Developing an IoT Forensic Methodology. A Practical Concept Proposal

By:
Juan Manuel Castelo Gómez, Javier Carrillo Mondéjar, José Roldán Gómez and José Luis Martínez Martínez

From the proceedings of

The Digital Forensic Research Conference

DFRWS EU 2021

March 29 - April 1, 2021

Developing an IoT Forensic Methodology. A Practical Concept Proposal

Juan Manuel Castelo Gómez, Javier Carrillo Mondéjar, José Roldán Gómez and José Luis Martínez Martínez

UCLM Universidad de Castilla-La Mancha

I3A Instituto de Investigación en Informática de Albacete
Albacete Research Institute of Informatics

DFRWS EU 2021 – 31st March 2021 – Cyberspace

Introduction and Motivation

Introduction

- Internet of Things:
  - There are more IoT units than non-IoT ones (12 billion)
  - Weak security measures of IoT devices
    - 100 million attacks were detected in 2019
    - 85% of attacks on Q3 2020 targeted Telnet
  - Several contexts, some of them managing critical operations and/or very sensible data
    - eHealth, Smart Cities, Smart Homes, Wearables, Smart Vehicles

Introduction and Motivation

Motivation

- Differences between conventional forensics and the IoT:
  - ○ Number of devices in a network
  - ○ Exchange of data
  - ○ Use of the cloud
  - ○ Accessibility

Introduction and Motivation

Motivation

- Therefore, using conventional solutions might not be the best approach to follow in in order to ensure the effectiveness and completeness of examinations
- However, there are factors which hinder the creation of brand new proposals
  - Laws regarding forensic investigations
  - Lack of IoT-centered forensic tools
- Possible solution: adapting conventional solutions to the requirements of the IoT

Proposed Methodology

- Uses a conventional model as a reference (Yusoff et. al., 2011) and follows an eminent practical approach
- Phases:
  - Pre-Process
  - <u>Identification</u>
  - Acquisition & Preservation
  - Analysis
  - <u>Evaluation</u>
  - Presentation and Post-Process

Proposed Methodology
Pre-Process

- Prepare in advance for the investigation and develop the action plan
  - Learn the characteristics of the IoT network and its devices
  - Establish the degree of forensic soundness required
  - Obtaining warrants

Proposed Methodology
Identification

- The range of the investigation is far greater than in conventional forensics
  - Devices can be miles away and still be part of the same network. Therefore, the investigator must rely on logical connections
- Crucial to establish an order of examination
  - Importance of the device and its data
    - Lifetime, quantity and relevance of the data
    - Significance of the device in the environment
    - How difficult would it be to acquire its data

Proposed Methodology
Acquisition & Preservation

- Same techniques than in conventional forensics
- Live acquisition gains importance
  - Soldered storage and compatibility with JTAG or chip-off
- Acquiring the network traffic is crucial, as most of the data is exchanged on-the-fly
  - Due to compatibility, it might be captured from other devices such as routers or central nodes

Proposed Methodology
Analysis

- Two key aspects:
  - Feasibility of the acquisition process
  - Requirements regarding the integrity of the evidence
    - Every country has different laws regarding digital forensics
- Certain flexibility should be allowed so that live analysis becomes a more common approach
- Limitations:
  - Execution of demanding tasks
  - Variety of devices and systems

Proposed Methodology
Evaluation

- New phase needed due to the holistic aspect of the IoT
- Goals:
  - ○ Gather all the evidence collected and confirm that the individual conclusions drawn are correct
  - ○ Determine whether any pieces of evidence can be linked together and how they fit into the whole environment
  - ○ Draw conclusions from the perspective of the environment

Proposed Methodology
Presentation and Post-Process

- Actions needed for the closing of the investigation
  - Writing and presenting the report
  - Returning the original sources of evidence
  - Restoring the systems
    - Clean the environment
    - Restore the systems
    - Evaluate the effectiveness of the actions performed

Conclusions

- Conventional solutions might not be suitable for the investigation of IoT cyberincidents
- An interesting option might be adapting these conventional solutions to the requirements of the IoT
- There are few proposals that follow an eminent practical approach for the development of IoT methodologies
- This work is a first step for the design of a practical IoT forensic methodology

Developing an IoT Forensic Methodology. A Practical Concept Proposal

Juan Manuel Castelo Gómez, Javier Carrillo Mondéjar, José Roldán Gómez and José Luis Martínez Martínez

UCLM
Universidad de Castilla-La Mancha

I3A
Instituto de Investigación en Informática de Albacete
Albacete Research Institute of Informatics