Header Protection (HP) Use Cases / Requirements

LAMPS @ IETF-104, Tue Mar 26, 2019

draft-luck-pep-header-protection-01

Bernie Hoeneisen

p≡p

Privacy by Default.

draft-luck-pep-header-protection-01

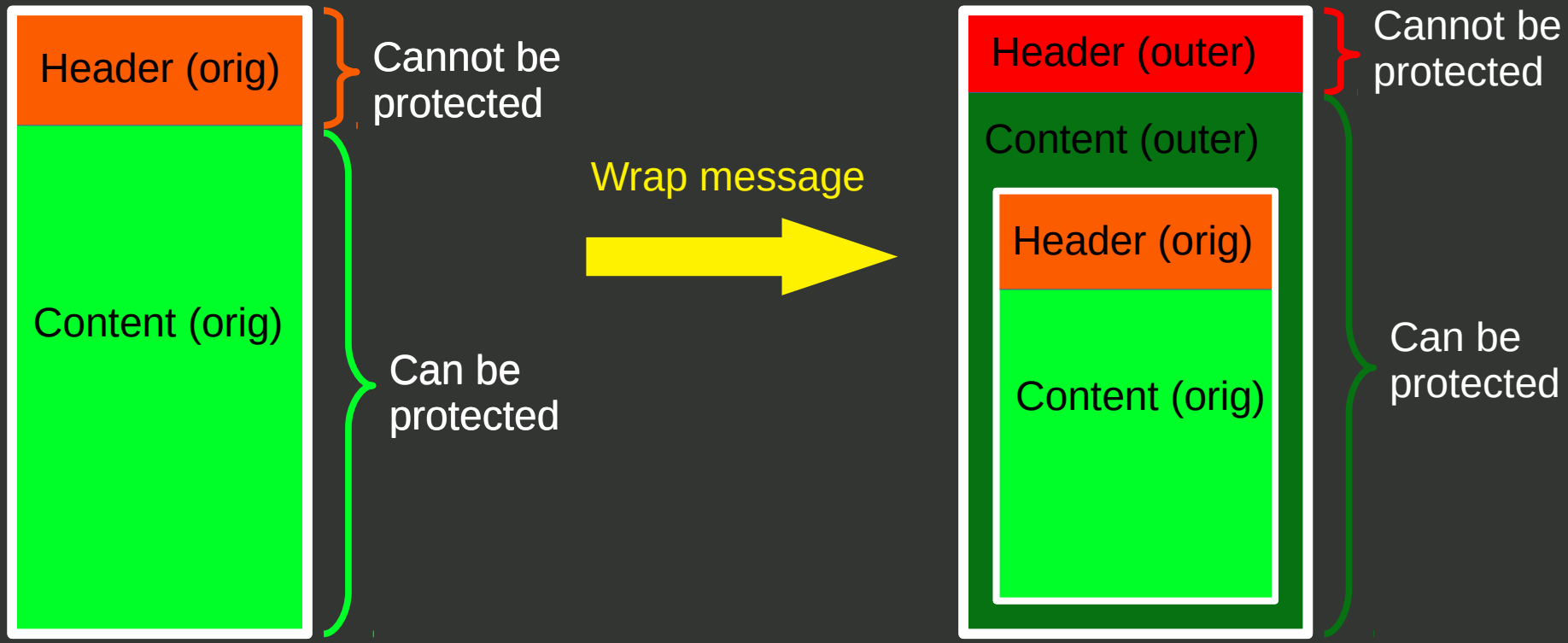
- Generic Use Cases for Header Protection (HP)
- Requirements
  - First draft as basis for discussion
- pEp implementation experience and description of HP
  - Progressive Header Disclosure (pEp message format version 2)
  - Not covered in these slides

Background

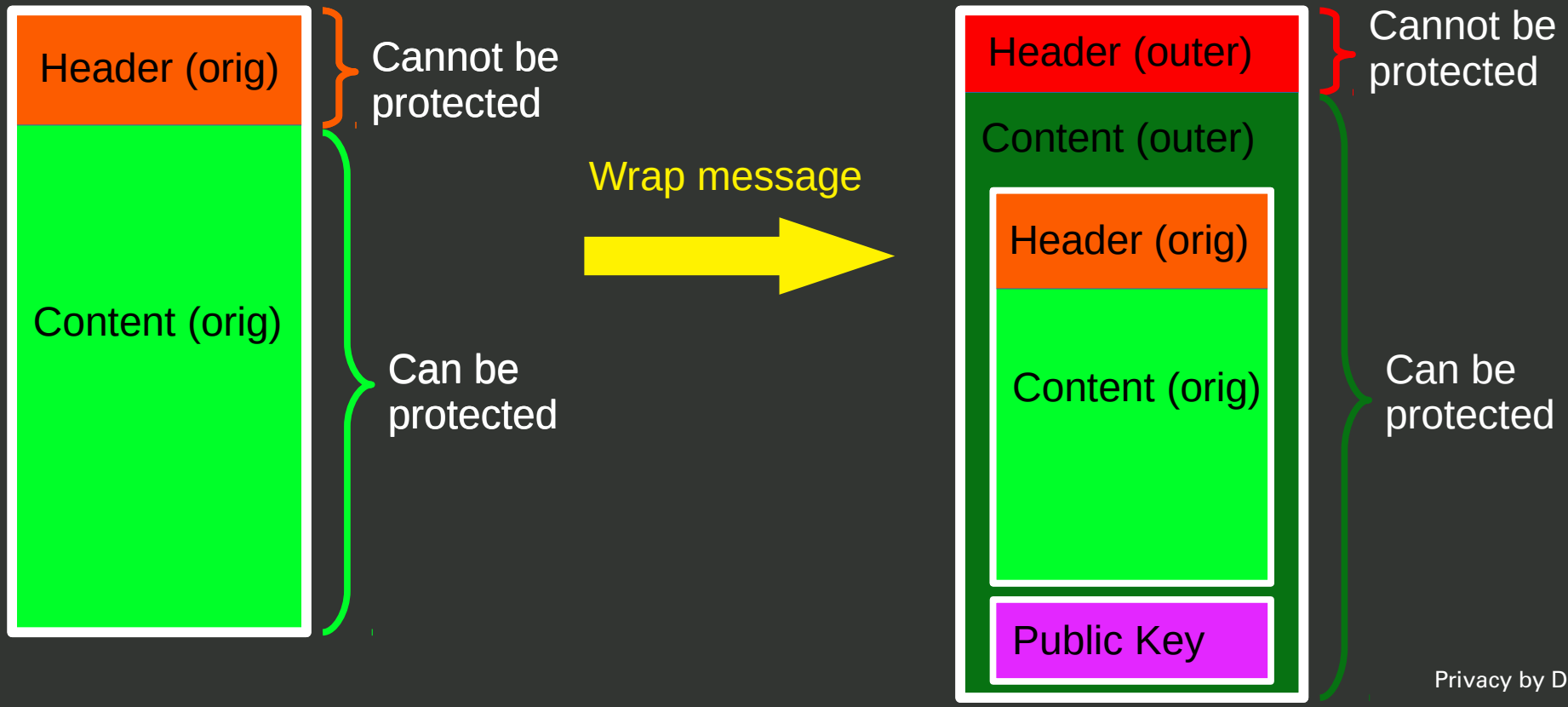
- New Work Item on Header Protection (HP) to be added to the LAMPS Charter requested from IESG:

  Update the specification for the cryptographic protection of email headers -- both for signatures and encryption -- to improve the implementation situation with respect to privacy, security, usability and interoperability in cryptographically-protected electronic mail. Most current implementations of cryptographically-protected electronic mail protect only the body of the message, which leaves significant room for attacks against otherwise-protected messages.

HP in S/MIME since version 3.1



HP in pEp message format version 2



Privacy by Default.

Protection Levels

- Which protection level use cases are in scope?

  a) signature and encryption

  b) signature only

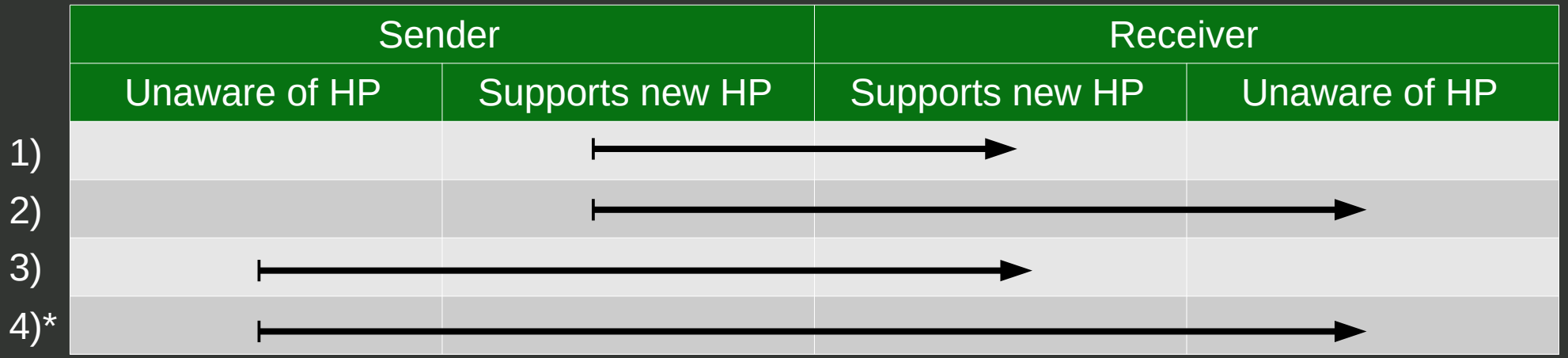
  c) encryption only

  (unclear whether this is relevant or whether it can be treated the same as a)

Note: In pEp only a) is relevant

Interaction Cases (1/2)

- Which interaction cases are in scope?



* trivial case

Interaction Cases (2/2)

- Which interaction cases for interoperability with legacy HP are in scope?
  - S/MIME HP since version 3.1
  - Other implementations (incl. PGP)?

	Sender		Receiver	
	Supports legacy HP	Supports new HP	Supports new HP	Supports legacy HP
5)		←	→	
6)	←	→		

General Requirements (High Level)

- G1: Format (MIME structure, Content Type, etc.)
- G2: Transport of Public Keys
- G3: Easily implementable
- G4: Mitigation of MITM (incl. downgrade) attacks

- B1: Distinguish between forwarded and wrapped messages [depends on solution]

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)

- BS1-BS2: Indication / detection for support of new HP
- BS3: Ensure Subject HF can be displayed to users of HP unaware clients

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

- BR1: Indication / detection for support of new HP

Interoperability Requirements legacy HP

- Not covered in this presentation

MEDUP Mailing List / Non-WG Meeting

- New mailing LIST for MEDUP
  - Missing Elements for Decentralized and Usable Privacy
  - https://www.ietf.org/mailman/listinfo/medup

- Non-WG meeting, Thursday, 18:15 - 19:30,
  Room Tyrolka (Mezzanine floor), including:
  - Introduction to MEDUP / pEp
  - Privacy Threat Modeling (Uni Luxembourg)
  - User Interfaces to Support Privacy (Uni Luxembourg)
  - Status Update on documents

  https://pep.foundation/dev/repos/internet-drafts/raw-file/tip/medup/ietf-104/agenda.txt

Questions / Discussion