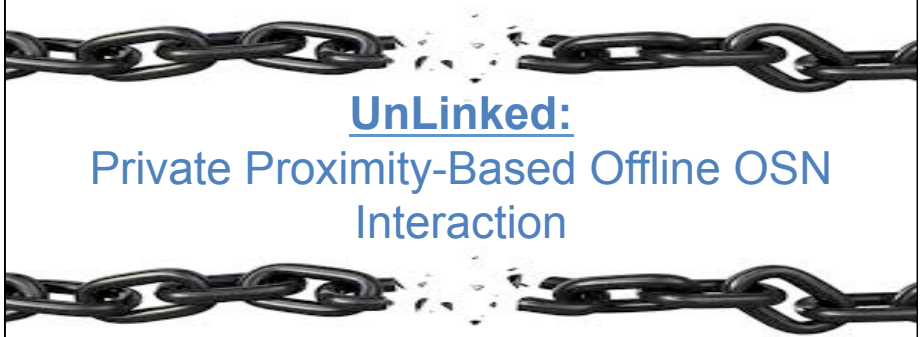
UCI University of California, Irvine



UnLinked:
Private Proximity-Based Offline OSN Interaction

G. Tsudik (CS@UCI)
gene.tsudik@uci.edu
Joint work with R. Petrlic (Univ. of Saarland) and S. Faber (UCI)

1

UC Irvine

Current Research

- Privacy in Social Networks
  - Stylometric Linkability and Attribution
  - Off-Line Networking via Cryptographic Techniques
- Genomic Privacy
- Security of Embedded/IoT Devices
- Private Database Querying
- Usable Security
- Biometrics
- S&P in Future Internet Architectures

For more info: **sprout.ics.uci.edu**

2

UC Irvine

Outline (privacy-preserving)

- Topic 1
- Topic 2
- Topic 3
- …
- …
- …
- Summary

3

UC Irvine

Today's OSNs

- Facebook, RenRen, Tumblr, VK, LinkedIn, etc.
- Global heaven for voyeurs and exhibitionists
- Percolated into many aspects of life
- Enormous worldwide popularity
- Membership leads to many other services
- Reached the limit of penetration
- **What's next?**
- OSN for pets? Inanimate objects?
- Ventriloquistic operation

4

UC Irvine

My $0.02:

- Off-line OSN support
- OSN for the dead

5

UC Irvine

OSN PRIVACY?

- Lots of righteous noise about lack of privacy
- Is it reasonable to expect it?
- Expecting total (even strong) privacy is silly…
- How about at least some?
- What/who to blame for lack of privacy?
  - Ignorant user? Centralization?
- Distributed (p2p) OSNs have been proposed
  - e.g., DIASPORA, SAFEBOOK
  - unlikely to succeed

6

UC Irvine

Why Offline OSN Interactions

Want limited OSN functionality in case of:

- Poor connectivity: low bandwidth, intermittent, lossy (lousy?) links.
- Expensive connectivity: e.g., abroad, on trains, planes and cruise-ships.
- No connectivity: e.g.: in air, under water, under ground, EMI-shielded environments, remote locations, disasters.
- OSN service outage
- Personal preference not to connect to OSN, i.e., want to use OSN in off-line mode

7

UC Irvine

Offline Interactions (1)

Scenario 1:

1. Alice and Bob meet (physically)
2. They talk
3. Discover some common factors
4. Both decide to later connect (good for OSN)

   Or
5. Nothing further happens because:
   - Neither is interested
   - One is interested, the other isn't

NOTE: OSN learns nothing if (5)

8

UC Irvine

Offline Interactions (2)

Scenario 2:

1. OSN USER X and OSN USER Y meet
2. They discover common factors
3. If mutually sufficient, they reveal themselves as Alice and Bob
4. They talk
5. Both decide to later connect (good for OSN)
   Or
6. Nothing further happens because:
   – Neither is interested
   – One is interested, the other isn't

NOTE: OSN should ideally learn nothing if (6)

9

UC Irvine

Claim

Private off-line OSN interactions are good:

- For OSN users

and

- For OSN itself

10

UC Irvine

Generic Scenario

- Alice and Bob are near e/o
- Unaware of e/o identities
- Discover e/o presence as OSN* users
- Privately compare their profile features, determine common factors or # thereof
- If insufficient, drop it
- Otherwise: reveal identities, chat, record

…

- Optionally connect on OSN

11

UC Irvine

Whose job is it?

- OSN itself

OR

- Separate service

12

UC Irvine

Who are you?

- On the Internet, no one knows you're a hog (or a dog)
- Off-line OSN user can be anyone, could claim arbitrary friends/connections
- Need authenticity & integrity of OSN profiles
  - Motivates new service

13

UC Irvine

UnLinked Design Goals

1. Support for Off-line Interaction
2. Anonymity wrt Peers (debatable)
3. Profile Privacy wrt Peers
4. Interaction Privacy wrt OSN provider
5. OSN Connection Spillover
6. OSN Profile Authenticity and Owner Authentication
7. OSN-Independent Operation
8. OSN-Agnostic Design
9. Voluntary Participation

14

UC Irvine

UnLinked – bird's eye view

LinkedIn: a somewhat "professional" OSN

Android smartphone platform

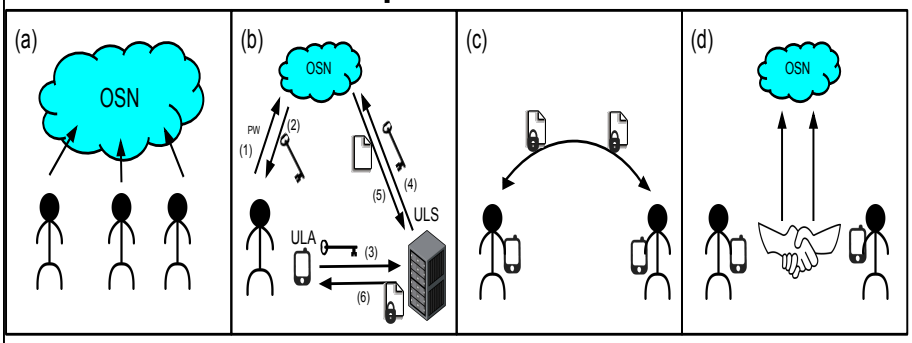
Components:

- UnLinked App (ULA):
  - ATW-PSI and ATW-PSI-CA
  - Android framework
  - Bluetooth communication
- UnLinked Server (ULS): CA, reg-n, OSN i/f

15

UC Irvine

Operation



In online phase (b):

- Alice installs ULA (UnLinked App)
- Alice logs into OSN
- ULA contacts ULS, provides OAuth
- ULS pulls profile, extracts features, signs/certifies, returns

16

UC Irvine

More Details

- OSN independence
  - OAuth token
  - Profile API
- Communication medium independence
  - Broadcast channel
- Off-line, proximity-based
- Underlying PSI/PSI-CA protocol independence
  - We use OPRF-DH-based PSI, can also use GC or HE
  - Need to convert to two-way and introduce authorization

17

UC Irvine

Protocol Properties

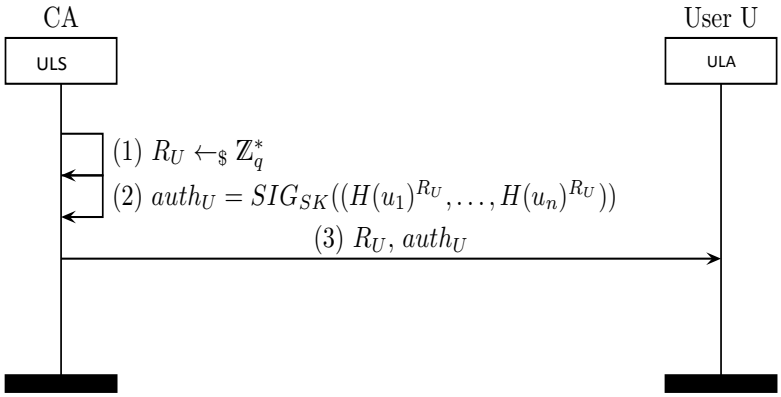
- Correctness
- Peer Input Privacy
- Pseudonymity
- Authenticity
- Input Binding (for 2-way)
- Output Integrity (beyond auth+corr)
- Early Termination Resistance

18

UC Irvine

On-Line ULA-ULS protocol

Part b in Operation

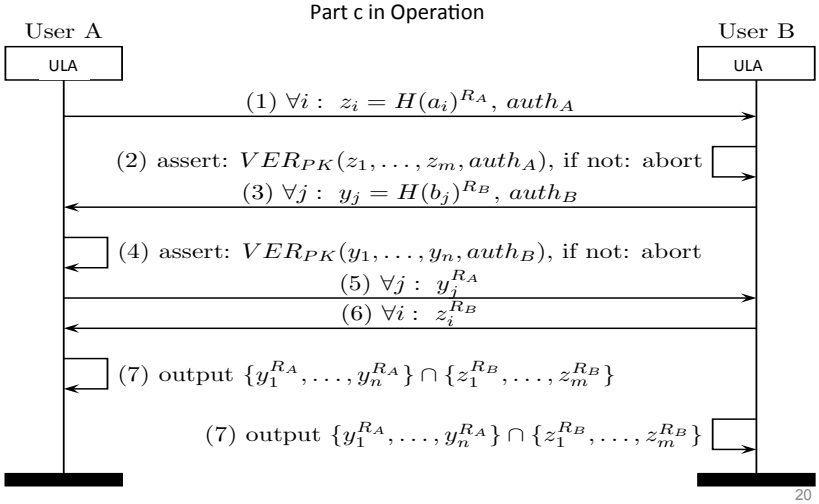


19

UC Irvine

Off-Line ULA-ULA protocol

Part c in Operation



20

UC Irvine

ATW-PSI

- Mirrored, two-way protocol that privately computes set intersection
- Each party has ULS-authorized input
- HbC model but extensible to malicious
- Assume ULA does not collude with ULS
- Internal adversaries (external trivial)
- Security based on OMG-DH in ROM

21

UC Irvine

ATW-PSI-CA

- Mirrored, two-way protocol that privately computes **cardinality** of set intersection
- Each party has ULS-authorized input
- HbC model but extensible to malicious
- Assume ULA does not collude with ULS
- Internal adversaries (external trivial)
- Security based on OMG-DH in ROM

22

UC Irvine

ULA Notification Policy

- Automatically notify user when criteria met (set by user)
  - Execute a more revealing protocol
  - Alert user to presence of peer
  - Request ID exchange
  - Send message(s) to peer
  - Receive/display messages and ID exchange requests
- Criteria – function on any protocol output
  - Presence of specific element in ATW-PSI
  - Threshold wrt size of ATW-PSI-CA
- Benefits
  - Spam/DoS prevention
  - Usability
  - Efficiency

23

UC Irvine

Policy contd.

Current Coarse-Grained Policies

- Open
  - Any other ULA user
- Low
  - At least one friend in common, and one school or employer.
  - At least three friends in common.
  - Common current employer or current academic institution.
- Medium
  - At least three connections in common, and at least one employer or academic institution, other than current one.
  - At least five connections and one institution in common.
  - More than seven connections in common

24

UC Irvine

Policy Management

- Policy is a complicated beast
- Alice and Bob can have many combinations of policies/thresholds
- Some policy combinations are incompatible

25

UC Irvine

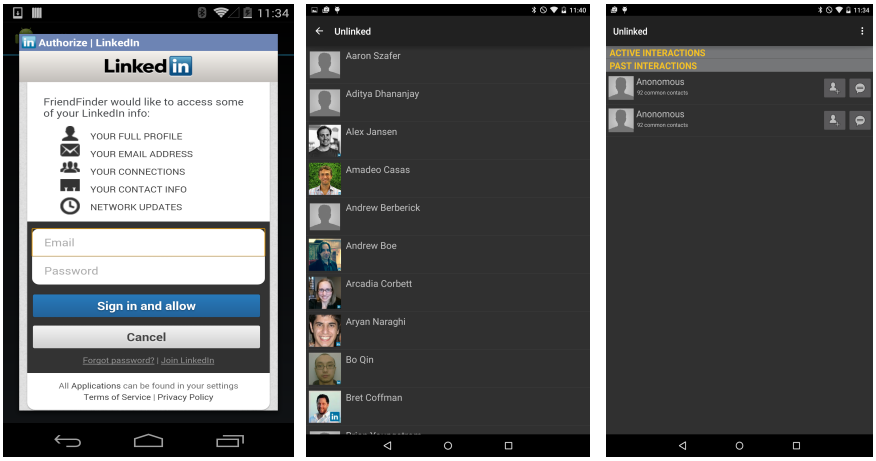
Performance Evaluation

Input Size	Setup Time (s)	Signature Size (kb)	Offline Time (ms)	Offline Band. (kb)
10	0.0739	3.41	143	9.2
100	0.837	25.2	508	75
1000	8.57	243	8790	2941
10000	86.4	2420	14530	7337

26

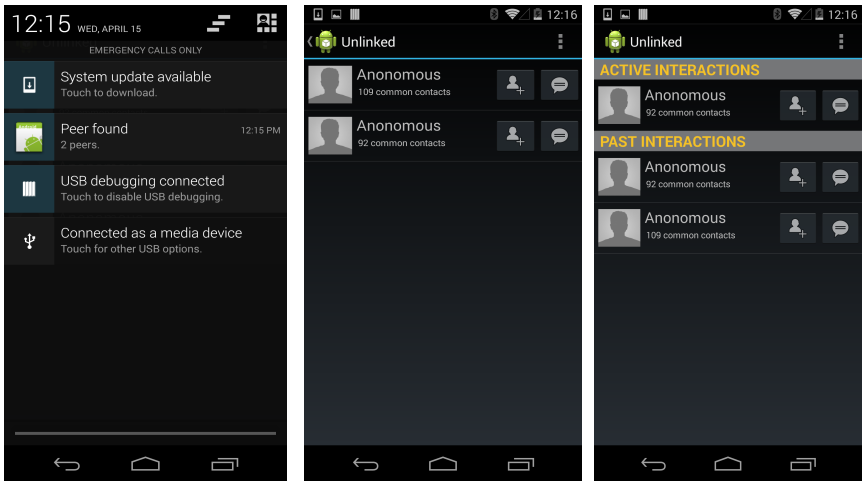
UC Irvine

Screenshots 1



UC Irvine

Screenshots 2



UC Irvine

Extensions

- Existing Friend Early Detection
  - Introduce oneself into set input to ATW-PSI
- Authenticated Channels
  - Start conversations with DH key exchange.
- Unlinkability
  - Download many authorizations
  - Need to modify network addresses
    - e.g., Bluetooth or WiFi MAC
- Detecting misbehavior via auditing
- WiFi Direct + IP
- Other OSNs, e.g., facebook
- Secret handshakes to obscure OSN affiliation

29

UC Irvine

Related Work

- M. Nagy, et al. “Do I know you? efficient and privacy-preserving common friend-finder protocols and applications”, ACSAC 2013.
- E. De Cristofaro, et al. “Private Discovery of Common Social Contacts”, ACNS 2011.

30

UC Irvine

Summary

- UnLinked: off-line private OSN interactions
- Reasonably strong privacy possible
- Is it desired? Need user studies & trials
- Bootstrapping problem
  - Ideally should run as independent service
  - But, being part of OSN would make it easier
- Lots of things left to do…

31

UC Irvine

QUESTIONS?

32