Leveraging Social Links for Trust and Privacy

Antonio Cutillo, Refik Molva, Melek Önen, Thorsten Strufe
EURECOM
Sophia Antipolis
refik.molva@eurecom.fr
Some side effects
Depressed woman loses benefits over Facebook photos

A Quebec woman on long-term sick leave is fighting to have her benefits reinstated after her employer’s insurance company cut them, she says, because of photos posted on Facebook.

Nathalie Blanchard, 29, has been on leave from her job at IBM in Bromont, Que., for the last year and a half after she was diagnosed with major depression.

The Eastern Townships woman was receiving monthly sick-leave benefits from Manulife, her insurance company, but the payments dried up this fall.

When Blanchard called Manulife, the company said that “I’m available to work, because of Facebook,” she told CBC News this week.

She said her insurance agent described several pictures Blanchard posted on the popular social networking site, including ones showing her having a good time at a Chippendales bar show, at her birthday party and on a sun holiday — evidence that she is no longer depressed, Manulife said.

Security and privacy issues in OSNs

Threats

- Cloning
- Harvesting
- Hijacking
- ID Theft
- DoS
- Pollution

Current Status of OSNs

- Ease of data leakage
- Ease of impersonation
- Limited privacy support
- Lack of flexibility in privacy

OSN as “Big Brother”
The “Big Brother” problem with OSN

- Privacy protection against
  - Intruders
  - Crawlers
  - Third parties

Does not prevent Application Server from disclosing/exploiting your data

All existing OSN suffer from it!
Current solutions

Interest based P2P Networks (Prosa, Bittella)

P2P

SN

Darknets (GNUNet, Freenet)

Privacy settings or Crypto patches (NOYB)

Security
Safebook - Design Principles

- **Decentralization**
  - P2P architecture

- **Cooperation enforcement**
  - Friends cooperate

- **Leveraging existing Trust**
  - Social trust $\Rightarrow$ trusted link
  - Friend = neighbor

- **Privacy**
  - Simple anonymous routing
  - Based on trusted links
  - Group Encryption
Safebook - Components

1. Matryoshka
   - Data storage
   - Cooperation
   - Communication with privacy

2. Peer-to-peer substrate
   - Lookup

3. Trusted Id System
   - Id Management
Safebook - Overlays

Social network overlay

Peer to peer overlay

Internet
Safebook - Matryoshka

Safebook - Leveraging Social Links for Trust and Privacy
User Registration

Get credentials

Join the DHT

Create Matryoshka

Join process


**a looks for b**

- **lookup**
  - a looks for b’s entry nodes
  - k provides b’s outer shell nodes

- **data request**
  - a sends profile data request to an entry node serving b

- **Data reply**
  - One of b’s inner shell nodes answers

b’s outer shell: h(b), e, h(b), f
Data retrieval

• User 1 wants to get User 2’s profile data

• User 2’s data is stored by User 3
Privacy by Design

- Privacy through layering
- Unlinkability of IDs across layers
- Anonymous communication in matryoshkas
Safebook Prototype

Safebook = Resident Program

User
- User interface
- Trust logic
- P2P logic
- Encryption logic
- Communication Interface

http://localhost:8080
Evaluation of the scheme (1)

- Privacy: Friendship relations hidden through Matryoshkas
  - Untraceability through pseudonymity and anonymous routing
- Cloning prevention
- Dos prevention
- Access control: Key management
- Availability: Data replication at friends’ nodes
Evaluation of the scheme (2)

- Performance
- Feasibility
- P2P Overlay
- Matryoshka
- Existing studies
- Derive architectural parameters
- Reachability
- Privacy
- Delay
Reachability

90% probability of having at least one valid path through the matryoshka, spanning ratio=2

Too many contacts?

Increase spanning ratio!

15 to 25 contacts required to be reachable at 90% with 3 or 4 hops

Number of contacts in the inner shell

(Skype data)
Delay

Total lookup time:
\[ T_{dl} = T_{DHT} + T_{Mat} \]

- Further lookups: \( T_{DHT} = 0 \) thanks to caching

\( 90^{\text{th}} \) percentile: 5.42 s

Median: 1.73 s

Average: 2.71 s

(*) Data computed by applying the montecarlo sampling technique on single hop delay measurements and on delay measurement for a successful DHT key lookup in KAD.
Privacy

Probability of disclosing the shell behind the outermost one with span=1 when the attacker knows the friendlists of all the outermost shell nodes

![Graph showing probability vs. number of nodes in the outermost shell with different values of \( \eta \).]
Publications

• Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe: **Safebook: a Privacy Preserving Online Social Network Leveraging on Real-Life Trust**, IEEE Communications Magazine, Consumer Communications and Networking 2010

• Alessandro Sorniotti, Refik Molva, **Secret Interest Groups (SIGs) in Social Networks with an Implementation on Facebook**, ACM SAC 2010

• Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  **Privacy preserving social networking through decentralization**
  WONS 2009, 6th International Conference on Wireless On-demand Network Systems and Services, February 2-4, 2009, Snowbird, Utah, USA

• Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda
  **All your contacts are belong to us : automated identity theft attacks on social networks**
  WWW'09, 18th Int. World Wide Web Conference, April 20-24, Madrid, Spain

• Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  **Leveraging Social Links for Trust and Privacy in Networks**
  INetSec 2009, Open Research Problems in Network Security, April 23-24, 2009, Zurich, Switzerland

• Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  **Safebook: Feasibility of Transitive Cooperation for Privacy on a Decentralized Social Network**
  3rd IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications