Verifiable Limited Disclosure

Reporting and Handling Digital Evidence in Police Investigations

Thein Tun Loakthar
thein.tun@open.ac.uk

September 12, 2016

Acknowledgement

- Joint work with the Open University colleagues (BABY): Blaine Price, Arosha Bandara, Bashar Nuseibeh, Yijun Yu
- In collaboration with police partners

- The Open University Centre for Policing Research and Learning

Outline

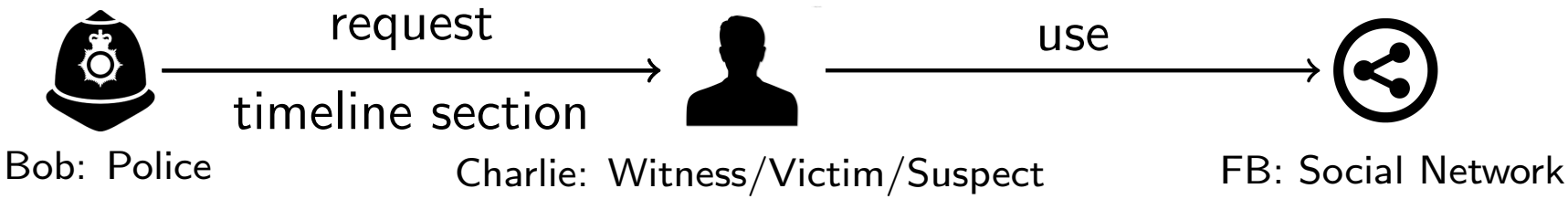
Changing Patterns of Cybercrimes

- People nowadays own a lot of private digital information
  - on smart phones, tables, computers, laptops, cloud etc
- 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:
  - evidence extraction from disks, memory, network
  - data size can be huge; triage takes time and it is difficult to find relevant evidence
  - information privacy of citizens could be violated

The Need for Information and the Need for Information Privacy

- Sometimes people want to give the private digital information to police investigations
  - *Witness*: Someone who saw something, potentially illegal
  - *Victim*: Someone who believes that something illegal has happened to them
  - *Suspect*: Someone who may have done something illegal, wants to share some information with police investigations
- When disclosing, the information irrelevant to the request must remain private
  - good for privacy; good for search & for court evidence

Example



- Criminals like using Facebook.
  Charlie likes using Facebook.
  (beware of "confusion of the inverse")
- Policeman Bob needs to access a section of Charlie's FB timeline
- How can Bob do that?

Table : Charlie's timeline

1 Jan 15	Upload photo5, photo9 Like url7 Post Wisewords18 Share catpic202.
5 Jan 15	Post Wisewords23 Share catpic391.
...	....

Possible Solutions

- Bob takes a disk image of every storage medium on every device Charlie uses in order to extract relevant FB information
  - takes time
- Bob asks FB to reveal a section or the entire timeline of Charlie
  - Charlie is not in control; How can Charlie trust Bob's evidence?
- Charlie voluntarily give a section of his FB timeline, e.g., by means of screenshot
  - How can Bob ensure the evidence has not been tampered with?

Verifiable Limited Disclosure

Information disclosure should be **limited** and **verifiable**.

- Limited
  - When the police asks someone to disclose their private information as evidence, the asked person should never have to reveal more than what the police has requested
- Verifiable
  - The police or the asked person cannot tamper with the evidence or withhold evidence without the world knowing

The whole truth and nothing but the *relevant* truth

When Charlie gives a section of his FB timeline to Bob,

- Charlie needs to make sure that he is not disclosing anything other than what Bob has requested (relevant)
- Bob needs to know that Charlie has made no modification or insertion in the disclosed information (nothing but the truth)
- Bob needs to know that Charlie has made no concealment of relevant information (the whole truth)

The whole truth and nothing but the *relevant* truth

When Bob presents Charlie's timeline as evidence to court, Charlie needs to make sure that

- Bob has made no modification or insertion to the information he has disclosed to him (nothing but the truth)
- Bob has not concealed any relevant information he has disclosed to him (the whole truth)

Requirements for Verifiable Limited Disclosure

Requirement 1: Charlie does not over-disclose

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

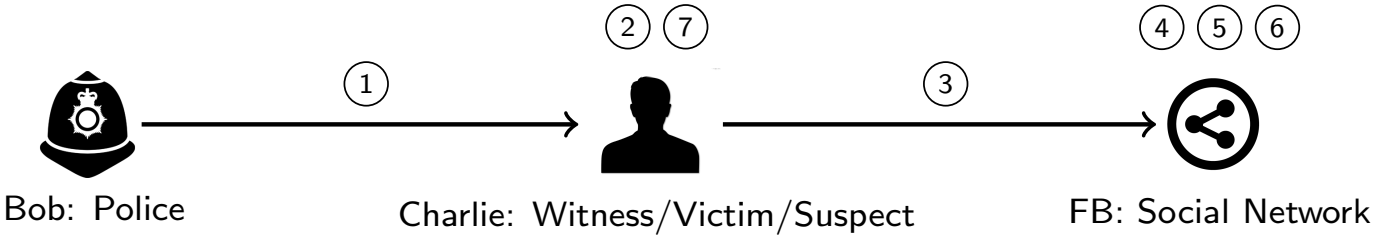
Requirement 2: Charlie and Bob cannot lie

Charlie can prove to the world that the information he gives to Bob has not been modified by him. Likewise, Bob can prove to the world that the information he shows to the court has not been modified by him.

Requirement 3: Charlie and Bob cannot conceal

Charlie can prove to the world that he has not withheld information relevant to Bob's request. Likewise, Bob can prove to the world that he has not withheld information revealed to him by Charlie.

Candidate Protocol #1



1. Bob requests the section s of Charlie's timeline
2. Charlie announces his public key ($PK_{Charlie}$) to the world
3. Charlie requests encrypted timeline from FB
4. FB encrypts every object in Charlie's timeline using $PK_{Charlie}$
5. FB computes the cryptographic hash value (CHV_k) of all encrypted objects along Charlie's timeline
6. FB announces CHV_k and its timestamp to the world
7. Charlie decrypts a section of his timeline and gives the entire timeline to Bob.

Steps 4 5 6

Table : Charlie's timeline

1 Jan 15	Upload photo5, photo9 Like url7 Post Wisewords18 Share catpic202.
5 Jan 15	Post Wisewords23 Share catpic391.
...	....

Table : Charlie's encrypted timeline

1 Jan 15	Upload  Like  Post  Share  .
5 Jan 15	Post  Share  . ....
...	

Concatenate all  objects and compute their CHV_k.

Properties of Protocol #1

Requirement 1: Charlie does not over-disclose

Yes, because without Charlie's private key, Bob can only read the section of Charlie's timeline Charlie has decrypted for him.

Requirement 2: Charlie and Bob cannot lie

Yes, because any modification of the information by Charlie or Bob will be caught by someone who replays steps (4) (5) (6).

Requirement 3: Charlie and Bob cannot conceal

No, because there is no way of proving that Charlie or Bob is concealing.

Meta-data

- Without knowing Charlie's daily activities on FB (meta-data), Bob cannot prove that Charlie is concealing.
- What if FB announces Charlie's meta-data to the world?
  - Bad for Charlie's privacy.
- What if Bob asks FB to check if Charlie is concealing?
  - Too much work for both Bob and FB.

Can we do better?

Candidate Protocol #2

When FB encrypts, every encrypted object contains the timestamp of the previous and the next object along Charlie's timeline.

Table : Fully-sequenced objects in Charlie's timeline

1 Jan 15	Upload (ts(...); photo5; t(photo9)), (t(photo5); photo9; t(url7)) Like (t(photo9); url7; t(Wisewords18)) Post (t(url7); Wisewords18; t(catpic202)) Share (t(Wisewords18); catpic202; t(Wisewords23)).
5 Jan 15	Post (t(catpic202); Wisewords23; t(catpic391)) Share (t(Wisewords23); catpic391; t(...)).
...	....

Properties of Protocol #2

Requirement 1: Charlie does not over-disclose

Yes, because without Charlie's private key, Bob can only read the section of Charlie's timeline Charlie has decrypted for him.

Requirement 2: Charlie and Bob cannot lie

Yes, because any modification of the information by Charlie or Bob will be caught by someone who replays steps (4) (5) (6).

Requirement 3: Charlie and Bob cannot conceal

Yes, because if Charlie does not decrypt any relevant object, the timeline of the section he reveals will not join up.

Properties of Protocol #2

Bonus Requirement 4: Charlie does not reveal the meta-data of his timeline

Charlie can prove that he has not concealed anything relevant to Bob's request without revealing the entire meta-data of his timeline.

Implementation Considerations

- The protocol uses standard security tools
  - Public Key Encryption, Cryptographic Hash Function
- The protocol cannot handle arbitrary queries from Bob (e.g., all posts and uploaded photos withing a date range)

Future Work

- We are creating a Facebook plug-in/application
- Challenges
  - No Facebook buy-in
  - Key management infrastructure

Thank you!