BIRMINGHAM CITY
University

Scenario-based Learning for Multidisciplinary Digital Forensics Education

Syed Naqvi, Ali Abdallah
Centre for Cyber Security & Forensics

11 June 2015

BIRMINGHAM CITY University

Outline

- Introduction
- Digital Forensics scenarios
- Some problem areas
- Summary & perspectives

Outline

- Introduction
- Digital Forensics scenarios
- Some problem areas
- Summary & perspectives

Introduction

- Scenario-based learning (SBL)
  - Learning best takes place in the context where it is going to be used.
  - It involves students working their way through a storyline, usually based around a real-life case study.
  - Students are encouraged to play active role by using their subject knowledge, critical thinking and problem solving skills in real-world environment.

- SBL in the area of digital forensics
  - Set of scenarios to cover various stages of digital forensic analysis from evidence collection to the events correlation.
  - Legal dimension: Chain of custody, paperwork, evidence handling, etc.
  - Technical dimension: Imaging, password extraction, pin code, device connectors, etc.

Project ConSoLiDatE

- Multi-disciplinary Cooperation for Cyber Security, Legal and Digital Forensics Education
- Objectives:
  - Development of educational resources conveying:
    - essential cyber security knowledge
    - essential digital forensic investigations
    - essential legal principles
  - Provision of educational audio-visual resources that facilitate active student learning, debate, critical thinking and classroom engagement.
  - Development of strong links between theory and practice through consolidation of student's understanding of principles by examining applicability to carefully constructed practical scenarios.

BIRMINGHAM CITY University

Outline

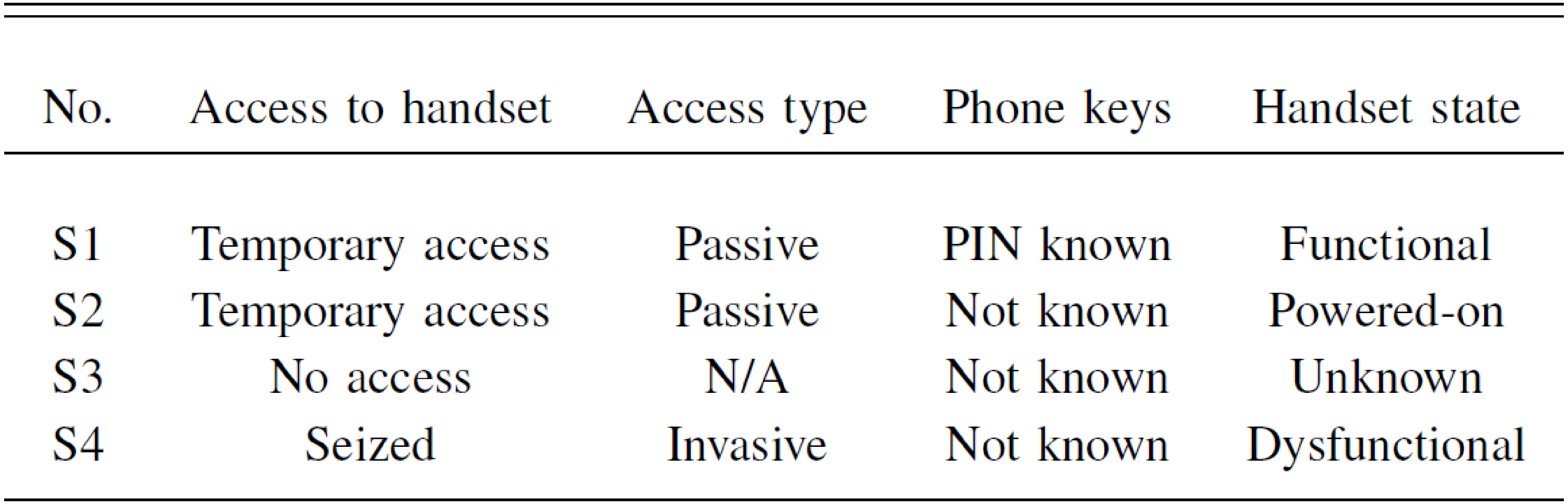
- Introduction
- Digital Forensics scenarios
- Some problem areas
- Summary & perspectives

Common acronyms

- BTS: Base Transceiver Station
- SIM: Subscriber Identity Module
- PIN: Personal Identification Number
- PUK: Pin Unlock Key

Digital Forensic Investigations

Example scenarios



No.	Access to handset	Access type	Phone keys	Handset state
S1	Temporary access	Passive	PIN known	Functional
S2	Temporary access	Passive	Not known	Powered-on
S3	No access	N/A	Not known	Unknown
S4	Seized	Invasive	Not known	Dysfunctional

Naccache et al. 2006

BIRMINGHAM CITY
University

S1: Data recovery method

- Standard mobile data extraction
- Use of write-blockers, license dongles, …
- Evidence files (physical, logical, …)

S2: Data recovery method

- Signal analysis
  - EM Monitoring
  - Power analysis
  - Fault injection
  - …

Naccache et al. 2006

S3: Data recovery method

- Traffic interception

- Cloning BTS unit

- Cloning target

- Privacy, legal issues!

S4: Data recovery method

- Chip-off forensics
  - Remove flash memory chip
  - Read it externally
- Handset is destroyed
- Risk of thermal destruction

Outline

- Introduction
- Digital Forensics scenarios
- Some problem areas
- Summary & perspectives

Examples of technical implications

- To extract data when encryption keys are **not known** and the access type is not **invasive**.

- Moreover, Chip-off is pointless
  - If BlackBerry device is attached to a BES (BlackBerry Enterprise Server), and you don't have access to the BES
  - The data cannot be decrypted by any commercial tool at this time
  - Real world scenario: hostile BES, BlackBerry seized and is usually PGP encrypted then you are at a dead end, even with chip-off

BIRMINGHAM CITY University

Examples of legal implications

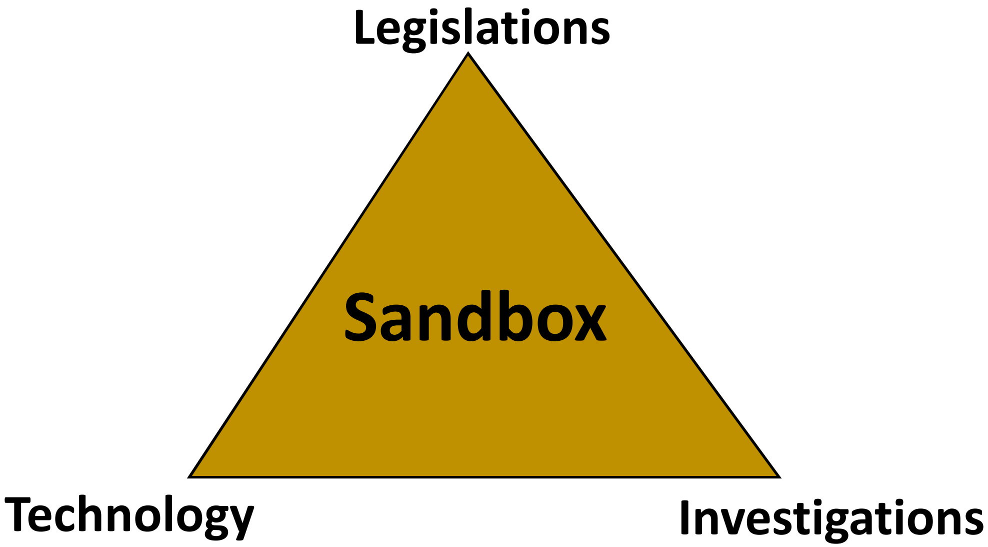
- Chain of custody of the evidence collected including equipment
- Legal means of data recovery.
  - Traffic interception is generally achieved by cloning BTS (Base Transceiver Station) and target units.
  - A digital forensic analyst needs to know the corresponding legal procedures before intercepting mobile traffic.
  - Lack of awareness and/or failure to follow the legal guidelines result in adverse effects in the investigations.

Outline

- Introduction
- Digital Forensics scenarios
- Some problem areas
- Summary & perspectives

Convergence

- We need to work on the **harmonisation** of digital forensic analysis methodologies and the governing policies
  - Scenarios-based testing
  - Identification of grey areas
  - Mutual validations



Perspectives

- We need to remain “at least” a step ahead of cyber criminals
- New technological landscapes require different perception of
    - Security
    - Investigations
    - Privacy & trust?
- At BCU, we are working on the technical side of cybercrime investigations
    - With close cooperation with the other stakeholders

"… when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived."

(Edmond Locard, 1910)