Demo:E-Witness - Preserve and Prove Forensic Soundness of Digital Evidence

Priyanka Samanta
The Graduate Center of CUNY
New York, NY
psamanta@gc.cuny.edu

Shweta Jain
CUNY John Jay College of Criminal Justice
New York, NY
sjain@jjay.cuny.edu

ABSTRACT

In this demo we present E-Witness, a system that uses blockchain technology to prove the integrity and spatio-temporal properties of digital evidence captured through a smart-phone. The system consists of a smart-phone application that computes robust hash of pictures or videos taken from the phone camera, a location attestation service and a public blockchain which contains ledger entries to preserve the evidence file's hash and location certificate. The human witness can remain anonymous in this process. An investigator who receives the evidence (by any means) can verify the integrity and spatio-temporal claims of the evidence by querying the blockchain.

CCS CONCEPTS

• **Networks** Location based services; • **Applied computing** Evidence collection, storage and analysis;

ACM Reference Format:
Priyanka Samanta and Shweta Jain. 2018. Demo:E-Witness - Preserve and Prove Forensic Soundness of Digital Evidence. In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3241539.3267720

1 INTRODUCTION

Civilians are increasingly taking on the role of journalists, reporting eye-witness accounts of injustice in digital format [1]. For example, video recording of incidents of police brutality were uploaded on social media by civilians who were not afraid of revealing their identities and their locations. Posting evidence clips on social media, gives the incident, time and location stamps, both of which are necessary to prove the authenticity of the evidence in the court. Unfortunately it is not always safe for a whistle-blower to publicly publish an evidence. Often discreetly uploading to secure drop sites [2] may also be unsafe. However, a digital evidence collected but not published soon, might be subject to challenge in the court in the absence of an immutable spatio-temporal alibi.

E-Witness empowers civilians and journalists who need to protect their identity while ensuring that the evidence they collect are forensically sound and hence worth the risks. In this demo, we present the functionality of the three main components that make up the E-Witness system - (a) a smart device application that captures and stores digital multi-media evidence and computes a robust image hash [3], (b) a location attestation service that validates the location context of the evidence when the location is recorded by on-board(untrusted) sensors on the device and (c) a Blockchain, maintained by non-profits and social activists, that maintains ledger entries to serve as an immutable time-stamp of the evidence available to an investigator for verification.

2 EXISTING TECHNOLOGY

We evaluated "i-Witness" [4], a smart-phone app available with paid subscription. It is an emergency app that allows users to broadcast live videos to their contacts. They can instruct the app to place emergency calls to 911 or sound an alarm to attract attention. E-Witness, in contrast is an app for social journalism rather than emergency services and hence takes special measures to preserve user privacy.

Keeex [5] and TruePic [6] are photo proof applications in which users can anchor cryptographic hashes of pictures of personal contracts, receipts, rental agreements etc. in the Bitcoin Blockchain. The goal is to create photo proofs and locations of important transactions so that they can be used as a proof in case of a dispute. Both applications provide the means to verify integrity of the pictures through their websites. Unlike E-Witness, anonymity is not a goal in these apps and they are commercial applications which people would pay to use for personal and financial purposes.

Camera-V [7] is an application developed by the Guardian project [8] as a free solution to securely preserve digital evidence. It encrypts and password protects each multimedia

MobiCom '18, October 29-November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10.
https://doi.org/10.1145/3241539.3267720

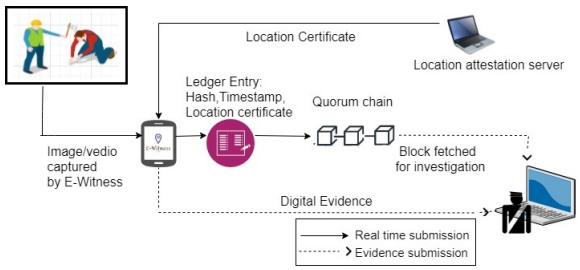

Figure 1: E-witness System Diagram

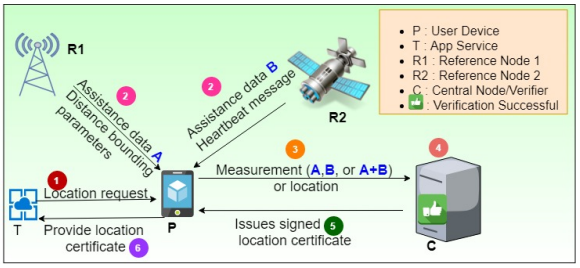

Figure 2: System Model of location attestation

file captured through the device camera using the application. The user has an option to generate a unique code for the media file they create and share the code on social media or through instant messaging. Sharing the code notarizes the file and creates an alibi to attest its integrity and timestamp. CameraV's goal is aligned with E-Witness, however the design philosophies are different. CameraV completely resides on the smart-phone and puts the burden of forensic verification on the investigator. In contrast, by using blockchain to act as an alibi and by using network based location attestation service, E-Witness reduces this burden by enabling fast verification of three important aspects of digital evidence: integrity of the evidence file, immutability of the time-stamp and verifiable location. E-witness does not encrypt images in the device but that is a minor addition which can be added if there is a demonstrated need. We downloaded CameraV from Google Play and found that it is quite slow due to the heavy cryptographic process involved.

3 ARCHITECTURE AND DESIGN DETAILS

The architecture diagram of E-Witness is shown in Figure 1. In order to use a smart phone as an E-Witness device, a user first installs the E-Witness application on the phone. At first use, the application asks the user to register with the E-Witness system to create a pseudo identity. This pseudo identity is tied to the application as long as it is installed on the device. Users can capture pictures and videos through the application using the device camera. The application computes a robust image hash [3] of this digital evidence which is different from cryptographic hash as it can match slightly modified versions of an image with its original. The application requests a location certificate from a location server that resides in the network. The hash and location certificate are transmitted to any node in the E-Witness consensus network. An E-Witness ledger entry, shown in Figure 3, is created by the consensus node and eventually added to the E-Witness blockchain. When an investigator receives the evidence at a later time, she can compute the robust hash of the file and query the blockchain to find the corresponding ledger entry to verify the file's integrity. From the timestamp t_i on the ledger entry, the investigator is assured that the evidence was captured at a time T which is no later than t_i. The location certificate gives the investigator the assurance that the evidence was indeed taken at the location it claims. Developing a smart-phone app is relatively straightforward, but the real research challenges lie in the two supporting components: the blockchain and the location attestation service. Primary concerns are efficiency, scalability, correctness and security. In the following paragraphs, we describe our design choices that bring us closer to these goals.

There is a large body of literature on various alternatives for consensus algorithms that form the core technology in any blockchain. For the purpose of this demo, we have selected Quorum Chain [9] since the consensus nodes in this system have a light weight design which can be deployed as a virtual box [10] based virtual machine on any computer. This inexpensive setup presents a low barrier to entry and hence common people driven by altruism may be willing to participate in the consensus process. Quorum chain is a distributed ledger protocol based on Ethereum [11] except it uses a voting based consensus protocol instead of the compute intensive proof of work. Any reasonable voting based algorithm can be used although the current implementation uses Raft [12]. Thus, unlike crypto-currency miners, consensus participants in Quorum Chain are not burdened with high energy costs to participate in the consensus process. This is important due to the lack of monetary incentive in this system. All consensus nodes in the Quorum Chain validate each transaction in the blockchain to ensure the security and integrity of all ledger entries. Thus, E-Witness ledger entries are at low risk of removal or reordering after they have been placed in the chain. Quorum Chain is designed to be a permissioned chain but this logic can be easily changed to make it a public chain since security in E-Witness sepends on having lower risk of collusion through participation from a large number of participants. Quorum Chain has an open source implementation freely available to download from Github [13]. Therefore, using the Quorum Chain reduces our development effort.

Location authentication has been discussed in literature for atleast three decades, yet there is no working implementation

Figure 3: Quorum ledger entry: Hash, encrypted location certificate, time-stamp

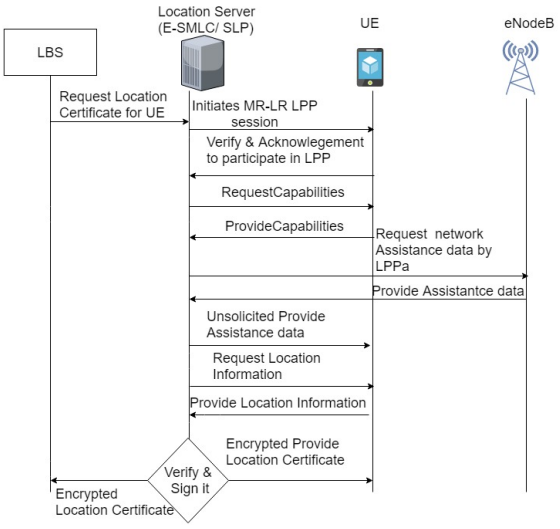

Figure 4: LTE Positioning Protocol with location attestation

for public use. Moreover, location proof as a certificate is merely a concept discussed at first by Tablas et al [14] but not implemented in practice. In this demo, we will use the location attestation architecture described in their work [15] and shown in Figure 2. Any location determination technique, such as crowd sourced or infrastructure supported, can be used with this process as long as signal measurements are attested by the nodes that served as reference and the security of the location claim can be verified. We advocate for an LTE based location attestation in which the location server is maintained by the cellular carrier, verification is performed through signal measurements at the user device (UE) as well as the eNodeB (LTE base station). The eNodeB securely provides the measurements during the location attestation process, the location server issues a signed certificate to attest the location and all communication takes place using the LTE Positioning Protocol (LPP) over the LTE user-plane [16]. For this demo, we will use an emulated location server which will run on a laptop situated at the conference venue. This server will implement protocol messages needed for location attestation using LPP as shown in Figure 4.

4 DEMONSTRATION

We will demonstrate the E-Witness application and its capabilities. The setup consists of E-Witness app on a phone and a laptop hosting a location attestation server connected to the conference wireless network. The quorum chain will be maintained remotely at our lab. In order to engage the conference attendees, we will make the app freely available from the Google Play store. Attendees can collect digital evidence and share them with us (investigator). We will demonstrate the process of querying the ledger entry from Quorum Chain and verify the integrity and space-time attributes of the evidence. Attendees can edit their files and tamper with the metadata to challenge us. This demo does not have any additional space or equipment needs beyond the default setup at the conference.

5 ACKNOWLEDGEMENT

Acknowledgements: This work is supported by the National Science Foundation under Grant No. 1742919 and PSC-CUNY Grant No. 60814-00 48

REFERENCES

[1] Leah Donella. Two Days, Two Deaths: The Police Shootings of Alton Sterling and Philando Castile. *Code Switch, Race and Identity, Remixed, National Public Radio*, 2016.

[2] Kevin Paulsen Aaron Swartz. SecureDrop: Freedom of Press Foundation, https://github.com/freedomofpress/securedrop.

[3] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao. Robust Hashing For Image Authentication Using Zernike Moments And Local Features. *IEEE Transactions on Information Forensics and Security*, 8(1):55–63, 2013.

[4] i-Witness: The App That Could Save Your Life, https://iwitness.com/.

[5] Keeex: Create Your Own Photographic Proof in A Single Clic!, https://keeex.me/products/photo-proof.

[6] TruePic: Seeing is Now Believing!, https://truepic.com/.

[7] CameraV: Secure Verifiable Photo & Video Camera, https://guardianproject.info/apps/camerav.

[8] The Guardian Project: People, App And Code You Trust, https://guardianproject.info/.

[9] Quorum Advancing Blockchain Technology, https://www.jpmorgan.com/global/Quorum.

[10] Oracle VM VirtualBox, https://www.virtualbox.org/.

[11] Ethereum Blockchain App Platform, https://www.ethereum.org/.

[12] Diego Ongaro and John K Ousterhout. In Search Of An Understandable Consensus Algorithm. pages 305–319, 2014.

[13] A Permissioned Implementation Of Ethereum Supporting Data Privacy: Quorum Chain,https://github.com/jpmorganchase/quorum.

[14] Ana Isabel González-Tablas Ferreres, Benjamín Ramos Álvarez, and Arturo Ribagorda Garnacho. Spatial-Temporal Certification Framework And Extension Of X. 509 Attribute Certificate Framework And SAML Standard To Support Spatial-Temporal Certificates. pages 321–329, 2007.

[15] A. I. Gonzalez-Tablas Ferreres, B. Ramos Alvarez, and A. R. Garnacho. Guaranteeing the Authenticity of Location Information. *IEEE Pervasive Computing*, 7(3):72–80, July 2008.

[16] 3GPP TS 36.355 V14.5.1 (2018-04) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP) (Release 14).