Guardianship for MLS

Elsie Fondevik, Britta Hale, **Xisen Tian**

NPS
Kongsberg Aerospace & Defense

July 27, 2023

* **The ideas and opinions presented are those of the authors and do not reflect the official policies or positions of their respective organizations**

Introduction and Motivations

Users w/multiple devices operating in limited or receive only mode and still wants security properties of MLS

Traveling user with limited bandwidth

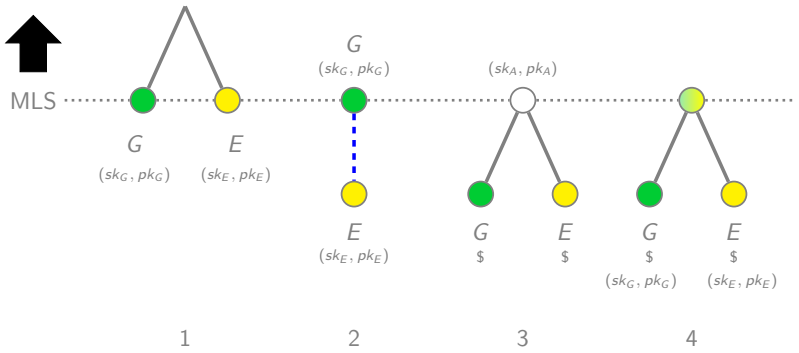
Remote IoT devices with periodic connectivity

Wearable devices operating in receive mode only

- Improved Forward Secrecy (FS): Guaranteed (periodic) updates even when edge is in limited mode
- Post-Compromise Security (PCS): A compromised device must perform an update to 'self-heal'
- Guardianship PCS (GPCS): Designated *guardian* performs key updates on behalf of a paired *edge* to heal [1]

[1] Requires some pairing / key-sharing between guardian and edge

Constructions Mapping



Shared Leaf	Shared Signature	Shared Randomness	Construction
0	0	0	1
0	0	1	*
0	1	0	*
0	1	1	*
1	0	0	2 / 6
1	0	1	4a/b
1	1	0	5
1	1	1	3a/b

Constructions (shortlist)

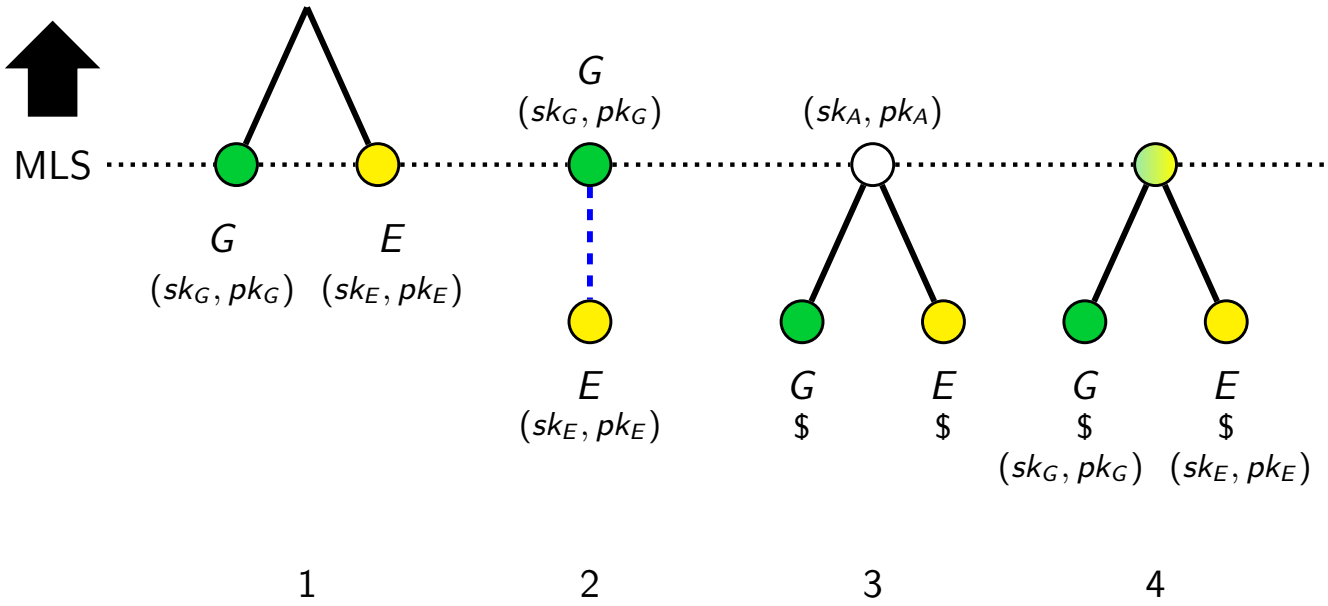


Figure: Options 3 and 4 are separated into cases depending on if (**a**) the shared randomness is kept in active memory (e.g., part of state) or (**b**) pre-installed in a secure module as may be done with signature keys.

Options 5 and 6 mirror 3 and 4 except with distinct random tapes (this necessitates an external channel between G and E for both 5 and 6).

Key Architectural Feature Comparison

Feature	1	2	3a	3b	4a	4b	5	6
Extensible to multiple edges	○	●	●	●	●	●	●	●
Guardian can be offline	●	○	●	●	●	●	●	●
Guardian removal without edge	●	○	○	○	●	●	○	●
Traceability of guardianship	●	○	◐	◐	●	●	◐	●
Low impersonation risk	●	○	○	○	●	●	●	●
FS	●	◐	●	●	●	●	●	●
PCS	●	◐	○	●	○	●	●	●
GPCS	○	○	○	●	○	●	○	○

Table: Architectural feature comparison. Depending on use case, different features may be desirable.

Options 5 and 6 mirror 3 and 4 except with distinct random tapes (this necessitates an external channel between G and E for both 5 and 6).

Questions?