LoKI: Location-based PKI for Social Networks

Randy Baden
http://www.cs.umd.edu/~randofu/loki
Sigcomm 2011 in Toronto, ON
August 16, 2011

This work is supported by NSF grants
CNS-0917098 and IIS-0964541

Goal

Build a PKI for online social networks by using real-world meetings as a way to verify identity.

Insight

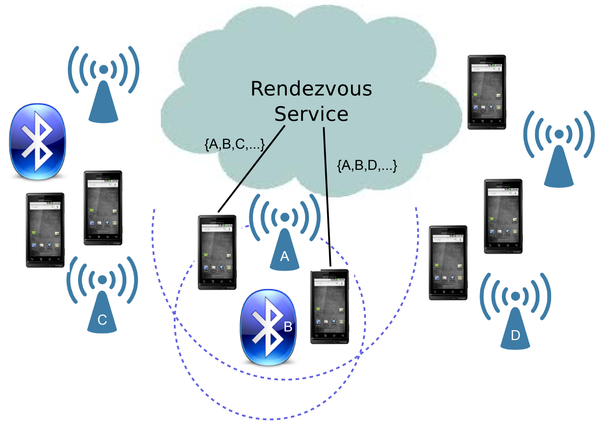
Shared secrets exchanged between proximal mobile devices via bluetooth can later be used in-band for the purposes of identity verification. The user need only remember when the real-world meetings with that user occurred.

Mobile P2P

Most android devices (< 3.1) can only communicate in the background if one device can somehow learn the other's bluetooth MAC address.

We do so with a **Rendezvous Service** that provides a form of location privacy.

The rendezvous service is a general service that matches users to each other based on some set of attributes or tags. In this case, we match based on colocation, inferred from shared visible wifi and bluetooth MAC addresses..



The rendezvous service:

- Matches proximal devices to each other based on visible wifi and bluetooth MAC addresses
- Does not learn the device's bluetooth MAC address and cannot associate a device to a location; only someone with knowledge of the visible MAC addresses at a location can recover the device's MAC address.

Protocol

Let:

$H(\cdot)$ be a one-way hash function.
$E(\cdot, K)$ be encryption with symmetric key K.
$S(\cdot, \cdot, k)$ be the function to produce a secret share for Shamir's Secret Sharing s.t. k shares can reconstruct the value.

Then for each epoch t, for each visible wifi and bluetooth MAC address M, the device with bluetooth MAC address B publishes to the rendezvous service :

$\cdot H(M \circ t)$
$\cdot E(S(B, M \circ t, k), M \circ t)$

The rendezvous service can match and return requests by comparing the hashes of the MAC addresses to ensure they have a suitable number of matches.

Only others who know the visible MAC addresses at that location at that time can decrypt the secret shares and reconstruct the device's bluetooth MAC address.

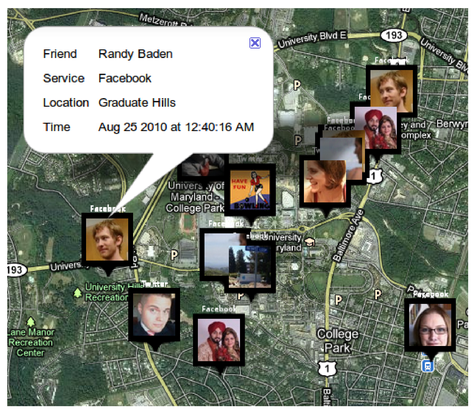
Ongoing Experiments

Do social network friends meet in person?

We've collected user-supplied checkin data on Facebook, Twitter, and Foursquare.

Twitter locations are too coarse-grained, and Foursquare does not provide friend checkins. We have checkin data for 1033 Facebook users, but find almost no spatial and temporal matches between users because of the sparse nature of manual checkins.

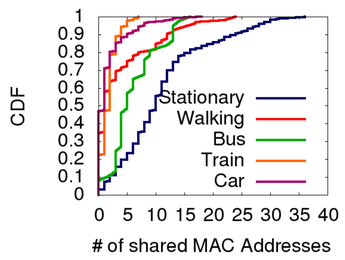
One notable exception: one user had checkins that match for 7% of his friends; this is due to the ability to tag friends in checkins. We will explore this feature of the Facebook data further to estimate the relationship between social networking and real-world meetings.

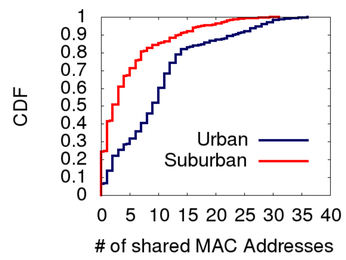


https://bowser.cs.umd.edu/locus

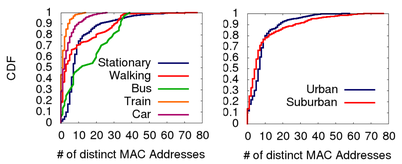
Do proximal mobile devices see the same MAC addresses?

We have collected wifi scans and bluetooth inquiries from two Motorola Droids kept less than a foot apart, while simultaneously tracking GPS location. We classify each sample for each unit of time according to how we are moving at the time and according to the estimated population density of the space that we're moving through.

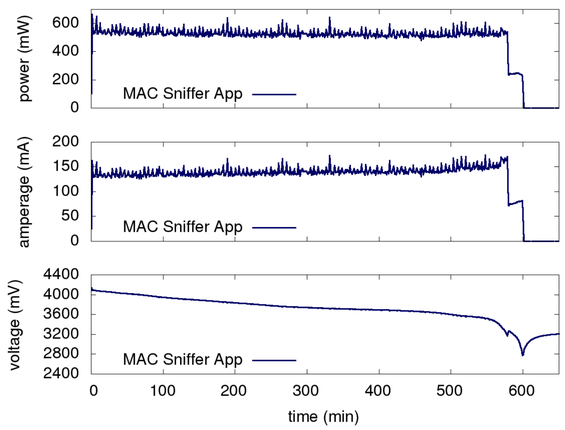




We expect most meetings to occur in stationary settings, so there usually are a sufficient number of MAC addresses seen by both devices even though there are also many that are seen by only one device.



What are the resource requirements on the phone?.



Naively scanning for wifi and bluetooth MAC addresses every 30 seconds drains the phone's battery in about 10 hours, compared to specifications of 6.4 hours of talk time and 11.3 days of standby.