Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations

Thein Tun Blaine Price Arosha Bandara Yijun Yu Bashar Nuseibeh

firstname.lastname@open.ac.uk

Background Online crime patterns are changing. Many of the criminal cases investigated by the UK police forces now involve examination of digital evidence from the social media, primarily the Facebook and Twitter platforms. Furthermore, there is an emerging class of social media offences that include "cyber bulling", "trolling" and "virtual mobbing". When handling evidence from the social media, existing digital forensic technologies have a number of limitations in terms of scalability, effectiveness and increased public trust.

Challenge How can witnesses, victims and suspects give evidence from their social media accounts to police investigations in such a way that they have to disclose only the relevant information, and yet their evidence can be verified automatically for authenticity and completeness by the police forces? Currently, there is a need for an evidence collection process for social media offences that is forensically sound, scalable and privacy-sensitive.

Proposal We propose the notion of *verifiable limited disclosure* that can be achieved by means of a protocol using two main security tools: cryptographic hash function and public key encryption. When a user of a social media platform (SMP) wishes to give evidence, the user requests the encrypted timeline from SMP. SMP encrypts all objects in the timeline, concatenates them into a string, and computes the hash value of the string. The hash value is then announced publicly. The user decrypts any parts of the timeline before giving the partially decrypted timeline to the police investigation as evidence. Authenticity of the evidence can be checked by re-encrypting the decrypted parts before computing and comparing the hash value. The data structure of the timeline can be modified slightly to deal with the issue of evidence concealment.

Evaluation We are currently implementing a Facebook application as a prototype for *verifiable limited disclosure*. The aim is that citizens will be able to send evidence to police investigations from their Facebook account directly. This will have a number of benefits to the police forces: for example, officers will no longer have extract the data themselves from Facebook accounts, and yet prove the continuity of evidence easily. Similarly, citizens will not have to share their passwords with police investigations, thus improving cyber security and increasing public trust. We will share our prototype of Facebook application with the consortium in due course for feedback and for potential deployment.

Information T. T. Tun, B. A. Price, A. K. Bandara, Y. Yu and B. Nuseibeh (2016). Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations. *International Workshop on Requirements Engineering for Investigating and Countering Crime*, Beijing, China. Available from: http://oro.open.ac.uk/46914/ Winner of "Best Short Paper" Award