Einladung
zum Doktorandenkolloquium

Stärkung der Sicherheitsgrundlagen in drahtlosen Next-G-Telekommunikationssystemen

von Felix Klement

am Mittwoch, 6.11.2024 ab 13:50 Uhr im 027, WiWi, Innstr. 27
und online per Zoom (die Zoomdaten wurden intern gemailt)

(Betreuer: Prof. Dr. Stefan Katzenbeisser,
Lehrstuhl für Technische Informatik)

Abstrakt: Die neuesten Fortschritte im Bereich des sechsten Mobilfunkstandards (6G) sowie die wachsende Komplexität drahtloser Netzwerke spielen eine maßgebliche Rolle bei der effizienten Umsetzung der fortlaufenden Digitalisierung in unserem täglichen Leben. Die Vielfalt der eingesetzten Technologien erweitert sich kontinuierlich mit stetig steigenden Anforderungen, wodurch die Gefahr für potenzielle Sicherheitsrisiken und Schwachstellen in Bezug auf die Informationssicherheit dieser Netzwerke verstärkt wird. Drahtlose Kommunikationsnetzwerke nehmen häufig eine Schlüsselposition in kritischen Infrastrukturen ein, was sie zu attraktiven Zielen für potenzielle Cyberangriffe macht. Hiebei besteht aus Sicht der Forschung ein erheblicher Bedarf an effektiven Methoden zur Lösung dieser Probleme. Diese Arbeit widmet sich den Sicherheitsgrundlagen für Next-Generation (Next-G) drahtlose Telekommunikationssysteme. Im Zentrum der Arbeit stehen innovative Konzepte solcher Kommunikationssysteme, die anhand von Fallbeispielen untersucht und analysiert werden. Ein Schwerpunkt liegt dabei auf dem Ansatz von offenen Radio Access Networks (RANs). Dadurch sollen offene und interoperable Netzwerkarchitekturen ermöglicht werden, was im Gegensatz zu aktuell traditionellen RAN-Systemen steht, die oftmals proprietär und herstellerspezifisch sind. Wir entwickeln einen empirischen Ansatz, um Bedrohungen in Telekommunikationssystemen wie dem RAN durch Analysen zu identifizieren und anschließend detailliert zu bewerten. Im weiteren Verlauf unserer Arbeit zeigen wir Sicherheitslücken in drahtlosen Kommunikationssystemen auf. Für unsere Angriffsszenarien präsentieren wir eine detaillierte Vorgehensweise zur Ausführung der Attacken sowie effektive Methodiken zur Vermeidung beziehungsweise Detention der von uns identifizierten Schwachstellen.