Location Services with Built-In Privacy

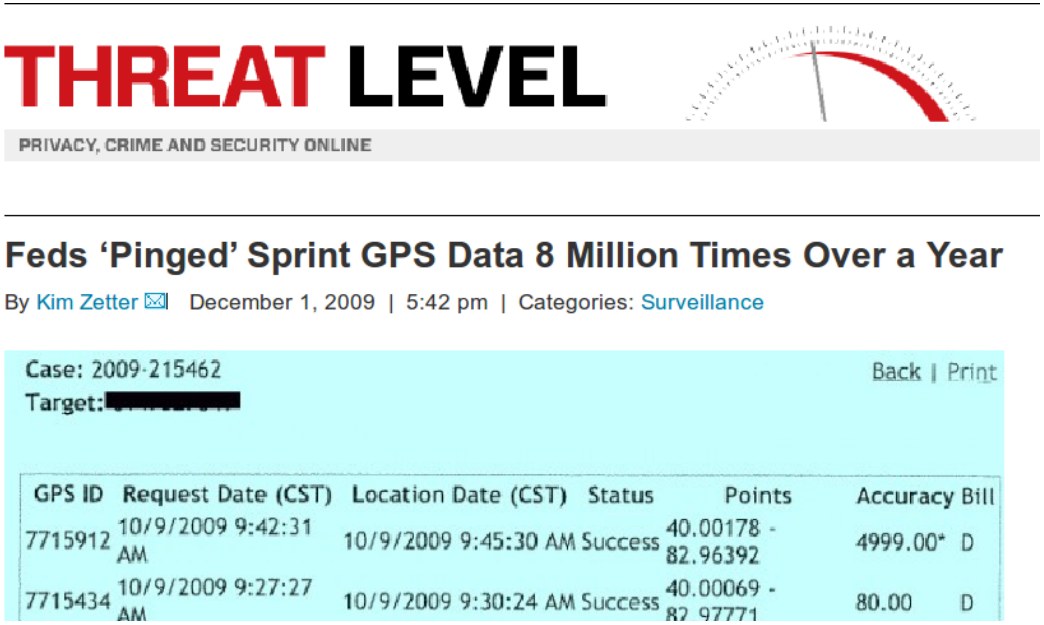
Arvind Narayanan
Stanford University

Joint work with Narendran Thiagarajan, Mugdha Lakhani, Dan Boneh

Location-based social networking

Finally taking off?

Why Privacy?



THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year

By Kim Zetter ✉ December 1, 2009 | 5:42 pm | Categories: Surveillance

Case: 2009-215462 Back | Print

Target: [redacted]

GPS ID	Request Date (CST)	Location Date (CST)	Status	Points	Accuracy	Bill
7715912	10/9/2009 9:42:31 AM	10/9/2009 9:45:30 AM	Success	40.00178 - 82.96392	4999.00*	D
7715434	10/9/2009 9:27:27 AM	10/9/2009 9:30:24 AM	Success	40.00069 - 82.97771	80.00	D

EFF, tech companies lobbying for ECPA revision

Why do service providers care? Positive externality

What can we do privately

Proximity testing: detect when friends are nearby

When not nearby, friends don't see your location

Server never sees location

Building block for more complex functionality

Proximity testing: some applications

Granularity must be user-configurable

Client-server vs. peer-to-peer

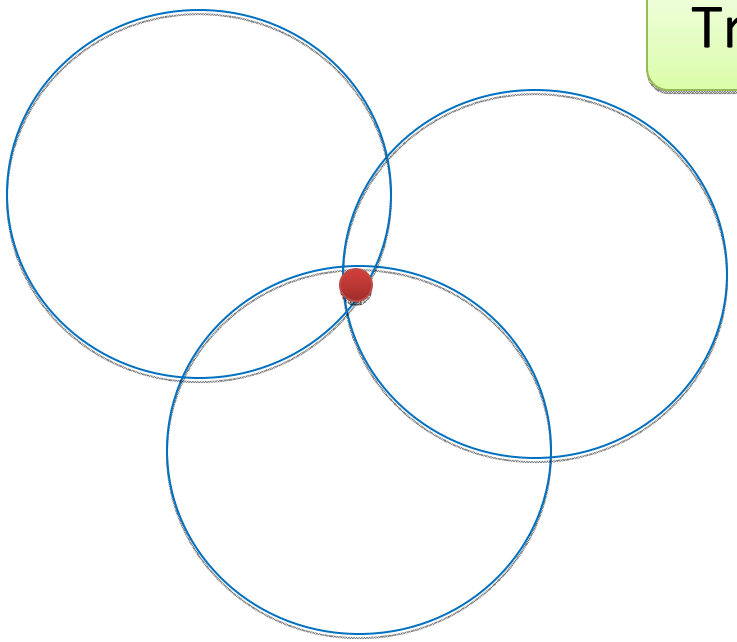
	All-pairs	Friends-only
Client-server	✗	✓
Peer-to-peer	✓	✗

Only client-server model supports configurable granularity

Poor/nonexistent infrastructure for complex peer-to-peer protocols

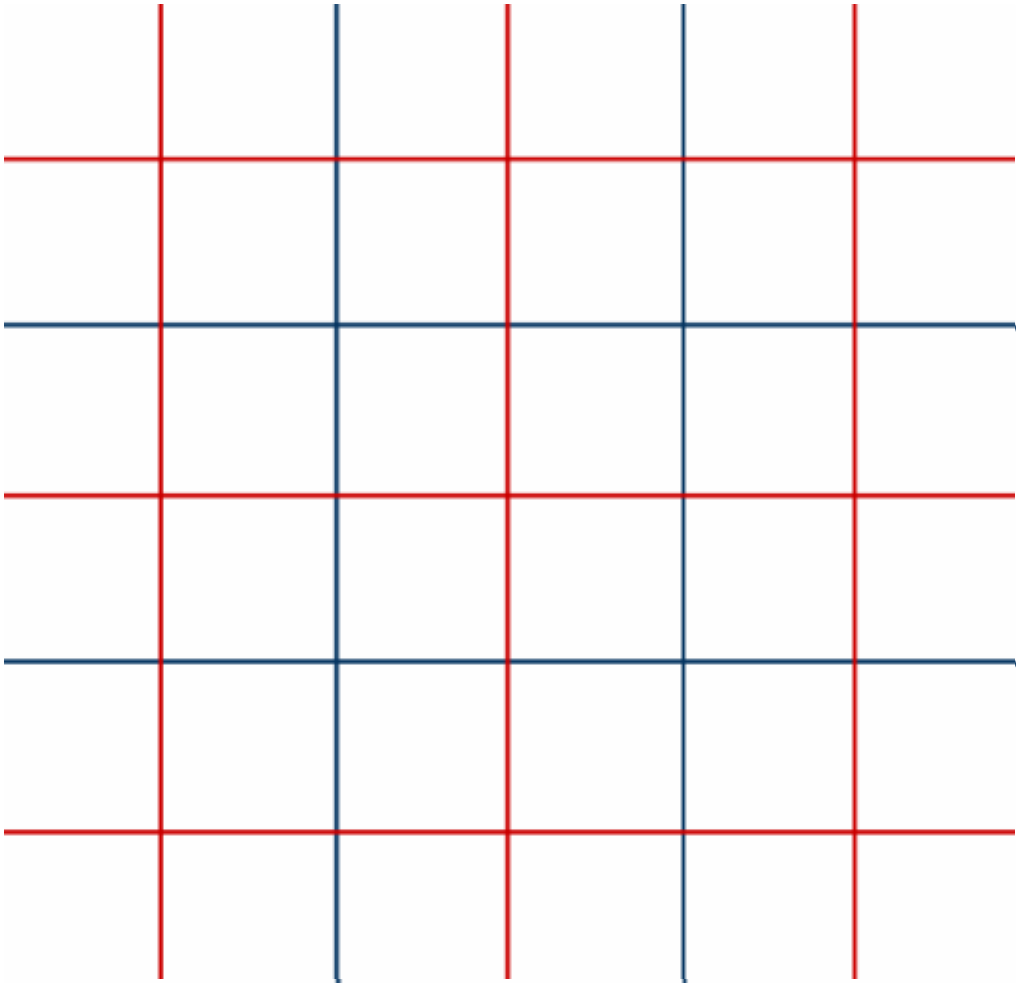
Mathematical formulation: not obvious

"Pairs of friends get notified whenever they are within 100ft of each other"



Triangulation attack

Reducing proximity testing to equality testing



Equality testing

x $\stackrel{?}{=}$ y

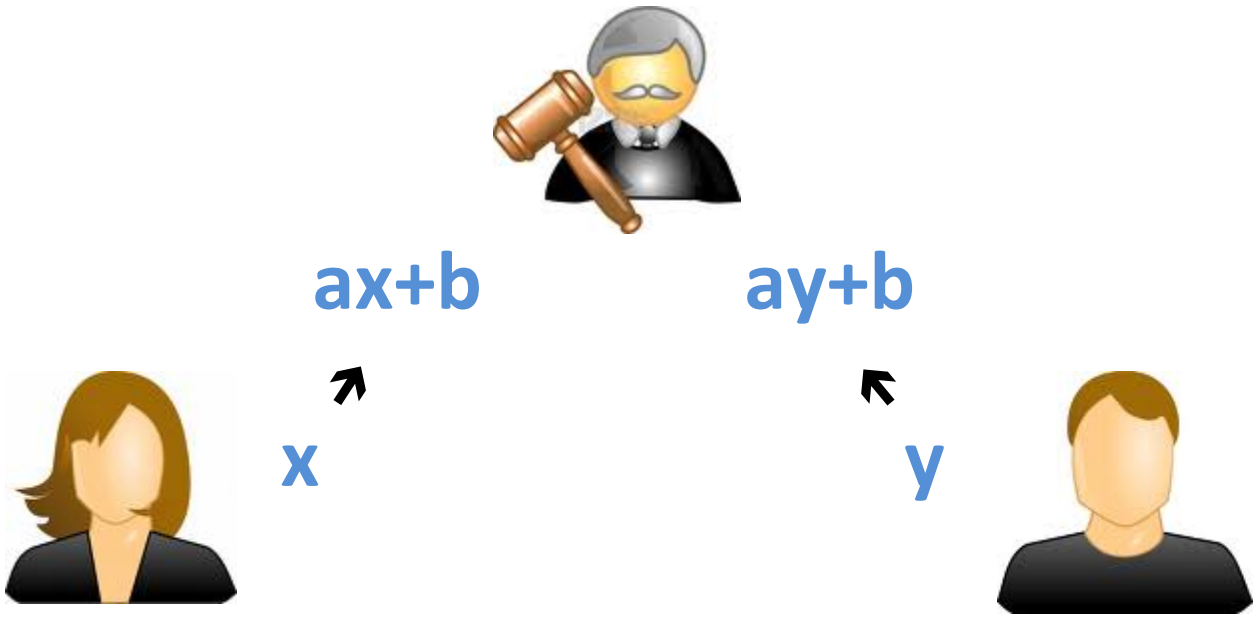
Space of possible locations is small!

ElGamal-like cryptographic protocol based on
Decisional Diffie Hellman (DDH) problem (Lipmaa)

Improved constant factor

Requires shared secret keys between pairs of friends

Server participation



Server can pretty much learn everyone’s location

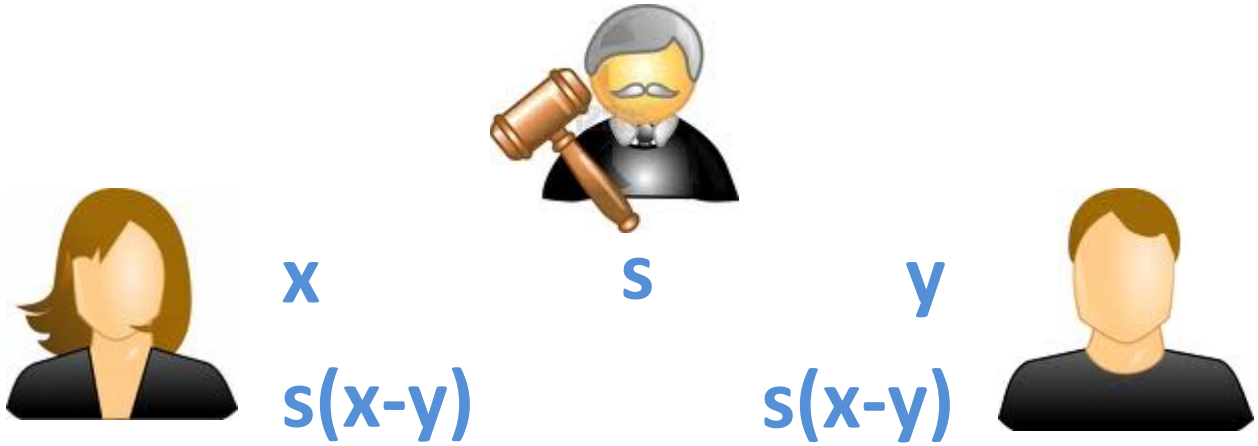
Server participation done right

Server can cause users to compute wrong answer

but cannot cause privacy breach

Avoids need for big integer arithmetic

Information-theoretic security



Problem: online brute-force attack

If only there were a way to verify that a user really is where they claim to be…

Location tags

Shared entropy pool

Properties of location tags

Location tag = vector + matching function

i.e., space-time fingerprint

Unpredictability

cannot produce matching tag unless nearby

Reproducibility

two devices at same place & time produce matching tags (not necessarily identical)

Location tags using WiFi packets

Discard packets like TCP that may originate outside local network

- DHCP, ARP, Samba etc. are local

15 packets/sec on CS/EE VLAN

Two different devices see about 90% of packets in common

Protocol	Device 1	Device 2	Common
ARP	1088	1071	832
BROWSER	262	286	255
DHCP	249	237	208
MDNS	600	551	541
NBNS	1134	1190	1117
All	3333	3335	2953

Location features

Each packet is a “location feature”

Timing, source/destination and other packet contents

At least around 10 bits of entropy

Tag with 15 location features gives > 80-bit security level

Comparing location tags

Need to compare two vectors that match approximately: fuzzy set intersection

Basic concept:
Alice encodes vector as polynomial
Sends random points on polynomial to Bob

Intersection size is large → few enough "errors" →
Bob can decode using Berlekamp-Massey algorithm

Shared secret keys

Traditional solution: PKI

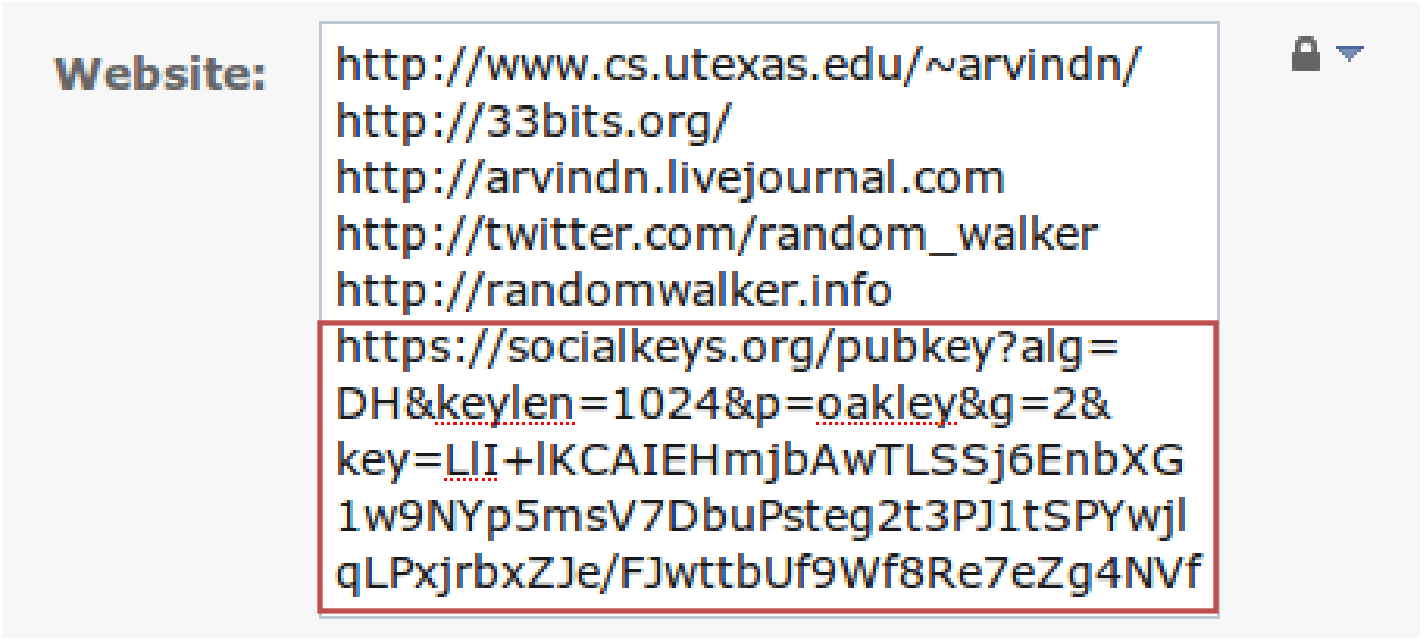
PGP (un)usability study

Better solution: Identity-based encryption

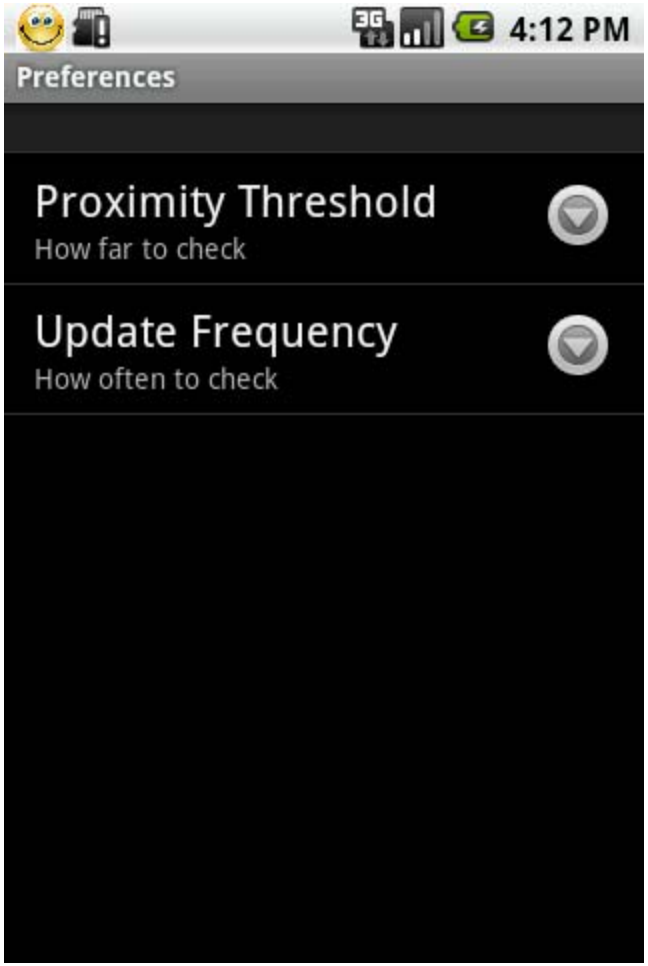
Our solution: bind public keys to social identities

SocialKeys

My Facebook profile

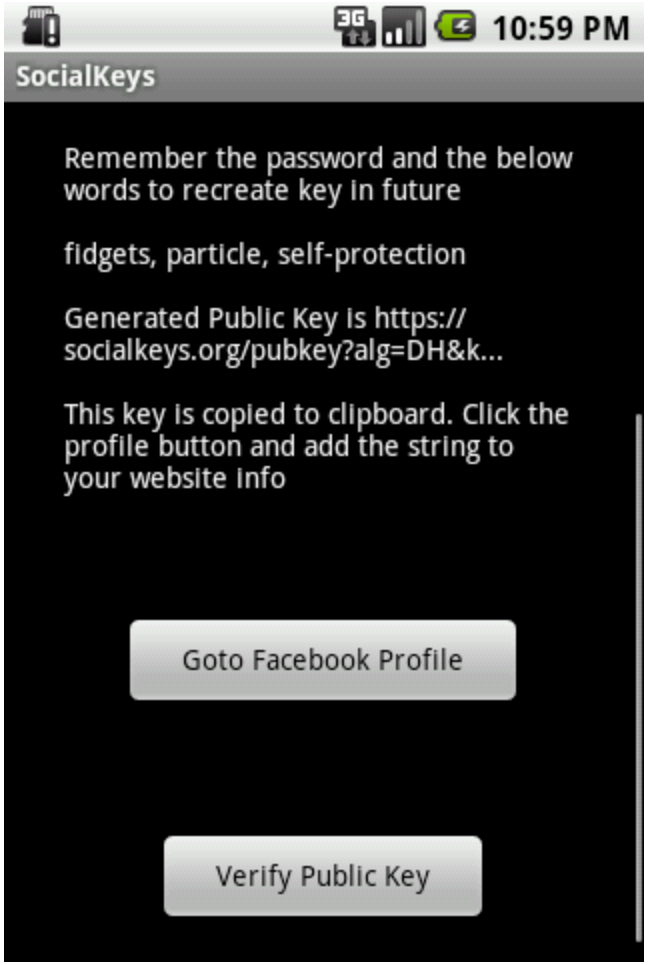


Android implementation

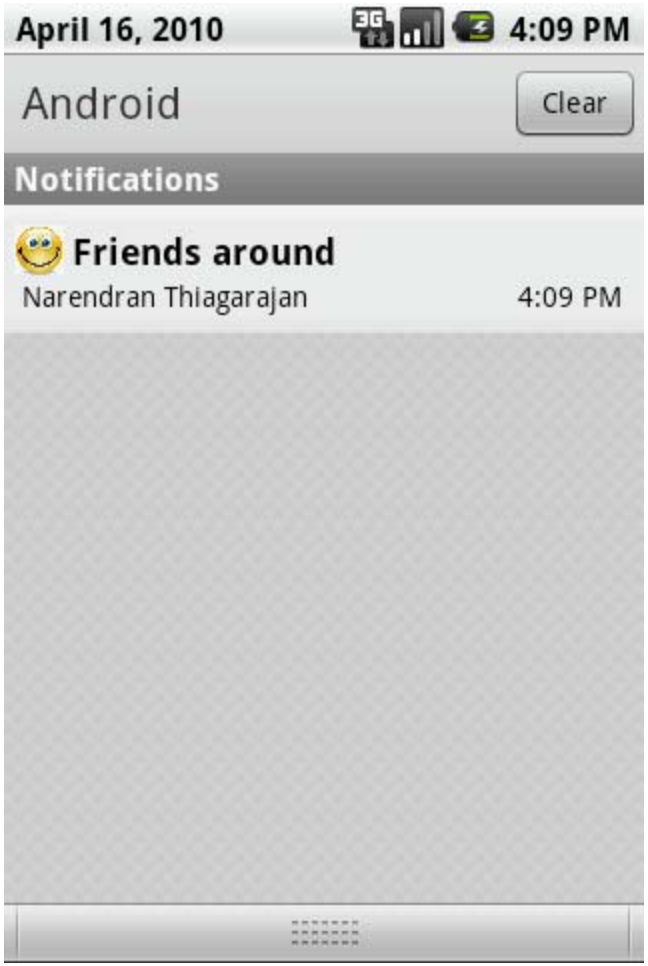


Android implementation

Android implementation



Android implementation



Other location privacy questions

Location based advertising

Location based search

Location statistics

Summary

Proximity testing: useful primitive, tricky to define!

Improve constant factor in crypto protocols for Private Equality Testing

Location tags to enhance location privacy

SocialKeys: transparent crypto via key sharing over social networks

Thank you