Security for Service Function Chaining

IETF-96 Berlin
SFC WG
Martin Stiemerling (mls.ietf@gmail.com)
History

• IESG review raised security issues
  – RFC 7498 Problem Statement for Service Function Chaining
  – RFC 7665 Service Function Chaining (SFC) Architecture

• Formation of security design team „SFC Security Analysis“ at IETF-93
  – draft-mglt-sfc-security-environment-req-01
  – draft-reddy-sfc-nsh-security-req-00.txt

• Plus: Authenticated and encrypted NSH service chains
  – draft-reddy-sfc-nsh-encrypt-00
  – (expired draft)
Today

- Discussion of SFC Security did not really progress
  - No real discussion in the WG
    - Neither on list nor at the meetings
    - A bit of discussion at IETF-94
  - Drafts did not progress as result
- Security topic not progressing
- Security is
  - not only required by IETF process
  - But is much more demanded by the market
- And my guess is: see next slide ;-)}
Five Stages of Grief
(Kübler-Ross model)

- Denial
- Anger
- Bargaining
- Depression
- Acceptance

We are here!
How to fix this and move to acceptance?
What do we have?

• Very high-level security considerations in RFC 7665
  – And even more high-level in RFC 7498
  – Service Overlay
  – Boundaries
  – Classification
  – SFC Encapsulation

• draft-mglt-sfc-security-environment-req
  – First thread analysis
  – First set of requirements

• draft-reddy-sfc-nsh-security-req
  – Discusses NSH related security requirements
However...

- SFC RFCs give only extremely high level ideas
- SFC security drafts jump to conclusions too early
- Missing: sober technical analysis of
  - SFC architecture
  - and components
- The fundamental question:
  What will SFC will screw up?
One Example: PII

• PII: Personally identifiable information
  – Anything which be used to identify a person
  – Important to protect user information!

• Analysis
  – But where do we have PII in SFC?
    • Find and document it.
  – Do we need to have PII in all these elements or stages?
    • Reason about it and document it.

– Provide guidance
  • On protocol design
  • On operational usage
  • On protecting PII (or what needs protection)
Leaking PII

- PII in SFC can leak to other unauthorized parties
- E.g. forwarding of tagged user traffic to different data center
  - Tagged data:
    - control plane carrying PII
    - SFC data plane carrying PII
- Issue: Data will run across public inter-data center links
  - Virtually everybody can read information
  - PII nightmare!
- Mitigation: Provide at least confidentiality
  - Control plane
  - Data plane
Summary – NO Conclusion

• Need to get security in SFC started
  – Not scoped to just one document
  – But take whole SFC „world“ into account
• Need proper and sober analysis
  – Take architecture and protocols
  – Think about real threats to all of them
  – Document threats in detail
    • Not just on a high-level
  – Can we mitigate the threats?
  – How can we mitigate the threats?
    • This will have to say what is Mandatory to Implement (MIT)
  – And what cannot be mitigated..