****

**Email Spoofing Detection Prevention & Alerting**

**“Winning Team” Under**

**Ministry of External Affairs**

**At**

**Smart India Hackathon 2017 Grand Finale**

**Techno Freakz**

**Team Members:**

**P.SEENIVASAN**

**R.SUJITHA**

**N.SATHISH KUMAR**

**M.R.REVATHY**

**C.VIKRAM KUMAR**

**M.NITHYA**

**Team Mentors:**

**Dr. A. JAMEER BASHA**

**T. S. Arun**

**Aim:**

To develop a prototype that can detect the spoofed mails and will be able to block the mails from entering into the receiver’s mailbox.

**Summary:**

Email Spoofing is a well-known threat to the information security. In the recent past several email spoofing attacks have been executed resulting huge losses in terms of Information Security and monetary loss. This proposal provides a comprehensive solution to provide immunity against Email spoofing attacks at the receiving mail server side. The solution provided in this proposal, primarily makes use of the MIME headers available in the email along with industry standard algorithms to detect spoofed emails, stop from reaching the inbox of the recipient and to send alerts to authorized persons as and when spoofed emails are received. The proposal provides three custom algorithms making use of MIME data and also make use of Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to provide a comprehensive solution in a fail fast manner. The results are demonstrated in a live system using Apache James Mail Server. The solution provided can easily be adopted to any messaging and communications server with minimal changes.

**Introduction:**

E-mail spoofing is a term used to describe (usually fraudulent) email activity in which the sender address and other parts of the email header are altered to appear as though the e-mail originated from a different source. Email spoofing finds a wide variety of victims who may be attacked for a multiple reason. Initially when a mail is sent from a server, it passes through the Domain mail server and passes through the receiver’s mail server environment. The proposed algorithm inside the mail server environment, which detects the spoofed mails using the raw MIME format associated with every mail. The MIME format consists of variety of details that are related to the specific mail. The proposed algorithm retrieves specific fields from the MIME format and use them in identifying the spoofed mails that differs from the legitimate mail. Once the spoofed mails are detected using the set of algorithm they are prevented from entering further into the standard algorithm that are associated with regular mail servers. Hence this mechanism prevents the spoofed mails from entering into the receiver’s mail box. This proposed solution not only prevents the mails from entering into the mail box but also adds an additional functionality of alerting to some authorized person regarding the spoofed mails.

**Objective:**

* The main objective of this proposed system is to detect the spoofed mails at server side itself.
* To stop the spoofed mails from entering into the receiver’s mailbox.
* To alert the authorized persons regarding the spoofed attack.
* To prevent data, lose due to fraudulent emails.
* To enhance the security in the receiver’s mail server.

**Status**:

The current status of our project is that our team has developed an “Mailet” using java programming language. Our team developed the prototype as an “Mailet” because Apache James server supports mailet feature. This developed mailet is added to Apache James 3.0 mail server which has been used as test server for testing our test cases regarding the detection of spoofed mails. The designed unique Mailet is placed inside the mail server before standard algorithm of the server. The prototype is unique in all cases and this kind of prototype has been developed and used by any mail servers. This prototype can be developed as a “Milter” which can be used with Oracle Communication Messaging Server, because oracle server supports only Milter feature. This can be done and added to the oracle server with minimal changes from the Mailet. This kind of prototype haven’t developed by any developer or servers and this is not in existence since it’s a unique prototype developed by our team.

**Novelty:**

* Smart India Mailet is unique in all the aspects and has been developed specifically for the **detection** of spoofed mails.
* No other mailet has been brought into existence with similar prototype.
* This is the only mailet which can detect spoofed mails and **prevent** them from entering into the mailbox.
* This mailet has been also embedded with an additional functionality of **altering** an authorized person/official of the designated server.
* This can be also developed as a Milter for oracle server.

**Work plan:**

Our team has planned to develop the prototype as a plugin/add-on for 3rd party cross platform applications like Mozilla Thunderbird. This plugin can be used by any of the cross platform email applications. And also aims in identifying the geometric location from where the mail has been generated and also in identifying the server from which the mail is composed. By identifying the server and geometric location of the fraudster, necessary actions can be initiated to prevent future spoofing attacks.

* **Open Source Technology Stack to be used**

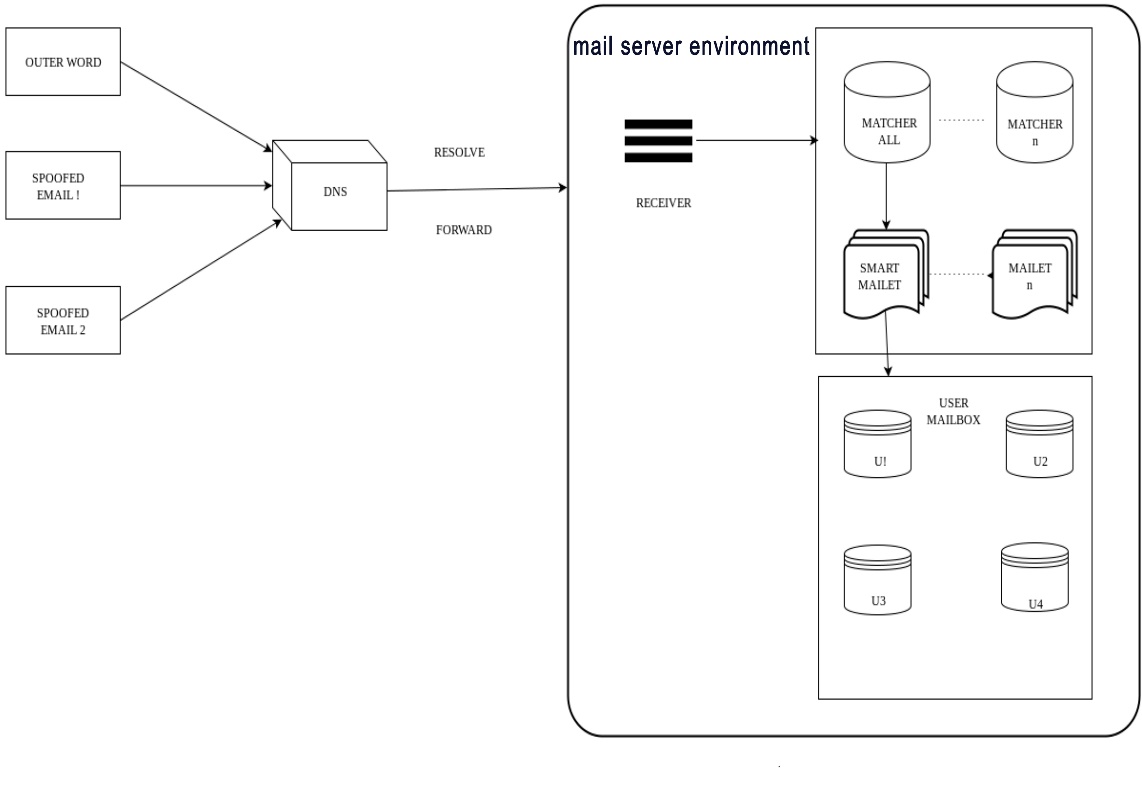
Apache James server for testing.

Language -java

* **Any technologies that you used during SIH2017 that you wish to change/ alter? Why?**

In SIH 2017, our team developed the prototype as an mailet which can be used by only Appache James server. Now it has been planned to develop as an plugin/add-ons, which can be used as per the user requirements in cross-platform applications like Mozilla thunderbird etc.

* **Architecture Block Schematic**

****

* **Time line and responsibility of participating team**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Particulars** | | **Time (months)** | | | | | |
| # | **Tasks** | **Team Member’s Name** | **1st Month** | **2nd Month** | **3rd Month** | **4th Month** | **5th Month** | **6th Month** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

* **Comprehensive budget**

Budget requirements (total as well as individual institutions/laboratory along with monthly break-up covering manpower, travel, contingencies, overheads, others (if any) and equipment for the 6 months project duration)

(***Rs. in lacs*)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Head of Expenditure** | **1st Month** | **2nd Month** | **3rd Month** | **4th Month** | **5th Month** | **6th Month** | **Total** |
|  | **Recurring** | | | | | | |
| Travel |  |  |  |  |  |  |  |
| Contingencies |  |  |  |  |  |  |  |
| Other research expenditure (e.g. Outsourcing) |  |  |  |  |  |  |  |
|  | **Non-recurring** | | | | | | |
| Equipment and accessories |  |  |  |  |  |  |  |
| Licensing cost (for using proprietary technology, if any) |  |  |  |  |  |  |  |
| **Total** |  |  |  |  |  |  |  |