ATTACKS REQUIREMENTS SOLUTION SCHETCHES

DRAFT-MATTSSON-PERC-SRTP-CLOUD-01
MATTSSON, NASLUND, WESTERLUND
IETF94 YOKOHAMA, PERC, FRI 6 2015

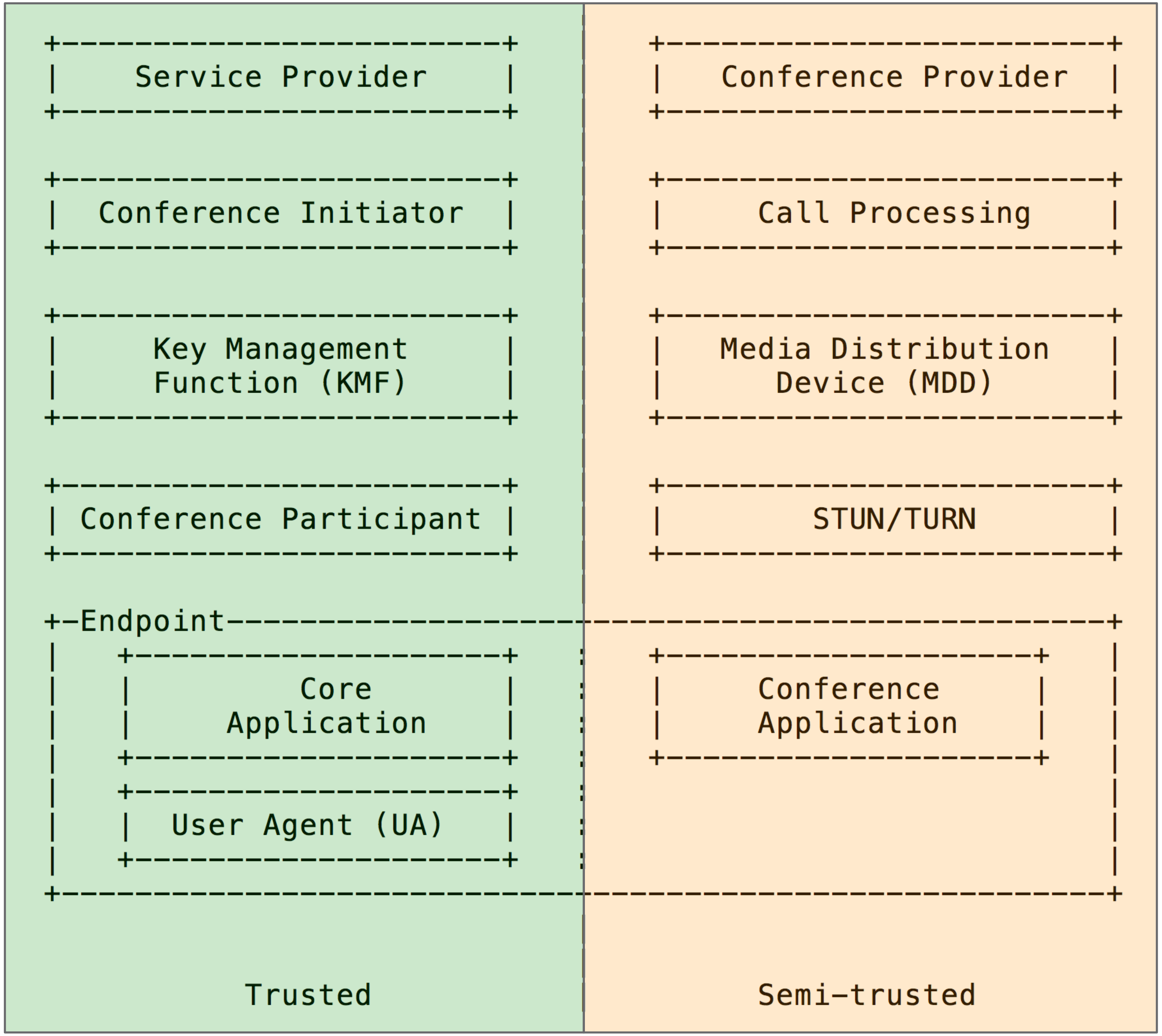
COMPLETE REWRITE

- draft-mattsson-perc-srtp-cloud-01 is a complete rewrite
- Based on proposal sent to mailing list, but substantially updated based on feedback and discussion on the mailing list as well as draft-westerlund-perc-rtp-field-considerations-00

TERMINOLOGY

- PERC need to agree on terminology for:
  - The different trust domains.
  - The various roles / entities.

- While the terms MDD and KMF are established, not much else is…



Service Provider

Conference Initiator

Key Management Function (KMF)

Conference Participant

Endpoint

Core Application

User Agent (UA)

Trusted

Conference Provider

Call Processing

Media Distribution Device (MDD)

STUN/TURN

Conference Application

Semi-trusted

UNIQUE E2E SSRC (SENDER SIDE)

- Design team agreement to use “SSRC” as the e2e source identifier.
  - This enables are current mechanisms using SSRC in RTCP to keep working.
  - But puts requirements on the SSRC.

- **e2e SSRC** is not the same as SSRC field (hbh SSRC).
  - They may be different.

- Sender side:
  - SSRC field = e2e SSRC
  - e2e SSRC used for e2e protection

UNIQUE E2E SSRC (RECEIVER SIDE)

- **Solution sketch**: Handling depends on Topology and MDD functionality
  - SFM without SSRC translation
    - e2e SSRC in SSRC field (e2e context identifier and e2e source identifier)
  - Switching RTP Mixer
    - e2e SSRC in CSRC field
  - SFM with SSRC translation
    - SSRC field is only e2e context identifier.
    - e2e SSRC previously taken from EKT and stored in e2e context.

MDD SPLICING ATTACK

- If there is a e2e SSRC collision during the lifetime of the conference. The MDD will be able to splice the two stream together.
  - E.g. first deliver stream A and then stream B making them look like they came from the same endpoint.
  - The MDD may cause collisions and may hide that there are collisions.
- **Requirement:** e2e SSRCs shall be unique (during the whole lifetime of the conference.
- **Requirement:** MDD shall not assign or affect any e2e security parameters.
- **Solution:** The e2e SSRCs are assigned uniquely by a higher management function (e.g. KMF).
  - This is also required for binding between the e2e source identifier and the conference rooster.

MDD DELAYED PLAYOUT ATTACK

- A receiver has to accept gaps in the e2e sequence number.
  - The MDD can delay delivery of a particular stream for chosen amount of time.
- **Requirement:** “The solution SHALL make it possible for a receiving endpoint to detect if the MDD delays packets for significantly longer than the network delay.”

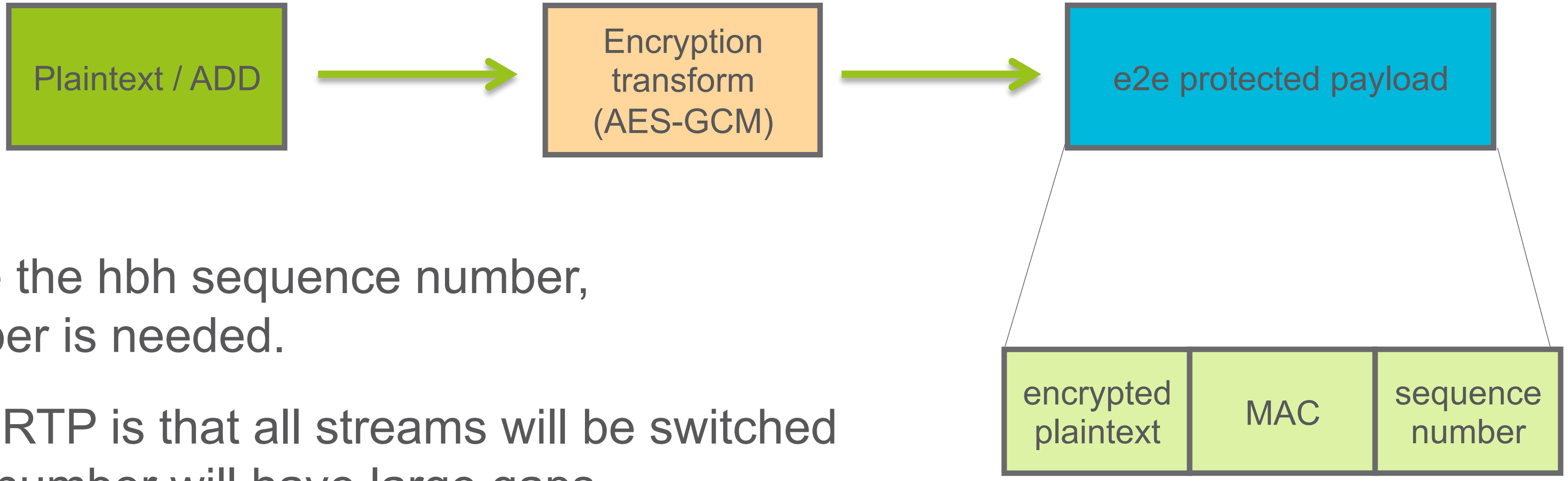
- **Solution sketch:**
  - Do time sync with trusted node when joining conference (e.g. KMF).
  - e2e authenticate the e2e timestamp
  - Provide the receiver with the e2e timestamps
  - Upon receiving new packet with timestamp *ts* at time *t*, receiver checks checks if *ts* >> *t*

TOPOLOGY REDUCTION?

- Given the severity of the attacks, and the complexity and overhead caused by mitigating them in general topologies, it makes sense to restrict PERC to:
  - SFM without SSRC translation

- The receiver will then always find:
  - e2e SSRC in the SSRC field
  - e2e timestamp in timestamp field

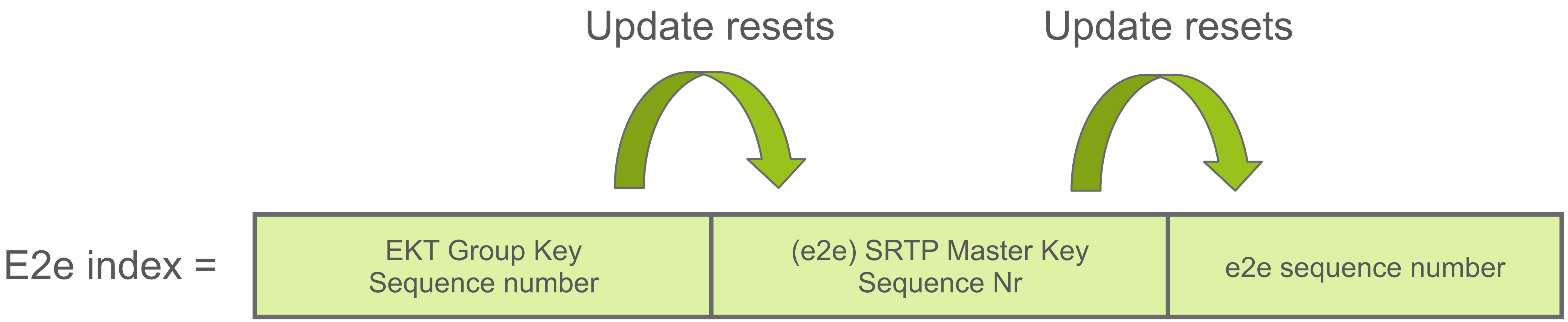
E2E SEQUENCE NUMBER



- As the MDD will rewrite the hbh sequence number, an e2e sequence number is needed.
- Different from normal SRTP is that all streams will be switched and the e2e sequence number will have large gaps.
  - I.e. while ROC sync is the exception in hbh SRTP (late joiners), it would be the default in PERC (each switch).
- **We propose a 32-bit explicit sequence number** handled by the e2e SRTP encryption transform (we anyway need to redefine AES-GCM for SRTP).
- We note that 32-bits are sufficient also for really high bit-rates.

REPLAY PROTECTION++

- **Requirement:** The e2e replay protection MUST be provided for the whole duration of the conference.
- To achieve this the e2e replay protection should be based on a single monotonically increasing number.
- **Solution sketch:** Use key counters for the different keys. Create e2e index from e2e sequence number and counters. Use e2e index for replay protection. Transfer sequence numbers in EKT.



Update resets

Update resets

E2e index =

EKT Group Key Sequence number	(e2e) SRTP Master Key Sequence Nr	e2e sequence number

HOP-BY-HOP PROTECTION

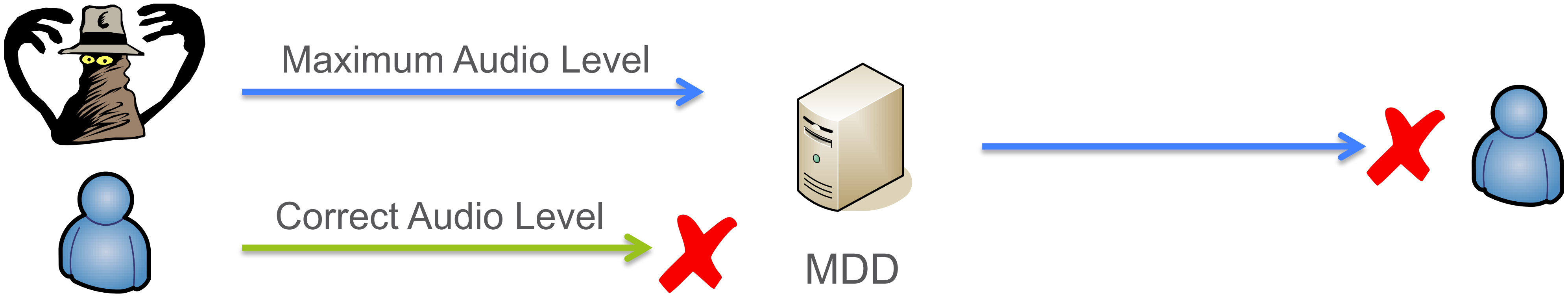
- The analysis in draft-westerlund-perc-rtp-field-considerations puts SRTP's design of leaving the RTP header fields in the clear into question.
  - Basically, does not live up to modern privacy standards.
  - We would recommend using DTLS for the hbh security.

- **Requirement:** The e2e layer shall not be dependent on the hbh layer. It shall be possible to use DTLS for increased confidentiality and privacy.

THIRD PARTY DENIAL OF SERVICE

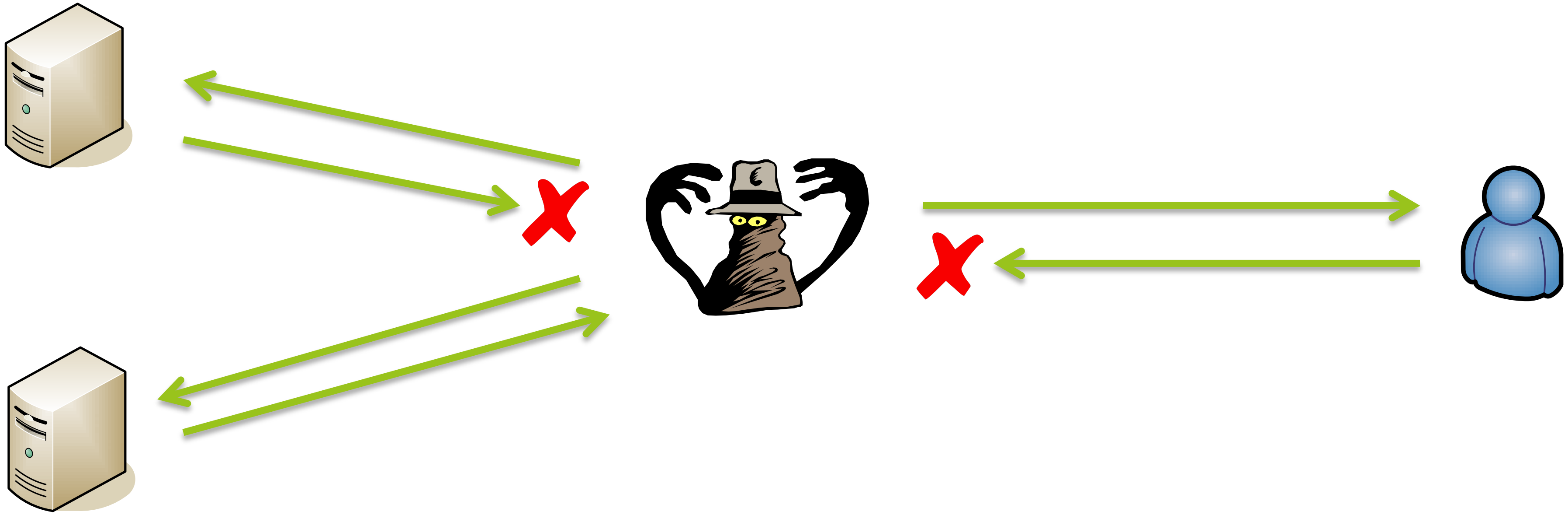
- On-path attacks will always be able to do (selective) blocking.
- Off-path attackers may perform DoS attacks by connecting to different PERC entities.

- An attacker may impersonate a participant, connect to the MDD and deliver specially crafted packets.



THIRD PARTY DENIAL OF SERVICE

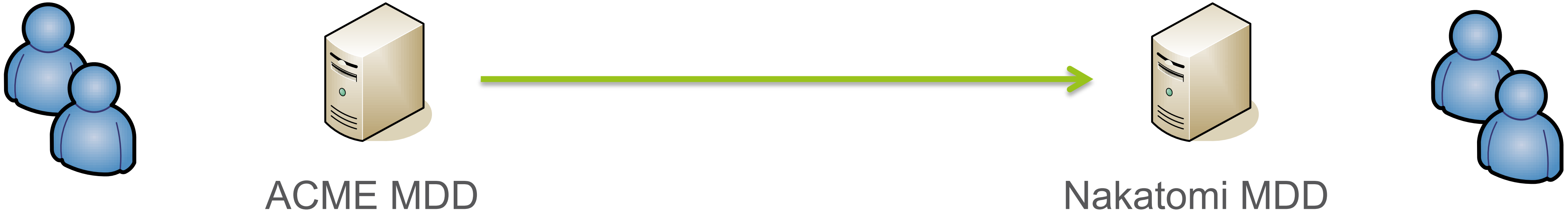
- An attacker may impersonate a MDD, and (selectively) blocking packet from participants or MDDs.



- **Requirement:** A third party shall not be able to impersonate any trusted or semi-trusted entities.
- **Further requirements:** Who should be able to impersonate who?

MDD WRONG META DATA ATTACK

- A MDD may send forged meta data (anything hbh protected) to another cascading MDD giving endpoints connected to the second MDD
  - a modified view of what is happening
  - or just degrading the quality of experience
- May even be incitement to do this if two different MDD vendors / service providers are involved



ACME MDD

Nakatomi MDD

- Similar effect could result from honest MDDs having very different algorithms, e.g. for selecting active speaker. When are participants joining "the same" conference?

E2E SECURE HEADER EXTENSIONS

- There exist RTP header extensions that needs e2e integrity.
- There exists RTP header extensions that needs e2e confidentiality
- Need to ensure that an MDD cannot remove e2e extensions without detection.

- **Requirement:** The solution shall provide a mechanism for e2e integrity and confidentiality for header extensions.

- **Solution sketch:** Use AES-CTR and AAD as described in [AES-GCM]. Only protect extension data (not ID). No reordering.
- Protect IDs or not? Provide confidentiality for header extensions without data?

E2E PROTECTED RTCP

- There exist RTCP messages that needs e2e integrity.
- There exist RTCP messages that needs e2e confidentiality

- **Requirement:** The solution shall provide a mechanism for e2e integrity and confidentiality for RTCP.

- **Solution sketch:** Two new new RTCP packet types used as wrappers. Wrappers have e2e SSRC, e2e sequence number and e2e timestamp.

MDD DENIAL OF SERVICE

- The MDD can rewrites the PT field to another codec. The MDD will usually know which PT corresponds to which codec.
- The effect is that an payload packetized and encoded according to one RTP payload format is then processed using another payload format and codec. Assuming that the implementation is robust to random input it is unlikely to cause crashes in the receiving software/hardware.
- However, it is not unlikely that such rewriting will cause severe media degradations. For audio formats, especially sample based, the attack is likely to cause highly disturbing audio, that can be damaging to hearing and the playout equipment.
- This draft proposes that the original PT is provided end-to-end. However, without knowledge about the stream source's original media format MIME parameters for each PT one can’t verify correct mapping. Only detect attempts of remapping during the session.

ERICSSON