



Building Blocks for Privacy-Preserving Decentralized Online Social Networks

iSocial Summer School



Sonja Buchegger, Assoc. Prof. Computer Science KTH

Online Privacy Problematic

- Current services (FB, GMail, GCal, Flickr, Pinterest) are “free” – users pay with their data, advertisement-based business model (“If you’re not paying, you’re the product”)
- Centralized data collection, privacy leaks
 - accidental
 - deliberate
- Information flow to third parties (companies, governments, the web-browsing public, hackers)
- Tracking
- Data Mining



Online Social Networks Worse

They have desirable functions

But:

- Personal, compound data collection
- Revealing increasing amounts, increasingly personal
- Not only what users upload, also data about them
- Not only about users themselves but others as well





KTH Computer Science
and Communication

Why so much data mining?

- Improve service
- Attention economy

Why Is This a Problem?

- Once leaked, the data cannot be revoked
- Potential audience exceeds expectations, copying easy
- Not known who has what information
- Pieces of information that are harmless, taken together can be identifying or damaging





KTH Computer Science
and Communication

Project Goal

- Privacy-preserving social networks
- Keeping functionality
- Giving control over the data back to the users



Our* Approach



- Provider independence by **decentralization**
- Data protection by **prevention** (access control, cryptographic means)
- Bonus: **locality**, off-line functioning, authentication by direct exchange of data between devices

- At KTH: **Oleksandr Bodriagov**, **Sonja Buchegger**, **Benjamin Greschbach**, **Guillermo Rodriguez Cano**.
- Collaborators: Anwitaman Datta NTU Singapore, Krzysztof Rządca U Warsaw. Alumni: KTH, EPFL, T-Labs

Longer-Term Goal

- Social networks are an important example
- ... but what we really want is building blocks for
 - privacy-preserving
 - provider-less / decentralized
 - future communications and applications





Research Question Categories

- How can we decentralize functionality?
- How can we preserve user privacy?

- Context: Decentralized system, heterogeneous resources and demand, requirements on availability, scalability, robustness, functionality, efficiency.



KTH Computer Science
and Communication

Research Questions: Distributed Systems

Design:

- P2P topology, social graph
- Storage, availability
- Asynchronous comm.
- Add/remove/update
- Search
- Scalability
- Incentives
- Direct exchange, DTN
- Self-contained system

Challenges:

- Geo-temporal diversity
 - Heterogeneous resources
 - Heterogeneous demand
 - Churn
 - Delay tolerance
-



KTH Computer Science
and Communication

Research Questions: Security/Privacy

Design:

- Encryption, credentials
- Key management
- Content/key revocation
- Authentication
- Usage control
- Transparency, usability
- Direct exchange for security
- Data chunking
- Anonymity, traceability

Challenges:

- Distributed system challenges
- Online social network properties
- Privacy of
 - Access
 - Location
 - Data existence, size
 - Relation



Distributed Storage, Availability

So far:

- concept [BD09]
- architecture [BSVD09]
- game-theoretic and complexity analysis [RDB10]
- ongoing: storage API



Distributed Access Control

So far:

- simple digital-envelope based [YA08]
- broadcast encryption based [BB11a,b]
- policy based (XACML, SAML) [RN11]
- predicate encryption [BKB14]

Ongoing:

- Combinations of encryption



Privacy of Access, Relations, Existence

So far:

- meta data [GKB12, GB12]
- access policy hiding encryption [BKB14]
- privacy-preserving user search [GKB13]

Ongoing:

- data structures



Distributed Authentication

So far:

- threshold-crypto based key recovery [VABD09]
- passwords in peer-to-peer [KBGRB12]





Wider Perspective Goal

- Privacy components as enabler for future communications:
 - More devices, more connections
 - Security concern: Higher complexity, more vulnerability
 - Quantity concern: More data collected (sensors, logging)
 - Quality concern: Improved data joining, mining, and crunching
 - Sensitivity concern: Increasingly personal (health, energy monitoring)
- Need privacy to make new applications possible: remote healthcare, independent living, nomadic work, smart home/office/city/grid, etc.



Summary: Toward Decentralized Privacy-Preserving Communications

- Privacy question has increasing relevance for society
- Will need privacy solutions for highly connected data-intensive applications
- Fundamental shift from provider-dependent to decentralized systems opens a wide range of research questions



References

- [BKB14] Oleksandr Bodriagov, Gunnar Kreitz, Sonja Buchegger. Access Control in Decentralized Online Social Networks: Applying a Policy-Hiding Cryptographic Scheme and Evaluating Its Performance.. At SESOC 2014, PERCOM 2014, March 28, 2014, Budapest, Hungary.
- [GKB13] Benjamin Greschbach, Gunnar Kreitz, Sonja Buchegger. User Search with Knowledge Threshold in Decentralized Online Social Networks (pre-proceedings version). At the 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies, June 2013, Berg en Dal, Netherlands.
- [KBGRB12] Gunnar Kreitz, Oleksandr Bodriagov, Benjamin Greschbach, Guillermo Rodriguez Cano, Sonja Buchegger. Passwords in Peer-to-Peer.. At IEEE P2P 2012, September 3-5, 2012, Tarragona, Spain.
- [GB12] Benjamin Greschbach, Sonja Buchegger. Friendly Surveillance - A New Adversary Model for Privacy in Decentralized Online Social Networks.. At Security 2012, Freiburg, Germany.
- [GKB12] Benjamin Greschbach, Gunnar Kreitz, Sonja Buchegger. The Devil is in the Metadata - New Privacy Challenges in Decentralised Online Social Networks.. At SESOC 2012, PERCOM 2012, March 19, 2012, Lugano, Switzerland.
- [BB11b] Oleksandr Bodriagov, Sonja Buchegger. Encryption for P2P Social Networks.. At SPSN 2011, Workshop on Security and Privacy of Social Networks, in conjunction with IEEE SocialCom, Boston, October 9-11, 2011.
- [BB11a] Oleksandr Bodriagov, Sonja Buchegger. P2P Social Networks With Broadcast Encryption Protected Privacy. At IFIP Summerschool on Privacy, Trento, September 2011.
- [RN11] Robayet Nasim. Privacy-Enhancing Access Control Mechanism in Distributed Online Social Network. KTH Master's thesis, May 2011.
- [RDB10] Krzysztof Rzdca, Anwitaman Datta, Sonja Buchegger. Replica Placement in P2P Storage: Complexity and Game Theoretic Analyses. In Proceedings of ICDCS 2010, Genoa, Italy, June 2010. pdf
- [VABD09] Le Hung Vu, Karl Aberer, Sonja Buchegger, Anwitaman Datta. Enabling Secure Secret Sharing in Distributed Online Social Networks. In Proceedings of Annual Computer Security Applications Conference (ACSAC) 2009, Hawaii, December 7-11, 2009. pdf
- [BSVD09] Sonja Buchegger, Doris Schiöberg, Le Hung Vu, Anwitaman Datta. PeerSoN: P2P Social Networking - Early Experiences and Insights. In Proceedings of SocialNets 2009, The 2nd Workshop on Social Network Systems, Nuernberg, Germany, March 31, 2009.
- [BD09] Sonja Buchegger, Anwitaman Datta. A Case for P2P Infrastructure for Social Networks - Opportunities and Challenges. In Proceedings of WONS 2009, The Sixth International Conference on Wireless On-demand Network Systems and Services, Snowbird, Utah, USA, February 2-4 2009. pdf bib
- [YA08] Youssef Afify. Access Control in a Peer-to-peer Social Network. Master's Thesis, EPFL, Lausanne, Switzerland, August 15, 2008.