Security and Privacy

Spontaneous interoperation

Privacy concerns about sensing

Hardware issues

- Portable devices can be more easily stolen and tampered with
  - Do not rely on the integrity of any subset of devices that could be feasibly compromised
  - Require presence in multiple locations at the same time
- Not sufficient computing resources for asymmetric (public key) cryptography
  - Which nodes share the same symmetric key?
  - Share with neighbours and rely on chains of mutually trusting nodes
- Energy is an issue
  - Sleep deprivation torture attack
- Avoid security protocols that rely on continuous online access to a server
  - Certificates

Secure spontaneous device association (1)

- Secure exchange of a session key for communication encryption
  - No trusted third party – man in the middle attack
- Out of band communication
- Physically constrained channel
  - Location limited channel
  - Side channel with certain physical properties
  - Receive constrained channels
    - Physical contact, Infrared, Audio, Laser, Barcode and camera
  - Limited degree of security, but when appropriately deployed attacks entail considerable effort
- Send constrained channel
  - Physically authenticate one device's public key

Secure spontaneous device association (2)

  - It is possible to implement a send constrained channel using a receive-constrained channel
- Optimistic but insecure key exchange and use of physically constrained channel for key validation
  - Diffie-Hellman protocol over physical and human mediated device association techniques
  - Use of send/receive constrained channels to validate the association by comparing secure hashes of the keys
    - Displayed hashes, or ultrasound
- The security achieved is only as good as the trustworthiness of the devices involved
- Resurrecting duckling protocol
  - Imprinting and killing the ducklings soul

Location-based authentication

- Controlling access to people physically in the smart space
  - Physically constrained channel that pervades the smart space but does not reach beyond it
  - Location authentication proxy
    - Trusted by location-specific services, connected to the channel
  - Temporally constrained channel implemented using ultrasound to verify location claims
  - Clients may still be malicious

Privacy protection (1)

- User provide identifiers of various kinds to smart spaces when they visit them and access services there
  - Names and addresses in service accesses
  - Bluetooth devices maintain constant MAC-level address visible to other devices and access points
  - RFID tags may be sensed at doorway and other pinch points for tracking or identifying objects the user carries
- Replace hard-wired identifiers with soft addresses
  - MAC addresses: tradeoff between communication disruptions and privacy
  - RFID tags: use one way hash functions to replace the stored identifier and to generate the emitted identifier each time it is read

PRIVACY PROTECTION (2)

- Software identifiers: anonymous identifiers or pseudonyms
  - Privacy proxy – central point of vulnerability
  - Traffic analysis is still a problem
    - Mixing – overlay network of proxies
- Obscure user location by exploiting the presence of many users
  - Mix zones: regions where users do not access location-aware services where they can their pseudonymous identities