Public-Key-Infrastrukturen

Beim Einsatz asymmetrischer Verfahren ohne zusätzliche Infrastruktur ergeben sich einige Probleme. Diese lassen sich in vier Bereiche aufteilen.

Authentizität der Schlüssel

Wie im vorigen Abschnitt bereits besprochen, haben wir ein Authentizitätsproblem. Wenn Alice Bob eine verschlüsselte Mail schreiben will, benötigt sie Bobs öffentlichen Schlüssel. Wenn Mallory es jedoch schafft, Alice seinen eigenen öffentlichen Schlüssel als den von Bob unterzuschieben kann er selbst die Mail entschlüsseln.

Das kann auf verschiedene Art und Wiese geschehen: Wenn Bob Alice seinen öffentlichen Schlüssel übers Netz zuschickt, kann Mallory den Schlüssel abfangen und durch seinen eigenen ersetzen (Man-in-the-Middle-Attacke). Dasselbe kann Mallory machen, wenn Alice Bobs Schlüssel von einem Key-Server herunterlädt. Ein Angreifer kann auch versuchen, seinen eigenen Schlüssel im Netz als den von Bob zu verbreiten. Einem öffentlichen Schlüssel kann man nicht ansehen, wem er gehört.