

Asymmetric Manifest-Based Integrity (AMBI)

Jake Holland <jholland@akamai.com>

Kyle Rose <krose@krose.org>

Akamai Technologies, Inc.

Problem statement

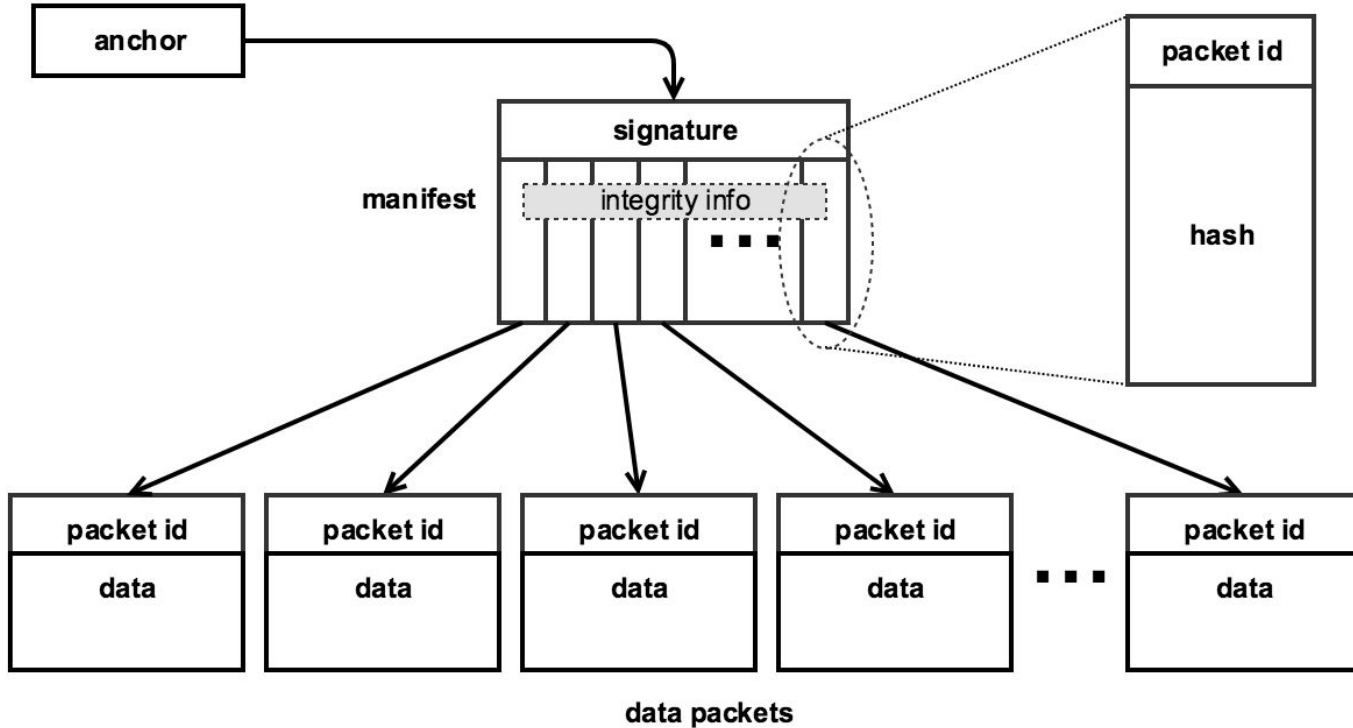
Inter-domain multicast has security issues

- Why multicast?
 - Same data to many clients
 - Loss is okay
 - Data with a deadline

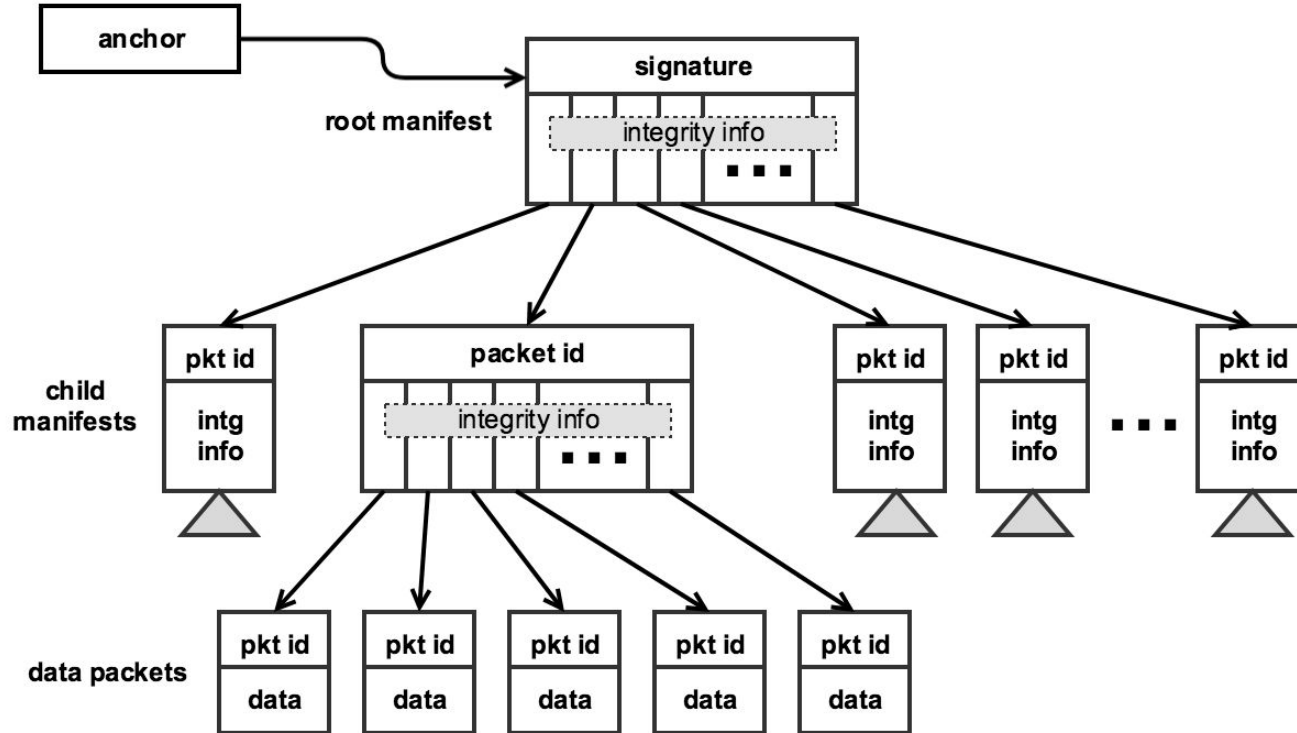
Integrity scheme requirements

- Line-rate verification
- Asymmetric crypto
- Efficient (power, CPU time)
- Loss-tolerant

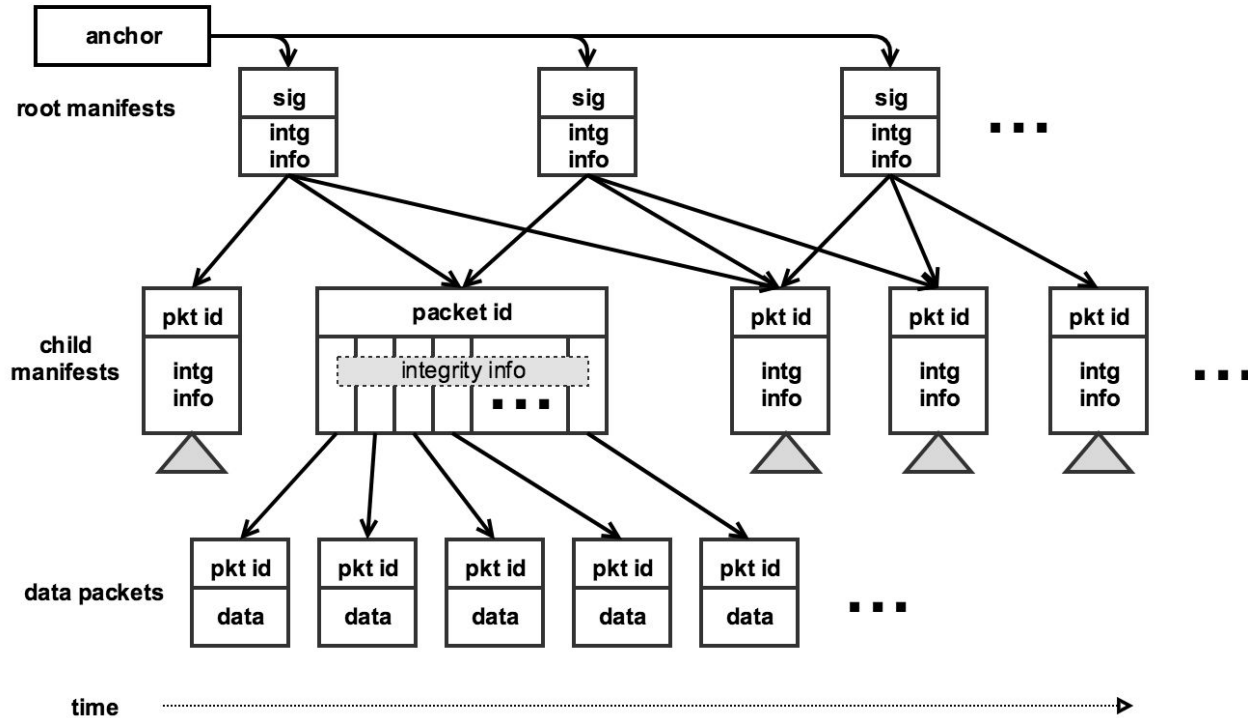
Single manifest



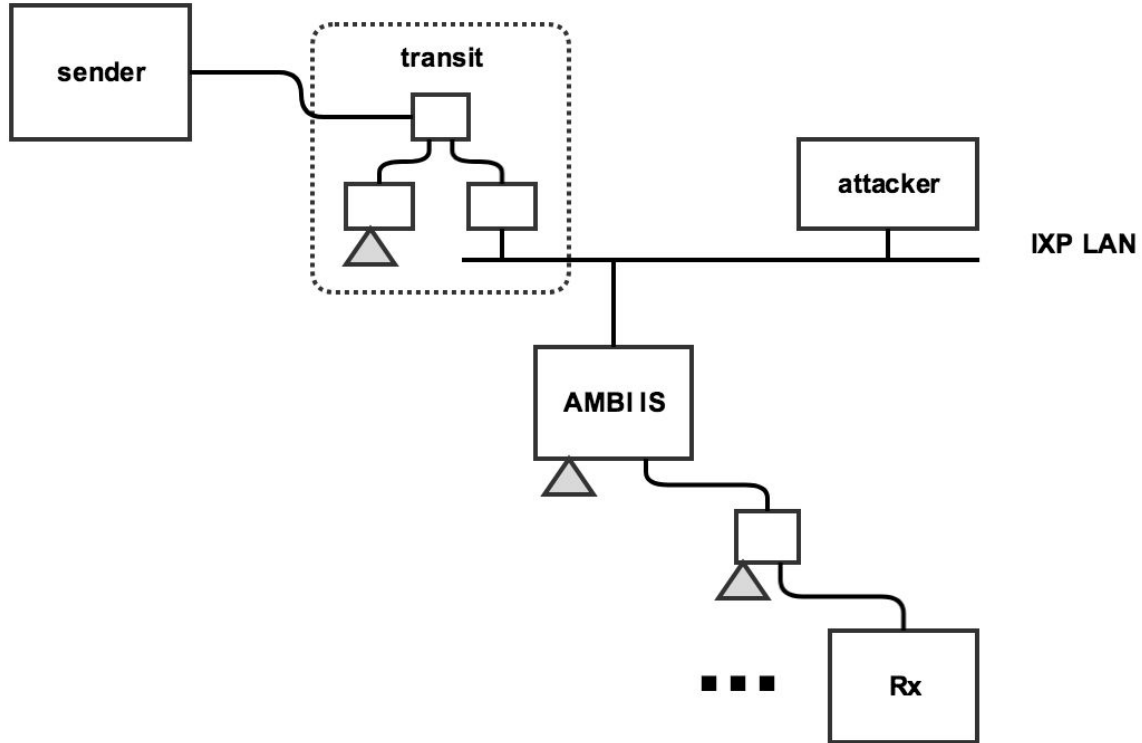
Manifest tree



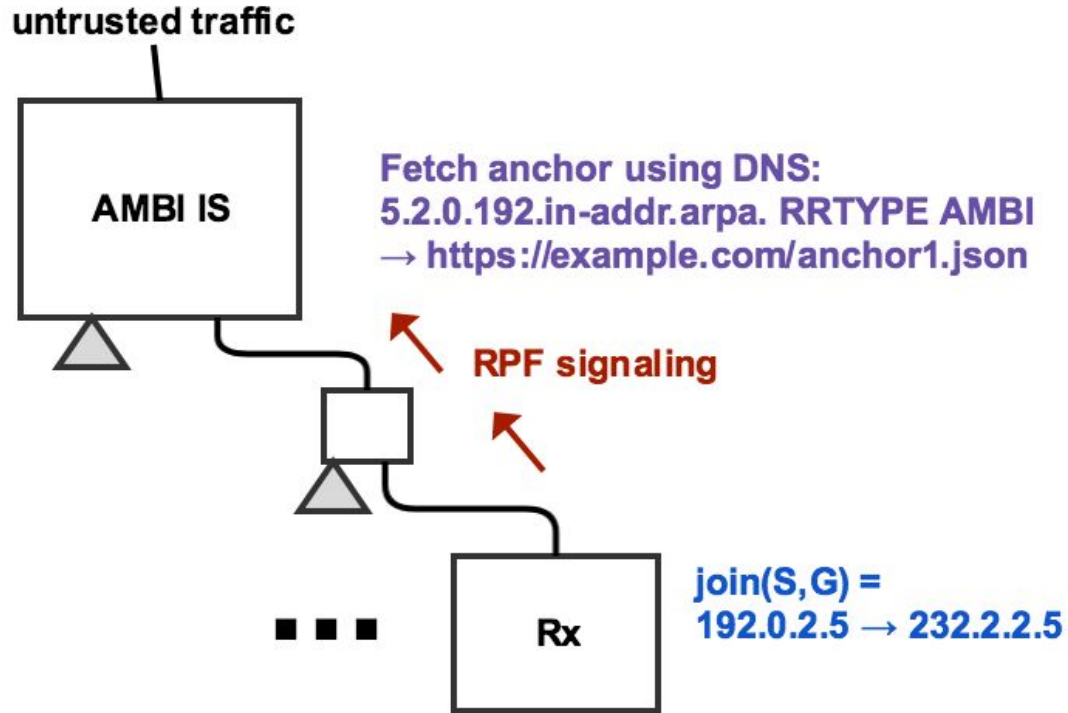
Rolling root manifest



Example threat model



Anchor discovery



Next steps?

- Analyze loss resiliency and determine optimal overlap/redundancy
- Use a Merkle tree-like structure to combine data and authentication in the same packet?

Reopen msec?

Looking for feedback

- Improvements to protocol
- Improvements to data model for anchor message
- Feedback on the DNS thing