload type
- Linux + CX-7 can run the full datapath offload

Linux forwarding fastpath with packet bulking
(Pablo Neira Ayuso / Steffen Klassert)

- Use Netfilter flowtable
- Skip full L3 datapath

- Create packet bulks (packets matching same SA processed together)
- Run on small code loops (cache frindly)

- Gives good performance results (factor 5)

ANIMA and use of IPsec
(Michael Richardson)

- Introduction to ANIMA
- IPsec usage in ANIMA

- Problem: Cross network namespaces with VTI interfaces

- Proposed solution: Use xfrm interfaces
- xfrm interfaces were created to replace VTI

IPTFS
(Christian Hopps)

- Introduction to IPTFS
- Presentation/Discussion about state of Linux implemention:
    - Aggregation / Fragmentation supported
    - Constant rate sending not yet supported

Draft-pwouters-ipsecme-multi-sa-performance (Steffen Klassert)

- Crtitsm on ML: Fallback SA is treated special
- Proposed solution: Remove fallback SA from the darft
- No architectural changes
    - ‚Low hanging fruit’
    - Can continue without charter changes

Re-designing ESP
(Steffen Klassert)

- Lot of proposals around to support multi cpu case, QoS classes, HW offloads
- Need separate anti-replay windows
- Proposed solutions:
  - Use some bits from SPI
  - Use some bits of anti-replay window
  - Add new field to ESP
- Google publishsed PSP for HW offload

» **Time to rethink ESP, maybe create ESP-v4**

Standardizing BEET mode
(Steffen Klassert / Antony Antony)

- Draft-nikander-esp-beetmode-09 (from 2008) unfinished
- BEET mode is implemented im Linux
- People use it!

» **Continue the work on BEET mode**