4.3 Nachrichten-Authentifizierungs-Code

Ein Nachrichtenauthentifizierungscode (engl. ***M**essage **A**uthentication **C**ode*, kurz *MAC*) ist eine Hash-Funktion *H(.)*, die einen *Authentifizierungsschlüssel s* für die Verifikation des Hashwertes enthält. Dadurch wird Authentizität ohne Geheimhaltung erreicht. Mithilfe eines *MACs* können die übertragenen Nachrichten beglaubigt werden, ohne komplexe Verschlüsselungsalgorithmen einsetzen zu müssen. Einzelne Benutzer können also mit *MACs* überprüfen, ob ihre Nachrichten geändert wurden (z.B. von Malware-Software). Abbildung 7 zeigt schematisch den Ablauf einer Nachrichtenübertragung mit *MACs*.

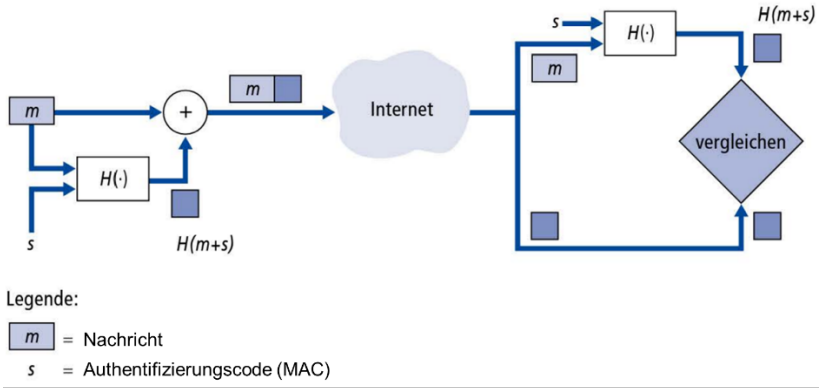

Abbildung 1: Nachrichtenübermittlung mit *MACs*

Der wichtigste Standard ist heute der *Hash-basierte Nachrichtenauthentifizierungscode* (engl. *Hash-based Message Authentication Code,* kurz *HMAC*) [1], der entweder mit *MD5* oder *SHA-1* verwendet werden kann. *HMAC* wendet die Hash-Funktion sogar zweimal auf die Daten und den Authentifizierungsschlüssel an und können beispielsweise in den Protokollen TLS und SSH eingesetzt werden.

[1] Siehe: HMAC – Wikipedia

© Copyright 2023, alle Rechte vorbehalten