Email Service
&
Amazon Simple Email Service

Tejas Parikh (t.parikh@northeastern.edu)

CSYE 6225
Northeastern University

The need for email service

- **SEND TRANSACTIONAL MESSAGES** - Keep your customers up-to-date by sending automated emails, such as purchase confirmations, shipping notifications, order status updates, and policy change notices.
- **SEND NOTIFICATIONS** - Keep your users informed by sending timely information, including system health reports, application alerts, and workflow status updates.
- **RECEIVE INCOMING EMAIL** - Close the loop on your email program by using Amazon SES to receive email. Incoming email can be delivered automatically to an Amazon S3 bucket. You can use AWS Lambda to execute custom code when messages are received, or use Amazon SNS to deliver notifications when you receive incoming messages that contain certain keywords.

Amazon Simple Email Service (Amazon SES)

- Amazon Simple Email Service (Amazon SES) is a cloud-based email sending service designed to help digital marketers and application developers send marketing, notification, and transactional emails.
- It is a reliable, cost-effective service for businesses of all sizes that use email to keep in contact with their customers.
- You can use SMTP interface or one of the AWS SDKs to integrate Amazon SES directly into your existing applications.
- You can also integrate the email sending capabilities of Amazon SES into the software you already use, such as ticketing systems and email clients.

Sending Email with Amazon SES

- When you use Amazon SES, Amazon SES becomes your outbound email server.
- You can also keep your existing email server and configure it to send your outgoing emails through Amazon SES so that you don't have to change any settings in your email clients.

Amazon SES and Deliverability

- You want your recipients to read your emails, find them valuable, and not label them as spam. In other words, you want to maximize email deliverability—the percentage of your emails that arrive in your recipients' inboxes.
- To maximize email deliverability, you need to understand email delivery issues, proactively take steps to prevent them, stay informed of the status of the emails that you send, and then improve your email-sending program, if necessary, to further increase the likelihood of successful deliveries.

Understand Email Delivery Issues

Understand Email Delivery Issues - Bounce

- In most cases, your messages are delivered successfully to recipients who expect them. In some cases, however, a delivery might fail, or a recipient might not want to receive the mail that you are sending. Bounces, complaints, and the suppression list are related to these delivery issues.
- **Bounce** - If your recipient's receiver (for example, an ISP) fails to deliver your message to the recipient, the receiver bounces the message back to Amazon SES. Amazon SES then notifies you of the bounced email through email or through Amazon Simple Notification Service (Amazon SNS), depending on how you have your system set up. There are hard bounces and soft bounces, as follows:
  - **Hard bounce** – A persistent email delivery failure. For example, the mailbox does not exist. Amazon SES does not retry hard bounces, with the exception of DNS lookup failures. You should not make repeated delivery attempts to email addresses that hard bounce.
  - **Soft bounce** – A temporary email delivery failure. For example, the mailbox is full, there are too many connections (also called throttling), or the connection times out. Amazon SES retries soft bounces multiple times. If the email still cannot be delivered, then Amazon SES stops retrying it.
- Bounces can also be synchronous or asynchronous.
  - A **synchronous** bounce occurs while the email servers of the sender and receiver are actively communicating.
  - An **asynchronous** bounce occurs when a receiver initially accepts an email message for delivery and then subsequently fails to deliver it to the recipient.

Understand Email Delivery Issues - Complaint

- Most email client programs provide a button labeled "Mark as Spam," or similar, which moves the message to a spam folder, and forwards it to the ISP.
- Additionally, most ISPs maintain an abuse address (e.g., abuse@example.net), where users can forward unwanted email messages and request that the ISP take action to prevent them.
- In both of these cases, the recipient is making a complaint. If the ISP concludes that you are a spammer, and Amazon SES has a feedback loop set up with the ISP, then the ISP will send the complaint back to Amazon SES.
- When Amazon SES receives such a complaint, it forwards the complaint to you either by email or by using an Amazon SNS notification, depending on how you have your system set up.
- It is not recommend to make repeated delivery attempts to email addresses that generate complaints.

Understand Email Delivery Issues - Suppression List

- The Amazon SES suppression list is a list of recipient email addresses that have recently caused a hard bounce for any Amazon SES customer.
- If you try to send an email through Amazon SES to an address that is on the suppression list, the call to Amazon SES succeeds, but Amazon SES treats the email as a hard bounce instead of attempting to send it.
- Like any hard bounce, suppression list bounces count towards your sending quota and your bounce rate.
- An email address can remain on the suppression list for up to 14 days.
- If you are sure that the email address that you're trying to send to is valid, you can submit a suppression list removal request.

Be Proactive

- One of the biggest issues with email on the Internet is unsolicited bulk email, or spam.
- ISPs take considerable measures to prevent their customers from receiving spam.

Be Proactive - Verification

- Unfortunately, it's possible for a spammer to falsify an email header and spoof the originating email address so that it appears as though the email originated from a different source.
- To maintain trust between ISPs and Amazon SES, Amazon SES needs to ensure that its senders are who they say they are.
- You are therefore required to verify all email addresses from which you send emails through Amazon SES to protect your sending identity.
- You can verify email addresses by using the Amazon SES console or by using the Amazon SES API.
- You can also verify entire domains.

Be Proactive - Authentication

- Authentication is another way that you can indicate to ISPs that you are who you say you are.
- When you authenticate an email, you provide evidence that you are the owner of the account and that your emails have not been modified in transit.
- In some cases, ISPs refuse to forward email that is not authenticated.
- Amazon SES supports two methods of authentication
  - Sender Policy Framework (SPF)
  - DomainKeys Identified Mail (DKIM)

Sender Policy Framework (SPF)

- An SPF record indicates to ISPs that you have authorized Amazon SES to send mail for your domain.
- When you use Amazon SES, your decision about whether to publish an SPF record depends on whether you only require your email to pass an SPF check by the receiving mail server, or if you want your email to comply with the additional requirements needed to pass Domain-based Message Authentication, Reporting and Conformance (DMARC) authentication based on SPF.

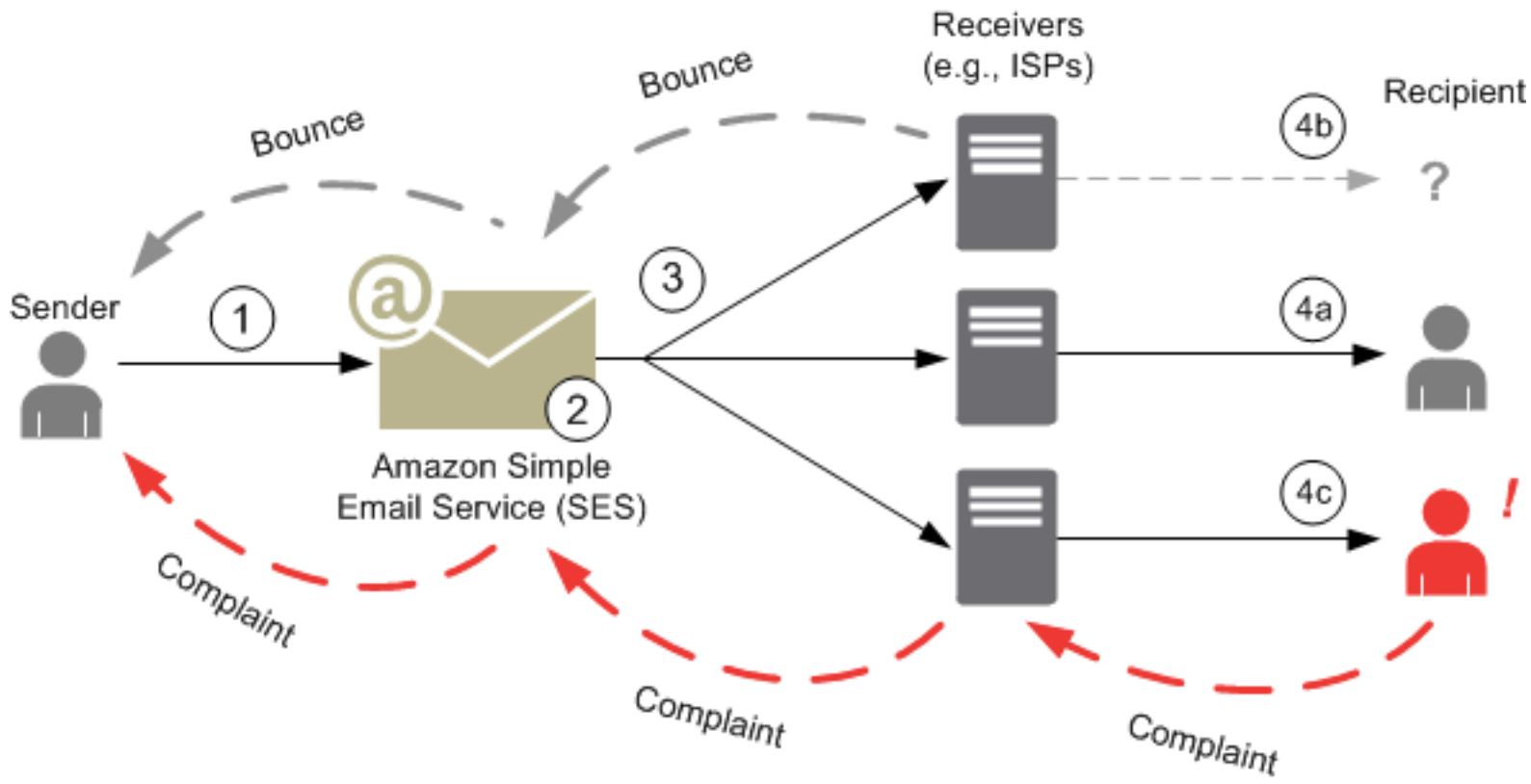
DomainKeys Identified Mail (DKIM)

- DomainKeys Identified Mail (DKIM) is a standard that allows senders to sign their email messages with a cryptographic key.
- Email providers then use these signatures to verify that the messages weren't modified by a third party while in transit.
- An email message that is sent using DKIM includes a DKIM-Signature header field that contains a cryptographically signed representation of the message.
- A provider that receives the message can use a public key, which is published in the sender's DNS record, to decode the signature.
- Email providers then use this information to determine whether messages are authentic.
- To learn more about DKIM, see http://dkim.org.

Be Proactive - Reputation

- When it comes to email sending, reputation—a measure of confidence that an IP address, email address, or sending domain is not the source of spam—is important.
- Amazon SES maintains a strong reputation with ISPs so that ISPs deliver your emails to your recipients' inboxes.
- Similarly, you need to maintain a trusted reputation with Amazon SES. You build your reputation with Amazon SES by sending high-quality content.
- When you send high-quality content, your reputation becomes more trusted over time and Amazon SES increases your sending limits.
- Excessive bounces and complaints negatively impact your reputation and can cause Amazon SES to lower your sending limits or terminate your Amazon SES account.

Amazon SES Email-Sending Process



Email Format and Amazon SES

- When a client makes a request to Amazon SES, Amazon SES constructs an email message compliant with the Internet Message Format specification (RFC 5322).
- An email consists of a header, a body, and an envelope, as described below.
- **Header**—Contains routing instructions and information about the message. Examples are the sender's address, the recipient's address, the subject, and the date. The header is analogous to the information at the top of a postal letter, though it can contain many other types of information, such as the format of the message.
- **Body**—Contains the text of the message itself.
- **Envelope**—Contains the actual routing information that is communicated between the email client and the mail server during the SMTP session. This email envelope information is analogous to the information on a postal envelope. *The routing information of the email envelope is usually the same as the routing information in the email header, but not always.* For example, when you send a blind carbon copy (BCC), the actual recipient address (derived from the envelope) is not the same as the "To" address that is displayed in the recipient's email client, which is derived from the header.

Additional Resources

See Lecture Page