



# Detecting the Spread of Virus Emails

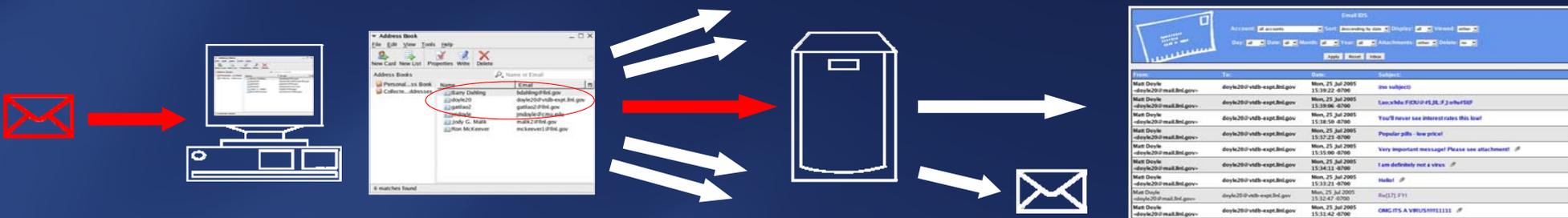
Matt Doyle, Carnegie Mellon University

Information Technology Protection Division, Barry Dahling

Lawrence Livermore National Laboratory

## Abstract

The uncontrolled spread of malicious, virus-bearing emails continues to pose a serious threat to modern computer networks. In order to successfully combat these outbreaks, system administrators must be able to detect and observe malicious emails as soon as possible. The goal of this project is to successfully implement a system which administrators can use to detect, capture, and observe these mass-mailing email viruses.



1. A virus-bearing email arrives in a client's inbox. The virus then forwards copies of itself to all contacts on the victim's address book.

2. One of these contacts corresponds to a unique monitored account on a dedicated machine. This account should only ever receive virulent emails.

3. The dedicated machine then notifies system administrator(s) via email. Received messages can then be inspected using a web-based interface.

4. Using the web-based interface, system administrator(s) can analyze virulent emails from a number of accounts, sort emails based on several fields, and inspect attachments.

## Implementation

This project is broken down into 2 primary programs:

`detect.php`: This program is run in the background as a daemon, where it monitors the email spool file(s) for changes using MD5 hashes. When new emails are detected, the raw message and attachments are separated into individual files and placed into an email repository. A database entry is also made for each email in order to facilitate sorting and searching.

`observe.php`: This program is designed to give the system administrator a web-based interface which can be used to sort and search through the virulent emails which have been received. `observe.php` presents basic data about the emails by way of MySQL queries, and can retrieve the raw message data and attachments from the email repository if necessary.

## Future Work

While this project has successfully implemented a system with the desired properties, there are areas which can be improved and expanded:

- The main area for future work in this project is the issue of deployment. In large environments such as LLNL, seeding every email client with the address of a monitored account is hardly a trivial task. Widespread deployment of this system will require significant amounts of policy work.
- Future enhancements could allow administrators to react to threats presented, not only observe them. (i.e. quarantining infected machines)
- The code in `detect.php` could be enhanced so that it scales better for larger deployments. While the current code can handle rates of several emails per second, significantly higher rates could degrade performance.