# Elektrotechnisches Kolloquium

der Bergischen Universität Wuppertal

Die Fakultät für Elektrotechnik, Informationstechnik und Medientechnik lädt zur Teilnahme an folgender Vortragsveranstaltung mit anschließender Diskussion ein:

Es spricht

**Denis Diemert, M.Sc.**
Lehrstuhl für IT-Sicherheit und Kryptographie
Prof. Dr.-Ing. Tibor Jager

über das Thema

**On the Tight Security of the Transport Layer Security (TLS) Protocol Version 1.3**

## Inhalt:

Kommunikation über das Internet ist heutzutage kaum noch aus dem alltäglichen Leben wegzudenken. Die Anwendungen sind vielfältig: So nutzt man das Internet, um mit anderen Menschen über Instant-Messenger oder Soziale Netzwerke in Kontakt zu bleiben bis hin zu heiklen Aufgaben, wie der Überweisung von Geld von zu Hause aus mithilfe von Online-Banking. Da potenzielle Angreifer die Kommunikation über das Internet mitlesen oder sogar unerwünschte Änderungen daran vornehmen könnten, muss das Internet als unsicherer Übertragungsweg betrachtet werden. Ohne Maßnahmen, die eine sichere Übertragung über das Internet gewährleisten, wäre dieses vermutlich nicht zu dem geworden, was es heute ist. Der de-facto Standard um eine sichere Übertragung zu gewährleisten, ist das Transport Layer Security (TLS) Protokoll. TLS ermöglicht es, dass zwei Parteien mithilfe von Kryptographie sicher über einen unsicheren Übertragungsweg, wie das Internet, kommunizieren können. Dazu führen die zwei Parteien die folgenden zwei Schritte aus. Zunächst führen sie ein Schlüsselaustauschprotokoll durch, den so genannten *TLS-Handshake*, um ein gemeinsames Geheimnis festzulegen, sich auf Parameter zu einigen und sich gegenseitig ihre Identitäten zu beweisen. Dann verwendet das *TLS-Record-Protokoll* das ausgetauschte Geheimnis und die Parameter, um einen sicheren Kommunikationskanal aufzubauen.
Viele Anwendungen erfordern sichere Kommunikation über das Internet, darunter auch Anwendungen (wie Online-Banking), die hochsensible Daten verarbeiten. Hier ist es von besonderer Bedeutung, dass sich ein so wichtiger Sicherheitsmechanismus wie TLS, strengen Sicherheitsanalysen unterziehen sollte. Moderne Kryptographie nutzt die Werkzeuge der Mathematik, um genaue formale Analysen von kryptographischen Konstruktionen, so genannte *Sicherheitsbeweise*, zu erstellen. Heutzutage ist es sogar üblich, dass neue Konstruktionen zusammen mit einem solchen Sicherheitsbeweis entwickelt werden. Ein Sicherheitsbeweis liefert nicht nur eine hervorragende Evaluierung der Plausibilität einer Konstruktion, sondern kann auch bei der Auswahl von Parametern verwendet werden, die in direktem Zusammenhang mit der garantierten Sicherheit eines kryptographischen Systems stehen. Hier ist insbesondere die *Schärfe* (engl. tightness) des Sicherheitsbeweises von Bedeutung. Scharfe Sicherheitsbeweise ermöglichen es nämlich, kryptographische Systeme mit theoretisch begründeten Parametern (d.h., die durch den Sicherheitsbeweis gestützt werden) einzusetzen, ohne dass ein durch den Sicherheitsbeweis verursachter Sicherheitsverlust ausgeglichen werden muss. Dies bedeutet in der Regel, dass bei der Benutzung des Systems keine Kompromisse zwischen Effizienz und Sicherheit gemacht werden müssen.
In diesem Vortrag diskutieren wir die scharfe Sicherheit („tight security“) der aktuellen Version des TLS-Protokolls, TLS 1.3, mit Fokus auf das TLS 1.3-Handshake-Protokoll. Insbesondere präsentieren wir eine scharfe Sicherheitsanalyse für den TLS 1.3 Handshake.

Der Vortrag ist auf Englisch.

**T e r m i n :** **1. Februar 2023, 14 Uhr**

**O r t :** **Online via Zoom** (Meeting ID: 971 8192 0770, Passcode: jj1vQZnd)
https://uni-wuppertal.zoom.us/j/97181920770?pwd=ZUc4Zmsxd0N3MW9wQXBER1Y4azNSQT09