Requirement Driven Proactive Verifiable Limited Disclosure: Handling Digital Evidence of Crimes in Social Media

Rejwana Haque[1]
[1](Department of CSE, Bangladesh University of Engineering and Technology, Bangladesh)

Abstract: *A digital forensics process aims to analyze digital evidence of storage unit of computer or other storage devices. But when a crime is committed is a social media the social media platform holds the evidence not necessarily the storage device used by the victim of the criminal. Moreover, the extensive use of social media and the huge amount of data shared through the social media has made the traditional investigation process gradually made it ineffective. Though the 'verifiable limited disclosure' protocol addresses this problem, it is also a reactive approach. Here we introduce 'proactive verifiable limited disclosure' for handling and investigating digital evidence in police investigation. This protocol also uses the storage of social media for storing evidence of crimes occurred in the social media, which minimize the problem of 'resource overhead'.[1]*

Keywords: *Digital Forensics, Proactive Investigation, Digital Privacy, Cyber Crime, Adaptive Forensics, Social Media*

I. Introduction

Traditional approaches of computer forensics focus on storage device such as hard drive of smartphone. But the increasing amount of storage makes this traditional approach inefficient. Moreover, if the crime occurs in social media than the evidence is contained in the social media environment, not necessarily device storage used by criminal or victim or witness. So it is needed to maintain digital privacy especially when examining the evidence from a victim or a witness. The 'Verifiable Limited Disclosure' protocol addresses this problem and maintains digital privacy for victim and witness. But this protocol does not give any guideline to the investigator about the hypothesis to be considered. To deal with the concealment the protocol handles metadata of the victim's profile. On the other hand, if some evidence is beyond the range of the investigator requested, some evidence may be hidden. So proactive analysis stores the relevant evidence and generates possible hypothesis to guide the investigator and also provide the relevant evidence to the investigator.[2]

II. Motivation

The investigation process should fulfill the following criteria, while the crime is committed in social media.
Criteria 1: The victim or witness must not be over disclosed. This means that the investigation process must maintain digital privacy for the victim or the witness. Only the relevant evidence must be disclosed.
Criteria 2: No one regarding the dispute can't lie. Neither the victim nor the investigator can lie.
Criteria 3: Neither the victim nor the investigator can hide anything. The relevant evidence must be disclosed.
Criteria 4: Social media should be a guide and witness to the investigation process automatically.

III. Methodology

The 'verifiable limited disclosure' [3] protocol meets the first three criteria. Here we propose a modified approach, which is proactive, collects the evidence for a crime committed in social media. And proactively stores all the evidence to guide the investigator. For this, we use 'requirement driven adaptive digital forensics' [4] with 'verifiable limited disclosure'.

3.1 Requirements Modeling

The social media designs the common pattern of crime committed in the media for the forensic requirement. These include a domain model of a crime content, common types of crime, which contents can be victim of crime and who have the permission and privilege to see and access it and which types of content are violation of criminal law. For example, Alice used an account on the social media of platform SM. SM monitors each activity of Alice. SM designs also some arguments. These may represent the event's conditions that must be hold to start and stop the evidence collection performed proactively (proactive argument). Alice uploads a photo on her timeline that matches the pattern of victim content. This argument starts the proactive analysis and evidence collection starts for Alice timeline. These also represent the hypothesis of the potential crimes that can be committed in the crime scene (reactive arguments).

3.2 Configuration

The social media have to configure the uses forensics requirements to configure the proactive and reactive activities for reporting and handling digital evidence in police investigation. Using the proactive analysis reporting is done and using the reactive arguments all possible hypothesis with evidence is given to the investigation by the social media to guide the investigation process.

3.3 Proactive Collection

After a user login the social media, the social media collects the data in every timestamp of the user, sends them to the Event Calculus Analyzer (Analyzer) [5] and stores them securely. The social media also tracks activities of the user having some privilege to each content uploaded on it and sand to event calculus analyzer and store them securely.

3.4 Proactive Analysis

Every time new evidence is available, the Analyzer matches if with start or stop argument. If the condition of start/stop argument is satisfied the evidence collection process is started or stopped. When the evidence collection is started the evidence are analyzed and stored in a secured storage by the social media platform. Also, the arguments for reactive analysis to check all possible hypotheses are generated to guide the investigator for a crime committed. For example, when content matches the victim pattern the proactive evidence collection is started. If a crime committed the proactive evidence collection is stopped and reactive evidence collection is started. The evidence is sent to the analyzer and the analyzer generates all the possible hypothesis. Deductive reasoning functionality of event calculus is used for checking conditions for start/stop the full evidence collection is satisfied.

3.5 Investigation Set-up

When a police investigation starts and investigator requests for the evidence related to a crime, the social media retrieves the data collected by the Proactive Analysis from the secure storage and sends the relevant parts to the investigator using “verifiable limited disclosure”[] protocol.

3.6 Modification of verifiable limited disclosure

Verifiable limited disclosure is slightly modified in this approach. In the original protocol, the victim selects the portion to be disclosed. Here we modified the protocol. Here the social media also guides the investigation process by analyzing and sharing relevant arguments stored in the secured storage. Here the social media also provides the possible hypothesis to the investigator.

IV. Scenario With Protocol

We will describe our protocol with an example first, than we will evaluate the performance of the protocol.

1. Alice uploads a photo to social media SM.
2. SM examines the pattern of the photo.
3. The photo matches some common victim pattern.
4. The proactive evidence collection and analysis of the photo starts.
5. Charlie comments on the photo that violates criminal law.
6. SM stores the comment as digital evidence.
7. Alice reports to police Bob for the comment.
8. Bob announces his public key (PKBob) to the world.
9. Bob request guidance from SM.
10. SM stops proactive evidence collection and the investigation process starts.
11. SM provides only the relevant evidence from storage and also provides the possible hypothesis generated in the proactive analysis using PKBob.
12. SM generates the cryptographic hash value of the shared evidence (CHVE) to the world.
13. Bob decrypts the evidence using his private key.
14. Charlie announces his public key (PKCharlie) to the world.
15. Bob sends the encrypted evidence to Charlie using (PKCharlie) and also requests sections of Charlie’s timeline.
16. Charlie decrypts the evidence and encrypts it using PKBob .
17. Charlie computes the hash value and compares it with the one announced by SM in step 12.
18. Charlie requests encrypted timeline from SM.
19. SM encrypts every object in Charlie’s timeline using PKCharlie
20. SM computes the cryptographic hash value (CHVk) of all the encrypted objects along Charlie’s timeline.
21. SM announces CHVk and its timestamp to the world.

22. Charlie decrypts a section of his timeline and gives the entire timeline to Bob.
23. Bob encrypts the decrypted section of Charlie's timeline, computes the hash value and compares it to the one announced by SM in Step 21.

V. Fulfillment Of The Criteria

The protocol fulfills all the criteria.

1. As SM provides only the relevant evidence and Charlie provides relevant parts to Bob, the digital privacy of Charlie is maintained.
2. As the evidence collection is two-dimensional (from the victim and social media), Charlie cannot lie. And as CHVE is known to Charlie Bob cannot lie.
3. All the evidence is given to both investigator and victim so no one can hide anything.
4. As the social media provides possible hypothesis so it acts as a guide. And as the social media provides the relevant evidence regarding the dispute it serves also as a witness.

VI. Conclusion

Our proposed protocol does not need to separately handle the metadata. It also needs not to violate any of the four criteria. Which makes it a better choice for handling crimes committed in social media. Though the protocol recovers the limitation of traditional reactive digital forensics for crimes committed in social media it also has limitation. It uses public key encryption where key management is a difficult issue. The protocol does not provide a clear rule for proactive evidence collection procedure. Analyzing and storing each object uploaded in social media can be a cause of storage and process overhead for social media. In future we plan to develop a working prototype for the protocol and evaluate it with real data. First we will develop a straightforward way to store and analyze evidence proactively. We plan to build an algorithm to reduce storage and process overhead for the social media platform..

References

[1] R. E. Overill, J. A. Silomon, and K. A. Roscoe, "Triage template pipelines in digital forensic investigations," *Digital Investigation*, vol. 10, no. 2, pp. 168 – 174, 2013.

[2] G. Palmer, "A Road Map for Digital Forensic Research," Air Force Research Lab, Rome, DFRWS Technical Report DTR-T001-01, 2001.

[3] Thein Tun, Blaine Price, Arosha Bandara, Yijun Yu and Bashar Nuseibeh, "Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations", 1st *International Workshop on Requirements Engineering for Investigating and Countering Crime, 12th September 2016*, Beijing, China.

[4] L. Pasquale, Y. Yu, M. Salehie, L. Cavallaro, T. T. Tun, and B. Nuseibeh, "Requirements-driven adaptive digital forensics", *21st IEEE International Requirements Engineering Conference*. IEEE Computer Society, 2013, pp. 340–341.

[5] S.Y. Willassen, "Using Simplified Event Calculus in Digital Investigation," in *Proc. of the Symp. on Applied Computing*, 2008, pp. 1438–1442.