Kurzfassung

Praktische Aspekte der informationstheoretischen Sicherheit für das Internet der Dinge

Das Internet der Dinge (Internet of Things (IoT)), bei dem die Kommunikationsknoten primär durch (kleine) eingebettete Systeme gebildet werden, gewinnt zunehmend an wirtschaftlicher Bedeutung. Das IoT wird als die nächste industrielle Revolution bezeichnet und wird die Interaktion mit der physikalischen Welt massiv beeinflussen. Hiervon sind auch eine Reihe Schlüsselindustrien betroffen, beispielsweise durch die Automatisierung im Maschinenbau oder der Telemedizin.

Seit einigen Jahren ist die Nachfrage nach erhöhter Sicherheit in IoT-Systemen dramatisch gewachsen. Wichtige Beispiele sind hier sichere Kommunikationsverbindungen (bei der Übertragung von Sensordaten und der Ansteuerung von Aktuatoren), Code-Aktualisierung, Funktionsfreischaltung oder Komponenten-Identifikation zur Bekämpfung der Produktpiraterie. Durch den enormen Preisdruck stellt sich jedoch eine große Herausforderung dar, da es schwierig ist moderne kryptografische Lösungen, wie beispielsweise Public-Key Zertifikate oder digitale Signaturen, in Kleinstsystemen zu integrieren. Der Grund hierfür liegt in der hohen Komplexität, den um 2-3 Magnituden erhöhtem Energieverbrauch, sowie dem zum Teil überwiegendem Ressourcenbedarf (bspw. Codegröße) für die Sicherheit.

In der vorliegenden Arbeit untersuchen wir angewandte informationstheoretische Sicherheitsansätze — die sogenannte Physical-Layer Security (PLS) — in Bezug auf effiziente Implementierungen und potenzielle Angriffe. Im Vergleich zur klassischen Kryptographie stellt PLS ein fundamental differenzierbares Paradigma dar, welches Sicherheitsziele durch die Verwendung von physikalischen Eigenschaften des Funkkanals und der physikalischen Umgebung erreicht.

Während in der Literatur bereits ein umfangreicher wissenschaftlicher Hintergrund zur klassischen Kryptographie vorhanden ist, ist die Sicherheit und Effizienz solcher PLS Konstruktionen, insbesondere auf Ressourcenbeschränkten und kostensensitiven Plattformen, noch nicht ausreichend erforscht. In dieser Arbeit werden daher neuartige Algorithmen und Mechanismen vorgestellt, evaluiert und diskutiert. Ein besonderer Fokus liegt auf der Entwicklung neuer Verfahren zur authentischen Schlüsseletablierung über nicht-vertrauenswürdige Infrastrukturen (bspw. WLAN Router oder Basisstationen). Wir werden zeigen, wie PLS die Sicherheit von IoT-Funknetzwerken komplementieren und signifikant verbessern kann.

Schlagworte.

Wireless physical layer security, Kanal-basierte Schlüsselextraktion, Authentifizierte Schlüsseletablierung, Proximitäts-basierte Gerätekopplung, Schlüsseletablierung über nicht-vertrauenswürdige Relais, Relai-Angriff-Verhinderung für Schliesssysteme, Software Implementierung, Sicherheitsanalyse, Performance Evaluierung