IETF 72 SIP WG meeting

SIP Identity issues

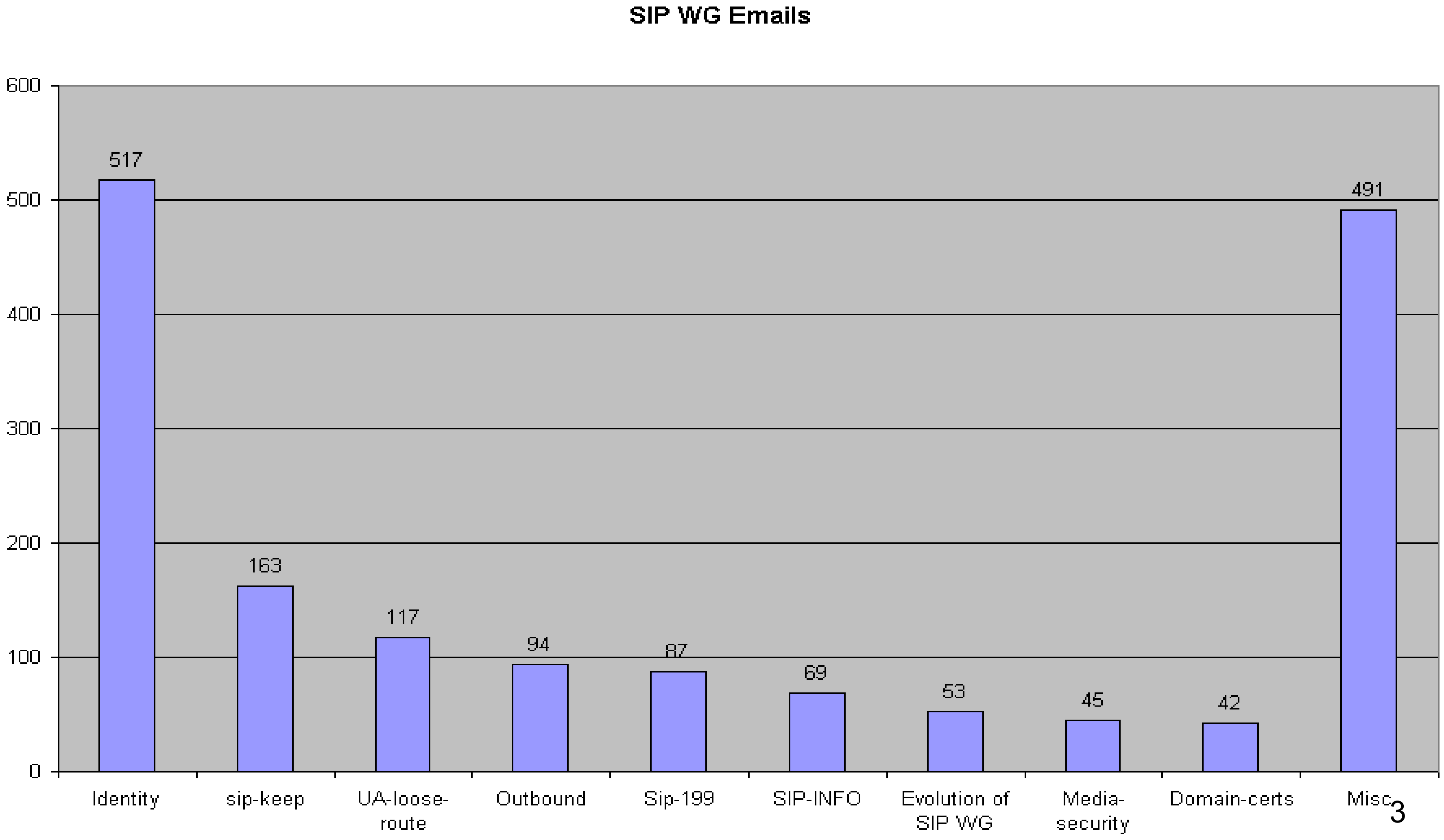
John Elwell et alia

SIP Identity - do we have a problem?

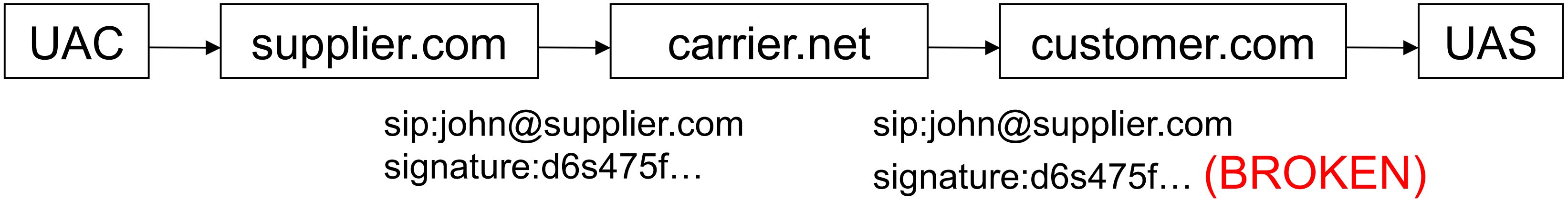
- 7 drafts cited in corresponding presentation at IETF 71
- 3 more drafts since then:
  - draft-elwell-sip-e2e-identity-important-00
  - draft-kaplan-sip-asserter-identity-00
  - draft-kaplan-sip-uris-change-00
- Huge amount of email traffic since IETF 71
  - by far the largest discussion topic based on list traffic
- So is there a problem?
  - It seems there must be, but disagreement on exactly what the problem is
  - Focus today on what the problem is – ignore solutions for now
  - Look at broader picture – what do UAS and called user need?
  - Ignore related issues of PSTN interworking and response identity

List threads since IETF 71

(as of a few days ago)



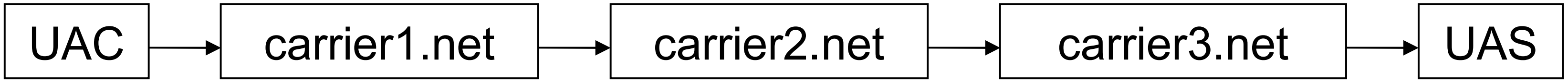
Use case showing media steering breaking signature on email-style URI

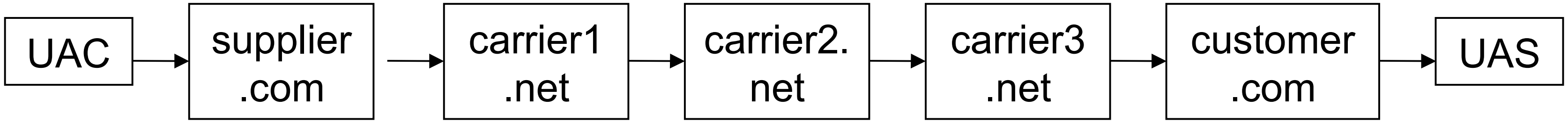

UAC → supplier.com → carrier.net → customer.com → UAS

sip:john@supplier.com
signature:d6s475f…

sip:john@supplier.com
signature:d6s475f… (BROKEN)

- Supplier.com submits signed caller ID sip:john@supplier.com
- Carrier.net has one or more SBCs doing media steering:
  - to ensure RTP media flow across QoS-assured paths (e.g., avoiding low bandwidth paths, or over the Internet via another ISP)
  - therefore changes IP addresses / ports in SDP
- Customer.com receives same caller ID but signature broken
- Applies to other scenarios with >=1 intermediate domains, e.g.:


UAC → carrier1.net → carrier2.net → carrier3.net → UAS


UAC → supplier .com → carrier1 .net → carrier2. net → carrier3 .net → customer .com → UAS

Potential work-arounds

- Carrier.net re-signs using its certificate (carrier.net as subject)
  - Can’t because it needs a supplier.com certificate (subject must match domain in From URI)
- Carrier.net changes the From URI and re-signs using its certificate
  - Can’t, without scrambling the URI somehow, such as sip:john_supplier.com@carrier.net
  - This would undoubtedly break any URI matching at the UAS or at a customer.com proxy, e.g., for white list or other automatic call handling (ACH) checks
  - If presented to the called user in this form, it might be confusing at best
  - Even worse if multiple carrier domains involved, resulting in something like sip:john_supplier.com_carrier.net@secondCarrier.net
  - Additional burden on carriers – they may not wish to do this
- Use a STUN relay to achieve media steering
  - This requires knowledge on part of the UA to insert the relay

Potential work-arounds (continued)

- Carrier.net, as a CA, could sign a certificate with subject supplier.com, and then use that to re-sign the message
  - Not precluded by RFC 4474
  - Requires verifier in customer.com to recognise carrier.net as a trusted CA
  - Allows re-signing without changing the From URI
- Limitations of above:
  - Effectively this introduces transitive trust, since the callee has to trust carrier.net, which in turn has trusted the upstream domain, and so on
  - Verifier in customer.com cannot see the trust chain – only sees that carrier.net has signed on behalf of supplier.com
  - Breaks if any domain on the path:
    - does not support re-signing (i.e., breaks the signature without re-signing)
    - does not trust the assertion by its upstream domain (might happen with ad hoc peering)
- Apart from not doing media steering, there does not seem to be an effective work-around with the present RFC 4474

Other issues

- The horse has already bolted with E.164-based SIP URIs
  - In present deployments, domain name is often changed as request crosses domain boundaries
  - In present deployments, there is no sense of the domain part of an E.164-based SIP URI representing “ownership” of the number
  - No consistency as to when user=phone is or is not used
  - Therefore don’t try to fix this- focus on non-E.164-based (or non-telephone-number-based) SIP URIs
- Handling of received identity information at UAS:
  - Use of PAI versus From/Identity
  - Various forms of URI representing the same user – how to cope with this for phone book look-up, white-listing, automated call handling (ACH)
  - From information received, what to present to the user (not how)
    - including aspects such as telephone number, non-telephone-number user part, domain name, PAI versus From, security level
  - Whole area is very undefined and would probably benefit from a BCP

Dan's Whitelist

- Goal: Identify a repeat caller who uses an IP device so we can whitelist
- Requirements:
  - Out of band media fingerprinting
  - Correlation of identity between calls, able to match identity of new caller to previous caller
  - Work through B2BUA/SBC

Questions for SIP WG

1. Does the WG wish to work on solving the problem of achieving end-to-end (or end-domain-to-end-domain) authenticated identity for non-number-based SIP URIs when media steering is performed by transit domains?
2. Does the WG wish to work on a BCP or similar saying how a UA should handle received identity information?