Security Area Advisory Group

Kathleen Moriarty

Eric Rescorla

IETF-99

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for
details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs
and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

agenda

1. WG/BoF Reports and administrivia (10 mins)
2. Invited/offered talks
    1. Post-Quantum Crypto, Kenny Paterson (30 minutes)
    2. Pretty Easy Privacy (pEp), Volker Birk (15 minutes)
    3. Certificate Limitation Profile, Dmitry Belyavsky (5 minutes)
3. open-mic (60 mins)

WGs

ace

- Chairs
  - Kepeng Li
  - Hannes Tschofenig

ACME

- Chairs
  - Ted Hardie
  - Rich Salz
  - Yoav Nir

CURDLE

1. Chairs
   1. Daniel Migault
   2. Rich Salz

DOTS

- Chairs
  - Roman Danyliw
  - Tobias Gondrom

I2NSF

- Chairs
  - Adrian Farrel
  - Linda Dunbar

ipsecme

- Chairs
  - Tero Kivinen
  - David Waltermire

kitten

- Chairs
  - Matt Miller
  - Benjamin Kaduk
- Not meeting

LAMPS

- Russ Housley

MILE

- Chairs
  - Nancy Cam-Winget
  - Takeshi Takahashi

oauth

- Chairs
  - Hannes Tschofenig
  - Rifaat Shekh-Yusef

openPGP

- Chairs
  - Daniel Kahn Gillmor
  - Barry Leiba

sacm

- Chairs
  - Adam Montville
  - Karen O’ Donoghue

SecEvent

- Chairs
  - Dick Hardt
  - Yaron Sheffer

tls

- Chairs
  - Joe Salowey
  - Sean Turner

tokbind

- Chairs
  - John Bradley
  - Leif Johansson

trans

- Chairs
  - Melinda Shore
  - Paul Wouters

Related WGs

© Brian Campbell

Prague, Czech republic

SAAG WG
IETF 99

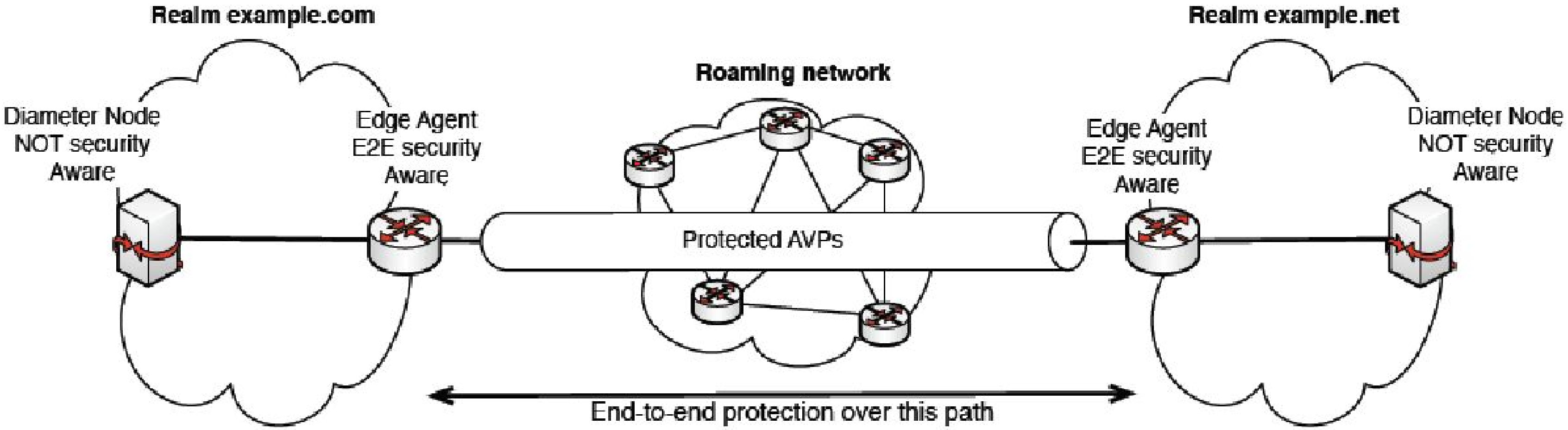
Diameter E2E security

Thursday, July 20th 2017

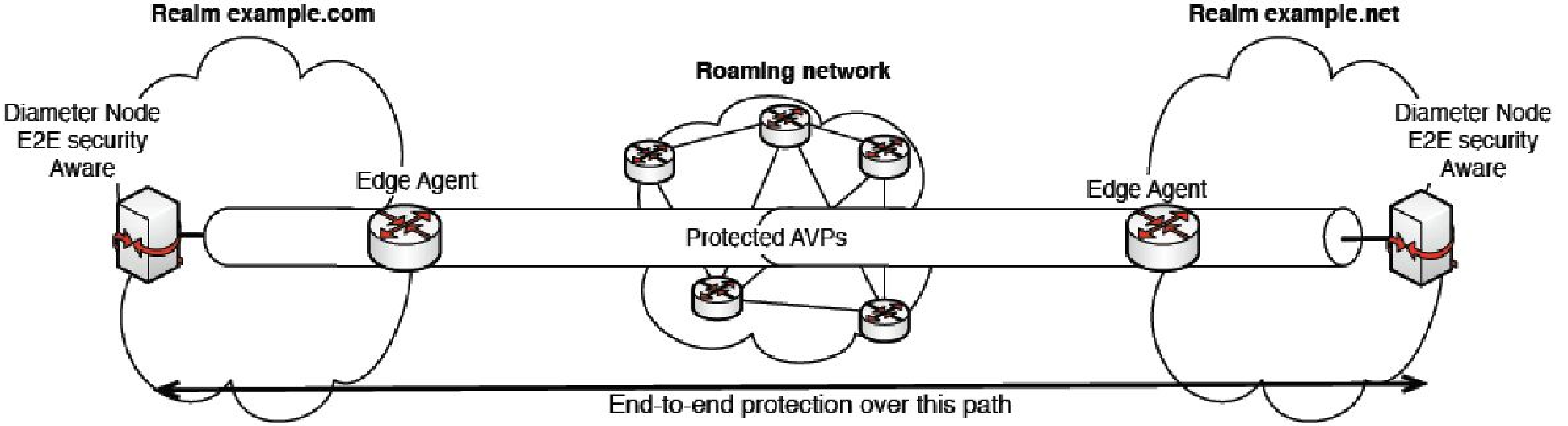
Victim: Lionel Morand

Diameter E2E security

Site-to-site


Realm example.com
Realm example.net
Roaming network
Diameter Node NOT security Aware
Edge Agent E2E security Aware
Protected AVPs
Edge Agent E2E security Aware
Diameter Node NOT security Aware
End-to-end protection over this path

End-to-end


Realm example.com
Realm example.net
Roaming network
Diameter Node E2E security Aware
Edge Agent
Protected AVPs
Edge Agent
Diameter Node E2E security Aware
End-to-end protection over this path

Status

- E2E sec requirement published in 2016 (RFC7966)
- Operational requirements:
  - Required by GSMA (roaming)
  - Required by operators
- Resurrecting old work in this area:
  - draft-korhonen-dime-e2e-security-02
  - AVP integrity and confidentiality protection.
- No progress on this work
  - -03 expired
  - Lack of resources
  - Lack of expertise

Strawman solution proposal

- Two new AVPs are defined for protecting other AVPs:
  - Signed-Data (octet string) for integrity protection of one or more AVPs.
  - Encrypted-Data (octet string) for confidentiality protection of one or more AVPs.
- Original proposal selected JSON-based approach:
  - JSON Web signature (JWS) for integrity protection.
  - JSON Web Encryption (JWE) for confidentiality protection.
- **New thinking:**
  - What about CBOR/COSE instead of Diameterified use of JSON??
  - Alternative?

HELP!!!!!!!!!!!!!!!!!!!!!!!

- Question?
- Note: hop-to-hop encryption is provided with TLS, but not necessarily well-deployed. The request for help is with E2E encryption.

wg/rg

- Security Related WGs/Topics
  - ANIMA
  - DBOUND
  - DIME
  - DISPATCH
  - DMARC
  - DPRIVE
  - HTTPBIS
  - QUIC
  - NETCONF
  - NTP
  - PERC
  - RADext
  - SIDR
  - TCPINC
  - UTA

- Security Related IRTF
  - CFRG
  - IRTFOpen
- IAB Programs
  - PrivSec
- External related
  - W3C

BoFs

Presentations

Presentations

1. Post-Quantum Crypto, Kenny Paterson (30 Minutes)
2. Pretty Easy Privacy (pEp), Volker Birk (15 minutes)
3. Certificate Limitation Profile, Dmitry Belyavsky (5 minutes)

OPEN MIC