Attestation
Center for Embedded Networked Sensing
Jonathan Yang
Urban Sensing

- Utilizes software and network technology to enable mobile devices such as smart phones to act as credible sensors in environments.

- Smartphones gather sample data with sensor and send to database. Data can be used for various studies.

- Example: Sound level mapping campaign for LA
  - Phones gather data samples, which include decibel level of sound. Samples are kept in database.
  - Helpful towards urban planners and developers.
  - Helpful for monitoring quality of life in city
Attestation Concept

• Location credibility equally as important as gatherer’s identity.
• Phones use GPS to measure location.
• Data from phone is sent to database via Wi-Fi.
• GPS location of the access points are known.
• Attestation is the network ability to attest to the location measured by the phone is within a certain radius from the access point location.
  - Used as an added layer of correctness and credibility.
  - Not designed to prevent hackers.
Network Infrastructure

- Two identical wireless mesh networks on UCLA campus.
- Each mesh has a root access point which is wired to the router.
- Network hardware donated by Cisco.
  - Devices use proprietary protocols for communication.
- Key network software
  - Campaignr: Application on the smart phones that gathers sensor data. Sends packets to database via Wi-Fi.
  - Perff: Database which collects sensor data for the various campaigns.
Network Map
Attestation Approach

- GPS location of access point is associated with AP’s MAC address.
  - Linking to IP would be too volatile.
- All packets sent from Campaignr must utilize one AP to reach the database.
- Verification calculation is achievable once the MAC address of the AP used for connection is known.
- Due to link layer protocol, the MAC address of any network node is in the packet only when the packet is being transmitted through the node.
One Possibility

- The mobile device must know the MAC address of the AP in order to send the packet.
- Use Campaignr to include the MAC address into the sensor data payload.
- Reasons why this approach was not taken:
  - Very difficult to program on Symbian OS.
  - Did not want to break existing functionality in Campaignr.
Extracting the MAC Address

- Due to Cisco proprietary protocol, it was unclear to which device could see the AP MAC address in the packets.
- Port mirrored traffic from multiple devices to a separate computer.
- Used Wireshark to analyze packet data.
- Concluded that the router was the only device that could obtain the AP MAC address.
Attestation Design

- Information about packet known by Perff
  - Source and Destination IP / port
  - Packet checksum
  - Packet timestamp
- Intercept packets at router and filter relevant traffic.
- Create a separate database with information about packet known by Perff as well as the MAC address of AP used by the packet.
- Perff can find matching packet entry in this database and obtain MAC address of AP.
Herbivore

- Herbivore is a program that intercepts router traffic and creates the separate database.
- Runs on a dedicated machine with network traffic mirrored from router.
- Uses `pcap` library in C to sniff packets on the network.
- The packets have eight separate layers and desired information is located in innermost layers.
- Must parse packet one layer at a time to extract needed fields.
- As of the end of the winter quarter, application was still in development.
Acknowledgements

Deborah Estrin
Jeff Burke
Jason Ryder
Vidyut Samanta
Ryan Dorn
Richard Guy
Derek Kulinski
Questions