Overview of IEEE 802.1X-REV Dynamic Session Key Agreement

Brian Weis

Overview

- IEEE 802.1AE-2006 (MACsec)
- IEEE 802.1X-REV
- MACsec Key Agreement

IEEE 802.1AE-2006

- Referred to as “MACsec” for short (or sometimes “Linksec”).
- Provides encryption and packet authentication to IEEE 802.1 frames
  - –The default crypto suite is 128-bit AES-GCM
  - –A Session key is called a “Secure Association Key (SAK)”
- Because some IEEE 802.1 networks are broadcast media, multiple stations may share a SAK.

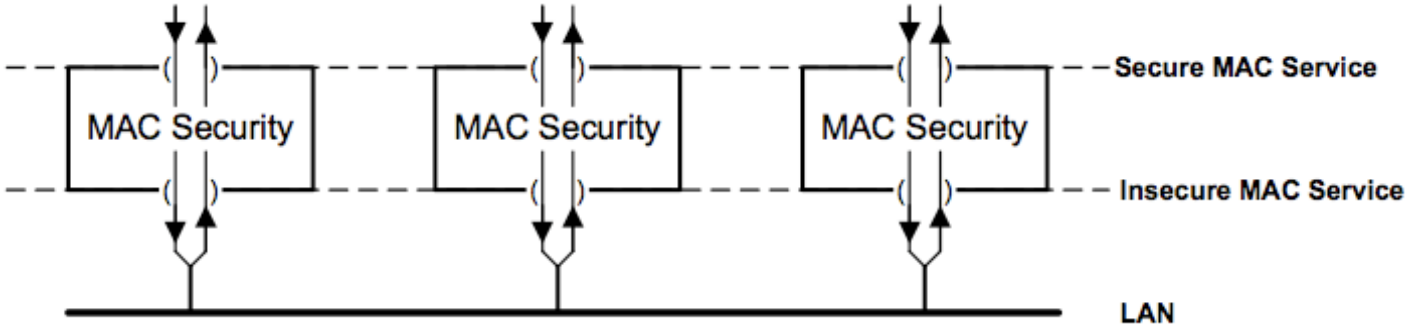


Figure 6-1—MACsec secured LAN with three stations

Connectivity Associations

- A new concept is added to IEEE 802.1 -- the Connectivity Association (CA)

  " security relationship … that comprises a fully connected subset of the service access points in stations attached to a single LAN that are to be supported by MACsec."

- The membership of a CA depends on policy
- A particular link may have more one CA for all stations, or multiple CAs, each with a subset of stations

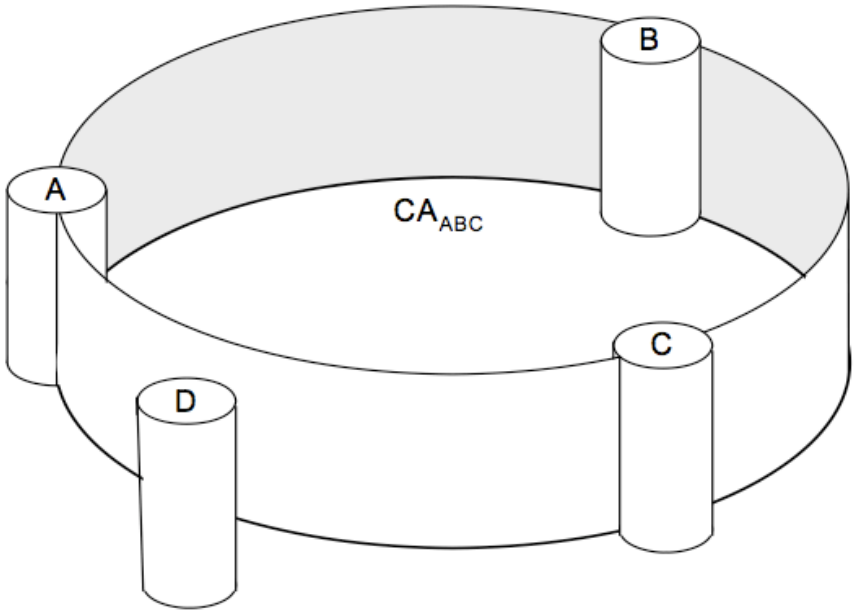


Figure 7-5—A CA including ports A, B, and C

IEEE 802.1X-REV

- Retains IEEE 802.1X-2004 semantics, nearly unchanged
- Adds several new capabilities, notably a MACSec Key Agreement (MKA) protocol for determining SAKs between stations within the same CA.

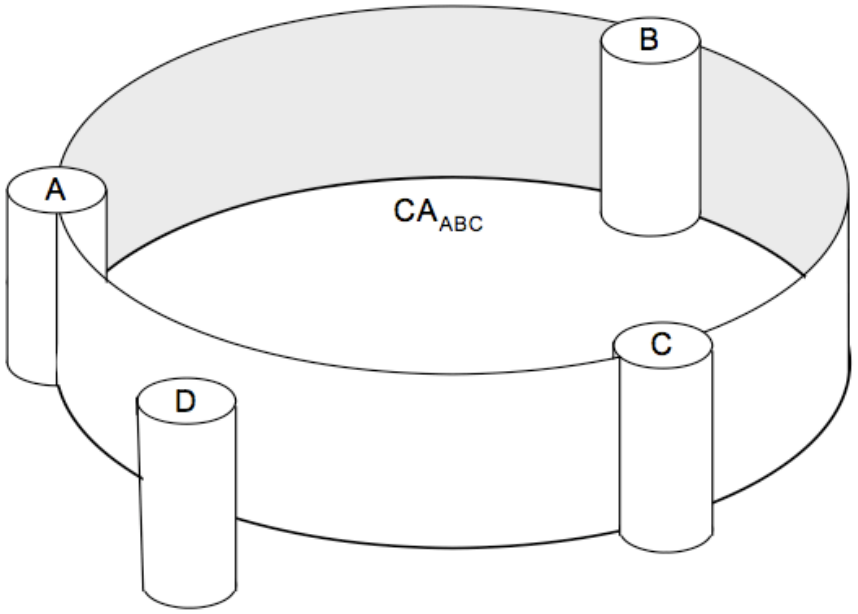


Figure 7-5—A CA including ports A, B, and C

IEEE 802.1X-REV

- Defines the Connectivity Association Key (CAK) - long term key used as source keying material for deriving keys for message integrity checking and SAK distribution
  - Integrity Check Key (ICK) protecting the key agreement protocol
  - Key Encryption Key (KEK) providing privacy for distributed keys

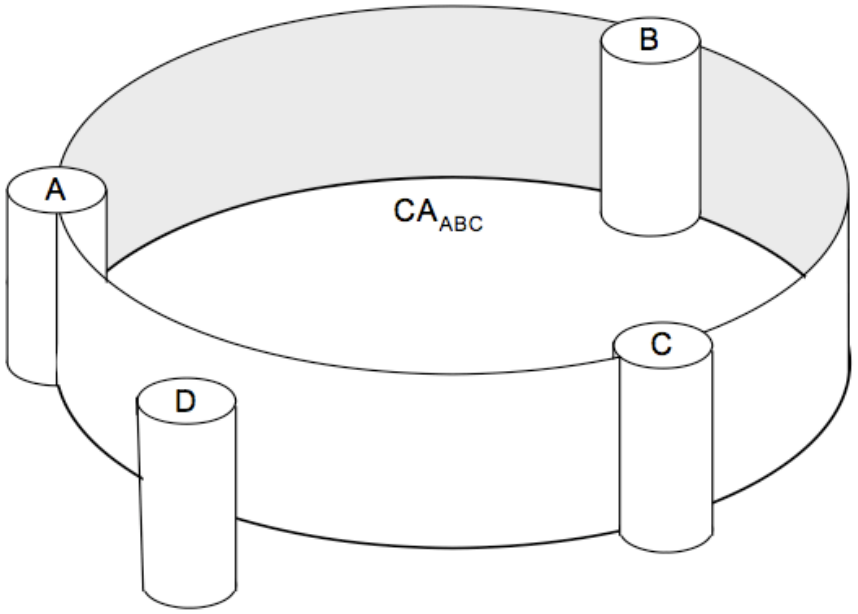


Figure 7-5—A CA including ports A, B, and C

CAK

- CAK sources:
  - Some IEEE 802.1X/EAP authentication methods (e.g., EAP-TLS or EAP-FAST) result in a shared key (MSK).
    - Pair-wise CAK is derived from the MSK
  - Group CAK can be Pre-configured (i.e., a form of “manual pre-shared key”)
  - Group CAK can be distributed through the key agreement method protected by one of the previous two methods

MACSec Key Agreement (MKA)

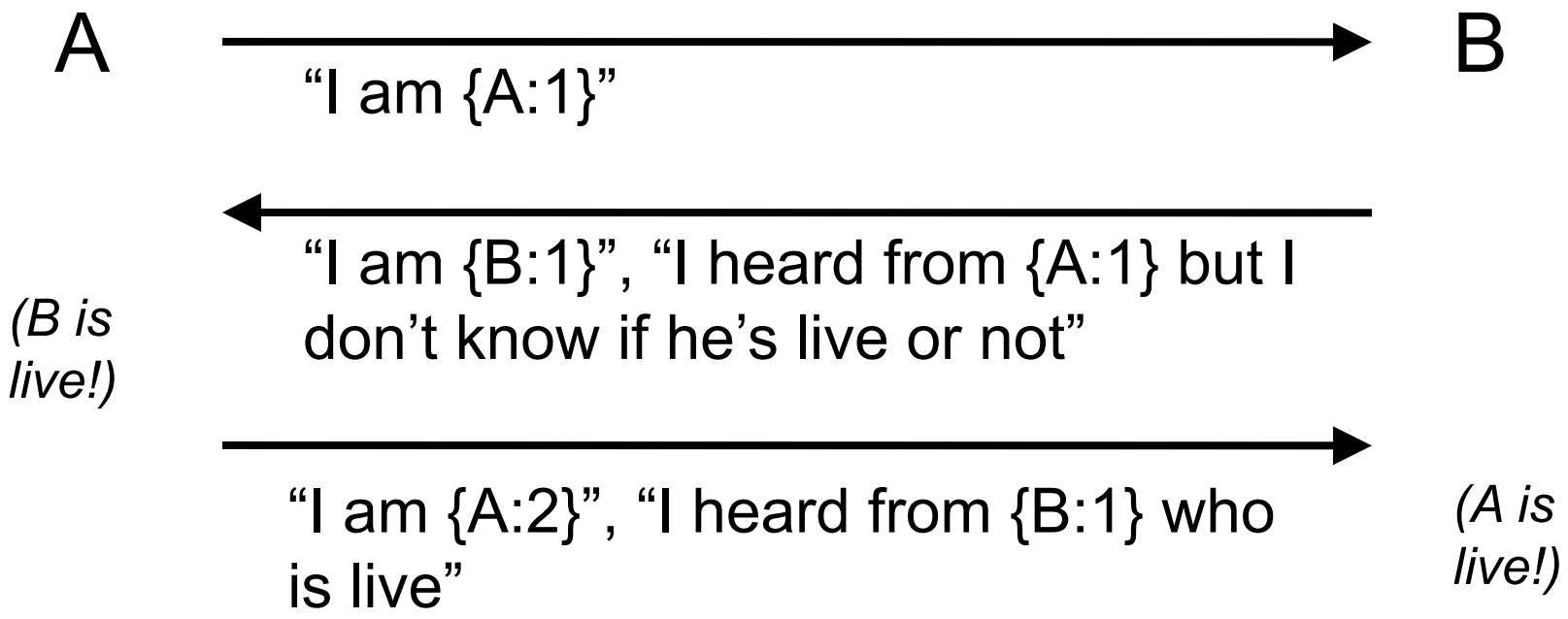
- One station on the LAN acts as a key server (KS)
  - –For redundancy & reliability all stations, or a subset of stations, can be prepared to act as the KS (depending on local policy)
  - –A simple election process is used to determine which station present should be the KS
  - –Each station broadcasts MKA “heartbeat” messages containing
    - Key Server Priority (may be weighted to allow the switch to be favored to be selected as the KS
    - Anti-replay information (lists of “live” and “potentially live” peers)
  - –Once all stations agree on the list of “live” stations, the one with the highest priority is chosen as the KS
    - It is possible to give the switch port the highest priority such that conforming implementations will not be able to take the role of KS as long as the switch port is operable.
  - –If the KS subsequently falls off the list of “live” stations, a new KS is chosen.

MKA Liveness & Replay Protection

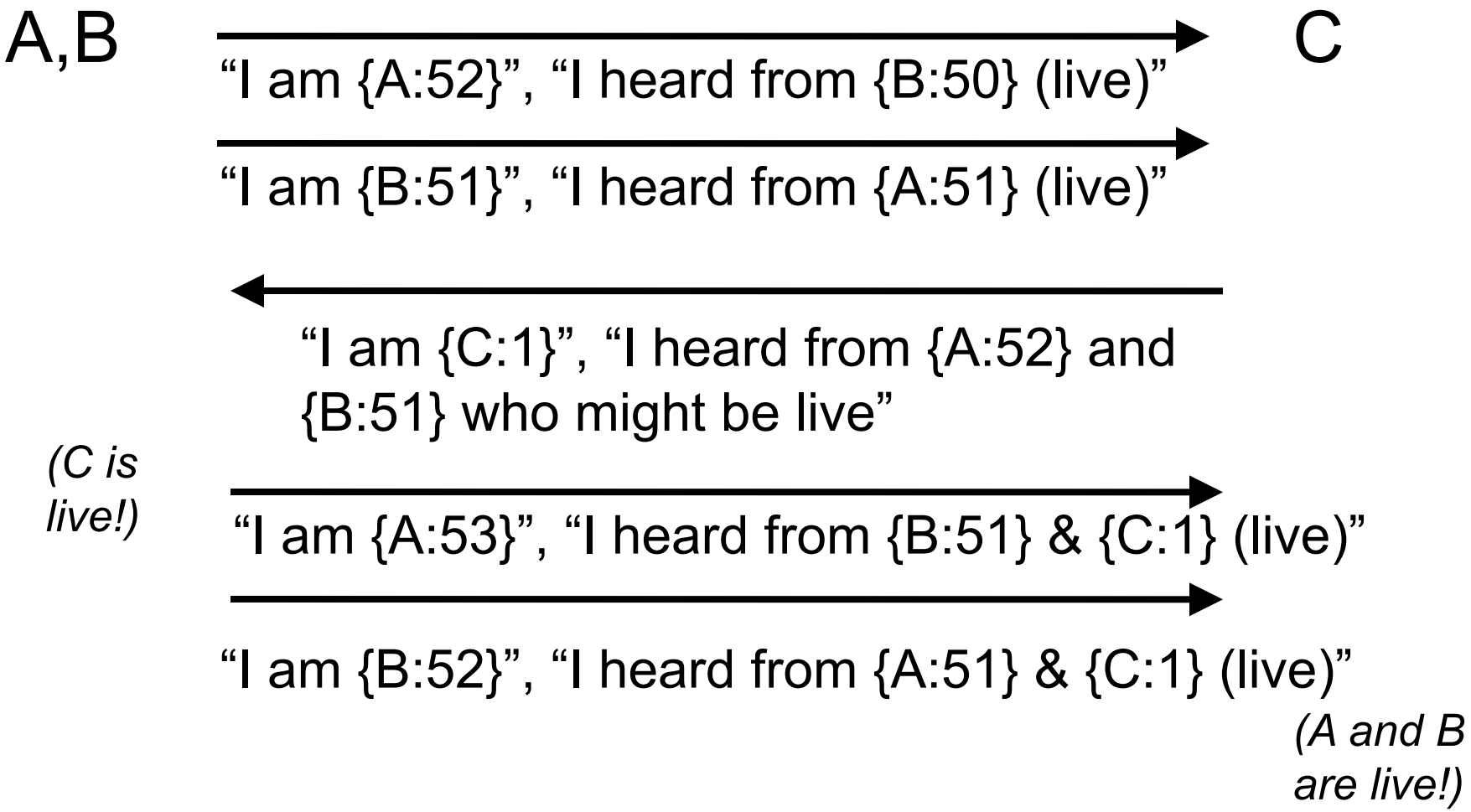
- MKA includes a peer “liveness” property based on the heartbeat messages (sent at 2 second intervals, or more frequently if necessary)
  - This results in early detection when a KS becomes non-responsive
- More importantly, it is the basis for replay protection
  - Each station chooses a nonce (“Member ID”) as its identity
  - Each station maintains a sequence number (“Message Number”) for it’s Member ID, reset to 1 when it chooses a new Member ID
  - Each station includes a list of peers it has heard from recently (Member ID/Message Number)
  - A station does not act upon the policy in a message unless the peer also includes a recent Member ID/Message Number in the message.

Liveness Example (2 devices)

- Initial contact is equivalent to a 3-way "handshake"



Liveness Example (3 devices)



SAK Distribution

- When policy dictates, the key server distributes a new SAK in an MKA message
  - SAK is protected by an AES Key Wrap (keyed with the derived KEK)

MKA Summary

- Allows a group of link-local peers to establish that they are a group
- Provides replay protection between peers in the group
- “Elects” a key server, which distributes common keying material between the link-local peers.
- Key server role is not fixed, which provides for redundancy & reliability

Applicability of MKA concepts to Link-Local Routing Protocols

Russ White

Link-local Routing Protocol

- The security of link-local routing protocols (e.g., OSPF) could be vastly improved by
  - Dynamically choosing session keys rather than depending on long-lasting manually configured session keys
  - Adding replay protection (some do and some do not inherently include replay protection, and those that do are often subject to attacks when sessions are reset)

Link-local Routing Protocol

- The key agreement requirements for link-local MACsec are similar to the key agreement requirements of link-local routing protocols
  - Dynamic session keys are derived from a long-term key when necessary (according to policy)
  - Replay protection is important, including replays of initial “Hello” packets, which can tear down existing state.
  - Dynamic choice of a link-local key server means never being left without a key server

Which link-layer protocols?

- OSPF, RIP, PIM
- IS-IS (Hello's only)
  - Compliments current HMAC-SHA LSP hash, cannot replace it

Implementation Choices

- Integrated into the routing protocol
  - Single state machine
  - Reuse of protocol state & messages
    - E.g., an OSPF already elects a Designated Router (DR), perhaps the DR should also be the key server
  - Adds a small amount of additional per-per state
- Protocol-independent
  - Separating liveness state from the routing protocol state allows it to be useful between sessions (e.g., replay protection of “Hello” packets (???)
  - Resulting session keys are added to a routing protocol “key chain”

Summary

- Does this make sense from a group security perspective?
- Is this something MSEC might want to formalize (or perhaps with KARP if it becomes a Working Group)?