Sound Bytes: From Memory to Audio Signals for Industrial Control Systems' Defense

Nehal Ameen[1], Ramyapandian Vijayakanthan[2],Adeen Ayub[1], Aisha Ali-Gombe[3], Irfan Ahmed[1]

[1] Virginia Commonwealth University [2] Towson University [3]Louisiana State University

Introduction

Industrial Control Systems manage and automate physical processes of critical infrastructure, which makes them a major target for attackers. The field of ICS is constantly facing challenges in **triaging** such attacks through current digital forensic practices. This work presents WaveSleuth, a novel approach that leverages memory signals to conduct heart-beat checks that can detect anomalies that occur as a result of these attacks in PLCs' memory.

Contributions

1. A methodology that requires zero-semantic knowledge, is easy to use, and can utilize process runtime execution contexts, making it more efficient
2. WaveSleuth: A triaging tool that proved to be extremely efficient at detecting attacks with even the smallest footprint in a very short time
3. A stress testing methodology for reliable evaluation

Motivation

American critical infrastructure was under attack on May7th, 2021. Colonial Pipeline suffered a ransomware attack that:

- Forced the US energy company to shutdown 45% of the East Coast's fuel distribution pipeline for 6 days
- Caused gas shortages, huge financial losses, and an emergency declaration

Colonial Pipeline decided to shutdown their own pipeline as a response to the attack, because they did not know the extent of the damage, so we need:

- A methodology to identify the size and impact of an attack without shutting everything down
- To build resiliency within the critical infrastructure sector so that if attacked, services could come back online quickly
- A tool to quickly and efficiently triage Physical Systems to detect whether they're infected and mitigate the attack

Challenges

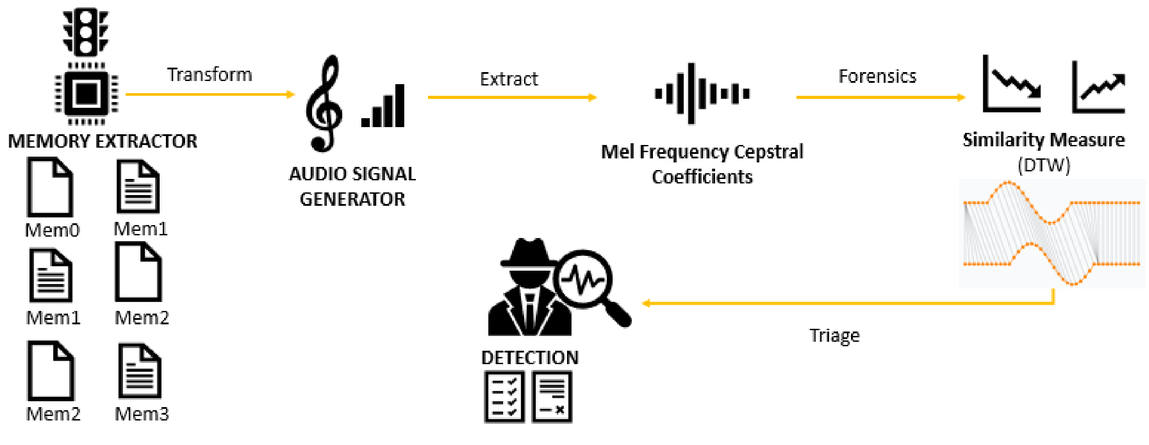
PLC memory forensics involves analyzing raw memory dump data, which is complex and time consuming as it:

- Contains vast amounts of complex data
- Is stored in a binary format, not human readable or easily interpreted
- Makes byte-to-byte comparison brittle and unstable
- Makes extracting relevant information from this raw format requires expertise in memory structures, data formats, and system architectures
- Requires efficient processing techniques, adequate computational resources, and appropriate storage capacities that are not easily available

System Design

WaveSleuth consists of 5 main components:

1) **A PLC Memory Extractor:** PEM, periodically extracts memory dumps
2) **Audio Signal Generator:** Lossless transformation of binary file to .wav file
3) **MFCC Extractor:** Set of features that encapsulates the overall shape of the spectral envelop
4) **Similarity Measurer:** Dynamic Time Warping Distance between consecutive audio signals
5) **Memory Signal Detector:** Compare Dynamic Time Warping Distance against threshold to determine the memory dump's integrity



Evaluation