Abstract der fertigen Arbeit

Social Engineering Attacks are one of the most dangerous threats for the company's cybersecurity. One technique for performing these attacks are spear-phishing e-mails, which are based on mail spoofing to pretend to be sent from a trustful person. Existing mechanisms for preventing mail spoofing and recognizing spoofed e-mails depend mainly on the configuration of both the sender's and receiver's e-mail server to work.

The approach of using machine learning for authorship verification as part of an e-mail client app for iOS takes the prevention mechanism directly to the end-user, to use it independently from any server configuration. The developed prototype learns the language used of the different senders/authors by analyzing already received e-mails. Prior e-mails are used as training sets for machine learning to create a model and to be able to match new incoming e-mails with the learned senders/authors. As a result, the app displays the probability of the sender, named in the e-mail headers having sent the given e-mail. A low likelihood or the assignment to another author would indicate that the classified e-mail might be suspicious.

The performed evaluations for this approach show that authorship verification with machine learning has some limitations. As an example, the occurrence of sender names in the trained documents, as well as in the classified e-mails, influenced the results significantly. To sum up, the results show that the approaches investigated and attempted with the app developed in this thesis are not useful to verify the authorships of e-mail in a way that cannot be bypassed by attackers. The overall accuracy in verifying legitimate authorships is less than 60 percent.

The results imply that the idea of authorship verification based spear-phishing prevention would need more extensive research to develop an algorithm that detects and extracts significant linguistic key features of e-mails to perform a high accurate authorship verification. Meanwhile, existing sender authentication techniques like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), or S/MIME (Secure/Multipurpose Internet Mail Extensions) should be more supported and their usage simplified. These mechanisms are proofed and increase e-mail security considerably, so the main downside of these techniques is their limited deployment.