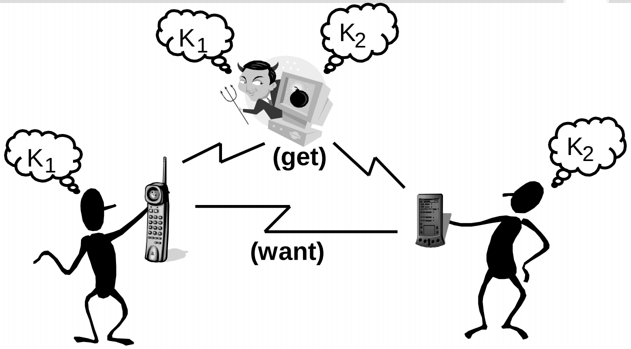
Security and Privacy Issues in Wireless Applications

Markus Jakobsson, Burt Kaliski,
Jan-Ove Larsson, Susanne Wetzel
RSA Laboratories

The Problem of Pairing



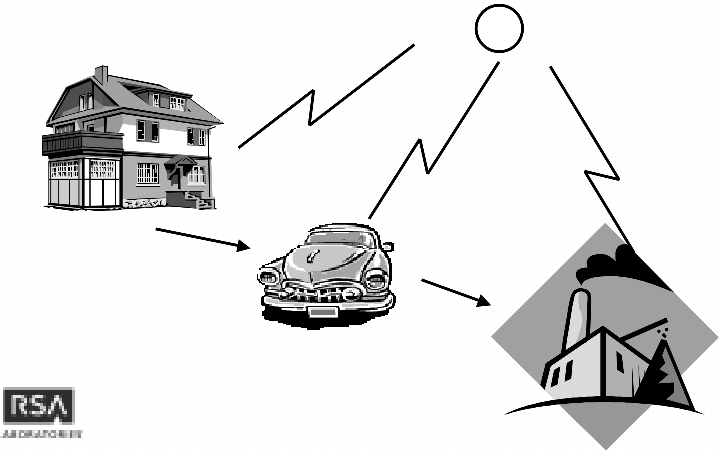
Key pairing problem ($K_1 \overset{?}{=} K_2$)

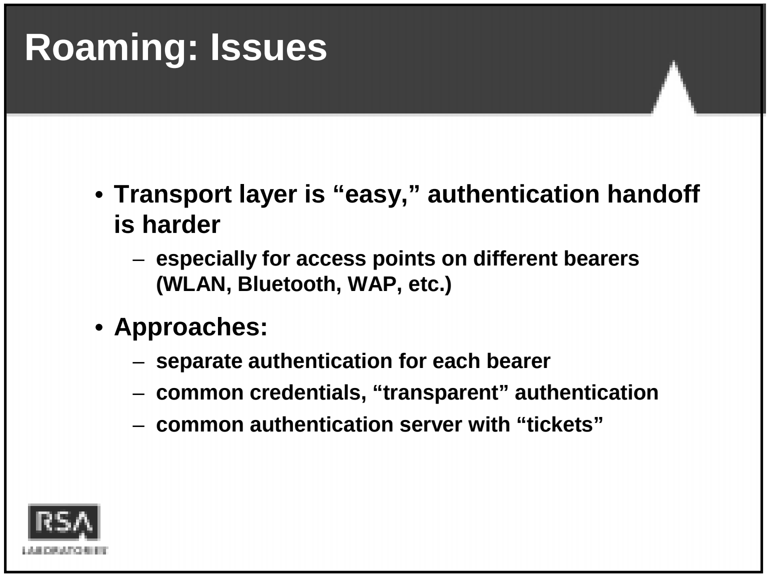
(verify no man-in-the-middle present)

Pairing: Issues

- Ad hoc pairing of devices
  - no prior shared secrets
  - no prior references
- General approach: User enters PIN into each device
- Various handshakes, with increasing security:
  - PIN, key exchange in clear
  - PIN-based challenge-response
  - PIN exchange under ephemeral Diffie-Hellman secret
  - PIN-authenticated Diffie-Hellman (e.g., SPEKE)
- Alternate approach: Confirmation codes

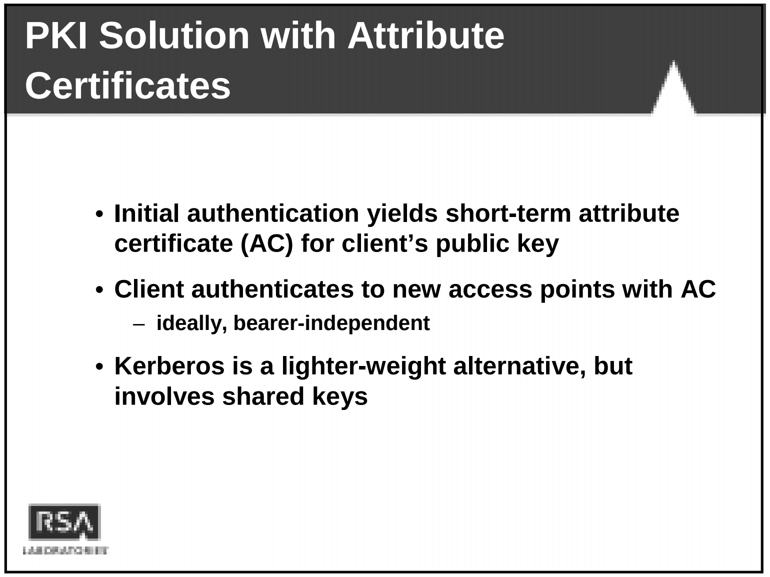
Roaming Across Different Access Points





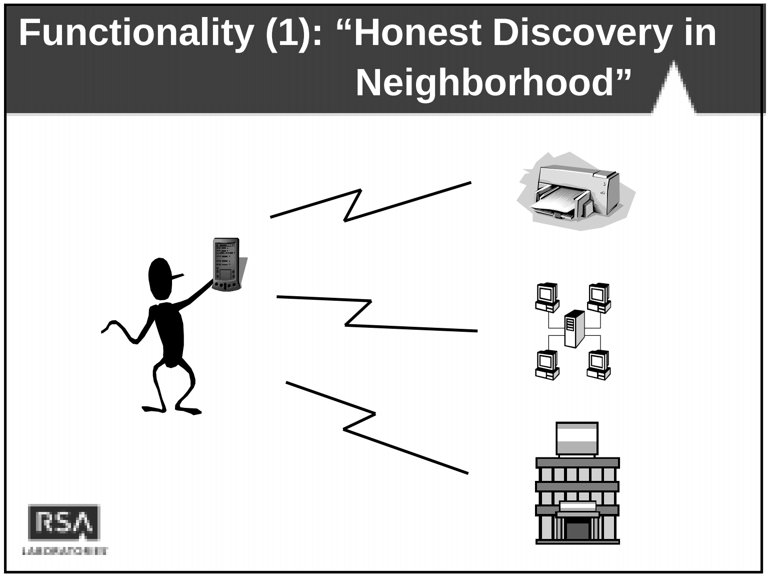
Roaming: Issues

- Transport layer is “easy,” authentication handoff is harder
  - especially for access points on different bearers (WLAN, Bluetooth, WAP, etc.)
- Approaches:
  - separate authentication for each bearer
  - common credentials, “transparent” authentication
  - common authentication server with “tickets”

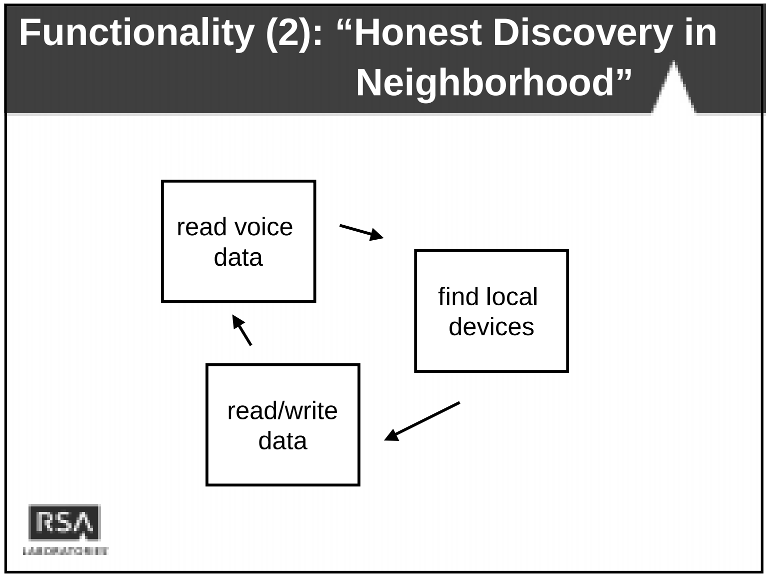


PKI Solution with Attribute Certificates

- Initial authentication yields short-term attribute certificate (AC) for client’s public key
- Client authenticates to new access points with AC
  - ideally, bearer-independent
- Kerberos is a lighter-weight alternative, but involves shared keys



Functionality (1): “Honest Discovery in Neighborhood”

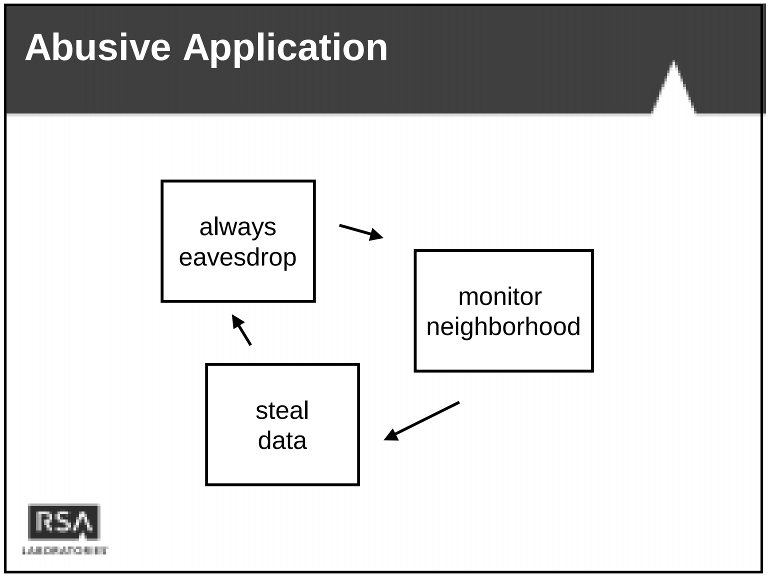


Functionality (2): “Honest Discovery in Neighborhood”

read voice data

find local devices

read/write data

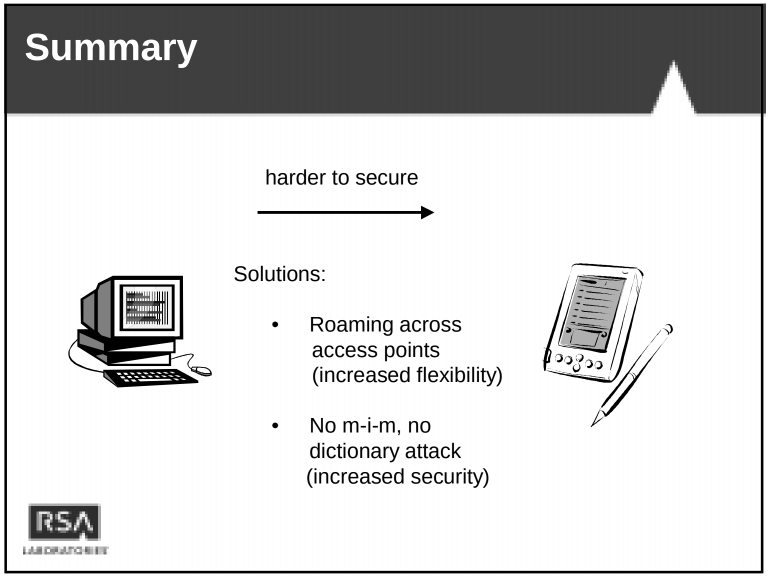


Abusive Application

always eavesdrop

monitor neighborhood

steal data



Summary

harder to secure

Solutions:

- Roaming across access points (increased flexibility)
- No m-i-m, no dictionary attack (increased security)