SEDF

A Spoofed Email Detection Framework

Employed by a Lightweight Web Browser Plug-In for Detecting the Spoofed Email

INSTITUT PENGURUSAN PENYELIDIKAN
UNIVERSITI TEKNOLOGI MARA
40450 SHAH ALAM, SELANGOR
MALAYSIA

BY:

ALYA@GEOGIANA BUJA

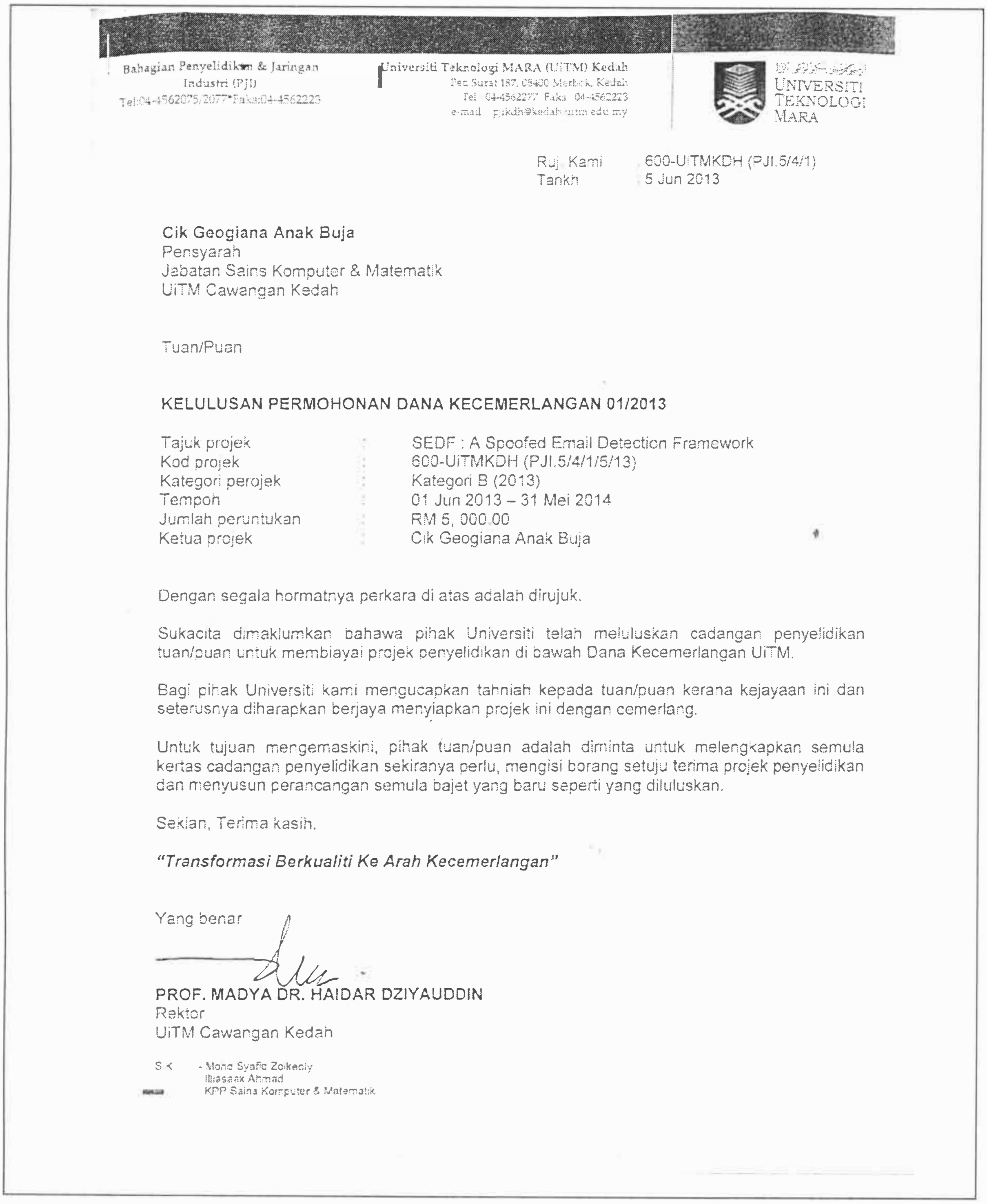
ILLIASAAK AHMAD

MOHD SYAFIQ ZOLKEPLY

NOVEMBER 2014

Contents

1.0 Letter of Offer (Research Grant)



Bahagian Penyelidikan & Jaringan
Industri (PJI)
Tel:04-4562075/2077*Faks:04-4562223

Universiti Teknologi MARA (UiTM) Kedah
Pet Surat 187, 08400 Merbok, Kedah
Tel 04-4562277 Faks 04-4562223
e-mail pjikdh@kedah.uitm.edu.my

UNIVERSITI
TEKNOLOGI
MARA

Ruj. Kami 600-UiTMKDH (PJI.5/4/1)
Tarikh 5 Jun 2013

Cik Geogiana Anak Buja
Pensyarah
Jabatan Sains Komputer & Matematik
UiTM Cawangan Kedah

Tuan/Puan

KELULUSAN PERMOHONAN DANA KECEMERLANGAN 01/2013

Tajuk projek	:	SEDF : A Spoofed Email Detection Framework
Kod projek	:	600-UiTMKDH (PJI.5/4/1/5/13)
Kategori perojek	:	Kategori B (2013)
Tempoh	:	01 Jun 2013 – 31 Mei 2014
Jumlah peruntukan	:	RM 5, 000.00
Ketua projek	:	Cik Geogiana Anak Buja

Dengan segala hormatnya perkara di atas adalah dirujuk.

Sukacita dimaklumkan bahawa pihak Universiti telah meluluskan cadangan penyelidikan tuan/puan untuk membiayai projek penyelidikan di bawah Dana Kecemerlangan UiTM.

Bagi pihak Universiti kami mengucapkan tahniah kepada tuan/puan kerana kejayaan ini dan seterusnya diharapkan berjaya menyiapkan projek ini dengan cemerlang.

Untuk tujuan mengemaskini, pihak tuan/puan adalah diminta untuk melengkapkan semula kertas cadangan penyelidikan sekiranya perlu, mengisi borang setuju terima projek penyelidikan dan menyusun perancangan semula bajet yang baru seperti yang diluluskan.

Sekian, Terima kasih.

"Transformasi Berkualiti Ke Arah Kecemerlangan"

Yang benar

PROF. MADYA DR. HAIDAR DZIYAUDDIN
Rektor
UiTM Cawangan Kedah

S.K - Mohd Syafiq Zolkefly
Illiasaak Ahmad
KPP Sains Komputer & Matematik

2.0 Enhanced Research Title and Objectives

2.1 Original Title as Proposed

SEDF: A Spoofed Email Detection Framework

2.2 Enhanced Title

SEDF: A Spoofed Email Detection Framework, Employed in a Lightweight Web Browser Plug-in for Detecting the Spoofed Email

2.3 Original Objectives as Proposed

1. To develop a mechanism (plug in) of open source email client for detecting email spoofing.

2. To evaluate the efficiency of a developed mechanism.

2.4 Enhanced Objectives

1. To address the criteria of the spoofed email based on the information in email header.
2. To develop a framework for detecting the spoofed email based on the defined criteria of the spoofed email.
3. To develop a lightweight browser plug-in by employing the developed framework for detecting invalid email.

4. To evaluate the efficiency of a developed mechanism (the framework).

3.0 Report

3.1 Proposed Executive Summary

E-mail spoofing is the one of the greatest thread among the computer user especially for those person or organization which always use an e-mail as a main medium to communicate. This fraud can affect the user and organization credential and lead to a serious problem information leak and so on. Most of the victims that involved in this case is an IT illiterate user who literally does not have enough knowledge to differentiate between the fake emails. There are sort of protection or mechanism that have been developed to help user but their complicated brings inconvenient and difficulties to the user. In this project, it introduce to a mechanism to detect an e-mail. The main idea is to identify an e-mail that user feel suspicious about the content and originality. The method used to detect fake e-mail is by tracing back the email header. Any email that sent out still have several stored in the mail header. Therefore, this research will propose the SEDF to overcome the problem of email spoofing. The algorithm use to match the word in the searching period in the mail header is based on The Boyer-Moore. Boyer – Moore algorithm was claimed to be the fastest algorithm among the others. Using this approached, it is guarantee that it is able to help user to identify fake mail.

3.2 Enhanced Executive Summary

The rapid changes in information and communication technology (ICT) have helped the advancement of communication medium (i.e. electronic mail) between networked users. The use of electronic mail or e-mail is essential is today's world. Communication via e-mail not only can deliver large amount of data but most importantly it can be delivered in split-second. E-mail spoofing is one of the well-known threats that can be used to get confidential information. Through this technique, the unauthorized person aka attacker will spoof the e-mail to become a valid email from a known sender. Without any knowledge of that, the recipient will truly trust the sender and respond to the spoofed email. This not only brings harm to the users but also the organization. One of the simplest ways to check the validity of the email is by validating the sender's email header. This paper discussed on the framework that can detect the spoofed email based on the defined criteria of the invalid email received. The results found that the proposed framework which have been employed in a lightweight web browser plug in for the purpose of detecting the spoofed email able to work out based on a few experiments that have been done on several samples of email headers.