# A Contribution to the Development of Counter Measures for Dead Dropping in Cyber Warfare

GJCST Classification (FOR)
D.4.6, K.6.5

Nayani Sateesh

***Abstract* - In recent years, cyber warfare has become the major threat to world safety. Terrorists are using the internet as their weapon to do suicide attacks, hijackings, bomb blasting, attacking the networks etc to create the grate damage. In order to defend against future attacking, it is important to understand how they are making use of the internet services and hence to create the counter measures. In this paper, we are considering an internet service called email - which is used for dead dropping to do cyber warfare, and developing a framework to counter it.**

*Keywords*-cyberwarfare, dead drop, Autherisation, Authentication.

## I. Introduction

Internet has become critically important to the financial viability of the national and global economy. Internet made this world as a global village and kept everything on the web in a single click distance. It makes the people to get connected regardless of their geographical areas and distances. internet provide various services to the users which includes e-mail, FTP, Telnet, Archie , GOPHER , finger, Usenet and Mailing list , WWW etc. These services facilitate the user to get connected to the remote users, resources and can share the knowledge. Apart from these, we are also witnessed the cyber terrorism by the terrorists who used internet as their weapon. One of such service used by them in the recent attacks is emails using the dead drop method. Dead drop is the method in which the users will share the username and password for the email account in which they will store and share the messages in the email drafts.

## II. Problem under Study

Permissions over the resources in the networks or internet are granted to the users with the help of authorization and authentication mechanisms.Authorization is the function of specifying access rights to resources, which are related to information security , network security etc. It involves defining the access policies Authentication is the process by which we can verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints. Once the username and password are shared, then any person can access the resources on the network. This pitfall has given strength to the attackers to share their credentials to access the resources over the networks who are geographically dispersed with the same credentials. This advantage has given a shape to dead dropping Dead drop is the method in which the users will share the username and password for the email account in which they will store the messages in the email drafts. Those who are shared the username and password can only login and read them, in which there is no scope to identify where the mail is generated or received as the contents are stored in drafts only. The identity of the sender or receiver is only known once the mail is sent over the internet. We can find the identity using the email headers using various email header analyzer tools. In this paper we are not focusing on these tools but can have a look at way we can analyze the headers to get the identity of sender and receiver.In the following section we will discuss on the framework that we are proposing and way it could work. This framework can be easily implemented from intranet to the internet level.

## III. Related Work

Whenever a cyber crime is done over the internet through emails, the identity of the accused is getting find out using the email headers only if and only if the mails are transmitted over the internet only.

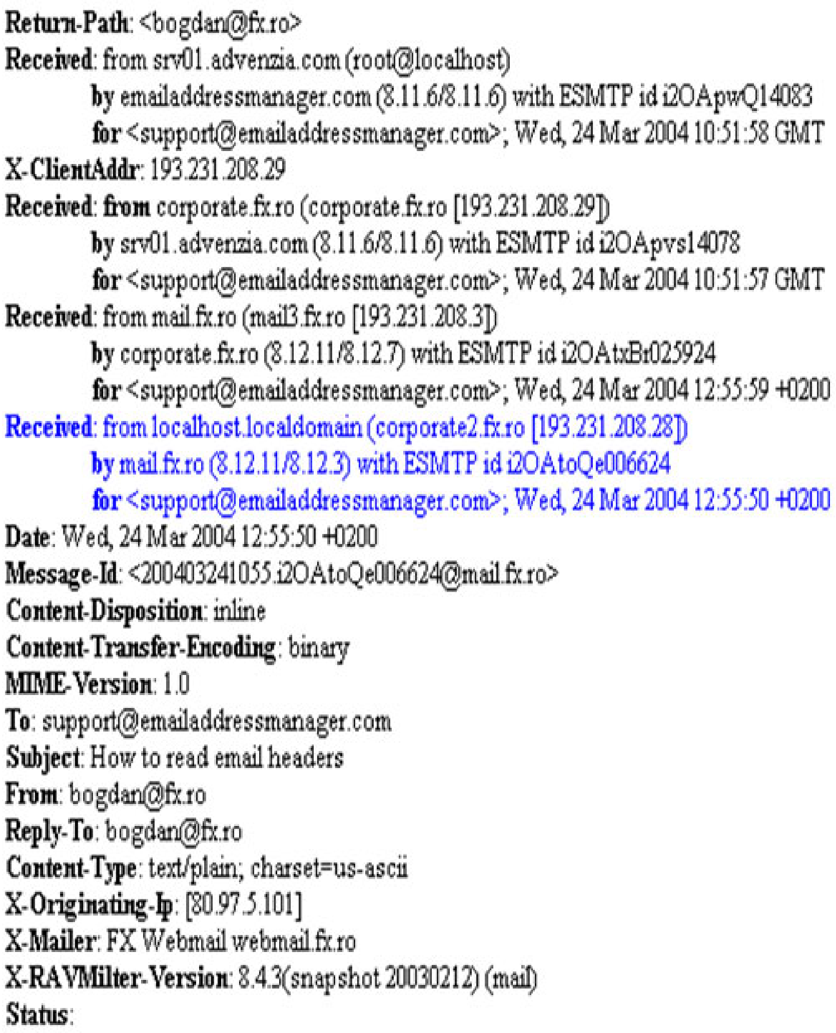
### *Email Header*

The email header is the information that travels with every email, containing details about the sender, route and receiver. It includes the details such as who sent the email, when the email was sent, from where it was sent and how did it arrived and who is the receiver and when it was received.

### *Email headers interpretation*

Let‘s take an example (we will ignore the header tags that do not give precise information about the sender). The following email was received by support@emailaddressmanager.com and we want to see who the sender is. Here is the email header of the message:

*About- Hyderabad, Andhra Pradesh, India – 500081nayanisateesh@gmail.com*



```
Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
        by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
        for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: from corporate.fx.ro (corporate.fx.ro [193.231.208.29])
        by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
        for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
        by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBr025924
        for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
        by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtoQe006624
        for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:
```

There are three paragraphs starting with the Received tag: each of them was added to the email header by email servers, as the email travelled from the sender to the receiver. Since our goal is to see who sent it, we only care about the last one (the blue lines). By reading the Receiving From tag, we can notice that the email was sent via corporate2.fx.ro, which is the ISP domain of the sender, using the IP 193.231.208.28. The email was sent using SMTP ("with ESMTP id") from the mail server called mail.fx.ro. Looking further into the message, you will see the tag called X-Originating-IP: this tag normally gives the real IP address of the sender. The X-Mailer tag says what email client was used to send the email (on our case, the email was sent using FX Webmail).

## IV. PROPOSED FRAMEWORK

We are proposing a framework to counter the dead drop using the MVC Architecture. The following figure shows the typical function of the each module.

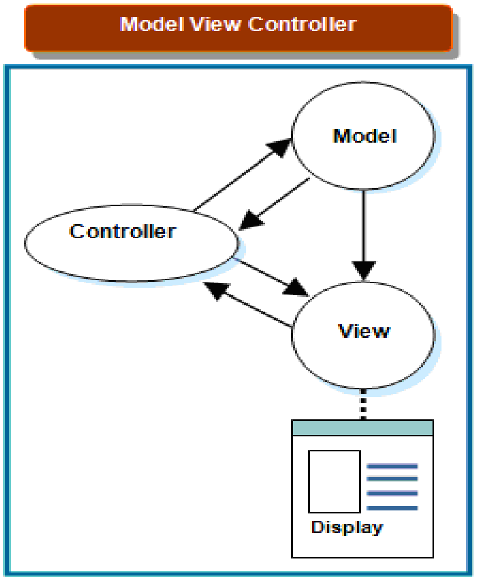


Fig: 4.1 – MVC Architecture

In MVC, View module deals with the user interfaces through which the user will get interact with the applications. Controller deals with the events and the invoking of the appropriate applications to provide the services. Model component deals with the underlying database. The controller module will be working an interface between the View and Model components in the MVC architecture In our proposed work, the user will be given an interface to login to the email service. The user will enter his user name and password. Once the user is logged in, we will take the IP address of the user through Server side Includes (SSI). Here is a typical syntax in javascript to get the IP address of the host.

```
<script language ="javascript">
var ip = '<!--#echo var="REMOTE_ADDR"-->';
</script>
```

Whenever an entry is made in the drafts or drafts were read, an event will be fired and the controller will send the mail content to the content analyzer where the mail contents will be analyzed. The content analyzer should be sophisticated with the text / data mining techniques such as classification, clustering, Bayesian classification etc.so that it will analyze the mail text or the attachment contents about the significance of threaten. The analyzer can be built-up with the capability to analyze the words, phrases, content type. If the content is significantly related to the cyber attack, then the controller will invoke an application saying that the draft is something related to malicious or threat and send to an appropriate authority as message or mail along with the IP address where the drafts entry is made or the draft is read.

## V. Limitations

Dial-up users may have a different IP address each time they connect, and many other users may be behind proxies so that hundreds of machines will all report the same IP address

## VI. Conclusion

Counter Measures for the Dead Dropping is still under research. The efficiency of this framework should be analyzed at the intranet lever before enhancing it to the internet mail applications.

## VII. Future work

We can also implement the biometric approach such as identifying the people by their typing patterns. Need to integrate the well-versed content analyzer algorithms for classifying the content correctly in email drafts.

## VIII. Acknowledgments

I would like to thank the anonymous reviewers for their insightful feedback, which greatly improved the quality of this paper. I also thank one and all who helped me in making this paper published

## IX. References

1) S. Sellke, N. Shroff, and S. Bagchi, Modeling and Automated Containment of Worms", IEEE Transactions on Dependable and Secure Computing, PP. 71-86, Vol. 5, No. 2, April-June 2008
2) How to read email headers" http://www.gradwell.com/support/howto/article/404
3) Behrouz A. Forouzan, Catherine Ann Coombs, Sophia Chung Fegan ―Data Communications and Networking
4) HTML Black Book - Steven Holzner
5) A Whitepaper on Effective Content Analysis for Email Inspection and Control", By Nemx Software Corporation, Canada.http://www.nemx.com/documents/Content%20Analysis%20Whitepaper.pdf