Security Area Advisory Group

CodiMD for notes: https://codimd.ietf.org/notes-ietf-109-saag

Meetecho link:
https://meetings.conf.meetecho.com/ietf109/?group=saag&short=&item=1

Benjamin Kaduk
Roman Danyliw
IETF 109
Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
Agenda

1. Welcome, Administrivia, and Agenda Bashing (5 mins)
2. WG Reports (10 mins)
3. AD Reports (5 mins)
4. Terminology: "on path" and "MITM" (10 mins)
5. Requirements for building a PKI (30 mins, Ryan Sleevi)
6. Open mic (remaining)
Remembering Jim Schaad

Working Group Summaries
ACE

Chairs

- Daniel Migault
- Jim Schaad

Report

https://mailarchive.ietf.org/arch/msg/saag/wBn5Z0OE99M4P4dcMQG1S84dWgc/
ACME

Chairs

- Rich Salz
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/o5uBwlcuBd8rdISv4QC-kFP3QRQ/
COSE

Chairs

- Matthew Miller
- Ivaylo Petrov

Report

https://mailarchive.ietf.org/arch/msg/saag/ipXwBOGtmDgiEnrlPXDpNnh1FxU/
CURDLE

Chairs

- Daniel Migault
- Rich Salz

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/fordawH-SNFERzDOohuNGS2u_lC/
DOTS

Chairs

- Valery Smyslov
- Liang Xia (Frank)

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/2gZV-tOv0mgCpUoHAi1nBQtJ6HU/
EMU

Chairs

• Joe Salowey
• Mohit Sethi

Report

Meets tomorrow
GNAP

Chairs

• Leif Johansson
• Yaron Sheffer

Report

https://mailarchive.ietf.org/arch/msg/saag/5FnU9JqndqQ-iF--BjRkQ Tu3Wa4/
I2NSF

Chairs

- Linda Dunbar
- Yoav Nir

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/czdc7ODQftB5ao-vD8UVqk38PVw/
IPSECME

Chairs

- Tero Kivinen
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/US1NUa02529_BdRlp3zskYb9J58/
KITTEN

Chairs

• Robbie Harwood

Report

Not meeting

https://mailarchive.ietf.org/arch/msg/saag/5QDGzIIEdA4VPUEWtusTu3hQEmE/
LAKE

Chairs

• Stephen Farrell
• Mališa Vučinić

Report

https://mailarchive.ietf.org/arch/msg/saag/UVeGQpLNNzRs7X4bRAbjb_brXxQ/
LAMPS

Chairs

- Russ Housley
- Tim Hollebeek

Report

https://mailarchive.ietf.org/arch/msg/saag/HUFFIM68O09j558dRBwqR1OyFOc/
MILE

Chairs
• Nancy Cam-Winget
• Takeshi Takahashi

Report

Did not meet
MLS

Chairs
• Nick Sullivan
• Sean Turner

Report

Meets later today
OAUTH

Chairs

- Hannes Tschofenig
- Rifaat Shekh-Yusef

Report

Did not meet
PrivacyPass

Chairs

- Benjamin Schwartz
- Joseph Salowey

Report

Did not meet
RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

https://mailarchive.ietf.org/arch/msg/saag/LaBfnRQj9kSxijrZvRj1Cc27rDI/
SACM

Chairs

• Chris Inacio
• Karen O’Donoghue

Report

https://mailarchive.ietf.org/arch/msg/saag/NQHqnarwozXYOs_4hHr8dcRBXII/
SecDispatch

Chairs

• Richard Barnes
• Francesca Palombini
• Kathleen Moriarty

Report

  xxx
SecEvent

Chairs

• Dick Hardt
• Yaron Sheffer

Report

  Did not meet
SUIT

Chairs

- Russ Housley
- Dave Thaler
- David Waltermire

Report

Meets tomorrow
TEEP

Chairs

- Nancy Cam-Winget
- Tirumaleswar Reddy

Report

https://mailarchive.ietf.org/arch/msg/saag/ChVmM48WLCqZWesHgHLYysW27sc
TLS

Chairs

- Joe Salowey
- Sean Turner
- Chris Wood

Report

https://mailarchive.ietf.org/arch/msg/saag/wNyzlu73FBS5i5RM0kz6yeIZW0U/
TOKBIND

Chairs

• John Bradley
• Leif Johansson

Report

Did not meet
TRANS

Chairs

• Melinda Shore
• Paul Wouters

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/bdfLMSur5sNPU36fID3bYqE-YgQ/
Related Non-SEC Area Activities

Security Topics in Related WGs
- ADD
- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- DRIP
- HIP
- HTTPBIS
- QUIC
- NETCONF
- NTP
- OPSEC
- PERC
- RADext
- SFRAME
- SIDROPS
- STIR
- UTA
- TAPS

BoFs
- MADINAS

Security Related IRTF
- CFRG
- PEARG

IAB Programs
- model-t

External related
- W3C
- IEEE
- ITU
Other SEC Area Highlights

AD Sponsored Drafts

- draft-foudil-securitytxt
- draft-gont-numeric-ids-sec-considerations

New Work

- Re-open OPENPGP

Looking for WG Chairs for ACE
SEC Area Highlights (2)

Vulnerability Disclosure Guidance

- For IETF LLC
  https://www.ietf.org/about/administration/policies-procedures/vulnerability-disclosure

- For IETF

Common SEC AD DISCUSS items

- https://trac.ietf.org/trac/sec/wiki/TypicalSECAreaIssues
SEC Document Pipeline

Documents for Roman Danyliw

<table>
<thead>
<tr>
<th>Document</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-D Exists Internet-Draft (1 hit)</td>
<td>2020-11-02</td>
<td>I-D Exists</td>
</tr>
<tr>
<td>BN-ISPF-CAPABILITY-YANG-Model-13</td>
<td>62 pages</td>
<td>Proposed Standard</td>
</tr>
<tr>
<td>I2NSF Capability YANG Data Model</td>
<td></td>
<td>Reviews: genart, opendr, reedir, tsvat, yangdoctors</td>
</tr>
<tr>
<td>AD Evaluation Internet-Drafts (6 hits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-bnisp-cap-owid-16</td>
<td>2020-11-02</td>
<td>15 pages</td>
</tr>
<tr>
<td>Concise Software Identification Tags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-ietf-access-token-jwt-10</td>
<td>2020-09-23</td>
<td>19 pages</td>
</tr>
<tr>
<td>JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-ietf-security-find-technical-interface-dm-10</td>
<td>2020-08-28</td>
<td>184 pages</td>
</tr>
<tr>
<td>I2NSF Network Security Function-Facets Interface YANG Data Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-ietf-security-authority-token-trauth-list-06</td>
<td>2020-05-09</td>
<td>14 pages</td>
</tr>
<tr>
<td>TNAuthList profile of ACME Authority Token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-ietf-acme-authority-token-05</td>
<td>2020-05-09</td>
<td>12 pages</td>
</tr>
<tr>
<td>ACME Challenges Using an Authority Token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-ietf-acme-registration-profile-01</td>
<td>2020-02-25</td>
<td>41 pages</td>
</tr>
<tr>
<td>Endpoint Posture Collection Profile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Documents for Benjamin Kaduk

<table>
<thead>
<tr>
<th>Document</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-D Exists Internet-Draft (1 hit)</td>
<td>2020-09-04</td>
<td>I-D Exists</td>
</tr>
<tr>
<td>draft-ietf-secvent-subject-identifiers-06</td>
<td>19 pages</td>
<td>Proposed Standard</td>
</tr>
<tr>
<td>Subject Identifiers for Security Event Tokens</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD Evaluation Internet-Drafts (5 hits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-tls-dtls-connection-44-08</td>
<td>2020-11-02</td>
<td>16 pages</td>
</tr>
<tr>
<td>Connection Identifiers for DTLS 1.2</td>
<td></td>
<td>Submitted to IESG for Publication: Proposed Standard</td>
</tr>
<tr>
<td>draft-ietf-tls-dtls-13-39</td>
<td>2020-11-02</td>
<td>16 pages</td>
</tr>
<tr>
<td>The Datagram Transport Layer Security (DTLS) Protocol Version 1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-tls-ticketrequests-05</td>
<td>2020-04-24</td>
<td>8 pages</td>
</tr>
<tr>
<td>TLS Ticket Requests</td>
<td></td>
<td>Submitted to IESG for Publication: Proposed Standard Nov 2020</td>
</tr>
<tr>
<td>draft-ietf-kitten-saml-saml-qc-19</td>
<td>2019-08-28</td>
<td>14 pages</td>
</tr>
<tr>
<td>SAML Enhanced Client SASL and GSS-API Mechanisms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SAAG - IETF 109
Thanks to the SECDIR Reviewers since IETF 108

<table>
<thead>
<tr>
<th>Derek Atkins</th>
<th>Yoav Nir</th>
<th>Robert Sparks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nancy Cam-Winget</td>
<td>Hilarie Orman</td>
<td>Takeshi Takahashi</td>
</tr>
<tr>
<td>Linda Dunbar</td>
<td>Derrell Piper</td>
<td>Sean Turner</td>
</tr>
<tr>
<td>Donald Eastlake</td>
<td>Radia Perlman</td>
<td>Mališa Vučinić</td>
</tr>
<tr>
<td>Shawn Emery</td>
<td>Derrell Piper</td>
<td>Carl Wallace</td>
</tr>
<tr>
<td>Stephen Farrell</td>
<td>Tirumaleswar Reddy</td>
<td>Samuel Weiler</td>
</tr>
<tr>
<td>Phillip Hallam-Baker</td>
<td>Vincent Roca</td>
<td>Brian Weis</td>
</tr>
<tr>
<td>Russ Housley</td>
<td>Kyle Rose</td>
<td>Klaas Wierenga</td>
</tr>
<tr>
<td>Christian Huitema</td>
<td>Stefan Santesson</td>
<td>Christopher Wood</td>
</tr>
<tr>
<td>Charlie Kaufman</td>
<td>Joseph Salowey</td>
<td>Liang Xia</td>
</tr>
<tr>
<td>Watson Ladd</td>
<td>Rich Salz</td>
<td></td>
</tr>
<tr>
<td>Chris Lonvick</td>
<td>Yaron Sheffer</td>
<td></td>
</tr>
<tr>
<td>David Mandelberg</td>
<td>Rifaat Shekh-Yusef</td>
<td></td>
</tr>
<tr>
<td>Daniel Migault</td>
<td>Valery Smyslov</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Terminology: "on path" and "MITM"
Previous list discussion

- Thread started at https://mailarchive.ietf.org/arch/msg/saag/FR9WP9Y-73QZVX6Org-ciNDwM0w/
- Michael did some summarizing at https://mailarchive.ietf.org/arch/msg/saag/m1r9uo4xYznOcf85Eyk0Rhut598/
Observations from the list

- Existing terminology is ambiguous/imprecise!
- “MITM” predates well-understood analysis of attacker capabilities and characterization of attacks
- Even “on path” can mean different things at different times
- “on path” and “MITM” presume a path; some attacks can change the path, too
- We aim to protect against Dolev-Yao attackers when possible, but other attackers exist and we need terms to talk about them and distinguish classes of attacks
Taxonomy from QUIC

● on-path
● limited on path (cannot delete)
● off-path

Taxonomy from Huitema

● M in the middle
● M on the side
● M in the rough

Taxonomy from DeKok

● malicious messenger
● oppressive observer
● chaos creator
Questions

● Are any of these terms fully unambiguous?
● Is the three-tiered taxonomy useful?
Future work?

Is a strict hierarchical taxonomy valid/useful (vs. distinct capabilities)? Do we want to cover capabilities, attacks, or both? Some candidates:

- read legitimate traffic
- send spoofed traffic
- send spoofed traffic that arrives before legitimate traffic
- suppress legitimate traffic
- [alter legitimate traffic is a combination of the above]
- how much of the network is attackable (from single node to “all”)
- change the path taken by legitimate traffic
- physical/network/transport/application/etc.-layer access
- [please join the mic queue]
Requirements for building a PKI
Open Mic