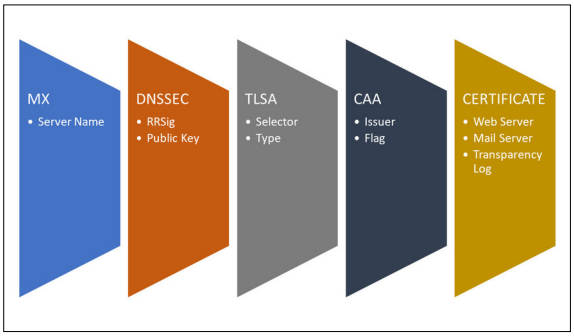
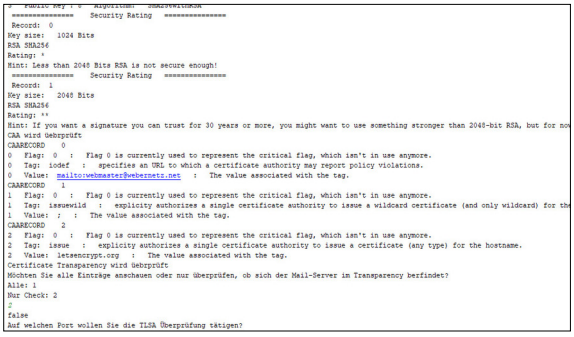
Diplomand	Shahab JAHANABADI
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit

Security Scoring for Destination Mail Servers

Projekt Logo



Abgefrage Kriterien



```
 ==============   Security Rating   ==============
 Record:  0
Key size:   1024 Bits
RSA SHA256
Rating: *
Hint: Less than 2048 Bits RSA is not secure enough!
 ==============   Security Rating   ==============
 Record:  1
Key size:   2048 Bits
RSA SHA256
Rating: **
Hint: If you want a signature you can trust for 30 years or more, you might want to use something stronger than 2048-bit RSA, but for no
CAA wird Gebprüft
CAARECORD    0
0   Flag:  0   :   Flag 0 is currently used to represent the critical flag, which isn't in use anymore.
0   Tag:  iodef   :   specifies an URL to which a certificate authority may report policy violations.
0   Value:  mailto:webmaster@webernets.net   :   The value associated with the tag.
CAARECORD    1
1   Flag:  0   :   Flag 0 is currently used to represent the critical flag, which isn't in use anymore.
1   Tag:  issuewild   :   explicity authorizes a single certificate authority to issue a wildcard certificate (and only wildcard) for th
1   Value:  ;   :   The value associated with the tag.
CAARECORD    2
2   Flag:  0   :   Flag 0 is currently used to represent the critical flag, which isn't in use anymore.
2   Tag:  issue   :   explicity authorizes a single certificate authority to issue a certificate (any type) for the hostname.
2   Value:  letsencrypt.org   :   The value associated with the tag.
Certificate Transparency wird Gebprüft
Möchten Sie alle Einträge anschauen oder nur überprüfen, ob sich der Mail-Server im Transparency befindet?
Alle: 1
Nur Check: 2
2
false
Auf welchen Port wollen Sie die TLSA Überprüfung tätigen?
```

Beispiel eines Scoring Outputs

Einleitung: Ein Web-Browser zeigt mit einem Schloss an, dass die Verbindung zu einem Web-Server sicher und vertrauenswürdig ist. Macht ein Mail Client eine solche Abfrage auch? Mit welchen Kriterien kann festgestellt werden, dass eine TLS-Verbindung zu einem Mail-Server vertrauenswürdig ist?

Aufgabenstellung: Es soll ein Tool erstellt werden, mit dem in einfacher Weise die gängigsten Sicherheitsparameter eines Mail-Servers abgefragt werden können. Diese beinhalten nicht nur das Server-Zertifikat, sondern auch Host-Informationen, die aus dem Domain Name System (DNS) bezogen werden können. Darunter fallen MX, DNSKEY, TLSA und CAA Resource Records. Es soll auch festgestellt werden können, ob ein gültig ausgestelltes Zertifikat von einer Certification Authoritiy (CA) in ein Transparency Log eingespiesen wurde. Die Ergebnisse der Abfragen sollen durch eine Java Library als Objekt zurückgegeben werden, damit diese flexibel weiterverarbeitet werden können.

Ergebnis: Mit der im Rahmen dieser Arbeit in Java realisierten Open Source Library können die wichtigsten Sicherheits-Indikatoren von einem Mail-Server abgefragt werden. Zusätzlich wird dem Benutzer mit einem automatischen Scoring die Entscheidung erleichtert, wie weit der Destinations-Server als sicher eingestuft werden kann.