**NANYANG TECHNOLOGICAL UNIVERSITY**

**2nd YEAR COMPUTER ENGINEERING**

**Windows Management Instrumentation Security**

****

Interim Report

Name: Chew Zhi Jie

Date: 30/1/2017

Table of Contents

**No table of contents entries found.**

# Introduction

Cyber attacks are on the rise, costing companies millions to tens of millions in average. Stolen private information and denial of service also affect individuals extensively. An example is the massive global ransomware cyber attack known as “WannaCrypt” or “WannaCry”. It affected more than 150 countries whereby tens of thousands of computers were infected, including critical infrastructures like hospital which forced them to stop servicing partially.

Malware, also known as file-based attack, has been a norm since the early computer era. In majority of the case, malware attacks can be track down easily by Security Analyst. However, several recent high-profile attacks have adopted “living off the land” technique where it is a file-less attack and leverages heavily on legitimate system management tool such as the Windows Management Instrumentation. The first file-less attack was first discovered in 2010 and it has been on a rise since then. These attacks normally go under the radar of security protection software and is nearly impossible to track as it is usually stored in very unusual places such as the Memory. These legitimate system management tools bring convenience to system administrator, however, the flip side is that it also increases the risk of the system being compromised.

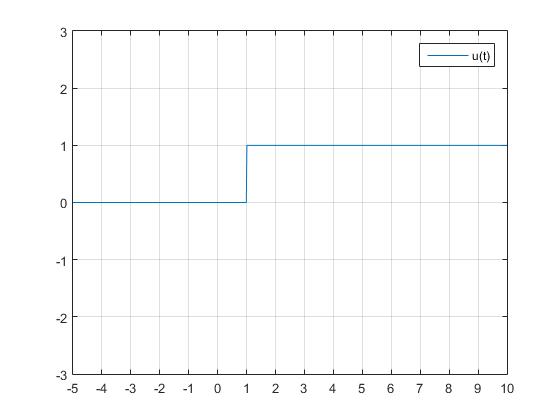
One of those system management tools is Windows Management Instrument, also known as WMI. WMI is preinstalled since the early Windows 2000 Operating System. It is a Web-Based Enterprise Management System for accessing computer information in an enterprise environment. Administrators are able to utilize Windows Management Instrumentation Command-line to interact with WMI. WMI consists of various privileged functions such as retrieve sensitive data, script automated task, manipulate system registry and many more. This is also where WMI becomes dangerous, attackers cloud use creative ways to abuse WMI. An example is using WMI to inject payload, normally an executable script, into the system registry and bind the payload to a startup event. Hence, the malicious script will be automatically executed upon startup and this technique hijacked the victim to actively listen to Control and Command Server. NotPetya, a cousin of WannaCry, is an example of a cyber attack that utilizes WMI. NotPetya uses PsExec and WMIC to spread its infection. Although NotPetya is not as deadly compared to WannaCry, it also infected over 12,500 machines and further the possibilities of WMI based attack.

This paper presents the study on both offensive and defensive components of WMI security. For offensive component, WMI is used to remotely abuse and attack victim computer without any use of payload while in the case of defensive component, a defensive tool will be created to mitigate and ultimately prevent WMI-based attack. Both components are then used to compiled into a penetration testing tool for cooperate usage.

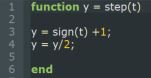
# 5.1 Defining and plotting step functions

Step Function u(t)

Graph:



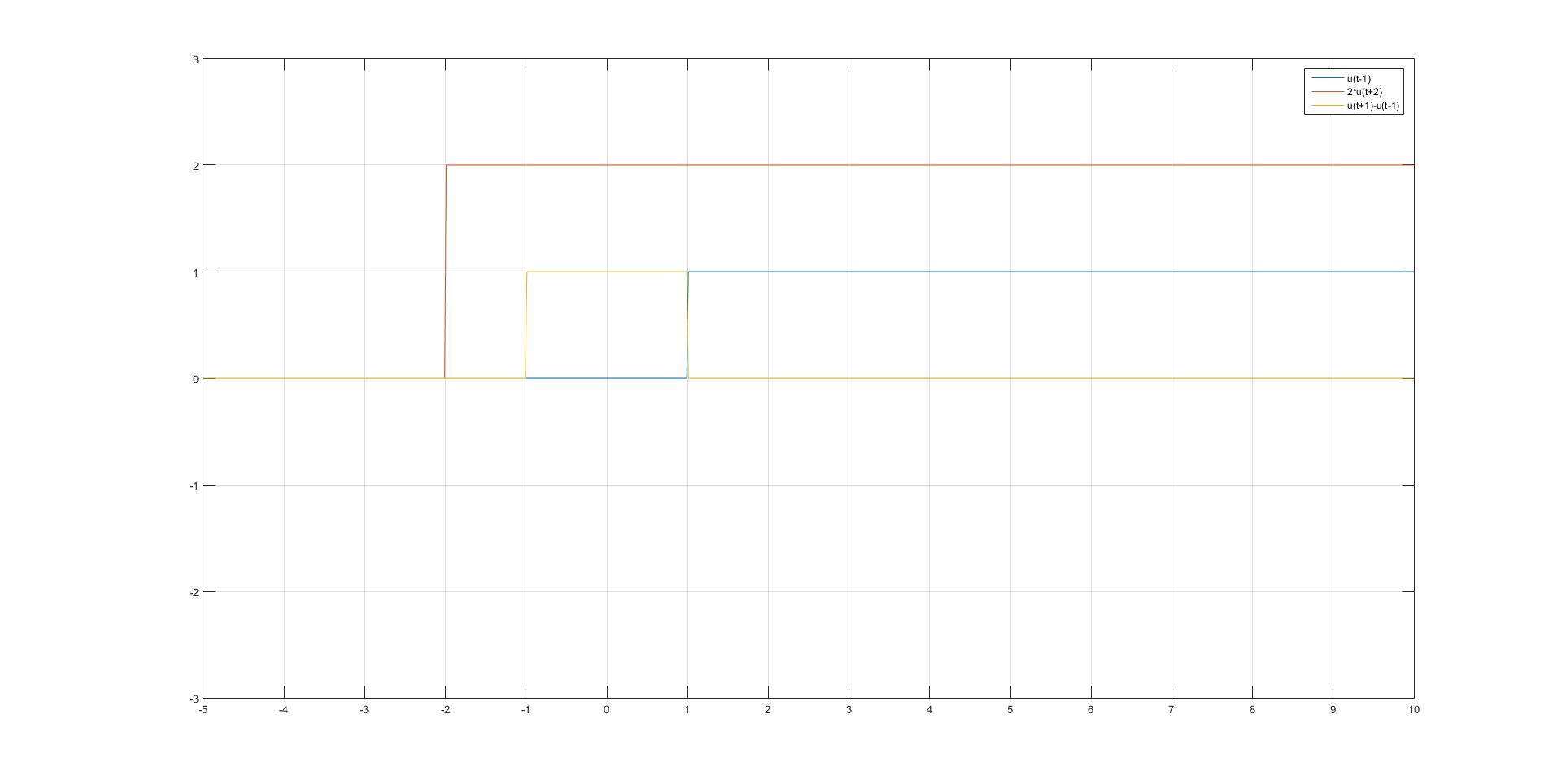
Code:

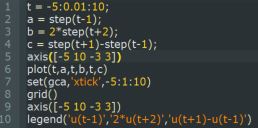


Since sign(x) function returns 1 when x is greater than 0, returns 0 when x is 0 and returns -1 when x is lesser than 0. Hence the Peak to Peak amplitude is 2. To get the step function we need to shift up the graph up 1, done using *line3*, which shifts the Peak to Peak to 2 to 0. After that, we need to reduce the amplitude from 2 to 1. This is where *line 4* comes in, which will reduce the amplitude from 2 to 1.

Exercise a, b & c in Experiment 5.1

Graph:



Code:

First, the independent variable t need to be initialise. The range of t ranges from 5 to 10 and the sampling size is 0.01. This is achieved by *line 1*.

After that, the three equation need to be initialise which is u(t-1), 2\*u(t+2) and u(t+1)-u(t-1) at *line 2,3 and 4* respectively