

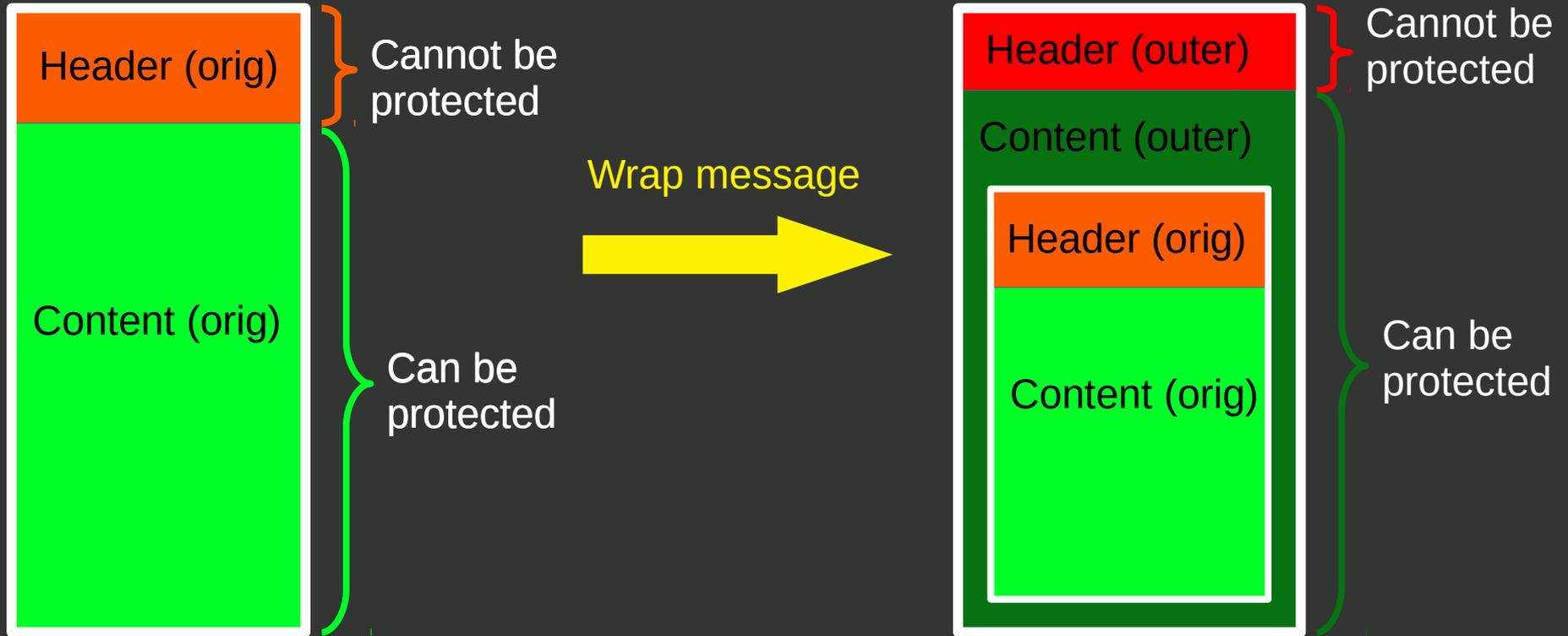
Header Protection (HP) Use Cases / Requirements

LAMPS @ IETF-105, Tue July 23, 2019

draft-ietf-lamps-header-protection-requirements-00

Bernie Hoeneisen / Alexey Melnikov

HP in S/MIME since version 3.1



draft-ietf-lamps-header-protection-requirements-00

- Merger of
 - draft-luck-pep-header-protection-02 (use cases & requirements)
 - draft-melnikov-lamps-header-protection-00
- Content
 - **Use Cases**
 - **Interaction cases**
 - **Protection Levels**
 - **Requirements**
 - Additional considerations (informational only)
 - Possible Solutions
 - Sending Side
 - Receiving Side

Goal

- Which protection levels are in scope
- Which requirements are we going to address in LAMPs
 - Completeness
 - Adjustments (as needed)

Protection Levels

- Which protection level use cases are in scope?
 - a) signature and encryption
 - b) signature only
 - c) encryption only
 - Yet unclear whether this is relevant or whether it can be treated the same as a)
 - LAMPS-Discussion @IETF-104 indicated that this is probably not relevant in practice, but needs to be documented

General Requirements (High Level)

- G1: Format (MIME structure, Content Type, etc.)
- G2: Easily implementable
- G3: Only one format for all protection levels
- G4: Mitigation of MITM (incl. downgrade) attacks

Requirements Sender (High Level)

- GS1: Which Header Fields (HF) to protect [signature case]
- GS2: Which HF to send in clear [encryption case]
- GS3: Which HF to not to send in clear (Data Minimization) [encryption case]
- GS4: Which HF to not to include to any HP part (e.g. Bcc)

Requirements Receiver (High Level)

- GR1: Conflicting information between protected and unprotected HF?
What to present to the user?
- GR2: Detection of MITM (incl. downgrade) attacks

Requirements Backward Compatibility

General:

- B1: Distinguish between forwarded and wrapped messages

Sender:

- BS1: Indicate full HP support
- BS2: Define how full HP support of the receiver can be detected or guessed.
- BS3: Ensure Subject HF can be displayed to users of HP unaware clients

Receiver:

- BR1: Detection for support of new HP

Next steps

- Confirm on Mailing list, what is in scope:
 - Protection levels
 - Requirements
- Reach out to implementers of clients and libraries to gain feedback
- Update requirements I-D
- Once confirmed, start new I-D on solutions

Questions / Discussion