Queensland University of Technology, EGB242

Code Challenge 8:
Decoding a Totally Legitimate Keylogger Output

Group 1:
Gennady Gennadyevich Golovkin n1152113
Saul Canelo Alvarez n1142114
Oscar De La Hoya n1182110

March 18, 2022

Introduction

Our firm has been engaged to unlock a password protected, legacy computer system. Unlocking this system will require the recovery of a 7 bit ASCII voltage waveform that has been distorted by a stray capacitor on the SCSI port of the computer used to log the keystrokes.

This report will detail the process undertaken to reverse distortion introduced by a stray capacitor by modelling the capacitance as a Linear Time-Invariant (**"LTI"**) system. Once the undistorted voltage waveform has been recovered, the report will set out the steps taken to decode the message given that it has been encoded as a 7-bit ASCII binary message.

1 Reversing Waveform Distortion

Our client has recorded an analogue voltage waveform of a binary password message. This analogue waveform has been distorted by a capacitor connected to the keylogging computer. This section will detail the processes undertaken to reverse the distortion introduced by the capacitor. The capacitor will be modelled as an LTI system and the inverse process will be applied to the saved waveform to recover the original binary message.

1.1. Modelling capacitor as a LTI system

The transfer function for the capacitor circuit has been modelled and stored in the `System.p` file. This transfer function is an LTI system which act on the voltage waveform as follows:

$$v_{distorted} = h_{Capacitor} * v_{binary}$$

The impulse response of the system ("$h_{Capacitor}$") can be found by passing an impulse into the LTI system. This impulse response was recovered from the `System.p` function in MATLAB by passing an impulse through the system.

```
10  impulse = [1, zeros(1, length(output)-1)];      % Approximate a dirac delta function
11  impulse_resp = System(impulse);                  % Pass an impulse through the
12                                                   % modelled capacitor system
13  impulse_resp = impulse_resp(1:length(output));  % Truncate response to output length
14  Freq_resp = fft(impulse_resp);                   % Find frequency response
```

By using this MATLAB script we can observe (Fig. 1.1) that the capacitor's impulse response exponentially decays over time and follows the expected impulse response of a typical low-pass RC filter circuit.[1] It's behaviour as a low pass filter is confirmed by observing the frequency response of the system.

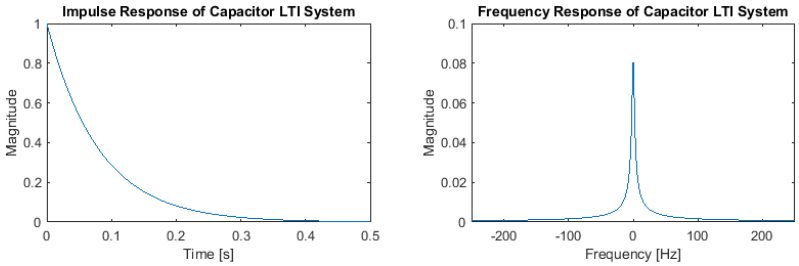

Figure 1.1: Impulse and frequency response of the modelled capacitor system.

1.2. Removing distortion from stored password waveform

The distortion introduced into the password's waveform has obscured the binary ASCII data saved from the keylogger and this distorted waveform can be seen in Fig. 1.2.

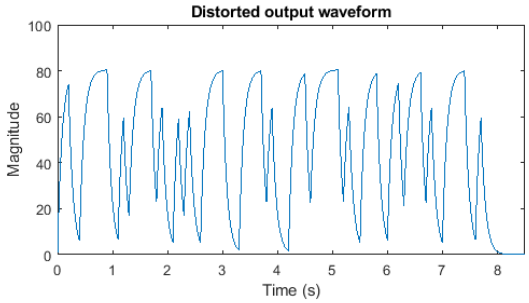

Figure 1.2: Distorted output voltage waveform.

The modelled response of the capacitor system found in Sect. 1.1 will be used to remove the distortion from the output waveform. This is done by noting that two functions convolved in the time domain are multiplied in the frequency domain, or explicitly:

$$f(t) * g(t) \overset{\mathscr{F}}{\rightarrow} F(f) \times G(f)$$

This means that if both the output waveform ($v_{distorted}$) and the impulse response of the capacitor system ($h_{capacitor}$) are transformed into the frequency domain then the distortion in the output signal can be removed by dividing the output signal by the (now) frequency response of the system. This process has been implemented in the MATLAB environment as follows:

```
22  Output = fft(output);                          % Find frequency domain
        representation of
23                                                 % output
24  Input = Output./Freq_resp;                     % Deconvolve in frequency domain
25  input = ifft(Input);                           % Find time domain equivalent of
        denoised
26                                                 % signal
```

This de-noised signal has been visualised in Fig. 1.3 and it can be seen that the original binary waveforms are now easy visible.

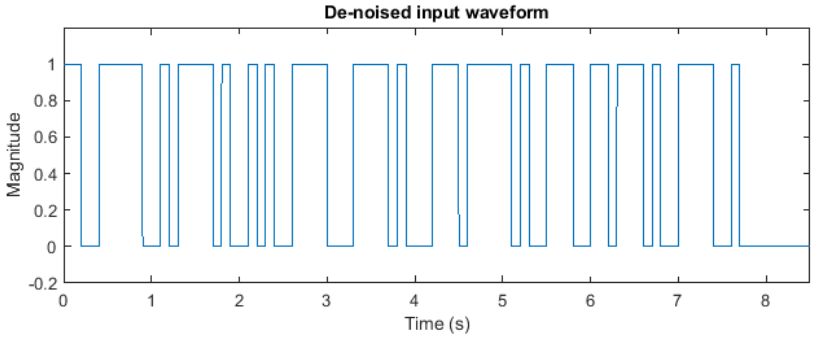

Figure 1.3: De-noised password waveform.

2 Decoding binary waveform

The binary waveform recovered in Sect. 1. respresents a password encoded in 7-bit ASCII. This allows MATLAB's inbuilt 7-bit ASCII interpreter to decode the stored password. However this password signal must first be manipulated into a form that MATLAB can properly interpret.

The first step in this process is to simplify the signal waveform into it's binary representation. This is done in MATLAB by first grouping all samples corresponding to a given bit and then finding the average of those samples to determine whether the bit is most likely a 1 or a 0.

```
37 % Simplify time to bits
38 input = input(1:end-mod(length(input),ptsPerBit)); % make length multiple of 100
39 input = reshape(input, ptsPerBit, []);          % Reshape to 1 bit duration per
       column
40 input = round(mean(input));                     % Find bit value for that duration
```

After determining the most likely binary sequence associated with our signal we can say that the first 7-bits of the signal (being the first letter of the password) are:

$$1100111$$

After determining the correct binary sequence we can decode the signal by grouping the binary sequence into 7-bit groups and feeding this binary matrix into MATLAB's `char()` function to recover the password as text.

```
42 % Find 7 bit characters
43 input = input(1:end-mod(length(input),7));      % make length multiple of 7
44 input = reshape(input, bitsPerChar, []).';      % reshape 7 bits per column, and
45                                                 % transpose for 7 bits per row
46 password =  char(bin2dec(num2str(input)));      % Decode, and transpose for reading
```

Which decodes the stored password for the legacy computer system as:

$$\text{getschwifty}$$

3 Reflection

Something about what the key learning objectives were in the assessment, what challenges you faced in the assessment and recommendations on what to change in the future so that you can improve your work in the future.

References

[1] "RC circuit." [Online]. Available: https://www.electronics-tutorials.ws/rc/rc_1.html