

Modul „Sichere Kommunikation“

Ziel

- Die Absolventen dieses Moduls kennen die Grundverfahren zur Teilnehmerauthentifikation und Schlüsseletablierung sowie eine Auswahl von im Internet verwendeter Sicherheitsprotokolle.
- Die Absolventen haben die Kompetenz, die subtilen Möglichkeiten eines Angriffes auf Kommunikation über ein offenes Medium, wie etwa dem Internet, zu verstehen und einzuschätzen.
- Sie sind in der Lage, komplexe Problemstellungen im Bereich Sicherheitsprotokolle systematisch zu analysieren und zu bewältigen.

Inhalt

Mit dem großen Erfolg des Internets und dessen zunehmender Nutzung für geschäftliche sowie private Transaktionen steigt der Bedarf an Technologien zur sicheren Kommunikation. Zum Beispiel ist es für E-Commerce und E-Business unbedingt notwendig, dass die Vertraulichkeit und Integrität übertragener Nachrichten garantiert werden kann. Die Bedrohung der Sicherheit einer Kommunikation, die über ein offenes Medium wie dem Internet abläuft, ist aber sehr groß: Ein Angreifer kann die übertragenen Nachrichten nicht nur abhören, sondern diese auch aktiv manipulieren.

In diesem Modul werden die wichtigsten Grundlagen und Mechanismen zur Sicherung von Kommunikation vermittelt. Es werden auch weitergehende Fragen betrachtet, wie zum Beispiel: „Wie stelle ich sicher, dass ich beim E-Banking tatsächlich mit dem Server meiner Bank und nicht etwa mit dem Rechner eines Angreifers kommuniziere?“, „Wie sicher ist mein Wireless LAN?“, „Wie kann ich analysieren, ob ein Sicherheitsprotokoll tatsächlich keine Lücke für einen Angreifer offen lässt?“, oder „Woher weiß ich, dass beim Geldabheben am Bankautomat, meine PIN nicht von einem kriminellen Bankangestellten abgefangen werden kann?“

Literatur

- J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2008

- J. Schwenk, *Sicherheit und Kryptographie im Internet*, 3. Auflage, Vieweg+Teubner, 2010
- W. Stallings, *Cryptography and Network Security: Principles and Practice*, Fifth Edition, Prentice Hall, 2010