Virtual Clients

How to deal with application messages?

Reminder

- one or more clients can collaborate in “emulating” a virtual MLS client
- emulator clients use an MLS group to sample the randomness of the virtual client
- the virtual client allows the use of a single leaf in an MLS group by multiple clients
- use-cases:

Motivation

- Potential efficiency gains due to smaller trees
- Can prevent metadata leaks (depends on the AS design)

Use-cases

- one user, multiple clients
- representing organizational hierarchies (e.g. a company group with one leaf per department)
- pairing of “strong” and “weak” MLS clients (also called “Guardianship” or “Paired MLS”)

Coordinating emulator client actions

- DS message ordering generally prevents disagreements among emulator clients
- what happens if two emulator clients send an application message at the same time?

Coordinating emulator client actions cont’d

How to preserve MLS functionality?

- if two application messages with the same epoch and generation are sent by a virtual client, recipients will only be able to decrypt one

How to preserve MLS security?

- using the same key/nonce pair twice leaks the message

Potential solution one: Allotted generations

- Each emulator client gets to use every *i*th iteration, where *i* is the leaf index of the emulator client in the emulation group

Advantage:

- works with vanilla MLS, no DS requirements, no extensions

Disadvantage

- recipients have to ratchet more, how much depends on the size of the emulation group and the behaviour of the emulator clients
- leaks which emulator client sent a given application message

Potential solution two: Challenge-based AM encryption

- instead of using a secret tree, clients use a PPRF to derive key/nonce pairs
- the sending client chooses and sends the challenge to use for derivation

Advantage:

- solves both functional and security problem nicely
- makes the secret tree design more flexible (e.g. enables message streams)

Disadvantage

- requires a (safe) extension with a new wire format

Potential solution three: Re-use guard and DS assistance

- Rely on the DS to prevent repeated use of the same key when sending AMs
- Add some structured information in the re-use guard to prevent nonce re-use

Advantage:

- works with vanilla MLS: recipients don’t need to be aware of virtual clients and no extension is needed

Disadvantage:

- Either requires the DS to support a distributed mutex, or requires keeping encryption keys longer than deletion schedule advises