SocialLift: Handling Facebook Evidence using Verifiable Limited Disclosure

Social Media and Policing Event

Wednesday, 8th February 2017

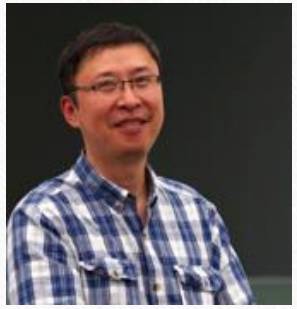
The Research Team

Thein

Danny

Arosha

Blaine

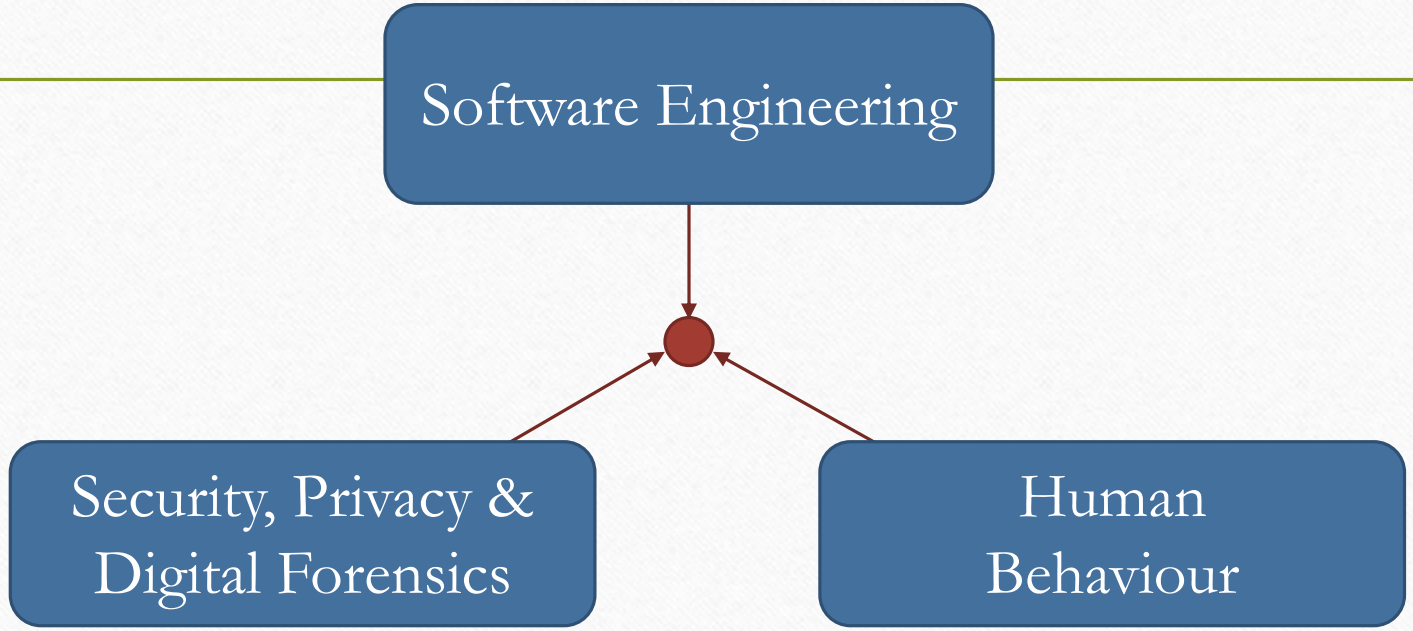


Yijun

Bashar

Main Police Partners

Our Research



T. T. Tun, B. A. Price, A. K. Bandara, Y. Yu and B. Nuseibeh, "Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations," in *International Workshop on Requirements Engineering for Investigating and Countering Crime*, 2016.

Outline

- Introduction (Bashar)
- Research: Verifiable Limited Disclosure & SocialLift (Thun)
- Demo: SocialLift (Danny)
- Exercise: Exploring SocialLift functionality (Arosha)
- Wrap-up

Background

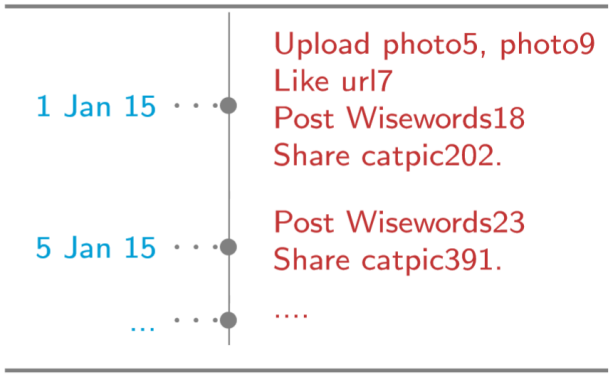
- Digital evidence from the social media increasingly important
  - Emerging classes of cybercrimes (trolling, cyber bullying)
  - Additional source of evidence for traditional crimes
- Traditional digital forensic tools focus on disks, memory, network
- Protecting privacy is important in police cases
  - A witness, victim, suspect may want to give the private digital information to police
  - Irrelevant information must remain private – good for privacy, trust and search

Social Media Example

Bob: Policeman

Charlie: Victim, Witness, Suspect

FB: Social Network



- Charlie wants to give a section of his timeline to Bob
- Existing approaches
  - Facebook: Print out and ink over
  - Forensics tools: Hand over the passwords/devices

Forensics Requirements

- **Requirement 1**: Charlie does not over-disclose

  Charlie never has to reveal more than what Bob has requested.

- **Requirement 2**: Charlie and Bob cannot lie

  Charlie and Bob can prove to the world that they made no modification of the information they have.

- **Requirement 3**: Charlie and Bob cannot conceal

  Charlie and Bob can prove to the world that they are not withholding relevant information.

Verifiable Limited Disclosure (VLD)

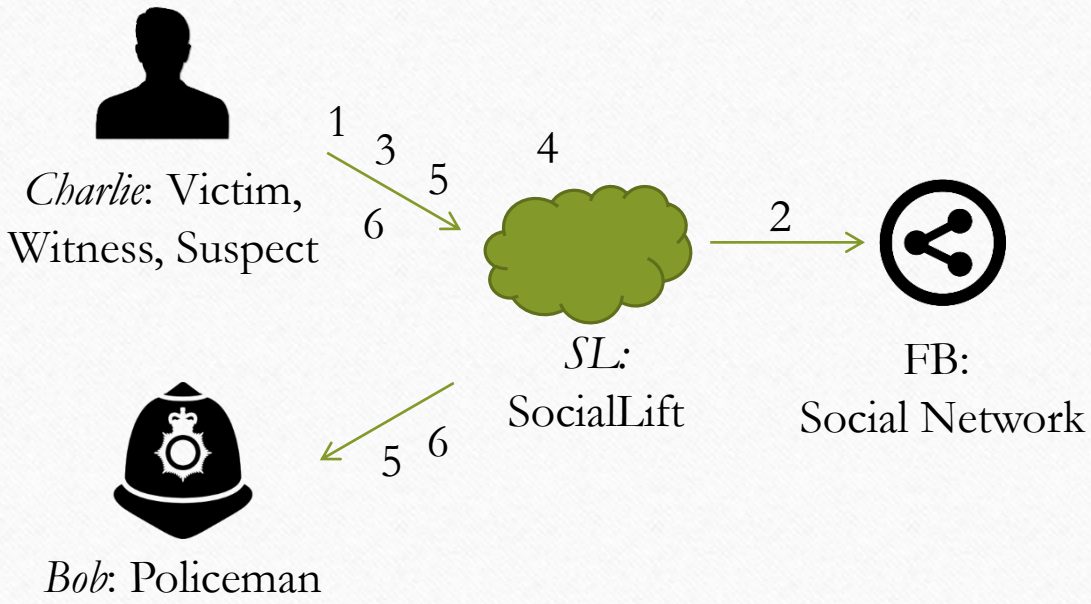
Bob: Policeman

Charlie: Victim, Witness, Suspect

FB: Social Network

1. Bob requests a section of timeline
2. Charlie announces his public key
3. Charlie requests encrypted timeline
4. FB encrypts timeline for Charlie
5. FB hashes encrypted timeline
6. FB announces hash and timestamp
7. Charlie decrypts a section and gives the entire timeline

SocialLift



1. Charlie logs in with FB credentials
2. SL gets Charlie's timeline
3. Charlie selects objects to disclose
4. SL creates a Merkle tree of objects
5. Objects and tree root sent by email
6. Verify by recomputing Merkle tree

Trade-offs

VLD

- Public Key infrastructure needed
- Requires Facebook buy-in
- Better security

SocialLift

- No encryption keys needed
- No need for Facebook buy-in
- Easier to use

SocialLift Demo

- Demos of SocialLift are available:
  - On our home page http://social-lift.com
  - On youtube http://youtu.be/XJ5N_-Weobc

Group Activity

- Visit http://www.social-lift.com/ to experiment with tool [optional]
- Discuss functionality in context of evidence collection practices
- Use the notepaper provided to write down
  - **Bugs:** Issues with current features of the tool
  - **Requirements:** Features needed to use tool in practice
  - **Enhancements:** Additional features that enhance capabilities of the tool

Conclusion

- Verifiable Limited Disclosure – forensically sound, privacy-preserving social media evidence collection.
- Prototype tool - SocialLift, implementing basic VLD features.
- Opportunity to collaborate on improving SocialLift and evaluating in field.

- Contact: Thein.Tun@open.ac.uk

Merkle Tree

- A binary tree of hashes
- Key property:
  - If top is good, all blocks are good
  - If one block is bad, top is bad
  - A bad block is identified in steps the logarithm of block size