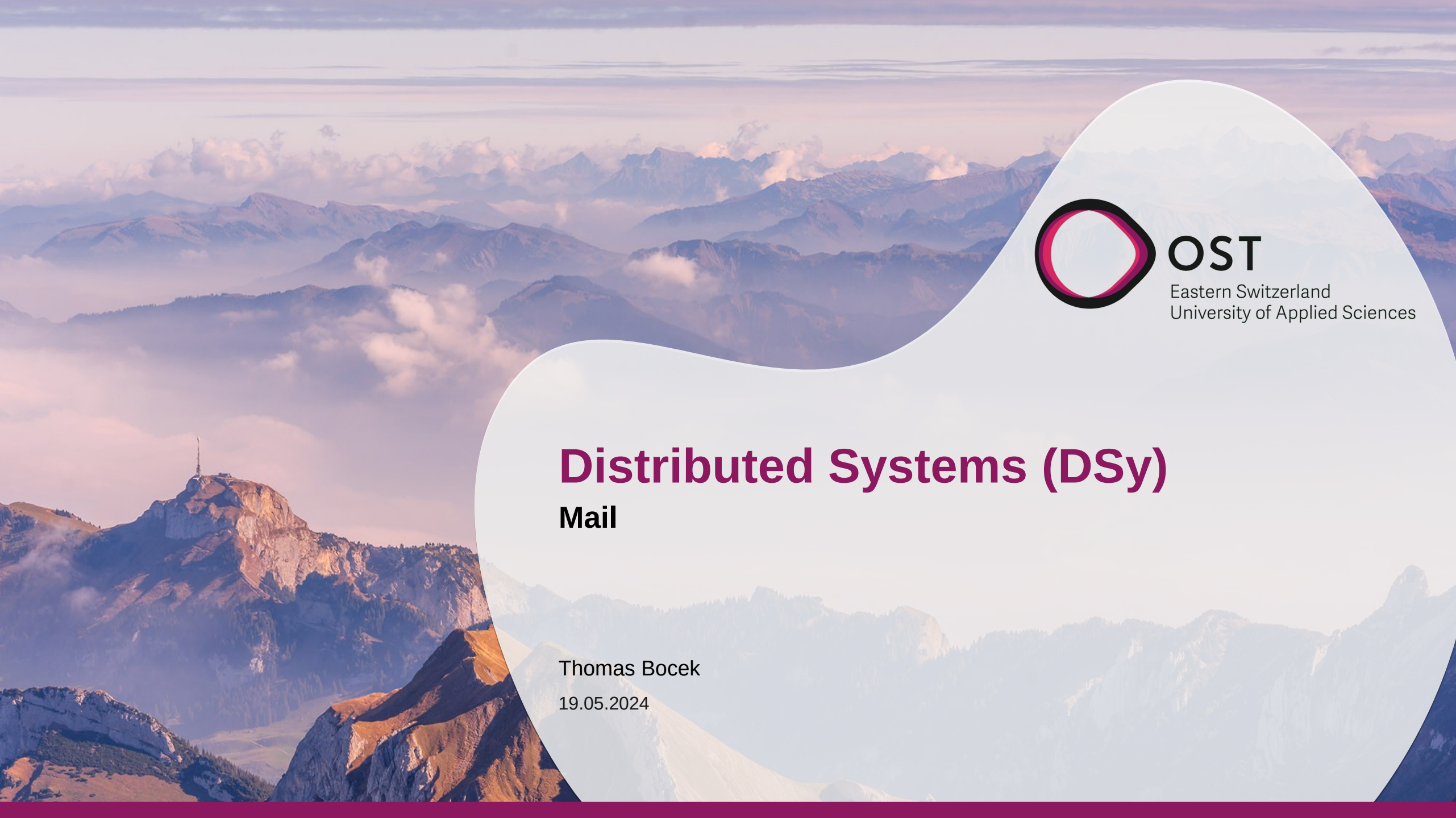


OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

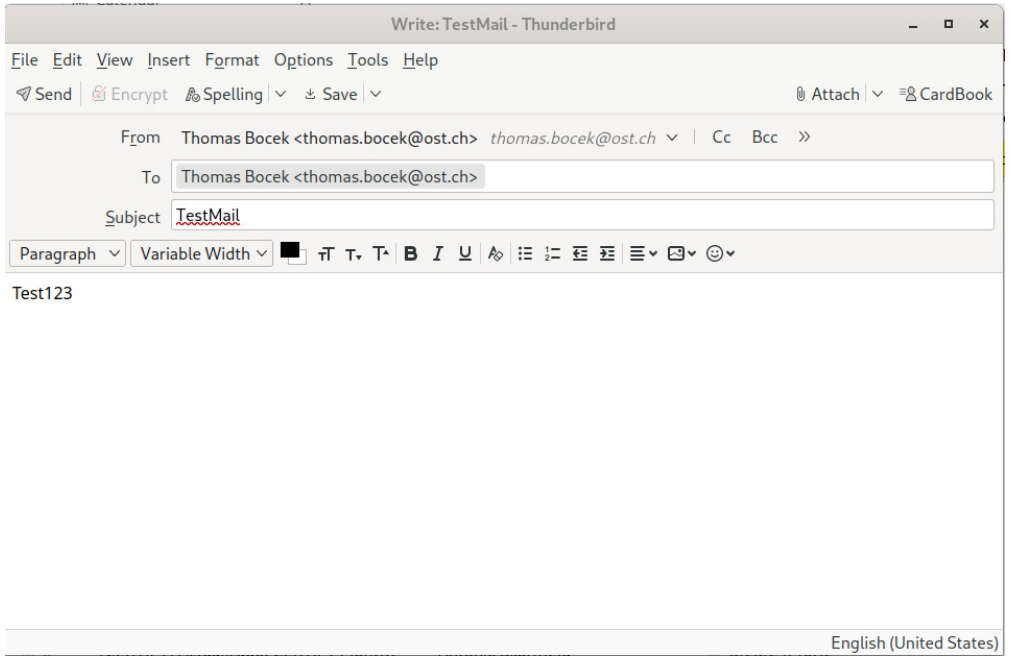
Mail

Thomas Bocek

19.05.2024

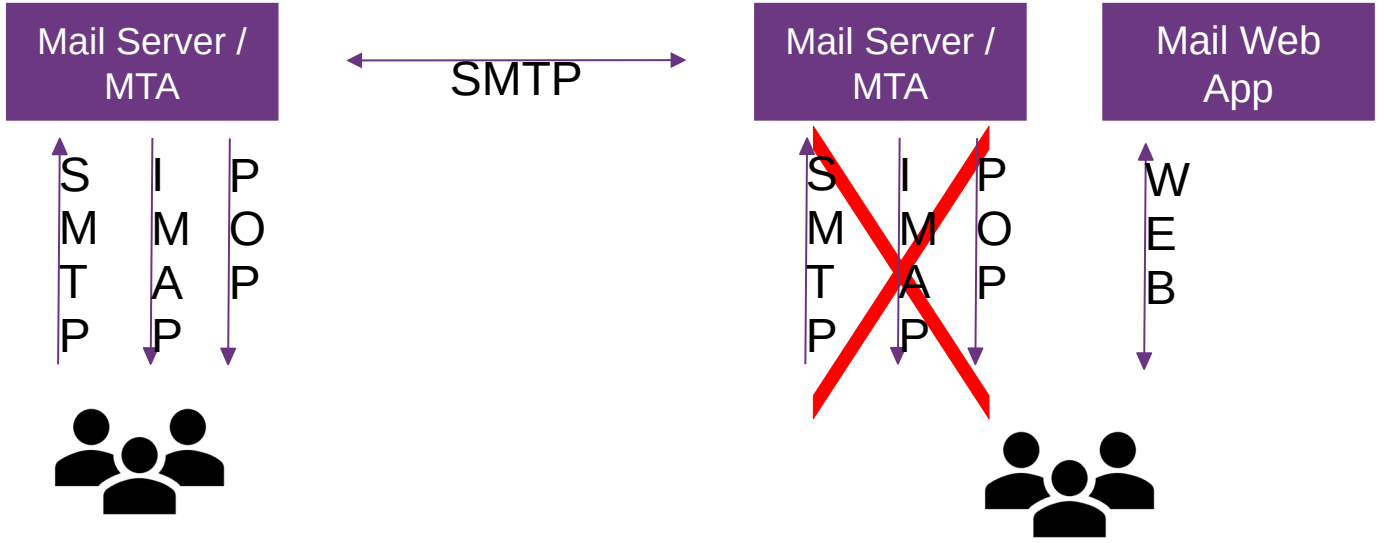
Introduction

- Understanding How Mail Works
  - Basics of Email, SPF, DMARC, DKIM, and their importance in email security.
- Email: backbone of personal, academic, and professional correspondence worldwide
  - Slack, Discord, Teams, Telegram, WhatsApp, Treema, Matrix, ...
- Send email / receive email – how hard can it be?
  - SMTP specified in 1982
  - POP specified in 1984
  - IMAP specified in 1988
  - Protocols were improved over time



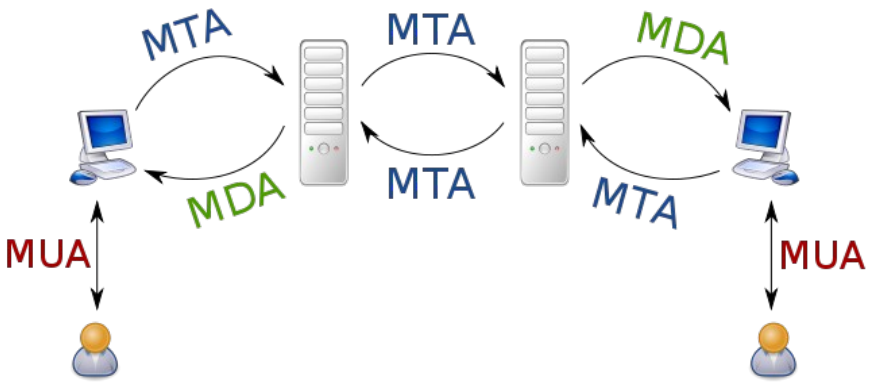
POP / SMTP / IMAP

- Traditional mail not that popular anymore
  - 2019 - Thunderbird now ~0.2%, K9 on mobile
- SMTP → Simple Mail Transfer Protocol
  - Standard protocol for sending/receiving emails
- Access to email mostly via Web – easier
  - Mailserver to mailserver still SMTP
  - JMAP to the rescue?
    - Combind IMAP / CardDav / CalDav
    - Integrated calendar / contact functionality



SMTP

- IMAP / POP is dead? (I'm still using it :)
  - Needed for interoperability: example
- Port Numbers
  - Port 25 for non-encrypted communication,
  - Port 587 for encrypted submission from email
  - Port 465 (deprecated but still in use) for SMTPS (SMTP over SSL)



- Sending emails: email client (MUA - Mail User Agent) uses SMTP to send to mail server (MTA - Mail Transfer Agent). The Mail Delivery Agent (MDA) receives emails from MTA and delivers them to the recipient's mailbox
- Routing: The MTA/MDA server processes the recipient's email address.
  - Domain == local → MDA
  - External → routes the email to another SMTP server closer to the recipient's MTA
- MDA: Once email reaches SMTP server that recognizes the recipient's domain, it forwards the email to the POP3 or IMAP server for retrieval by the recipient's email client
- DNS: MX records

https://commons.wikimedia.org/wiki/File:MTA-MDA-MUA_relationship.svg

Secure SMTP

- STARTTLS (25/587) vs. SMTPS (465)
  - STARTTLS can upgrade a plain text connection to an encrypted connection on same port.
  - Starts as a regular SMTP session, if both support TLS, the connection is upgraded to a secure connection using STARTTLS
  - If one party does not support TLS, the communication is unencrypted
  - Port: Typically uses port 587 for client submission and port 25 for server-to-server relay.
  - Advantages:
    - Backward Compatibility
    - Standard Compliance: Recommended approach by many standards
  - Considerations:
    - Can fall back to non-encrypted communication, it's potentially vulnerable to downgrade attacks

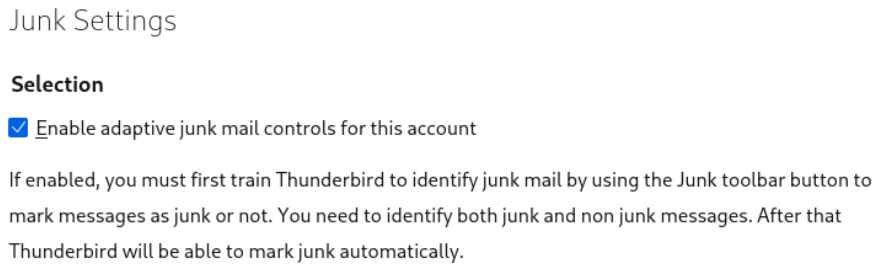
- SMTPS
  - SMTPS encapsulates the entire SMTP session in SSL/TLS from the beginning of the connection without the need for an upgrade command.
  - Port: Uses port 465. It’s worth noting that port 465 was initially registered for SMTPS, deprecated in favor of STARTTLS on ports 587/25, and later revived due to its widespread unofficial use.
  - Advantages:
    - Simplicity: Since the connection is encrypted from the start
    - Guaranteed Encryption: Provides a guarantee that the session is encrypted
  - Considerations:
    - Port Confusion and Legacy: Its status as a "revived" port for secure SMTP can cause confusion

Best Practices / Spam Prevention

- Security Best Practices: STARTTLS on port 587 is generally recommended
  - You can use Lets Encrypt for both
- Spam Prevention: Greylisting
  - Greylisting is an anti-spam technique that temporarily rejects emails from unknown senders
    - Email Received: When email arrives, receiving server checks if the sender's IP address, the envelope sender address, and the recipient address are on its "greylist."
    - Initial Rejection: If sender is unrecognized, the server temporarily rejects the email with "try again later"
    - Retrying: Legitimate email servers will retry sending the email after a delay, as per SMTP standards
    - Retry: Server recognizes sender as good, removes from greylist, and accepts email
    - Subsequent Emails: Further emails without delay
  - Advantages
    - Reduces Spam: Effectively filters out spam
    - Low Resource Usage: No scanning content
    - Simple to Implement: Can be easily added to existing email systems without extensive configuration
  - Considerations
    - Delayed Emails: Legitimate emails may be temporarily delayed
    - Spam Evolution: Spammers may adapt by programming their servers to retry

Spam Prevention

- SURBL Filters (Spam URI Real-time Blocklists) - Combatting Spam with URL Blacklists
  - How they work: Checking URLs in emails against real-time blacklists to identify spam or malicious content
- DNS Blocklists (DNSBL): Lists of IP addresses known to send spam
  - E.g., UCEPROTECT
  - Email servers query DNSBLs in real-time to decide whether incoming emails from those IPs should be accepted
- Bayesian Analysis
  - Uses machine learning to classify emails based on content
  - E.g., Thunderbird



  - Training Data:
    - Collect a large dataset of junk/notjunk emails
  - Word Probability Calculation:
    - Calculate probability of word marked as junk/notjunk
    - E.g., words like "discount" and "offer" might have higher probabilities, while words like "meeting" and "invoice" not

OST

Spam Prevention

- SPF (Sender Policy Framework) - Verifying Email Senders to Prevent Spoofing
  - Allows domain owners to specify which servers are permitted to send email on behalf of their domain
  - Email servers check the SPF record in DNS to verify the sender's IP
  - Helps in preventing email spoofing and phishing by verifying sender authenticity.
- DKIM (DomainKeys Identified Mail) - Ensuring Email Integrity and Authenticity
  - Associating domain name with email message
  - Digital signatures linked to a domain's DNS records. Recipients can verify the signature to confirm that the email hasn't been tampered with and truly comes from the stated domain
- DMARC (Domain-based Message Authentication, Reporting and Conformance) - The Ultimate Email Authentication Policy
  - Builds on SPF and DKIM, adding a reporting function for email receivers to send feedback to senders
  - Allows domain owners to specify how their emails should be handled if they fail SPF or DKIM checks (e.g., reject, quarantine, or allow)
- BIMI (Brand Indicators for Message Identification)
  - Publish standardized logo (usually in SVG format) in DNS
  - Uses TXT format, ~requires VMC