Should you Trust That Email? Technologies and Strategies That Can Help!

Dr. Sarbari Gupta

Founder and CEO – Electrosoft

"Email is such a security risk! That's why I prefer good old fashioned one-to-one gossip."

CartoonStock.com

Email is the #1 Threat Vector

- Email is the de facto standard for business communications
- Cyber criminals have adopted Email as their most utilized and effective tool
- Email Cyber Threats include:
  - Malware delivery
  - Spoofing
  - Phishing
  - SPAM
- Business Email Compromise has hit an all-time high
  - Verizon's 2021 Data Breach Investigations Report
  - https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

Email Trust Questions

Can I trust the Name/Identity of the Sender?

Can I trust the Organization of the Sender?

From: mickey.mouse@disney.net

Can I trust the body of the email?

Can I trust attachments or links?

Email Security – Not Working Well

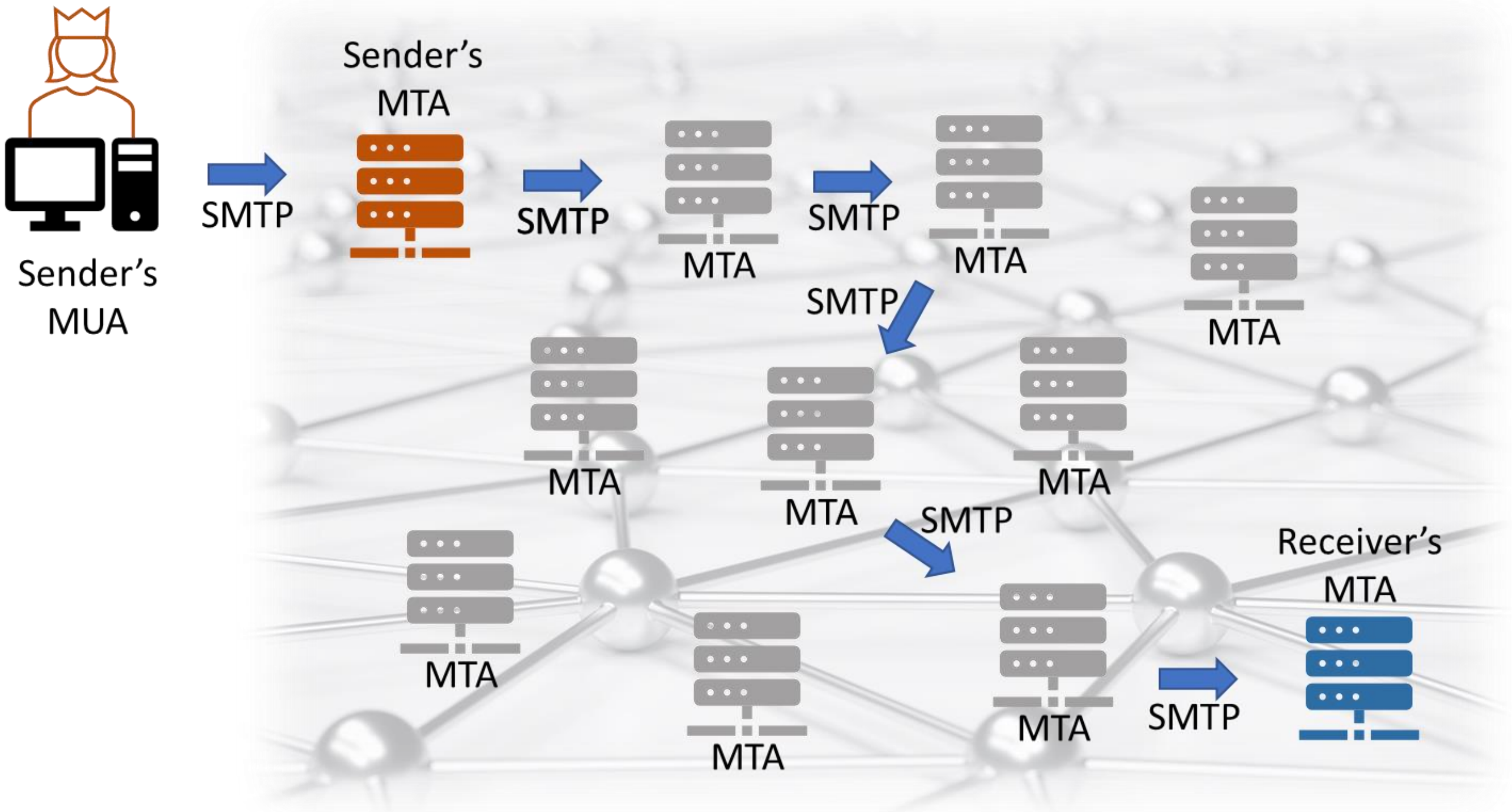
- Organizations use variety of email security mechanisms
  - Multi-factor Authentication for Users
  - Message Encryption
  - Policies and Rulesets to detect SPAM and JUNK email
- Organizations training their users on Email security
  - Emails with poor grammar
  - Attachments and links
  - Phishing attempts
- Yet, users are still falling prey to email threats!
  - Clicking on unsafe attachments and links
  - Taking other actions based on fake emails

Email Protocols

- SMTP – Simple Mail Transfer Protocol (IETF RFC 5321)
  - Used to route, send and receive emails across the Internet
  - Port 25 (default) and Port 465 (secure)
- POP3 – Post Office Protocol Version 3 (IETF RFC 1939)
  - Used to download emails from a remote server to a mail user agent
  - Port 110 (default) and Port 995 (secure)
- IMAP – Internet Message Access Protocol (IETF RFC 3501)
  - Used to access email from a remote server to a mail user agent
  - Allows simultaneous access by multiple email user agents
  - Port 143 (default) and Port 993 (secure)
- MIME – Multipurpose Internet Mail Extensions (IETF RFC 2045)
  - Extends format of SMTP to support rich text and various types of attachments

Quick Intro to SMTP

- Mail User Agent (MUA) – Outlook, Google mail
- Mail Transfer Agent (MTA) – Mail Server which receives the dispatch from MUA and sends to the target MTA
- Intermediate MTAs route the email to the destination MTA

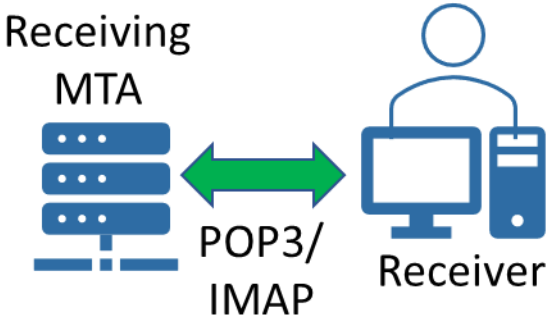


Email – Strengths and Weaknesses

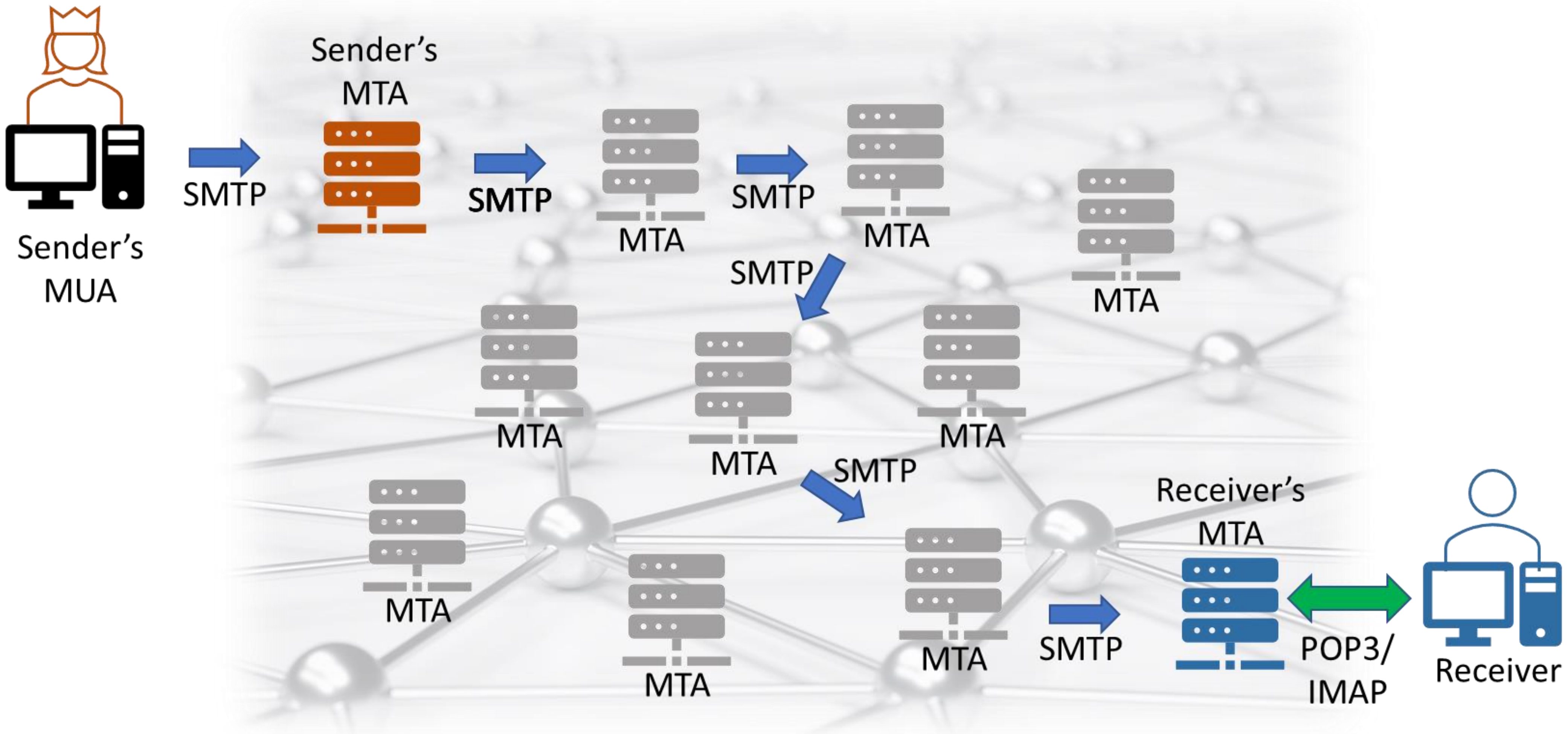
- Strengths:
  - Versatile and ubiquitous
  - Low Cost
  - Store and Forward mechanism very resilient
  - Allows rich set of formats (via MIME)
- Weaknesses:
  - SMTP includes no security by default
  - Relatively easy to spoof the sender and their company
  - Email content is visible to and modifiable by any MTA in route

POP3/IMAP

- Enables User to access emails from Mail Server
- Security
  - User Authentication
  - Secure session via TLS or SSL



SMTP, POP3/IMAP in Action



Reality of Email Systems

- By default, SMTP Servers (MTAs) are not required to authenticate users that send mail
  - Users can self-assert their identity and domain
- However, most Mail servers <u>are</u> locked down
  - Subscribers have to authenticate to send or receive email
  - Email can originate only from IP addresses within the domain
- SMTP Server that is not locked down is called an Open Relay
  - Used by spammers and fraudsters

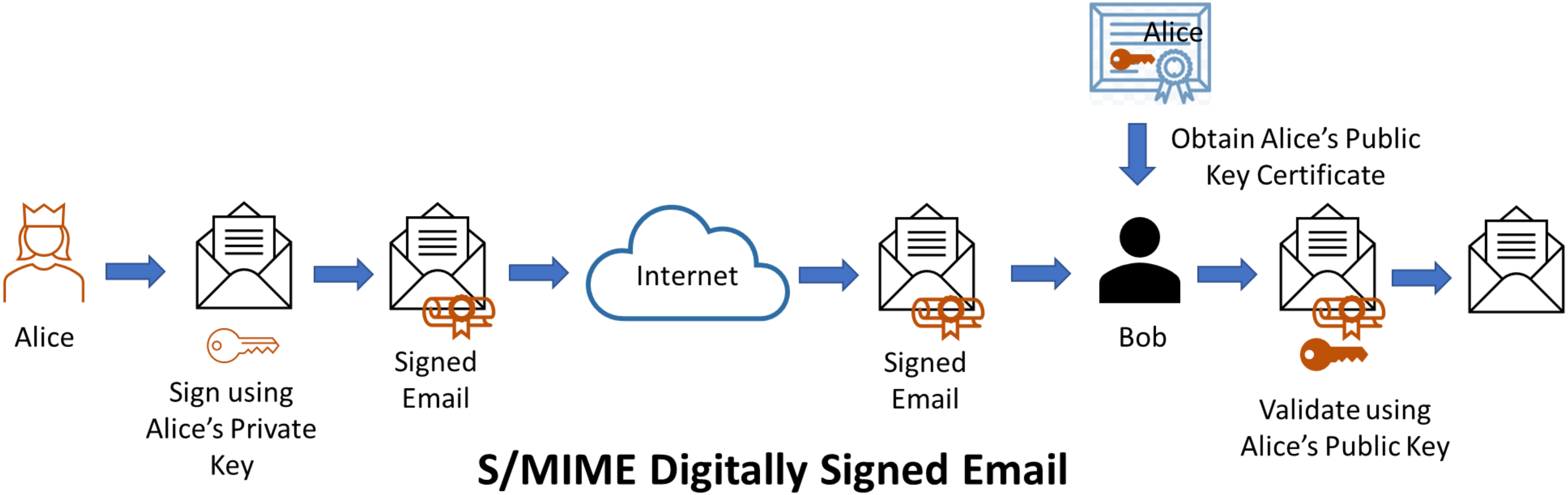
How to Improve Security of Email?

- S/MIME
- SPF/DKIM/DMARC
- Mail Transfer Agent-Strict Transport Security (MTA-STS)
- Domain Reputation
- Rule-based engines; AI/ML Techniques

S/MIME – Secure MIME

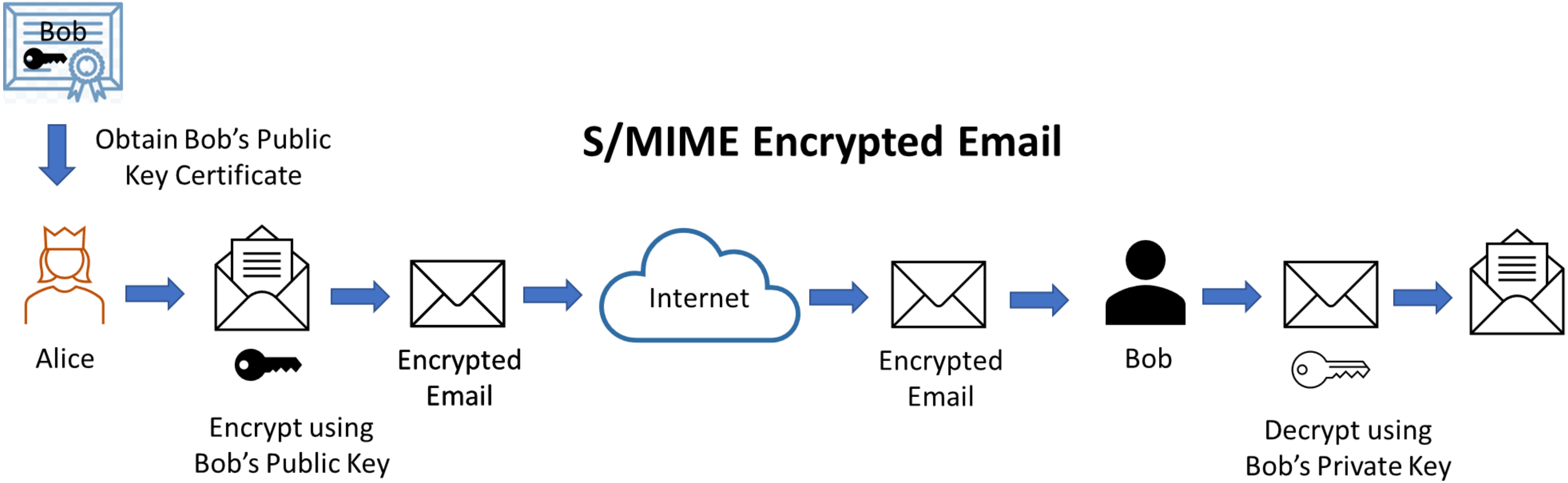
- Leverages asymmetric cryptography
  - Encrypt and/or sign emails end-to-end between Users
- User obtains public key certificate from Certification Authority
  - Has possession of a corresponding private key
- Digital Signature
  - Sender uses private key to sign outgoing emails
  - Receiver validates the signature using the sender’s public key
- Encryption
  - Sender obtains public key (via public key certificate) for target recipient
  - Sender encrypts the email message using the public key
  - Receiver decrypts email message using their private key
- S/MIME trust is based on PKI trust and path validation

S/MIME Digital Signature


Alice
Obtain Alice's Public Key Certificate
Alice
Sign using Alice's Private Key
Signed Email
Internet
Signed Email
Bob
Validate using Alice's Public Key

S/MIME Digitally Signed Email

S/MIME Encryption



S/MIME Encrypted Email

Bob

Obtain Bob's Public Key Certificate

Alice

Encrypt using Bob's Public Key

Encrypted Email

Internet

Encrypted Email

Bob

Decrypt using Bob's Private Key

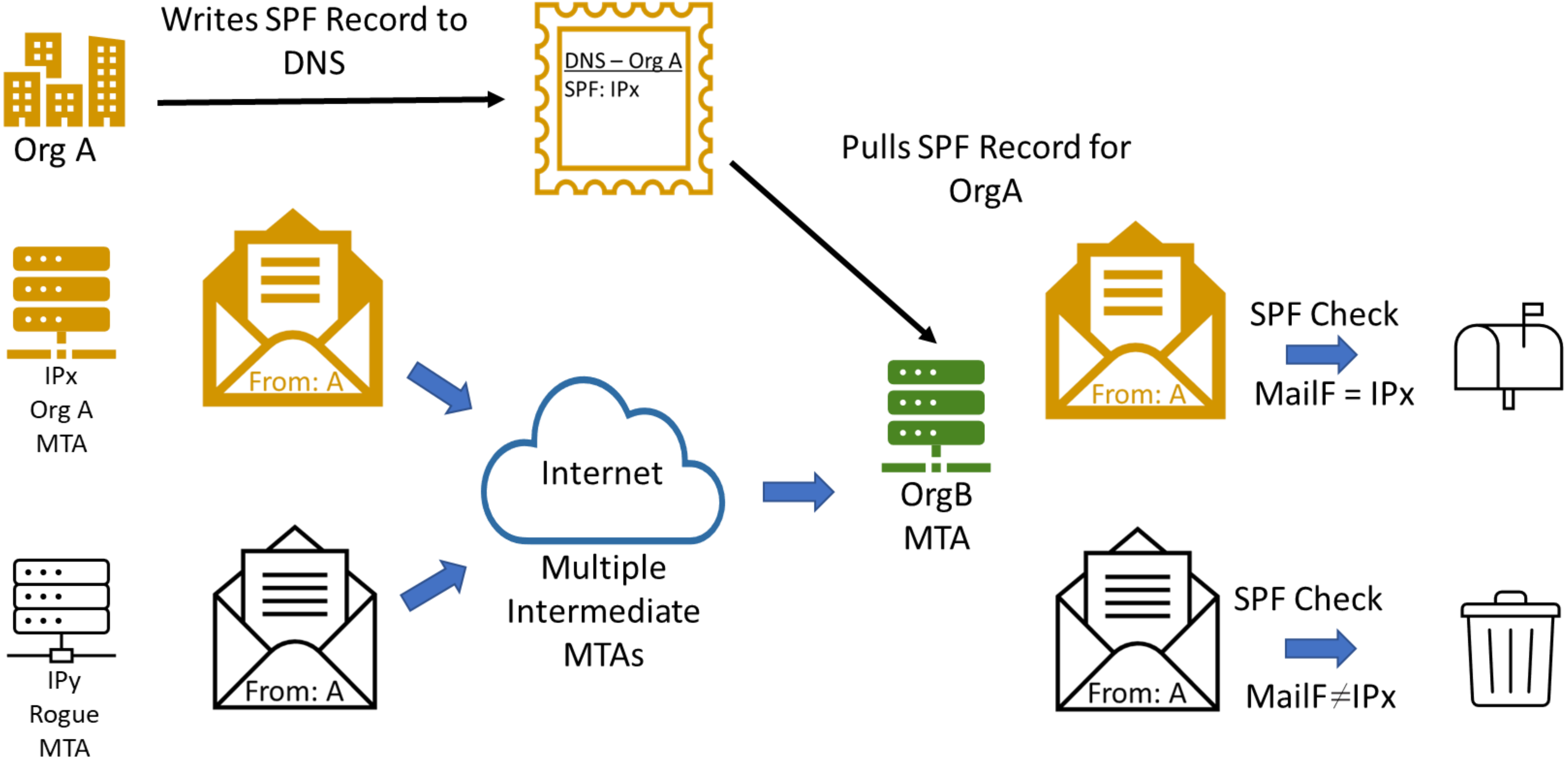
S/MIME – Strengths and Weaknesses

- Strengths
  - PKI-based trust is the gold standard for Internet-based trust
  - Provides strong sender authentication (signed messages)
  - Enables Sender non-repudiation (signed messages)
  - Protects confidentiality of message (encrypted email)
  - Suitable for large, IT savvy organizations
- Weaknesses (Drawbacks)
  - Expensive to issue/maintain PKI certificates for Users
  - Encrypted incoming email cannot be scanned for malicious content
  - Very complex to set up and use within typical email agents
  - Trusting PKI certificates for users outside the organization is tricky

What is SPF?

- Sender Policy Framework
  - DNS record that allows the domain owner to specify the IP addresses that are allowed to send emails on behalf of that domain
  - Sender provides the list of authorized IP addresses as part of their SPF record
  - Receiver needs to look up the DNS record for the Sender and verify that the message originated from one of the authorized IP addresses
- Limitations
  - Forwarded messages fail SPF verification
  - DNS records for SPF difficult to maintain over time
  - Verification performed using the Mail From (MFrom) domain, not visible to user

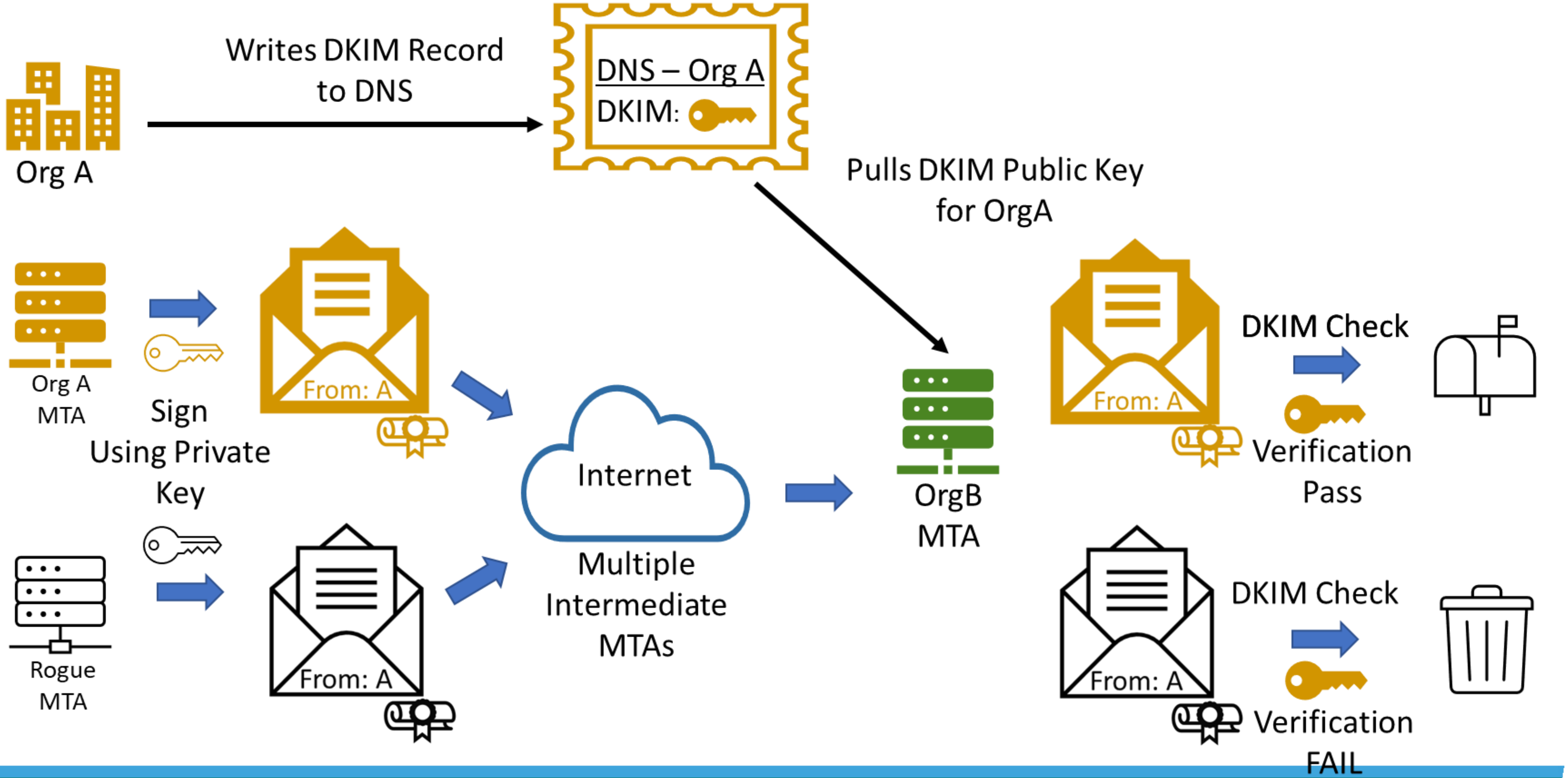
SPF in Action



What is DKIM?

- DomainKeys Identified Email
  - Allows receivers to validate that a message came from the legitimate domain and that it was not altered in transit
  - Domain is set up with public/private cryptographic key pair
  - Sending server uses private key to sign outgoing email
  - Sender's DNS record includes the corresponding public key
- Limitations
  - Receiving server expected to validate the signature using the sending domain's public key
  - Difficult to maintain over time and with multiple mail servers
  - Forwarded emails create verification challenges

DKIM in Action



What is DMARC?

- Domain-based Message Authentication, Reporting and Conformance
  - Allows the domain owner to specify what happens when a receiver gets an email message that fails the SPF or DKIM checks
  - Requests receiving email server to send DMARC failure reports to the sender
- Limitations
  - Receiving server may ignore the DMARC settings
  - DMARC policies may prevent emails from being delivered

How Do SPF/DKIM/DMARC work together and what is the benefit?

- SPF record indicates the MTAs that are allowed to send on behalf of an Organization
  - Enables Receiving MTA to check IP of originating MTA
- DKIM record provides public key of Organization
  - Enables Receiving MTA to verify DKIM signature
- DMARC tells the Receiving MTA what to do if SPF and/or DKIM fails
  - Receiving MTA can process SPF/DKIM failures based on DMARC policy and provide failure reports to Sending MTA

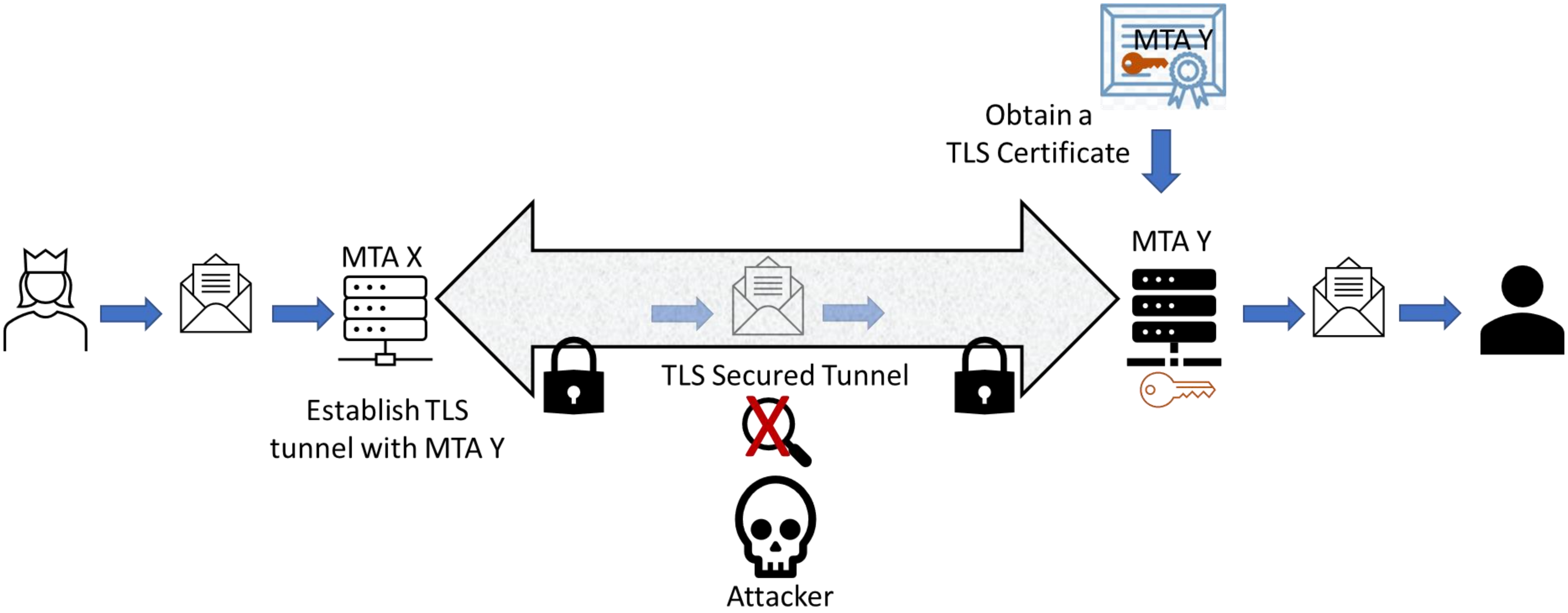
Strengths / Weaknesses of SPF/DKIM/DMARC

- Strengths
  - Relatively lightweight as compared to S/MIME for every user
  - Receiving MTAs can identify and act on spoofed emails
  - Sending MTAs can receive reports on (ab)use of their domain
- Weaknesses
  - SPF and DKIM are tricky to set up and maintain over time
    - Unmaintained SPF/DKIM records can result in rejected email
  - SPF/DKIM checks do not use human-readable “From” address
  - Receiving MTAs can still accept spoofed emails from your domain
  - *Does not prevent spoofing using similar-looking domain names!*
  - *Does not help for incoming messages from domains with no SPF/DKIM*

Mail Transfer Agent-Strict Transport Security (MTA-STS)

- Supports authentication and encryption (via TLS) between sending and receiving SMTP servers
- Domains that implement MTA-STS need to:
  - Obtain a TLS certificate
  - Configure DNS record with URL of MTA-STS Policy File
  - Publish MTA-STS Policy File with list of TLS-enabled mail servers authorized for inbound email
- Drawbacks
  - New standard; Not widely implemented
  - Tricky to set up and maintain over time
  - Incoming email to MTA-STS servers may be disrupted easily

MTA-STS in Action



Domain Reputation

- Indicates the health/condition of domain as sender of email
- Reputation Score depends upon
  - Volume of SPAM
  - Implementation status of SPF/DKIM/DMARC
  - Level of engagement on email
  - How long the domain has been around
  - Proprietary algorithms…
- ISPs and Mail Service Providers maintain their own domain reputation scores
- Popular Domain Reputation Tools
  - Cisco Talos Intelligence
  - Google Postmaster Tools
  - Microsoft Smart Network Data Services (SDNS)
  - BarracudaCentral
  - MXToolbox

Rule-based engines; AI/ML Techniques

- Leverage lists, signatures, and human-defined rules to identify incoming malicious email
- Offer safe zones to detonate attachments and follow links
- Tools trained using large sets of fraudulent/malicious emails
- Tools that continue to learn from actual incoming emails based on user reaction

Email Trust – Whose Perspective?

- Needs from Sender Perspective
  - Provide assurance that the sending domain and users are legitimate
  - Provide assurance that outgoing emails remain untampered
  - Make it difficult for fraudsters to spoof their identity
- Needs from Receiver Perspective
  - Identify fraudulent/spoofed emails
  - Identify messages with dangerous content (attachments, links, phishing attempts)
  - Have assurance that the email came from the claimed sender (source authentication)
  - Have assurance that the content of email and attachments remain unchanged from the time it was sent (integrity check)

Email Trust – What to do?

- Recommended Actions for Sender
  - Check Domain reputation and take steps to improve if needed
  - Lock down mail servers
  - Turn on and administer SPF and related DMARC policy
  - Turn on and administer DKIM and related DMARC policy
  - Support MTA-STS for outgoing email
  - Support S/MIME signature/encryption for outgoing email (if practical)
- Recommended Actions for Receiver
  - Check reputation of Sender’s domain
  - Perform SPF/DKIM/DMARC verification for incoming email (if present)
  - Use Rule/AI/ML engines to check content, attachments, links
  - Support S/MIME validation/decryption for incoming email
  - Support MTA-STS for incoming email (if practical)
  - Continue Security Training and Phishing Training!

Summary

- Email is the de facto standard for business communications
  - Yet, it remains the #1 vector for security attacks
- Several technologies exist to enable trust in email
  - Each has its pros and cons
  - There are NO FAIL-SAFE tools for email security!
- Knowing the options that exist and the maturity of your organization…
  - Will help you identify one or more email security technologies to leverage

THANK YOU

Contact Information

- Contact Info: Dr. Sarbari Gupta – Electrosoft
  - Email: sarbari@electrosoft-inc.com;
  - Phone: 571-489-6687
  - LinkedIn: https://www.linkedin.com/in/sarbari-gupta/

- Electrosoft
  - Web: http://www.electrosoft-inc.com
  - LinkedIn: https://www.linkedin.com/company/electrosoft/
  - Twitter: https://twitter.com/Electrosoft_Inc
  - HQ: 1893 Metro Center Drive, Suite 228
    Reston VA 20190