Implementation of uWatch Digital Forensic Tool

1 Introduction

In recent times, a lot of crime has gone unsolved in South African neighbourhoods due to insufficient evidence to prosecute the perpetuators[South African Police Service 2014]. Mobile devices can be employed as tools that can curb and minimise crimes, using their cameras, voice recording and image capturing functions as a real-time digital evidence-capturing tool. However, the challenges that arise as a result of using mobile devices as a digital evidence capturing tool are in threefold:

1. Proving the integrity of the acquired and stored potential digital evidence (PDE).
2. Protecting the identity of the individual who captured the potential digital evidence.
3. Managing access to the stored evidence[Omeleze and Venter 2014].

1.1 Project Name

Online Neighbourhood Watch Digital Forensic Tool, known as uWatch.

1.2 Project Vision and Objectives

uWatch is a digital forensic acquisition tool that is used by members of communities in South Africa, to assist in reducing crime. The main objective of uWatch is to create a neighbourhood watch application, that can collect and store PDE which can be accessed by the South Africa Police Services (SAPS). The collected and stored PDE helps to address the problem of insufficient evidence being available to law enforcement agents and digital forensic investigators to prove that a crime has taken place and who committed the said crime. To meet the legal requirements and standards for digital evidence admissibility in a court of law, the PDE integrity is proven using mathematical techniques such as, cryptographic hash algorithms, digital signatures and PKI cryptography. Access to the stored PDE in the repository is maintained using role based access control (RBAC) and attributes based access control (ABAC) system.

1.3 Project Owner

University of Pretoria

1.4 Project Scope

The scope of this project is to develop a prototype as a proof of concept using a web application that is accessible via desktop or mobile/portable device. The application must allow storage and retrieval of PDE like, video clips, audio and photo images.

There is to be mobile web client for the uploader, who can upload PDE to the repository, while the desktop interface is to be used by the law enforcement agent, digital forensic investigator, judiciary members, or other stakeholders, who can download or view stored potential digital evidence for furthering an investigation or to be presented as evidence in a court of law.

To meet the legal requirements of admissibility, the system’s integrity, reliability and auditability are core requirements and implemented using various security features, like, cryptography which guarantees confidentiality and cryptographic hash functions and digital signatures.
to ensure data integrity. Access control measures are in place to manage authentication and authorisation thereby allowing only the intended users access to download or view potential digital evidence in the repository.

1.5 Use Case

In Figure 1, the primary actors are the human users, the system administrator, the law enforcement agent, digital forensic investigator, and the judiciary.

1.5.1 The human user actor

In the ONW system the human actor is mapped to the use case of potential evidence capturing. The person in the street who captures and uploads the PDE of an incident, is referred to as the ‘uploader’. The uploader’s functions are to captures PDE of a crime with their mobile device, upload the captured PDE to the ONW repository and receive confirmation as depicted in the UML diagram Figure 1. The precondition for a user to participate, is to have access to the uWatch interface on their device.

1.5.2 The law enforcement agent

The function of the law enforcement agent is to download PDE to corroborate their physical scene investigation and/or validate the evidence. The law enforcement agent must manage the PDE, by either accepting the evidence as valid and useful to their investigation, or reject and discard PDE at the discovering of evidence inconsistency [Omeleze and Venter, 2015]. As depicted in Figure 1, the actor role of the law enforcement agent is bounded to the digital forensic investigator who may assume both roles when required or based on job description.

1.5.3 The Judiciary

The third group of actors are the members of the judiciary. These can be the judge, jury, prosecutor and legal counsel for the defendant. Their role entitles them to view potential evidence. The PDE from the ONW repository will give the judge and jury a deeper understanding of the
case, as some aspect of the crime that they are asked to adjudicate on, has been captured live, so to speak. Both the prosecutor and the defending legal counsel also could use the potential evidence to prepare their arguments in court [DP van der, 2008] [Bellengere et al., 2013].

1.5.4 The Pre and Post Conditions

The pre and post conditions must also be realised in order for an actor to concretely realise their functions. For example, one of the preconditions of the system is for an ‘uploader’ to have captured PDE before attempting to upload to the repository. This condition must be met for the system to proceed to completing a task otherwise an exception is raised. The preconditions to uploading PDE to the ONW repository include a user having a device that can capture video, audio or images, preferable a mobile device, and the acquired PDE must be within the system domain of the mobile device. Post conditions apply to the ONW system, such as, an error message which indicates that the data has been altered during transition. This condition ensures PDE originality is ascertained. Another postcondition is to identify a state where PDE’s acquisition location tag is identified to be different from upload location tag.

2 Architectural Requirements

Architectural requirements provides the infrastructure within which their system components realises the functional requirements at deployment [Solms, 2010]. To realise architectural requirements, architectural patterns and strategies are concretely applied to achieve the identified quality attributes of the system.

2.1 Quality Requirement

Quality requirements are the measurable and testable properties of a system. It is used to indicate how well a system satisfies functional requirements.

The core quality requirements of the uWatch system are as follow: (i) Security, (ii) Reliability (iii) Auditability (iv) Maintainability (v) Pluggability (vi) Usability

Other quality attributes of the ONW system, i.e., ‘nice-to-have’ can easily be traded-off in order to meet the core quality requirements of the system, these are interoperability, performance and modifiability and scalability. Architectural patterns such as, microkernel, pipe & filter and layered are some of the means to achieve the above stated core quality requirements. While architectural strategies like, redundancy, clustering and encryption is also another means to achieve the system’s main goal.

2.1.1 Integration and Access Chanel Requirements

User’s interaction with the system is through web mobile application and desktop application client - using the HTTPS.

2.1.2 Technology

Technology such as, Python Django framework, Java EE, OO Databases and other frameworks, like, bootstrap (Responsive web design (RWD), is encouraged. However technology flexibility is accepted.
3 Algorithm

In order to achieve confidentiality, integrity and availability, with some of the specified pre and post conditions for uWatch system, an algorithm should be implemented that could check that the specified conditions are met.

An algorithm should be designed to do the following:

- To design or use an algorithm that detects when a non-PDE (Junk) is uploaded to the repository for malicious purposes such as, denial of service attack (DoS) or just some sort of 'fun' to the 'uploader'. For example, the algorithm should detect photos not related to crimes, video clips from movies or other such instances or audio sounds or junk noise that are not in any way relevant to crime. In designing this algorithm, however, care must be taken in order not to discard a 'real' potential digital evidence in the process of eliminating junk from the repository.

- Another algorithm maybe the need to auto upload PDE to the repository at capture. An auto upload function is activated when uWatch domain is populated with PDE. Unless however, a user chooses not to upload. This option, then activates 'the differ capture and upload location function'. This function is explained below.

- Difference in captured and upload location functionality) - An algorithm to detect a difference between the PDE capturing zone (or postal code) location from the location where it is uploaded to the repository. For example, for an incident that occurred in Hatfield and uploaded in Polokwane, the algorithm must identify this, log it to the system audit database, as well as alert the uploader.

4 Project Deliverable

Listed here are the expected project deliverables.

- Maintainable code (service concrete and componentalization) and code testing.
- Building and deployment scripts.
- Documentation, such as, user’s manual, functional and architectural requirement specification and the realisations of architectural decisions with design and testing plans.
- Possible presentation to the SAPS for input and the opportunity for further research and development.
- Grant full access to the uWatch code repository with version control in place. For example, the use of GIT or Bitbucket version control.

References


