

BLERP: BLE Re-Pairing Attacks and Defenses

Tommaso Sacchetti, Daniele Antonioli

NDSS 26, San Diego, CA, USA

Bluetooth Low Energy (BLE)

BLE is a standardized wireless protocol for short-range data exchange

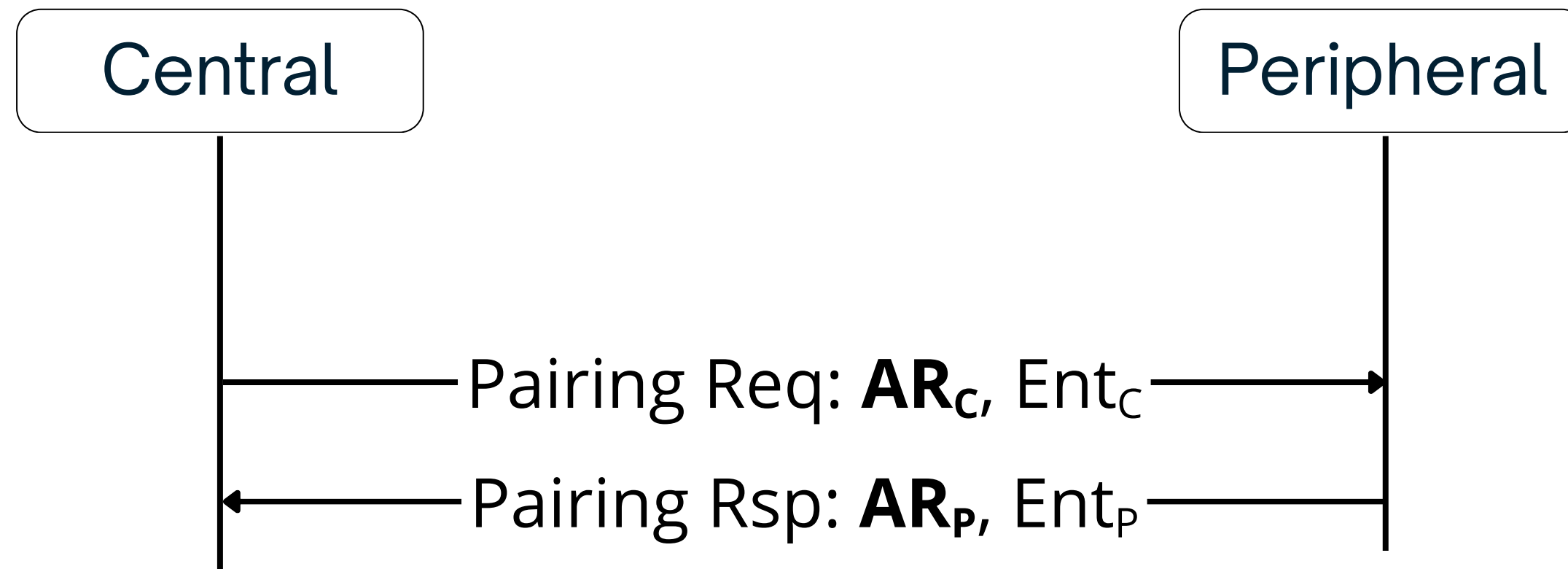
Used daily by **billions of heterogeneous devices** (🕒 📱 💻)

Connection roles

- **Central:** scans for advertisements, starts connections → 📱 💻
- **Peripheral:** advertises presence, responds to connections → 🕒

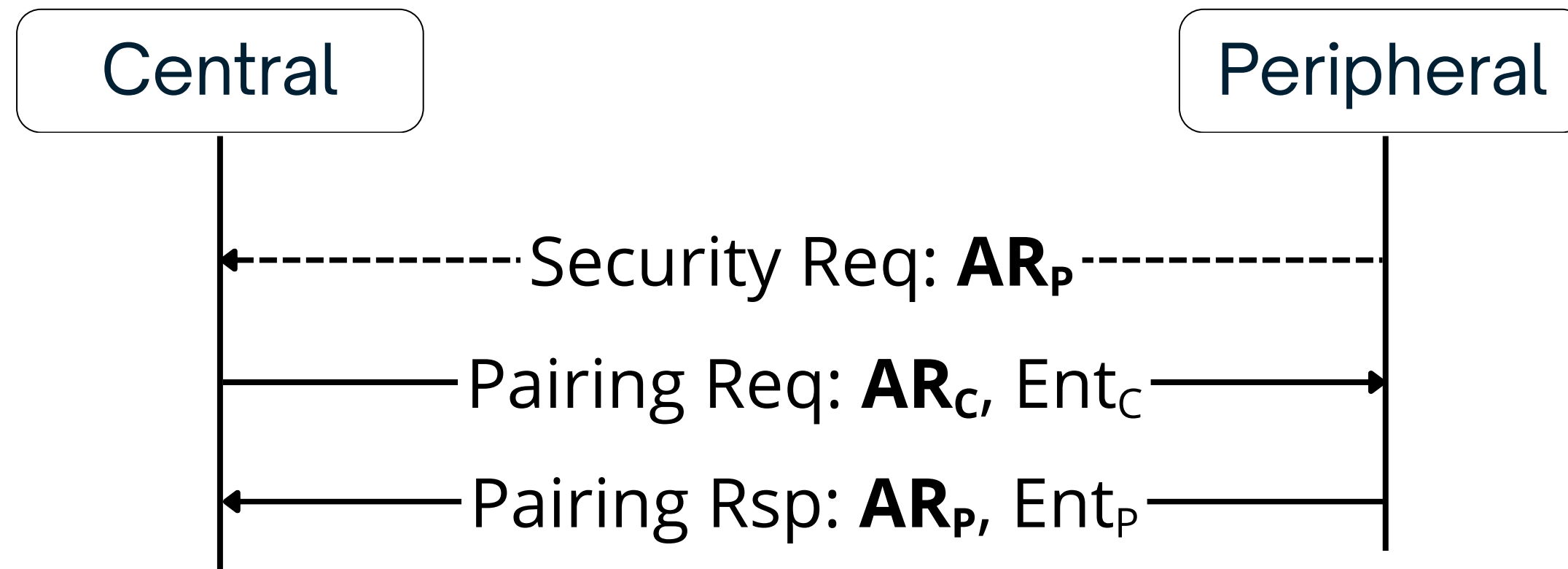
BLE Pairing

- Establish a long-term Pairing Key (PK)
- Allows negotiating features
 - Security Level (SC, MitM, bond, ...) → AR
 - Key Entropy (7-16 bytes)



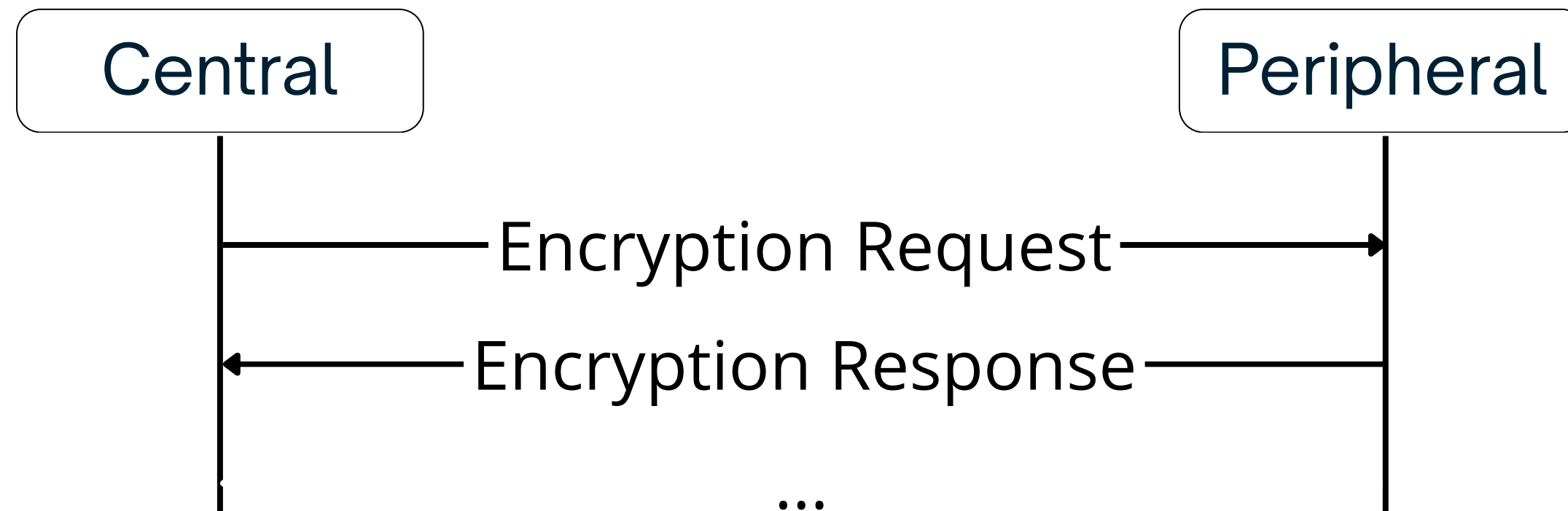
BLE Pairing

- Establish a long-term Pairing Key (PK)
- Allows negotiating features
 - Security Level (SC, MitM protection, ...) → AR
 - Key Entropy (7-16 bytes)



BLE Session Establishment

- Short-term key establishment protocol
- Encrypts the connection between paired devices



Focus on BLE Pairing Security

Prior attacks on BLE pairing

- **KNOB, Invalid Curve, Crackle** → force weak key
- **Method Confusion, NiNo** → bypass authentication

Threat model

- Dolev-Yao adversary
- Target initial pairing → devices connect for the first time
- **Re-pairing is not considered**

What about BLE Re-Pairing?

The standard allows re-pairing and **overwriting a PK**

Limited existing research

- **BLURtooth**: Cross-Transport Key Derivation (AsiaCCS' 22)
 - First mention of *re-pairing* between BR/EDR and BLE
 - Only mention of *re-pairing* in the literature

What about BLE Re-Pairing?

The standard allows re-pairing and **overwriting a PK**

Limited existing research

- **BLURtooth**: Cross-Transport Key Derivation (AsiaCCS' 22)
 - First mention of *re-pairing* between BR/EDR and BLE
 - Only mention of *re-pairing* in the literature

How secure is BLE re-pairing?

Our Contributions

1. Four new BLE re-pairing attacks
2. Four new protocol-level vulnerabilities affecting the standard
3. Low-cost toolkit to test attacks
4. Evaluation exploiting 22 devices
5. Designed and tested countermeasures
6. Updated BLE threat model to include re-pairing

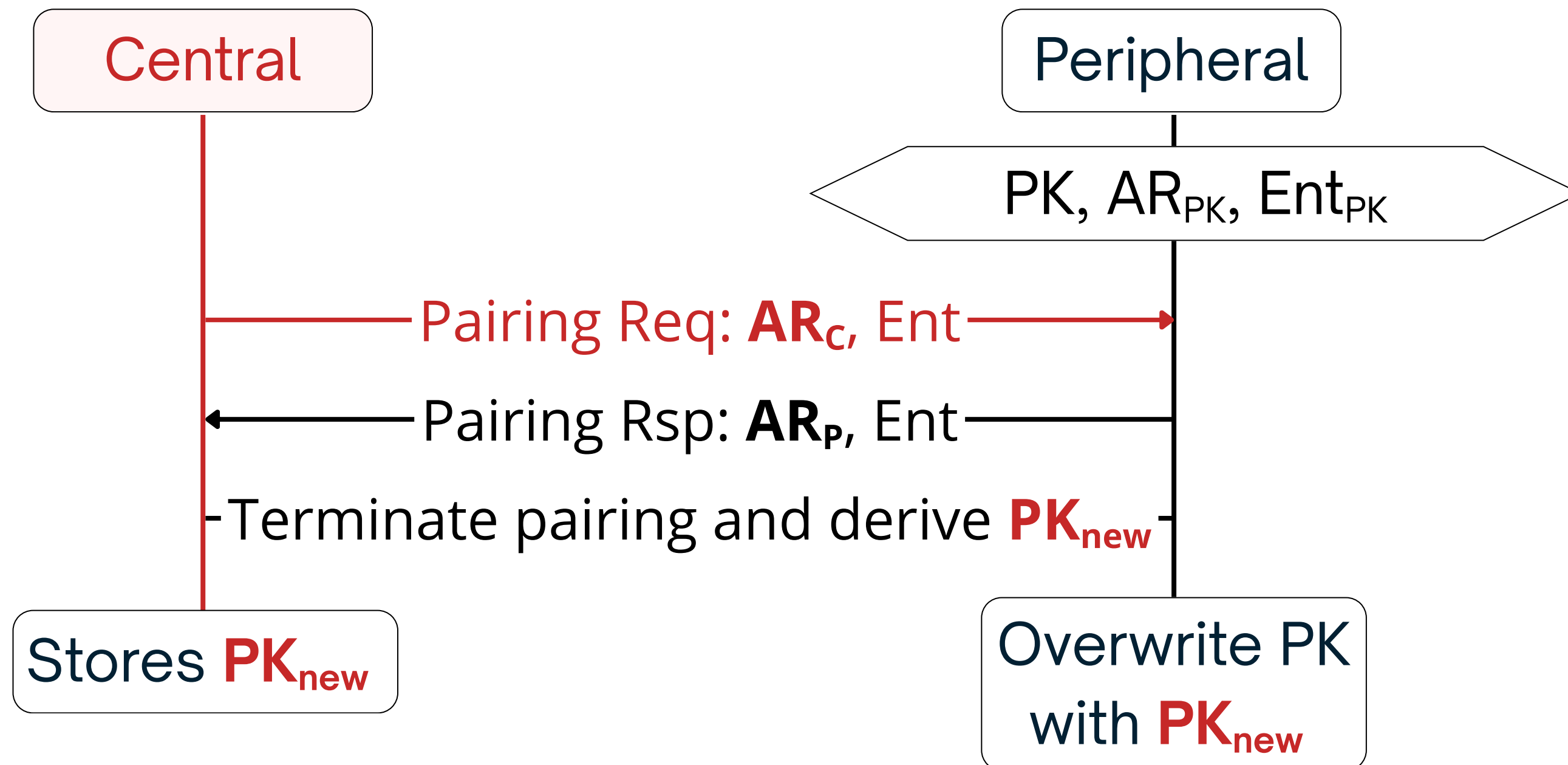
BLE Re-pairing Logic

Peripheral sends **Security Request**

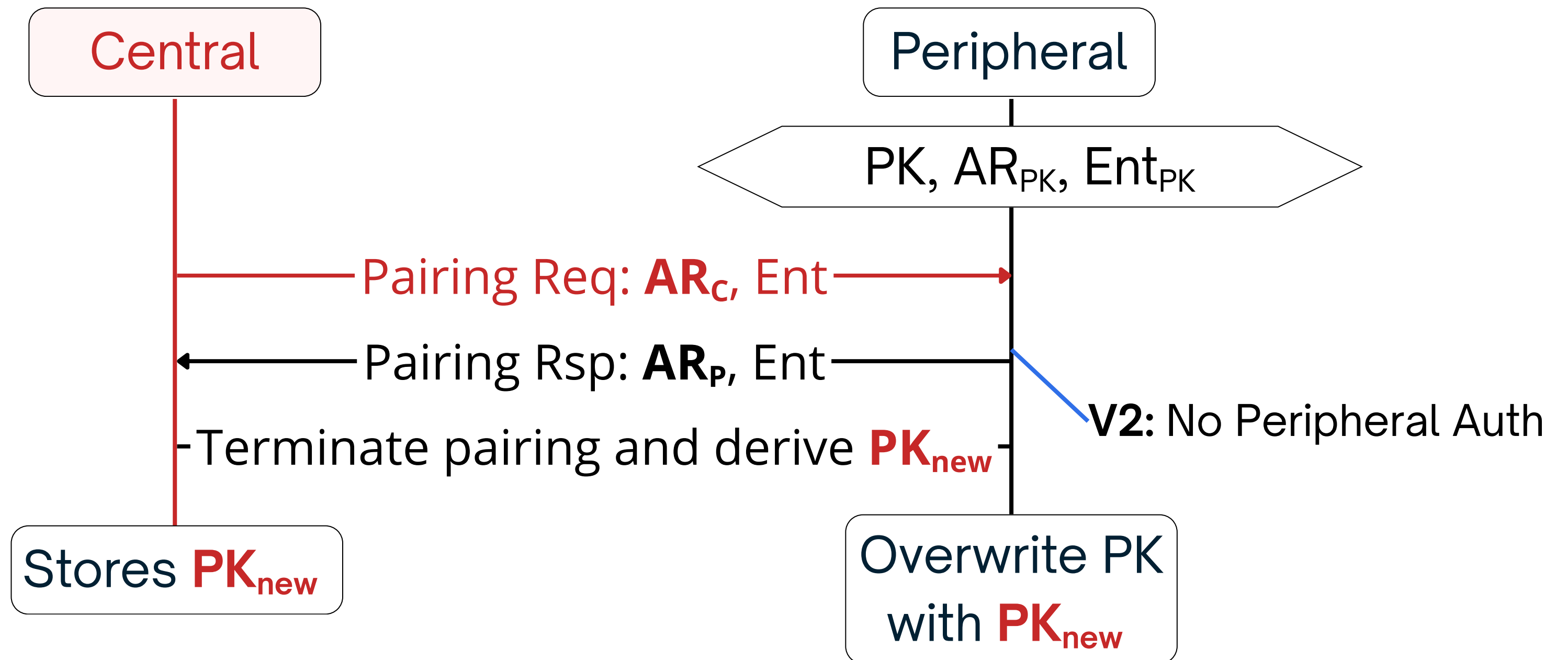
Central checks:
 $AR_{SR} > AR_{PK}$?

Yes → re-pair, overwrite PK ✓

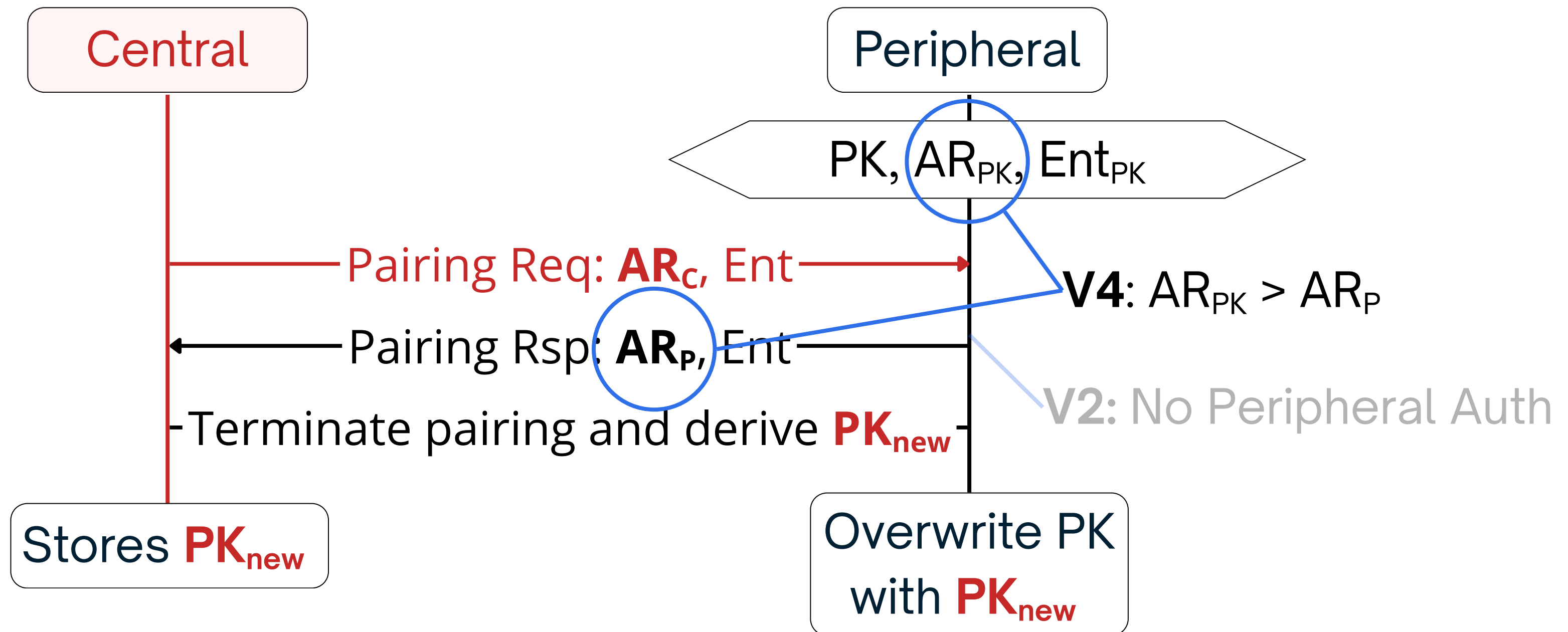
BLERP Central Impersonation



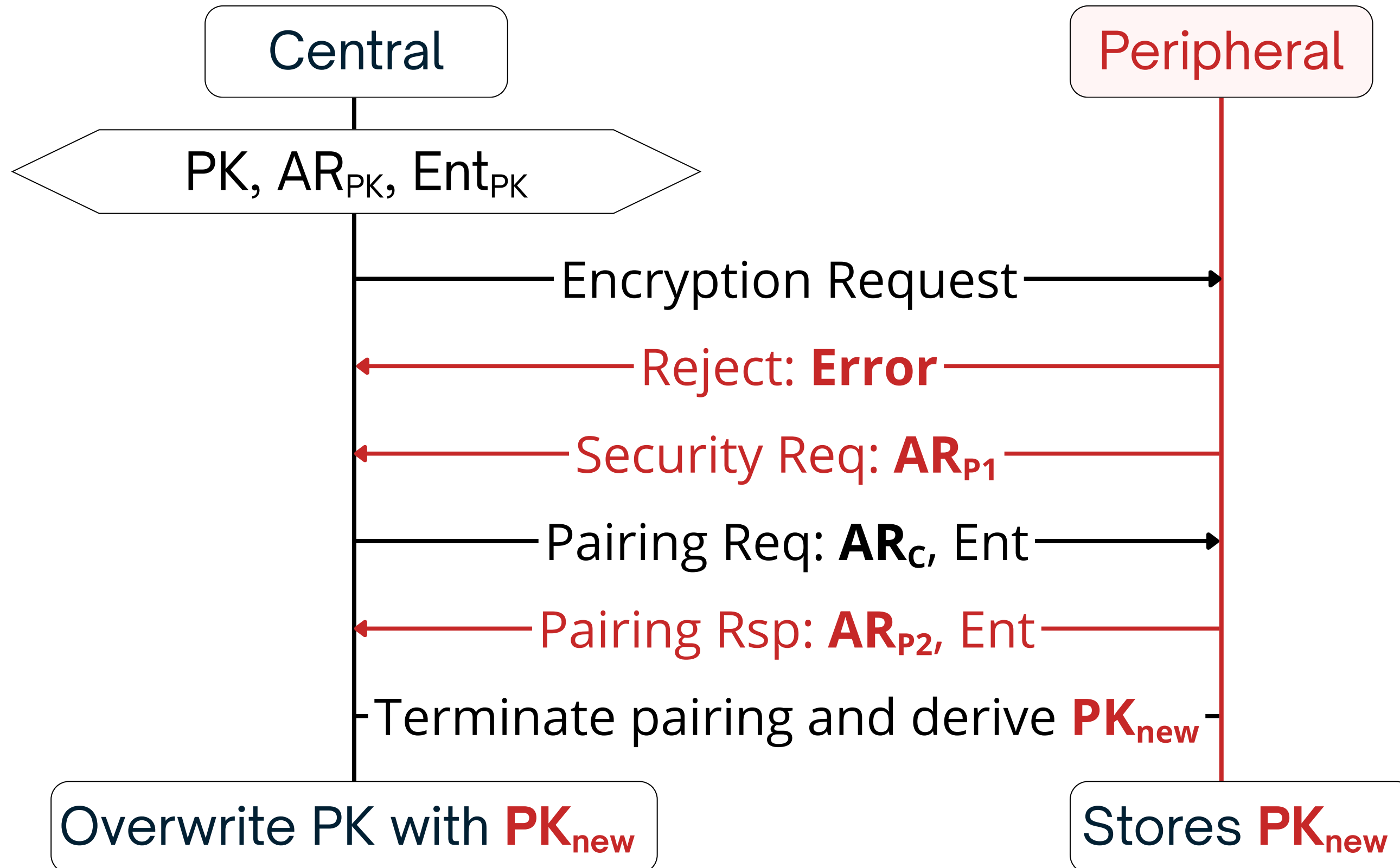
BLERP Central Impersonation



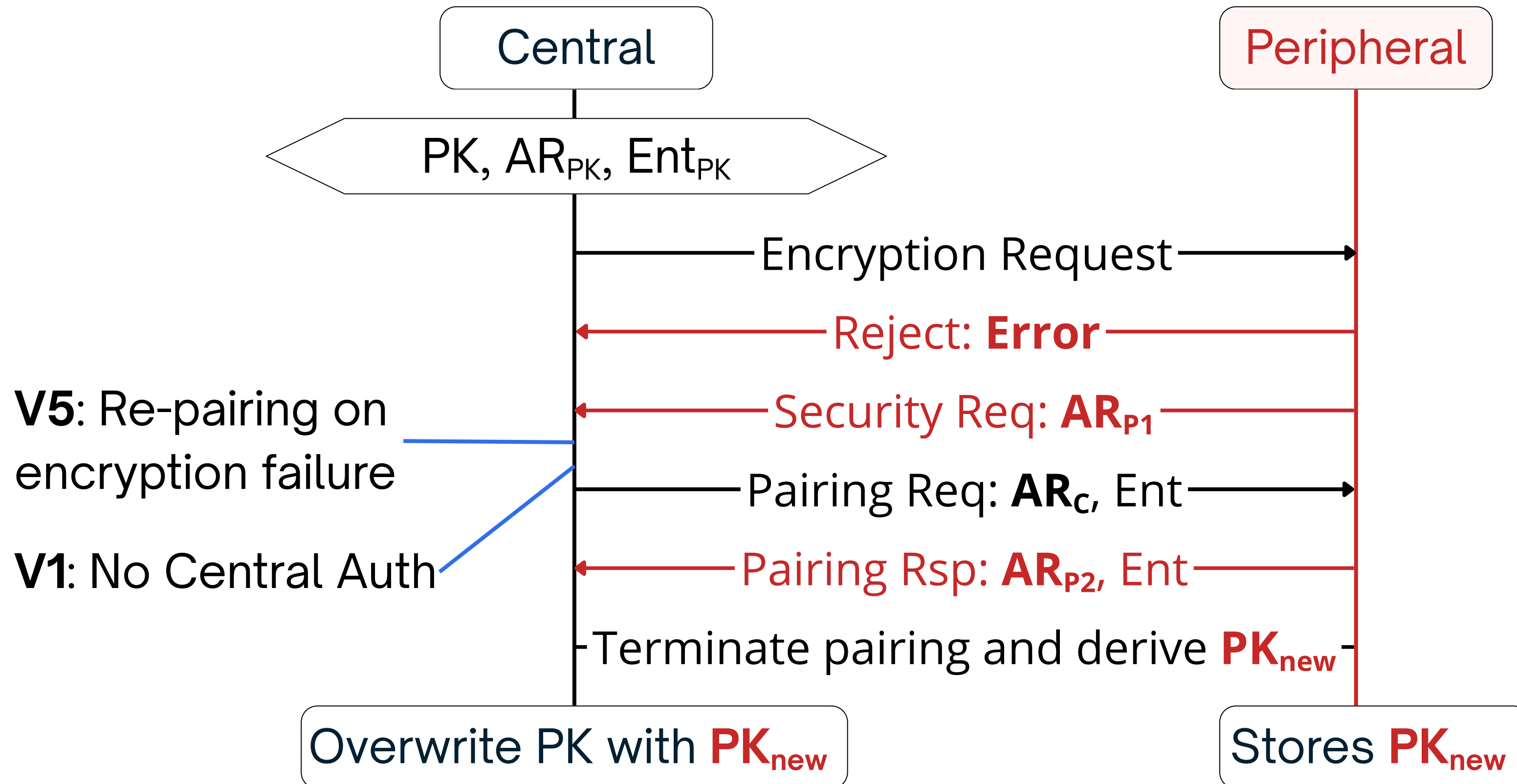
BLERP Central Impersonation



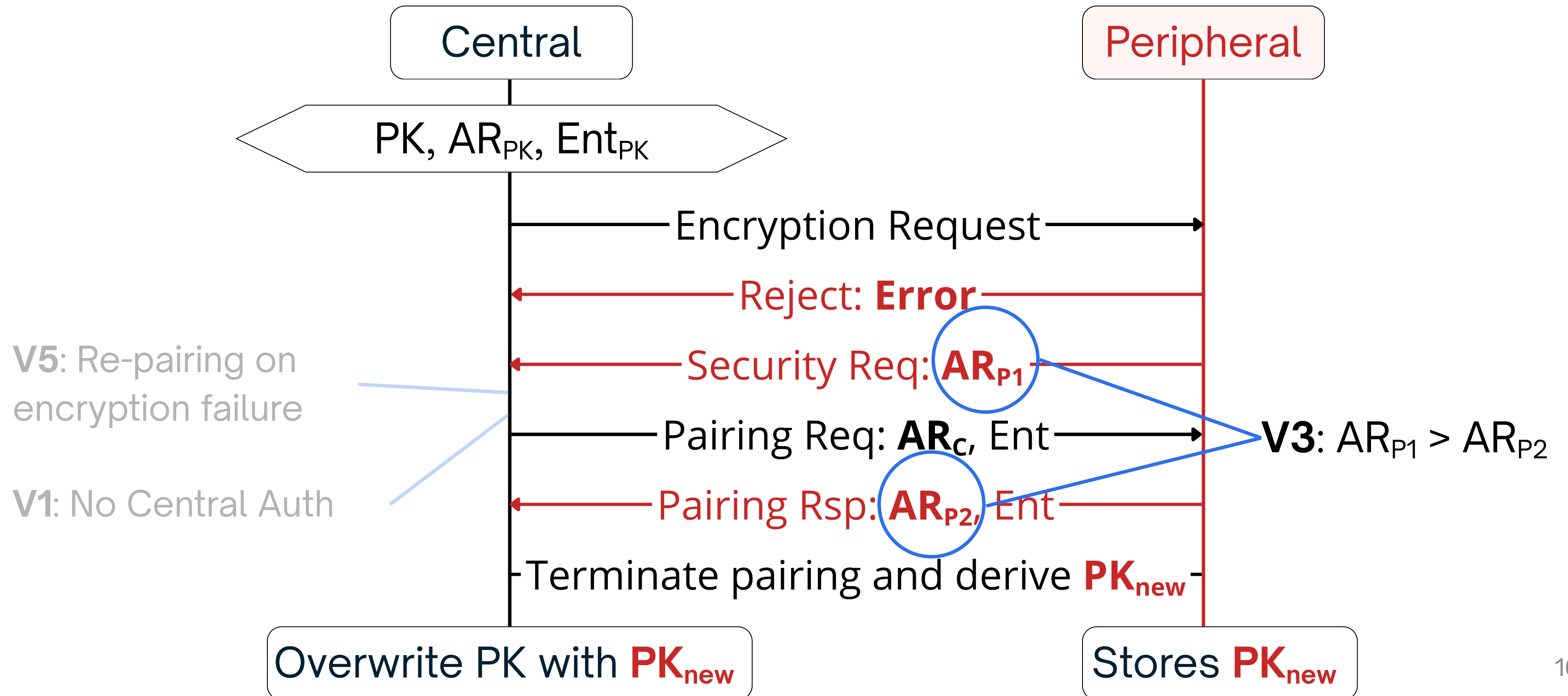
BLERP Peripheral Impersonation



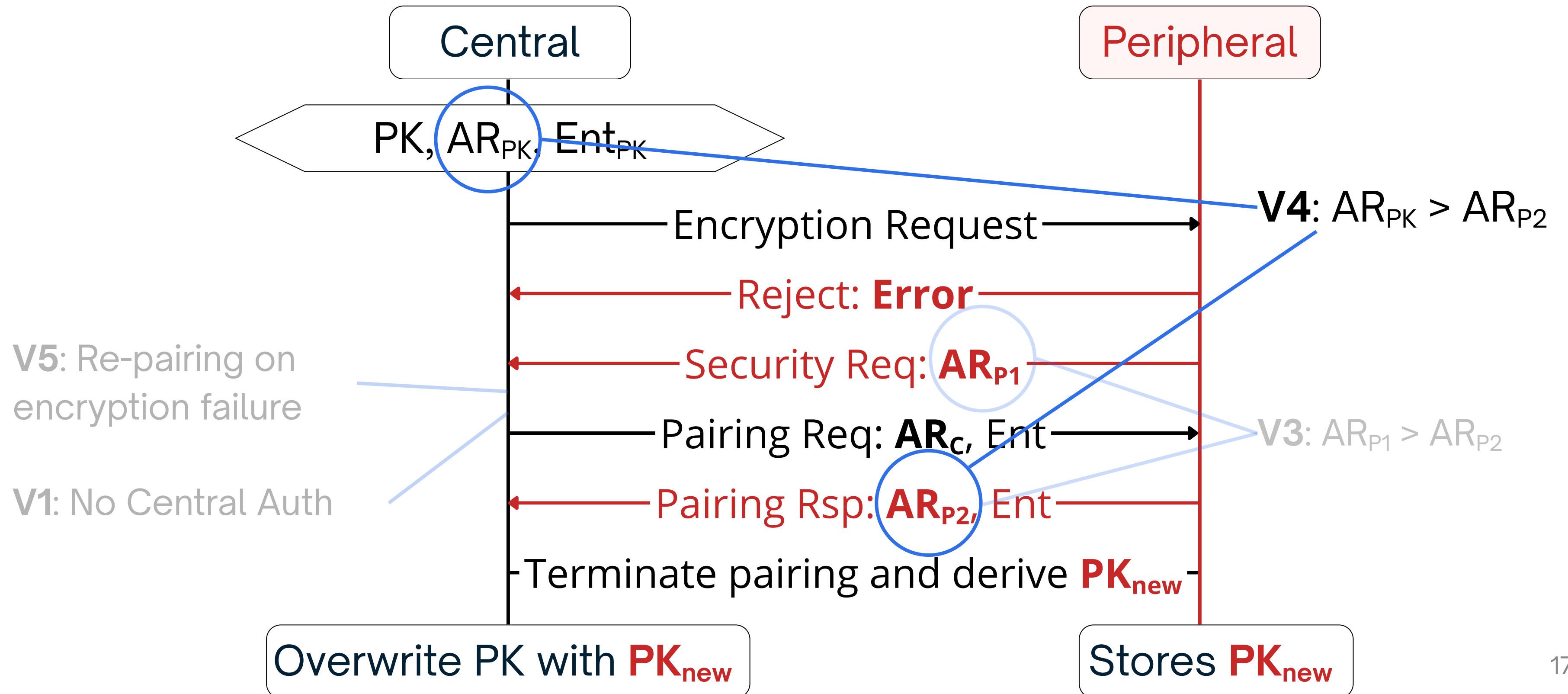
BLERP Peripheral Impersonation



BLERP Peripheral Impersonation

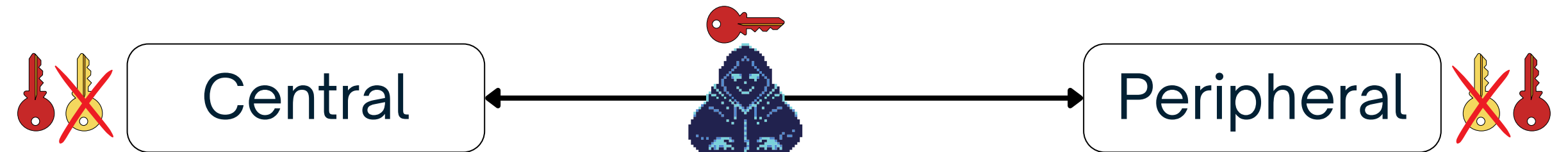


BLERP Peripheral Impersonation

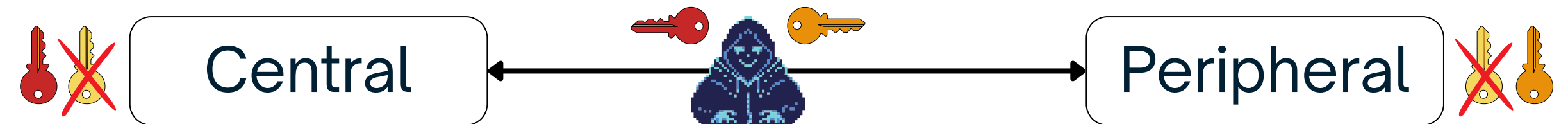


BLERP MitM Attacks

Single-Channel
MitM



Double-Channel
MitM



BLERP Vulnerabilities

V1: *Unauth. Central Re-pairing (**new**)*

V2: *Unauth. Peripheral Re-pairing (**new**)*

V3: *Peripheral Security Level Downgrade (**new**)*

V4: *Re-pairing Security Level Downgrade (**new**)*

V5: Re-pairing from failed encryption

V6: Re-pairing Key Entropy Downgrade

Evaluation Results Summary

22/22

Targets vulnerable
to 2+ vulnerabilities

4.2 – 5.4

Affected Bluetooth
Versions

SC, MitM, ...

Regardless of
security settings

0/1 – Click

One or zero user
interaction

Apple: Allows re-pairing if $AR_{SR} = AR_{PK}$

NimBLE: Allows re-pairing with **specific** AR_{SR} (CVE-2025-62235)

Android: Deletes PK after two encryption errors

Zephyr: Blocks re-pairing downgrade

Evaluation Results

Device	AuthReq	BLEv	V1	V2	V3	V4	V5	V6	PI	CI
MacBook Air	SC, MitM	5.0	●	-	●	●	●	●	●	-
Windows 11	SC	5.2	●	-	●	●	●	●	●	-
Linux 6.10.9	SC	5.2	●	-	●	●	●	●	●	-
Oculus Quest	SC	5.0	●	-	●	●	●	●	●	-
iPhone 15	SC, MitM	5.3	●	-	●	●	●	●	●	-
iPad 2022	SC, MitM	5.2	●	-	●	●	●	●	●	-
Google Pixel 8	SC	5.3	●	-	●	●	●	●	●	-
Realme X2 Pro	SC	5.0	●	-	●	●	●	●	●	-
Xiaomi Mi 11 Lite	SC	5.1	●	-	●	●	●	●	●	-
Samsung Galaxy A15	SC	5.3	●	-	●	●	●	●	●	-
TCL 43P638	SC	5.0	●	-	●	●	●	●	●	-

Evaluation Results

Device	AuthReq	BLEv	V1	V2	V3	V4	V5	V6	PI	CI
NimBLE	SC, MitM	5.4	●	●	●	●	●	●	●	●
NimBLE SC-Only	SC, MitM	5.4	●	●	●	●	●	●	●	●
Zephyr	LSC	5.4	●	●	●	●	●	●	●	●
BTstack	SC, MitM	5.2	●	●	●	●	●	●	●	●
ESP32-C3	SC, MitM	5.0	●	●	●	●	●	●	●	●
Xbox Joystick	SC	5.0	-	●	-	●	-	●	-	●
Logitech MX Anywhere 3S	SC	5.1	-	●	-	●	-	●	-	●
Logitech MX Keys S	SC, MitM	5.1	-	●	-	●	-	●	-	●
Logitech MX Master 3	LSC	4.2	-	●	-	●	-	●	-	●
Garmin Vivoactive 5	SC, MitM	5.0	-	●	-	●	-	●	-	●

BLERP Defenses

Hardened re-pairing (backward-compatible)

- Security Level enforcement
- Disconnect on encryption error

Authenticated re-pairing (protocol re-design)

- Key chaining
- Transcript hashing

Conclusion

Contributions

- 6 vulnerabilities • 4 attacks • 2 defenses
- BLERP toolkit • 22 devices tested • threat model update

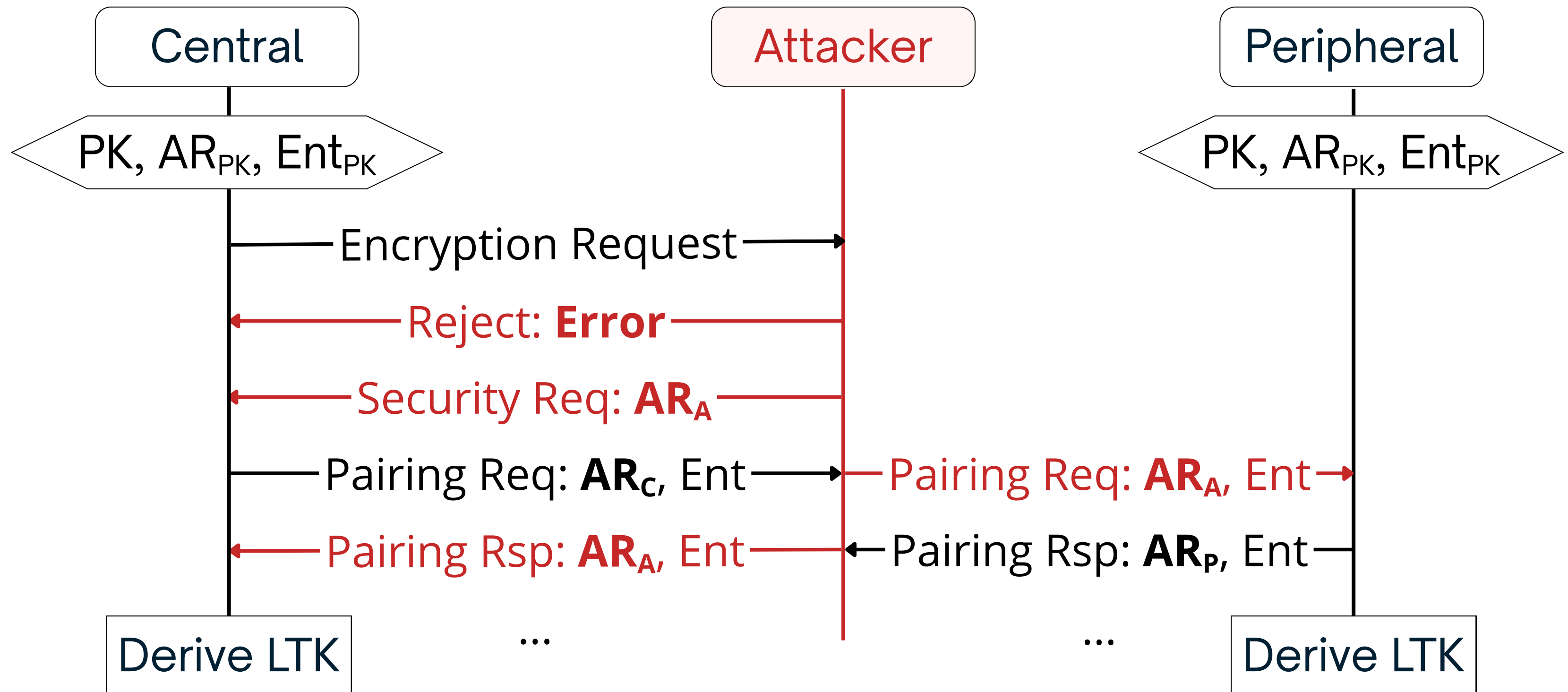
Takeaways

Vendors → harden stacks, update threat model

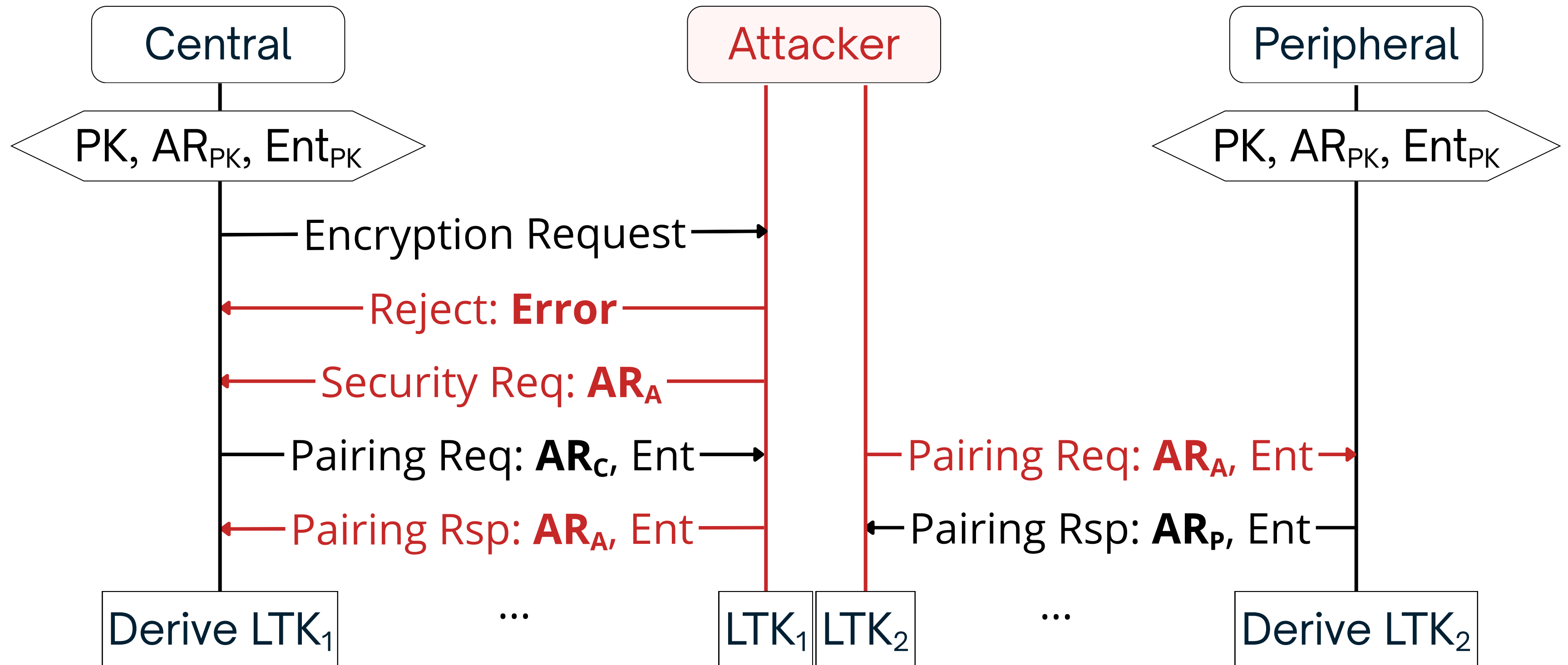
Bluetooth SIG → re-design their security protocols

BACKUP SLIDES

BLERP Single-Channel MitM



BLERP Double-Channel MitM



BLERP Toolkit

Reproducible, low-cost and open-source testing tool

- Hardware:
 - Nordic nRF52
- Software:
 - Mynewt/NimBLE with custom HCI, LL and SMP hooks
 - Python-based BLE Host with MitM orchestration

BLE Session Establishment

