

Obhajoba disertační práce Ing. Ondřeje Hujňáka z Ústavu inteligentních systémů Fakulty informačních technologií se bude konat ve čtvrtek 28.11.2024 od 13 hodin v zasedací místnosti G108 na FIT VUT, Božetěchova 2, Brno.

Studijní program: Výpočetní technika a informatika

Název práce: Zabezpečení bezdrátové komunikace u zařízení IoT/Security of wireless communication for IoT devices

Abstrakt/Abstract: Práce se zabývá tématem bezpečnosti a soukromí v kontextu internetu věcí. Zaměřuje se zejména na bezdrátové sítě určené pro zařízení internetu věcí, konkrétně LoRaWAN, Zigbee a Bluetooth Low Energy. Bezpečnostní slabiny a zranitelnosti těchto sítí jsou podrobně analyzovány a je navržen bezpečnostní monitoring na základě frameworku NEMEA. Pro monitorování sítí Bluetooth je představen nový princip, který je podrobně rozebrán od teoretického návrhu až po experimentální ověření a případné vylepšení na produkční úroveň. Dále je v práci představen návrh zabezpečení proprietární sítě IQRF, který je součástí jejího nového standardu. Tento návrh vychází z výše uvedené analýzy bezpečnostních slabín a výrazně zvyšuje bezpečnost této celosvětově používané sítě. V neposlední řadě se práce zabývá otázkami ochrany soukromí analýzou přenosu dat čtyř bran internetu věcí určených pro domácí použití. Zkoumá také možné metody anonymizace zařízení IoT v různých typech sítí, identifikuje problémy a navrhuje budoucí směry výzkumu./ The thesis explores the topic of security and privacy within the context of the Internet of Things. It particularly focuses on wireless networks designed for IoT devices, specifically LoRaWAN, Zigbee and Bluetooth Low Energy. The security weaknesses and vulnerabilities of these networks are analysed in detail and a security monitoring based on the NEMEA framework is proposed. A novel approach for monitoring Bluetooth networks is introduced. This approach is discussed in detail from theoretical design to experimental validation and eventual enhancement to production level. Furthermore, the thesis outlines the security design of the proprietary IQRF network, which is part of its new standard. This design is based on the aforementioned security weakness analysis and significantly improves the security of this globally used network. Finally, the thesis addresses privacy concerns by analysing the data transmission of four IoT gateways designed for home use. It also explores potential methods for anonymising IoT devices in various network types, identifying challenges and suggesting future research directions.

Školitel: doc. Dr. Ing. Petr Hanáček, ÚITS FIT VUT, Česká republika

Školitel-specialista: Ing. Ivan Homoliak, Ph.D., ÚITS FIT VUT, Česká republika

Oponenti: prof. Ing. Ivan Kotuliak, Ph.D., FIIT STU, Slovenská republika

doc. RNDr. Petr Švenda, Ph.D., FI MU, Česká republika