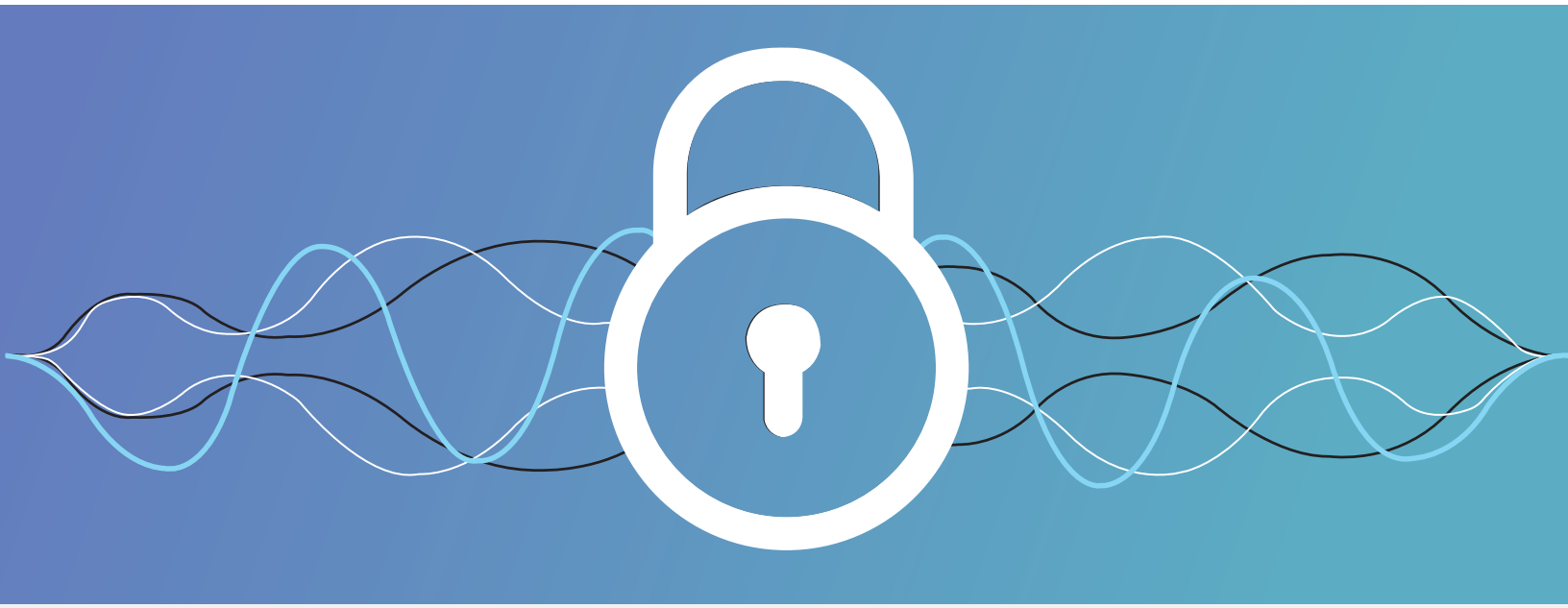
LISNR Tone Lock

The following attacks can be orchestrated by fraudulent parties at the expense of merchants and consumers.

Man in the middle attacks: Personal or sensitive data is read by unwanted devices, potentially used for setting up fraudulent accounts, stealing credit card information, trolling, etc.

Replay attacks: Signal transmissions are recorded and reused for verification through a listening device for authentication and payment.



Key Attributes

- Transmission sequence allows verification of intended receiving device prior to exposing sensitive data
- Supports RFC4122 compliant 16 byte UUIDs for device authentication
- Mismatched UUID shuts down processing within a single transmission prior to demodulation
- Data cannot be read by devices without the matching UUID
- With frequent or dynamic UUID issuance, precaptured or recorded data cannot be used to manipulate transactions without sharing the correct dynamic UUID

Benefits

- Prevents sensitive data from being read by unintended devices
- Secure well understood industry standard validation. Familiar customer implementation.
- Avoids needing additional OTP verification transmissions prior to sending sensitive payload data
- Stops signal snooping where sensitive data is compromised (man in the middle attack)
- Stops recorded or stolen validation payloads from being used for fulfillment (replay attacks)

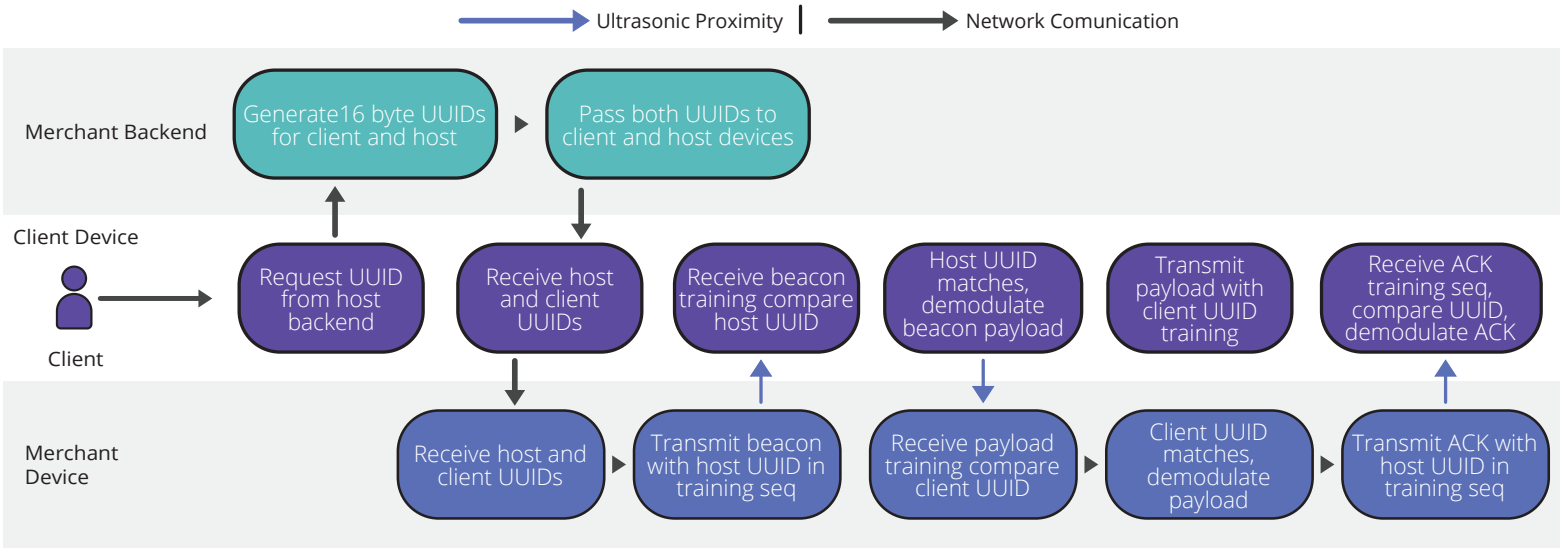
The Solution: Tone Lock

LISNR Tonelock protects against outside devices reading sensitive data by transmitting a pre-shared UUID within the transmission training sequence from the transmitting device to its intended receiving device. Without an exact match of the pre-shared UUID to the UUID embedded in the signal header, the receiving device will not demodulate the transmission and no payload data will be read.

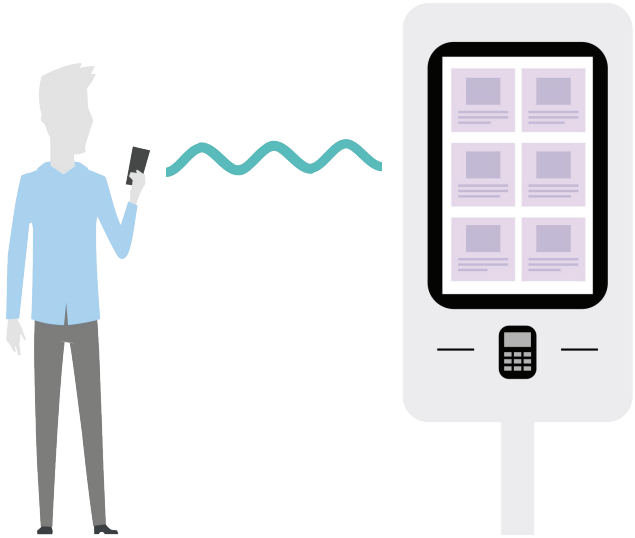
Security level protection of Tone Lock is dependent on the frequency of UUID issuance from the merchant network. One-time or infrequent issuance will protect from a man in the middle attack from a fraudulent party trying to read payload data from an active transmission. Frequent UUID issuance or issuance for individual transactions will protect against man in the middle and replay attacks, where a fraudulent party records and reuses the transmission for authorization or payment.

With Tone Lock enabled, devices are designated and secured for the data transmission, avoiding man-in-the-middle attacks from other devices running the LISNR SDK and replay attacks, from transmissions being recorded and reused.

Tone Lock Process Flow with 2.1



Tone Lock Use Cases:



- **Click and Collect (BOPIS, Curbside)**
- **In Aisle Pay**
- **Peer to peer**
- **Mobile Ordering**