BASICS OF EMAIL

By,
Dr. Akash Thakar
Assistant Professor
Rashtriya Raksha University
MO. - 99090 39066
EMAIL – akash.thakar@rru.ac.in

Email Investigations: Overview

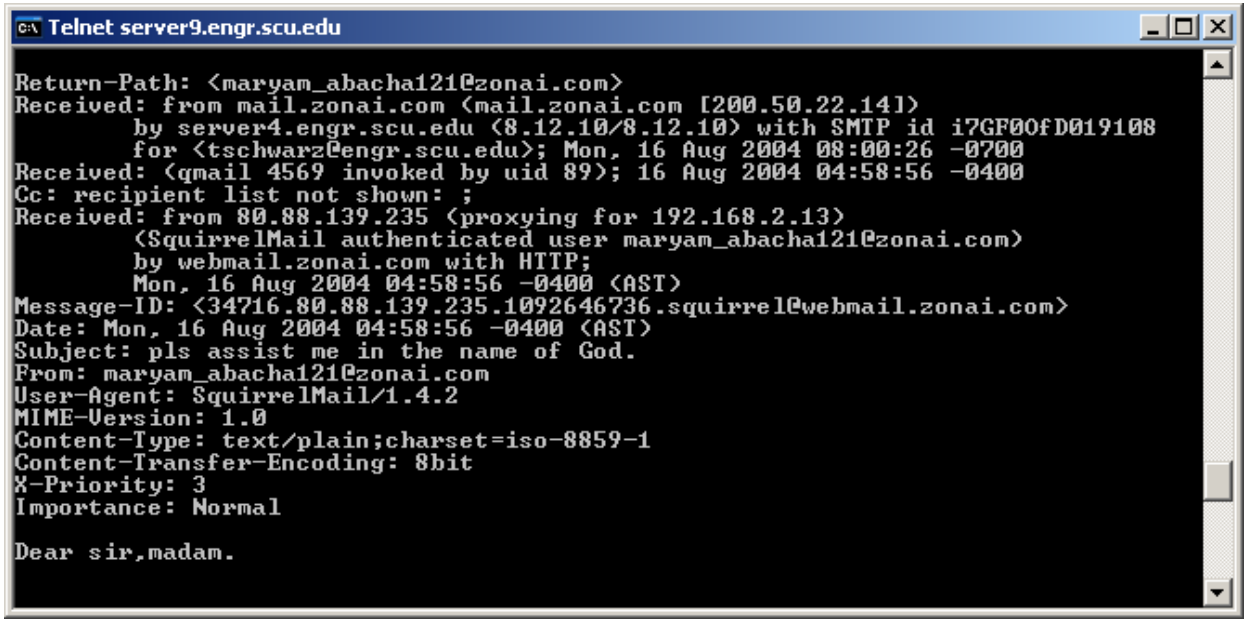
- Email has become a primary means of communication.
- Email can easily be forged.
- Email can be abused
  - Spam
  - Aid in committing a crime …
  - Threatening email, …

Email Investigations: Overview

- Email evidence:
  - Is in the email itself (header)
  - Left behind as the email travels from sender to recipient.
    - Contained in the various logs.
      - Law enforcement can use subpoenas
      - System ads have some logs.

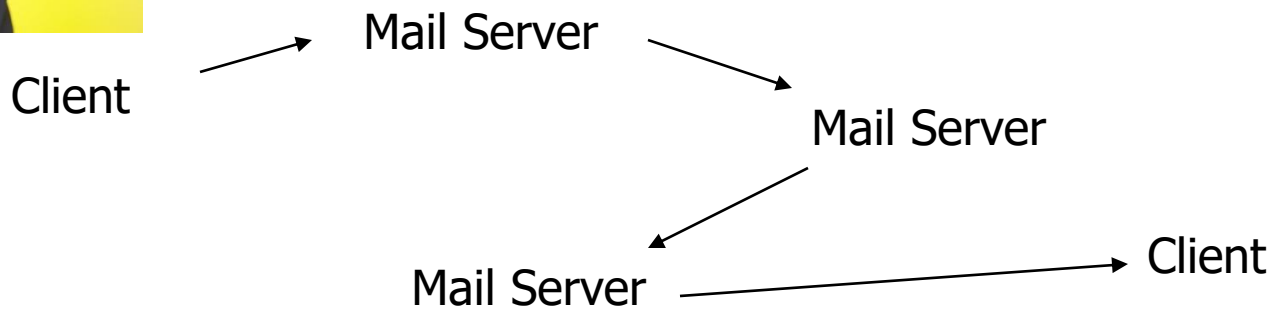
Email Fundamentals

- Email travels from originating computer to the receiving computer through email servers.
- All email servers add to the header.
- Use important internet services to interpret and verify data in a header.



Email Fundamentals

- Typical path of an email message:



Email Fundamentals: Important Services

- Verification of IP addresses:
  - Regional Internet Registry
    - APNIC (Asia Pacific Network Information Centre).
    - ARIN (American Registry of Internet Numbers).
    - LACNIC Latin American and Caribbean IP address Regional Registry.
    - RIPE NCC (Réseau IP Européens Network Coordination Centre).
  - Whois
  - www.samspade.org
  - Numerous other websites.

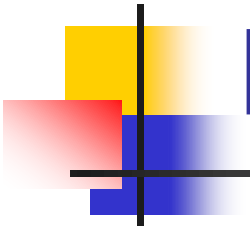
My Favorite.

Email Fundamentals

- IP-Addressing
- IP Version 4 is slowly replaced by IP Version 6.
  - IPv4: 4 digital numbers between 0 and 255.
  - IPv6: 8 digital numbers between 0000 and 0xffff.
- Static / dynamic addresses
  - Dynamic addresses assigned by DHCP within a local domain (with same leading portion of IP address).

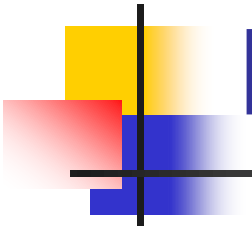
Email Fundamentals: Important Services

- Many organizations use Network Address Translation.
  - NAT boxes have a single visible IP.
  - Incoming I-packet analyzed according to address and port number.
  - Forwarded to interior network with an **internal** IP address.
  - Typically in the private use area:
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0-192.168.255.255
  - Private use addresses are never used externally.



Email Protocols:

- Email program such as outlook is a **client application.**
- Needs to interact with an email server:
  - Post Office Protocol (POP) (Port 110 and 995 {Secure})
  - Internet Message Access Protocol (IMAP) (Port 143 and 993 {Secure})



Email Protocols:

- A mail server stores incoming mail and distributes it to the appropriate mail box.
- Behavior afterwards depends on type of protocol.
- Accordingly, investigation needs to be done at server or at the workstation.

Email Protocols:

Post Office Service	Protocol	Characteristics
Stores only incoming messages.	POP	Investigation must be at the workstation.
Stores all messages	IMAP MS' MAPI Lotus Notes	Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.
Web-based send and receive.	HTTP	Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation.

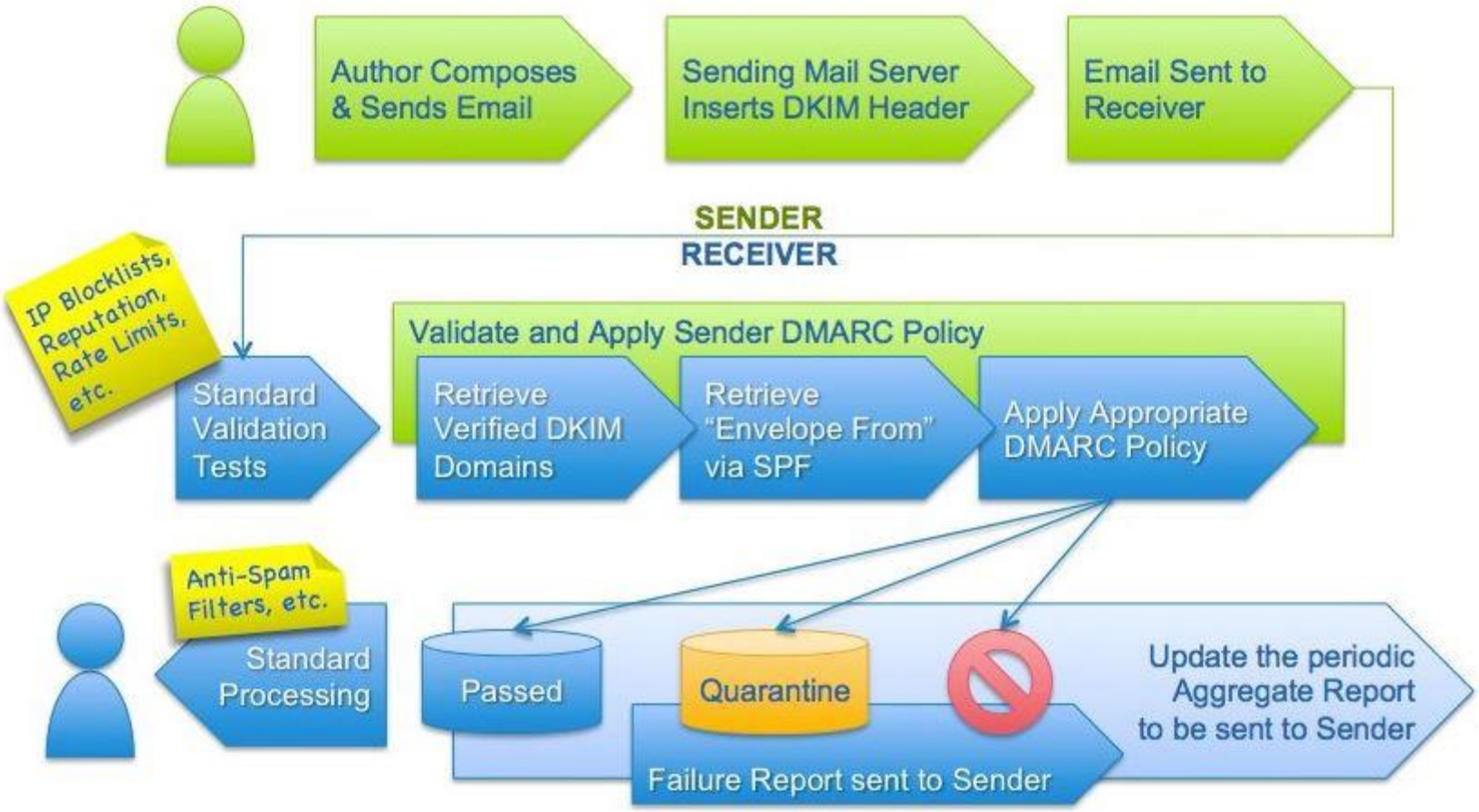
Basic Terminologies:

DMARC (Domain-based Message Authentication, Reporting and Conformance)

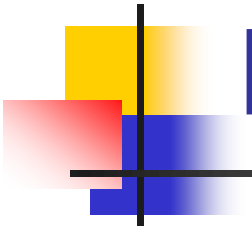
Sender Policy Framework (**SPF**)

DomainKeys Identified Mail (**DKIM**)

Email Authentication Process:



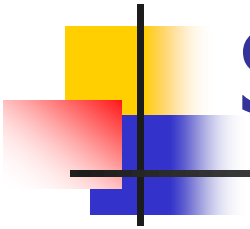
Email Protocols: SMTP



- Neither IMAP or POP are involved relaying messages between servers.
- Simple Mail Transfer Protocol: SMTP
  - Easy, but can be spoofed easily.

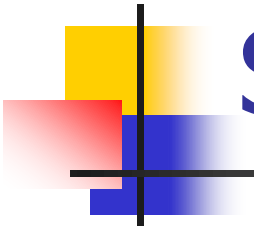
Email Protocols: SMTP

- SMTP Headers:
  - Each mail-server adds to headers.
  - Additions are being made at the top of the list.
    - Therefore, read the header from the bottom.



SMTP Headers

- Headers consists of *header fields*
  - Originator fields
    - from, sender, reply-to
  - Destination address fields
    - To, cc, bcc
  - Identification Fields
    - Message-ID-field is optional, but extremely important for tracing emails through email server logs.
  - Informational Fields
    - Subject, comments, keywords
  - Resent Fields
    - Resent fields are strictly speaking optional, but luckily, most servers add them.
    - Resent-date, resent-from, resent-sender, resent-to, resent-cc, resent-bcc, resent-msg-id

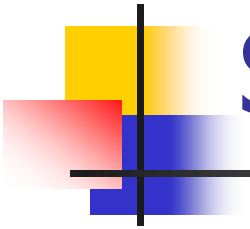


SMTP Header

- Investigation of spoofed messages
  - Verify all IP addresses
    - Keeping in mind that some addresses might be internal addresses.
  - Make a time-line of events.
    - Change times to universal standard time.
    - Look for strange behavior.
    - Keep clock drift in mind.

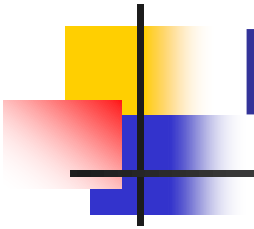
Server Logs

- E-mail logs usually identify email messages by:
  - Account received
  - IP address from which they were sent.
  - Time and date (beware of clock drift)
  - IP addresses



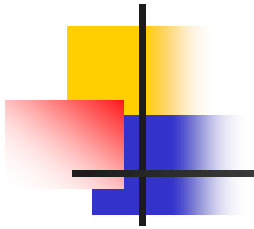
Server Logs

- Many servers keep copies of emails.
- Most servers purge logs.
  - Law-enforcement:
    - Vast majority of companies are very cooperative.
    - Don’t wait for the subpoena, instead give system administrator a heads-up of a coming subpoena.
  - Company:
    - Local sys-ad needs early warning.
    - Getting logs at other places can be dicey.



Demo

- Analysis of fake mail



THANK YOU