

# draft-kucherawy-dkim- transform

Murray Kucherawy <[superuser@gmail.com](mailto:superuser@gmail.com)> / IETF 108 / “Madrid”, July 2020

# Recognized Transformations under DKIM

## draft-kucherawy-dkim-transform

- First posted April 2015 during the early DMARC work
- Idea originated from some OpenDKIM debugging work (I think)
  - Could actually resolve what the breakage was
- Theory: Mailing list servers break DKIM signatures, which makes DMARC unhappy, but usually this damage is made in very small and/or well understood ways
- If that's true, then it should be relatively easy to recover the original message and thus get the author domain signature to validate again in most cases
  - ...as long as you know what the mutations were, and that they are *reversible* and *acceptable*
- Not designed to be bulletproof, only to solve the majority of use cases
- If you try this and it fails, you're no worse off than you were without even trying

# Recognized Transformations under DKIM

## draft-kucherawy-dkim-transform

- So record the *reversible* transformations that commonly occur, and decide what you consider to be *acceptable*
  - Probably the order matters, but maybe not if they don't overlap
- Reached out to Mailman, Sympa, and L-Soft; only Mailman replied
  - Got a comprehensive list of message mutations they make
  - Developed a first list of common, *reversible* transformations, and descriptions for these
  - Proposed a DKIM tag that contains the list of transformations the verifier should apply to try to recover the original message
  - Declared an IANA registry for known transformations

# Recognized Transformations under DKIM

## draft-kucherawy-dkim-transform

- Assume an original message (O) bearing an author domain signature (A) arrives via a Mailing List Manager; the arriving message (M) now also has a list domain signature (L)
- L verifies but A does not, as you'd expect
- But L has a tag on it claiming the MLM made transformations T1, T2, and T3
  - So  $M = T3(T2(T1(O)))$
- These transformations are well understood and *reversible*
  - Then in theory,  $T1'(T2'(T3'(M))) = O$
  - Now you can verify A against O and, if you concur that T1, T2, and T3 were *acceptable*, you can treat M the same as O in terms of trust

# Recognized Transformations under DKIM

## draft-kucherawy-dkim-transform

- Upsides:
  - No crypto, no need for DNS; lightweight and simple when compared to ARC
  - The first set of proposed transformations are well understood
- Considerations:
  - The MIME transformations seem easy to describe, especially when manipulated as objects, but whitespace mishaps might make precision difficult
  - An attacker can take a legitimate message and subject it to these mutations, adding spam to the body or header, and claim to be an MLM
    - Harkens back to the old “I=” tag problem
    - This is why I mentioned that the transformation also has to be *acceptable*