FLUX: A Forensic Time Machine for Wireless Networks

Kevin P. Mc Grath§ & John Nelson

§kevin.mcgrath@ul.ie

April 2006

Outline

1. Introduction
2. CoMo System Architecture + Results
3. Network Forensic Analysis Tool Requirements
4. FLUX: A Network Forensic Time Machine
5. Future Directions

OLLSCOIL LUIMNIGH
UNIVERSITY OF LIMERICK

Wireless Access
Research Centre

sfi
science foundation ireland
fondúireacht eolaíochta éireann

Introduction

The research community has approached the problem of wireless measurements and proposed several measurement/monitoring architectures

- *The first generation of wireless measurement systems include tcpdump and ethereal, which records network traffic on a monitored link*
- *The second generation introduced monitoring frameworks for collection and storage, e.g. CoMo, ORBIT OML, DAMON*
- *The next generation will focus on analysis, leading to forensic evidence based systems.*

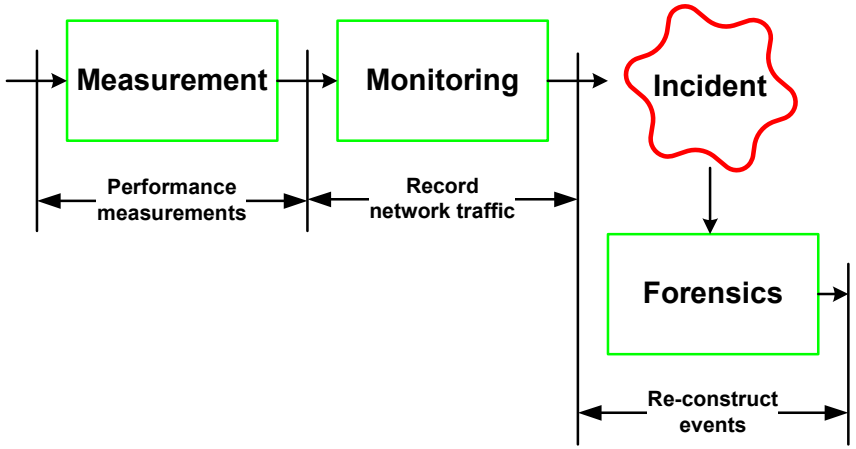
Network forensics is an emerging field and is becoming increasingly important as a means for enterprizes to identify certain information security risks, and abnormal network behavior.

We define network forensics as the ability:

- *To playback incidents using a non-intrusive continuous network traffic recording system.*
- *To collect forensic evidence in near real time.*
- *To detect long-term trends and in particular:*
  - *(i)* after the incident understanding of what actually happened and
  - *(ii)* substantiation of events.

This work enables a typical monitoring infrastructure for collection, storage and analysis of *forensic evidence*

- *We introduce FLUX, a network forensic time machine, that discovers useful information about the wireless environment necessary for network forensic investigations*



Forensic Process

Forensic Barrier

To provide an infrastructure for forensic data collection, storage, and dissemination, that satisfies the following:

- The infeasible prolonged storage of raw network data.
- Extraction of valuable data as forensic evidence.
- The long-term data retention period of forensic evidence.

A Network Forensic Analysis Tool Uses include:

- Traffic shaping/engineering
- Incident playback
- Long-term anomaly detection

The Monitoring Tool

After reviewing current state of the art monitoring infrastructures, the Intel CoMo platform is preferred for this work.

The ***Intel CoMo[1]*** platform is a passive network monitoring infrastructure, for:

- The fast prototyping of network data mining applications, i.e. traffic analysis methods
- Retrospective queries on past traffic

A set of core processes handle data flow movement

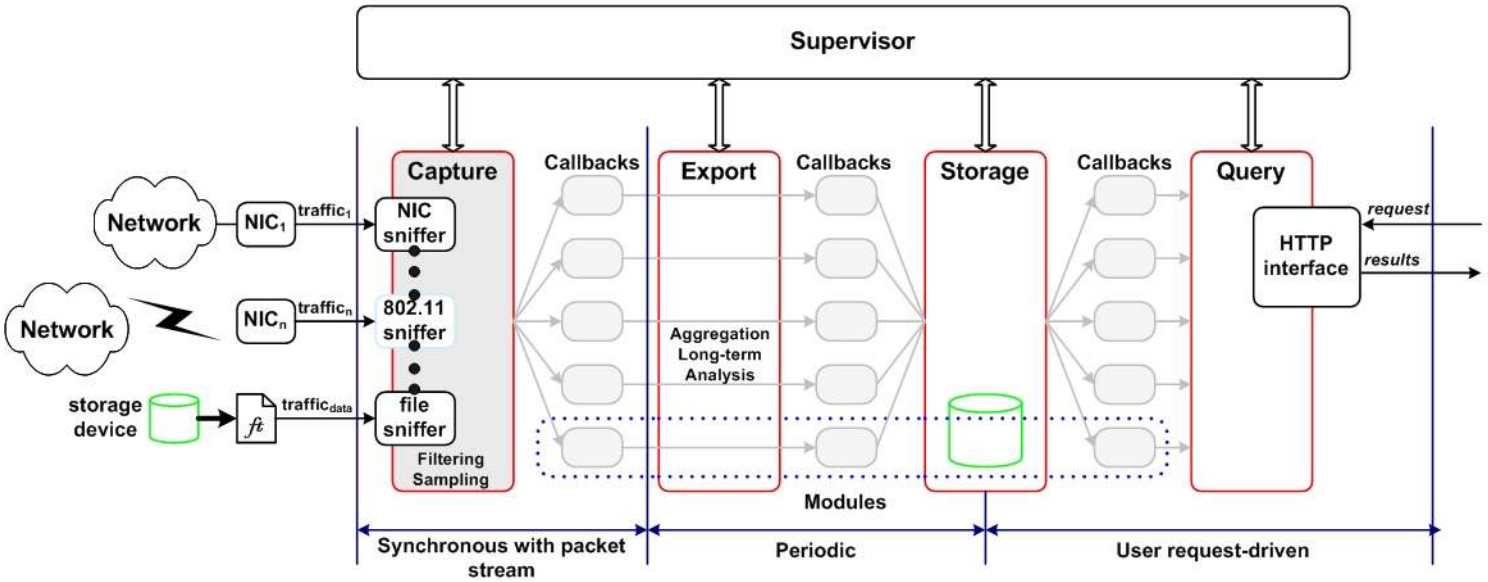
- CAPTURE, EXPORT, STORAGE, QUERY

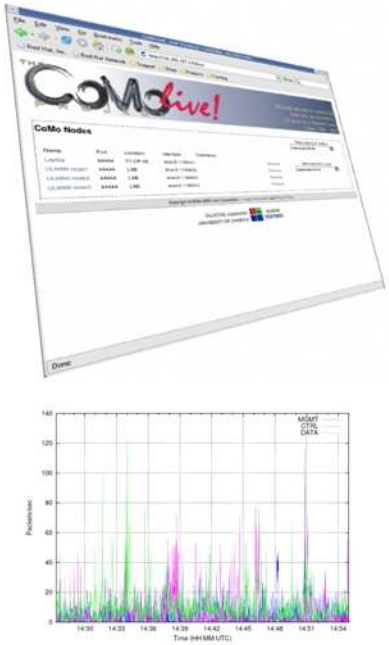
Implementation available @: http://sourceforge.net/projects/como

Users write traffic plug-in modules (queries reside in plug-in modules) that contain a set of predefined callbacks, in the C programming language to extract the relevant information.

Necessary 802.11 ***Intel CoMo[1]*** extensions

- Implemented a CoMo 802.11 packet processing parser
- Provided CoMo 802.11 support for ARM-based platforms, specifically the **Intel/xbow STARGATE** platform
- Implemented CoMo 802.11 software sniffer
- Coded a number of plug-in modules as proof of concept
- Generated a CoMo 802.11 macro library to provide a level of abstraction



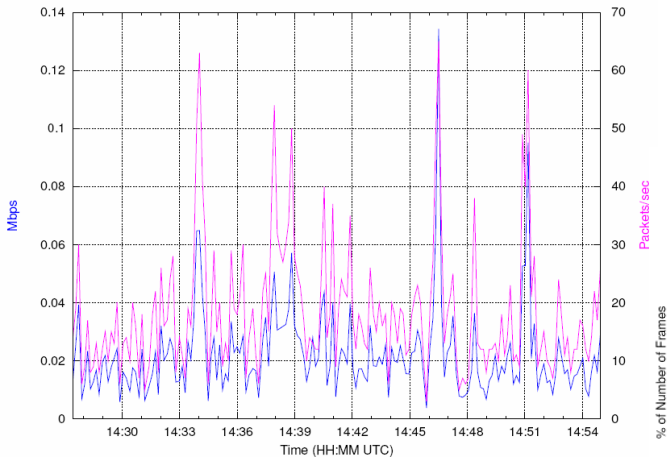


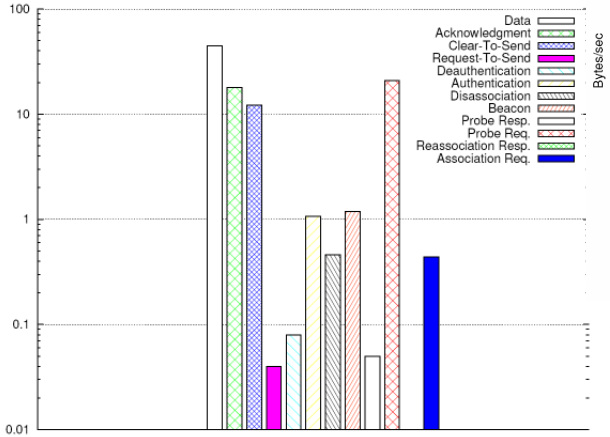
CoMo System Architecture

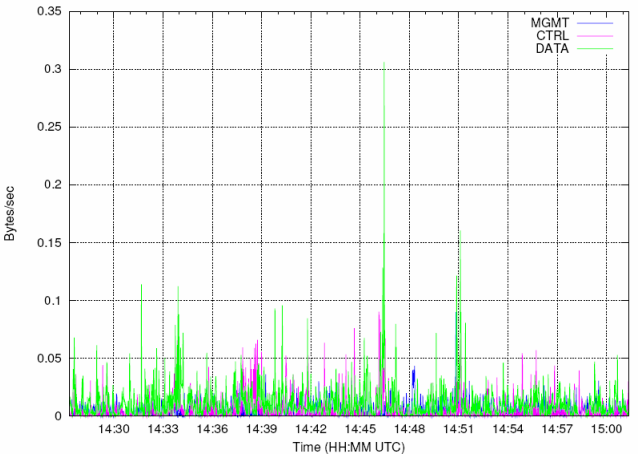
The CoMo platform is integrated into the ***ULMAN testbed***

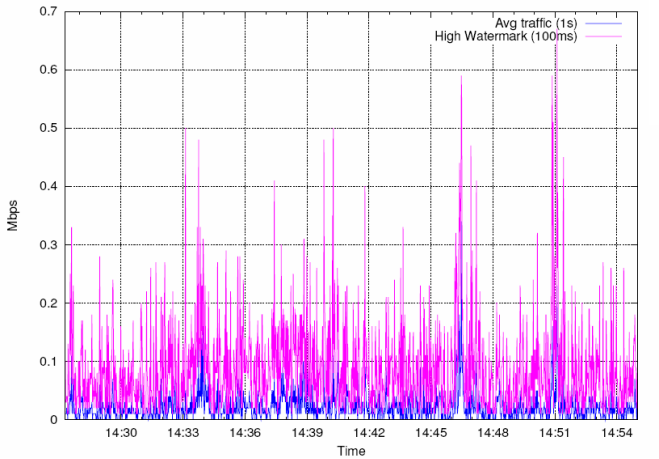
[1] **http://como.intel-research.net/**

802.11 MAC Traffic Characterization:
'The New CoMo Wireless Side'

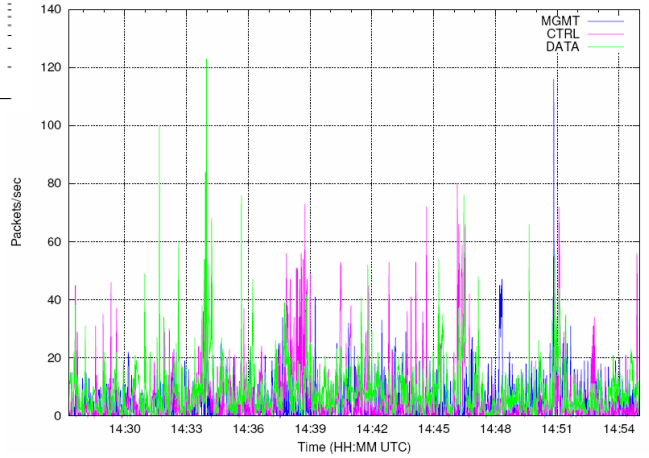








"Exposes the wireless medium characteristics in IEEE 802.11"



The defined queries expose the wireless medium characteristics (potential evidentiary data).

The purpose of forensic plug-in modules (queries reside in plug-in modules), is to reduce redundancy and provide potential forensically tamper-proof evidentiary data.

"Protecting the collected network evidence is imperative in network forensics"

Network Forensic Analysis Tool (NFAT)

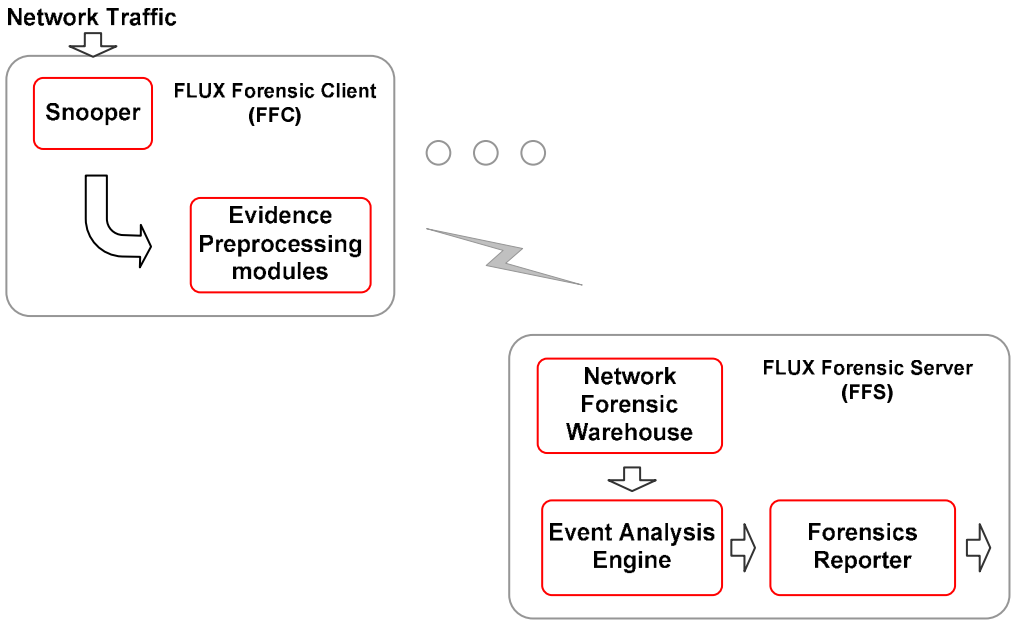
NFAT Requirements

- The NFAT shall automate the collection of forensic data on a live system
- The NFAT shall build a chronological incident playback component, to assist post-event analysis, which transforms raw data into meaningful knowledge.
- The NFAT shall transform the network evidence into a standard report format.

FLUX

"A Network Forensic Time Machine"

FLUX, enables a typical monitoring infrastructure for forensic data collection, storage and analysis in a wireless environment.



FLUX System Architecture

FLUX Forensic Client

Each FFC is a standalone resource constrained Linux platform, i.e. a PCM-9373 VIA low power Eden processor single board computer (SBC), with a PC104 expansion connector to support multiple radios

FLUX: A Forensic Time Machine

FLUX: A Network Forensic Time Machine

- The purpose of FLUX, a network forensic analysis tool, is to build intelligence about network usage, by uncovering long-term anomalous traffic through transforming raw network data into actionable knowledge
- FLUX reconstructs events, by utilizing a non-intrusive continuous network traffic recording platform
- The 'Time Machine' concept relates to the amount of dedicated storage to evidentiary data which can be forensically analysed
  - **"greater storage capacity implies greater time travel"**
- The anticipated data retention period for the network forensic devices is many weeks

FLUX Forensic Server

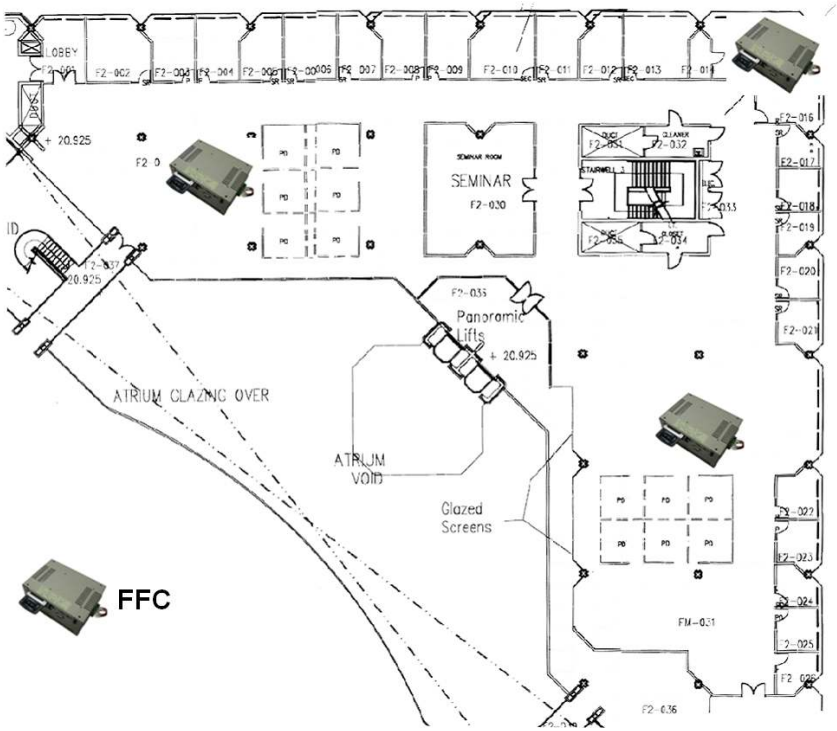
- Stores network forensic evidence
- Analyses a subset of the data warehouse evidence to identify events, and to rebuild incident patterns
- Protects sensitive data revealed by analysis

FLUX Forensic Client

- Snoops the RF environment, recording traffic flows, with plug-in modules to detect malevolent activity, network anomalies and security risks.
- The plug-in modules, are essentially evidence pre-processing modules to reduce redundancy, as storing raw network data would overwhelm the data warehouse

FLUX Tamper-Resistant Protocol

- The FLUX communication protocol is tamper-proof to preserve accuracy and integrity of findings



FLUX Forensic Client Indoor Deployment

Monitoring & Forensics Next Steps …

Validate the forensic system by leveraging the Intel CoMo monitoring infrastructure platform

Develop forensic scenarios, to prove, that longer term data storage enables new anomalies to be detected.

Investigate the use of IEEE802.11k standard extension to provide potential network evidence through defined measurements

Investigate DIT wireless traffic probe within FLUX

Integrate FLUX into project testbeds

Review FLUX suitability for heterogeneous systems, i.e. 802.16 and 802.11