Assignment 9

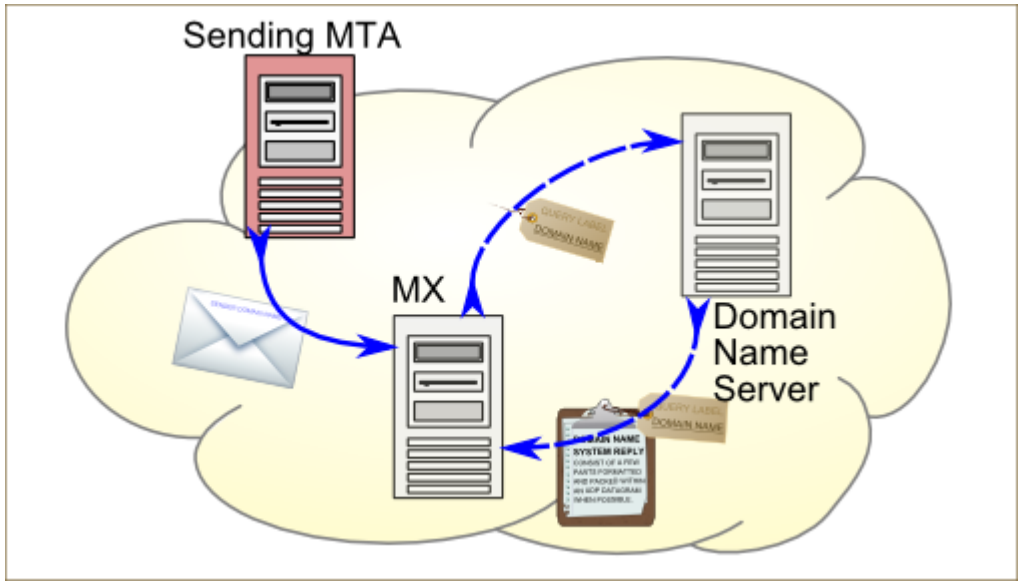
Email Security

Email security

- Reduce spoof, forgeries
- SPF (Sender Policy Framework)
  - DNS text entry which shows a list of servers that should be considered allowed to send mail for a specific domain – no spoofing
  - Authoritative for the domain due to use of DNS since owners/administrators are the only ones to have access to the domain
- DKIM (DomainKeys Identified Mail)
  - a method to verify that the messages' content are trustworthy - no forgeries
- DMARC (Domain-based Message Authentication, Reporting and Conformance)
  - empowers SPF and DKIM by stating a clear policy

SPF

- Upon receipt the message and the sender address are fetched by the receiving mail server
- The receiving mail server runs an TXT DNS query against the claimed domain SPF entry
- The SPF entry data is then used to verify the sender server



DKIM

- A new header, called “DKIM-Signature”, is added to the mail message by using the private part of the key on the message content
- From here on the message *main* content cannot be modified otherwise the DKIM header won’t match anymore
- Upon reception the receiving server will make a TXT DNS query to retrieve the key used in the DKIM-Signature field
- The DKIM header check result can be then used when deciding if a message is fraudulent or trustworthy