Securing Future Internet Protocol Evolution

Universal Security in all protocol layers
July 27, 2021
Side Meeting
Robert Moskowitz

Where best to secure Communications

- The Link Layer addresses the Risks and Liabilities of the Network owner
- The Networking Layer addresses the Risks and Liabilities of the System owner
- The Transport/Session Layer(s) addresses the Risks and Liabilities of the Application Owner
- The Data Layer addresses the Risks and Liabilities of the Data Owner

Where then to Secure?

- We need to do them ALL
- Transport and Session security are NOT interchangeable. Each has its place
  - Though either protects the application
    - In different ways

Pieces of the Puzzle

- Key Management is crucial and HARD!
  - Like REALLY HARD
- Secure data framing is well understood
  - But could use commonality over layers
- Integrating the two is good tactically and bad strategically
  - When all you have is a hammer, the world is all nails

Secure Key Management as a Service

- The basics for this exist in both IKE and HIP
- APIs needed
  - IETF does not do APIs…
- Architecture of what a KMP as a Service, available to all processes at all levels needed
  - Lots to manage here

Some Goals are

- Make network attacks uninteresting in that they do not disturb the security state
- Allow for very conservative message overhead while accommodating high performance networks
- Put the intelligence in the (independent) KMP, not the secure messaging format(s)
- Provide for security state survivablity and longevity
- Support mutli-flow, mulitcast, multipath, non-TCP/IP, and just about any other network design

The secure data wrapper

- ESP is a good starting point
- How to minimize the design and choices and meet all needs
- New lightweight Crypto for small devices
  - https://csrc.nist.gov/Projects/lightweight-cryptography
  - I have worked with Xoodyak
    - draft-moskowitz-hip-new-crypto
    - Implementation available in OpenHIP

My past work

- SSE – Secure Session Envelope
- SSLS – Secure Session Layer Services
  - Joint effort with Sue Hares, Igor Faynberg, Liang Xia, Pierpapolo Giacomin
  - See https://datatracker.ietf.org/meeting/88/materials/slides-88-saag-5

Questions?