INFOKOMMUNIKÁCIÓS ÉS INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

9TH eHEALTH SECURITY CONFERENCE

Medical (IoT) device vulnerabilities

Péter Pál Orosz NCSC-HU

infolab.nemzetilabor.hu infolab@nbsz.gov.hu

2024.11.06.

Our research network

National Research, Development and Innovation Office Hungary
PROJECT FINANCED FROM THE NRDI FUND

- National Research, Development and Innovation Office → National Laboratories
- Infocommunications and Information Technology NL → our research base
- Special Service for National Security – National Cyber Security Center → project owner

HUNGARIAN NATIONAL LABORATORY

INFOKOMMUNIKÁCIÓS ÉS INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

1996 SPECIAL SERVICE FOR NATIONAL SECURITY fortes fortuna adiuvat

NATIONAL CYBER SECURITY CENTER HUNGARY

Our research network

Key cooperative partners

Alverad Technology Focus Ltd.

University of Debrecen

Key professional collaborators

Semmelweis University – Health Servises Management Training Centre

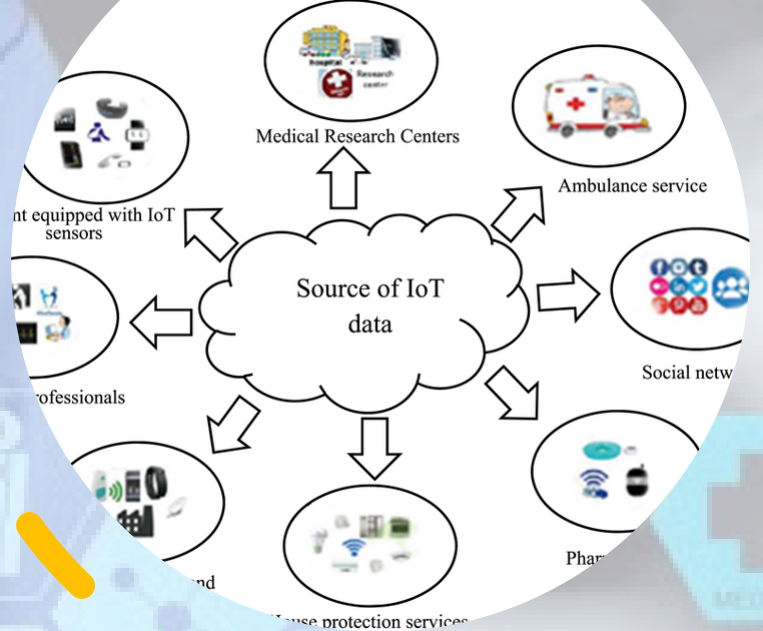
György Gottsegen National Cardiovascular Institute

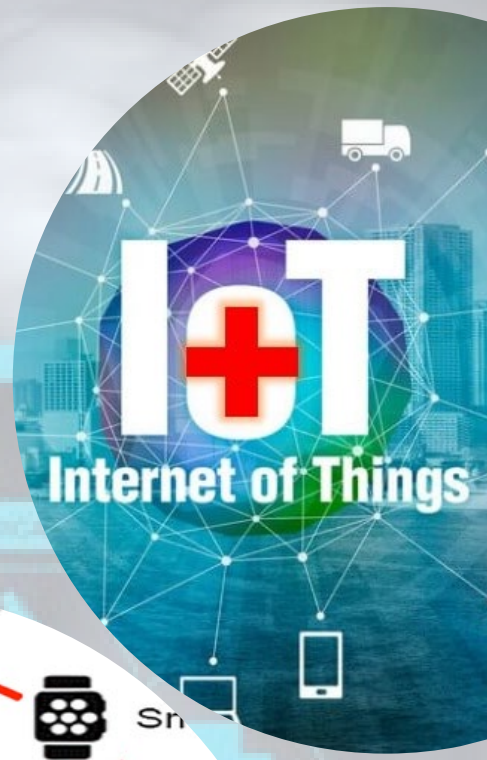
Hungarian Charity Service of the Order of Malta

Why we do research

- Heterogeneous environment in all respects
- Mass produced/used devices
- Safety is not the primary concern

  → cyber security challenge
- Definition of a typical IoT ecosystem, its components
- Creating an ecosystem catalog
- Drawing up a security situation
- IoT ecosystem security analysis method
- Examination, qualification, security recommendation of a selected IoT system (Telemedicine)





Our key focus – IoT devices/ecosystems security

- Classification,
- Security overview,
- Risk analysis / assessment,
- Selection of IoT eco.,
- Specific safety recommendations.

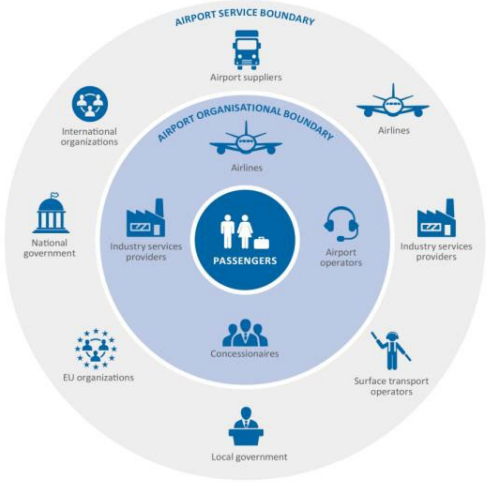
What we've done

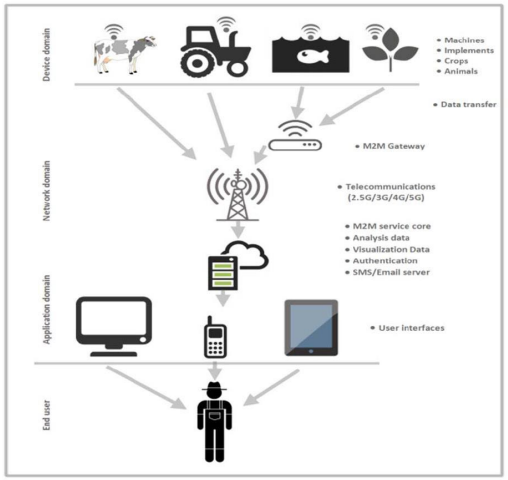
Classification – IoT ecosystems catalog (in general)

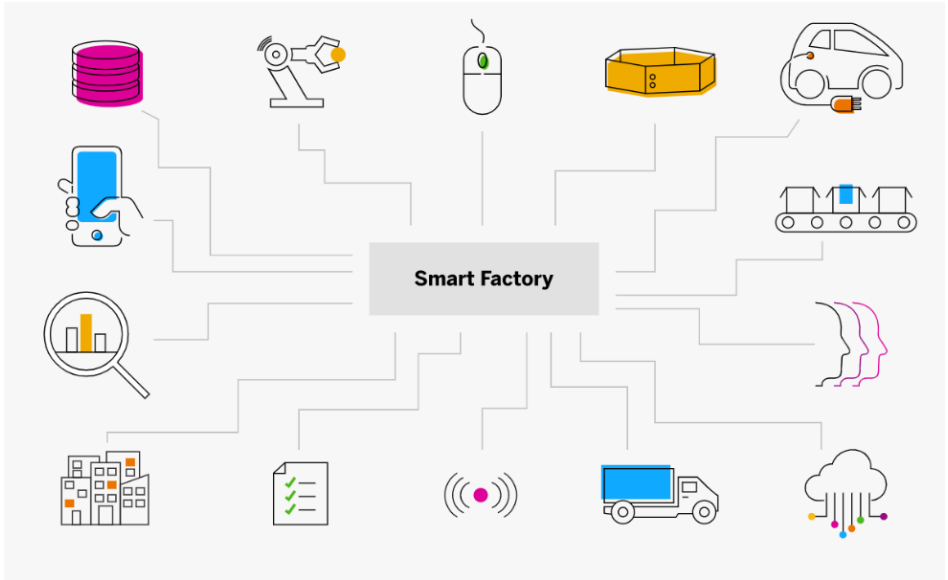
Identify similarities → creating groups

Intelligent/smart homes – cities – public transportation – airports – electrical networks – vehicles – factories – agriculture – public administration –

hospitals/eHealth ecosystems





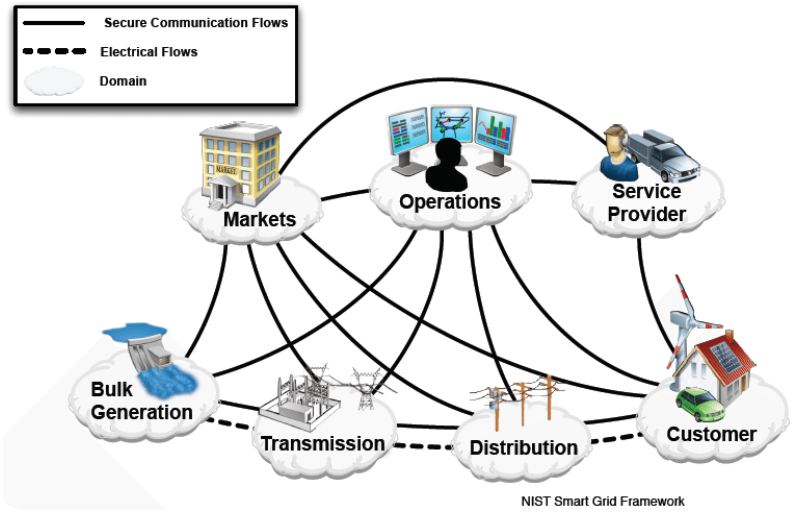


What we've done

IoT ecosystem – Security overview, risk/security analysis

Defining smart electrical networks's working modell

- applied technologies and communication protocols – phisical boundaries
- wide range controll and monitoring
- integration of distributed and centralized solutions
- custormer side systems/devices
- security solutions and procedures



NIST Smart Grid Framework

What we've done

Result of analysis – conclusions

Infrastructure / Operation / Data(management) protection

application of rules and regulations (inter)national level, standards (ITU, ETSI, 3GPP, etc.)

(known) threats, attacks

physical and environmental level

communication level, network level, **logical/cyber level**

Privacy threats

Study on Healthcare IoT Ecosystem Security Analysis

Modern **challenges** and **achievements** in healthcare:

- expensive devices, high costs of operation and maintenance
- privacy and security concerns – personal data, medical information
- private healthcare services – modern high-tech, but expensive too

Need for significant development → IT systems and modern healthcare devices

Widespread distribution and use of IoMT devices

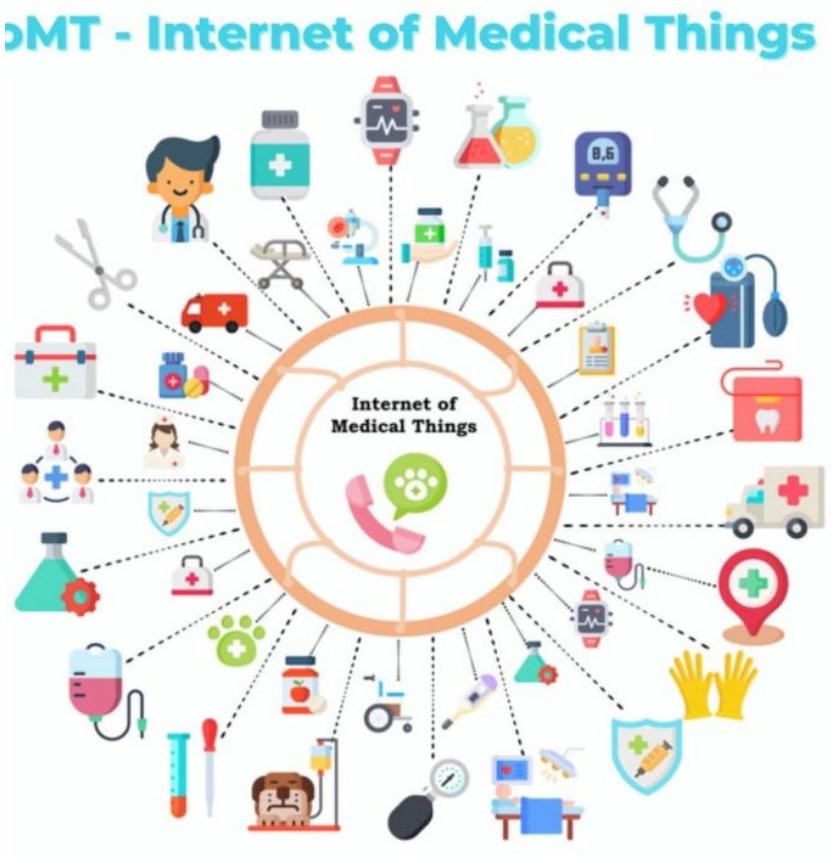
Cyber security threats

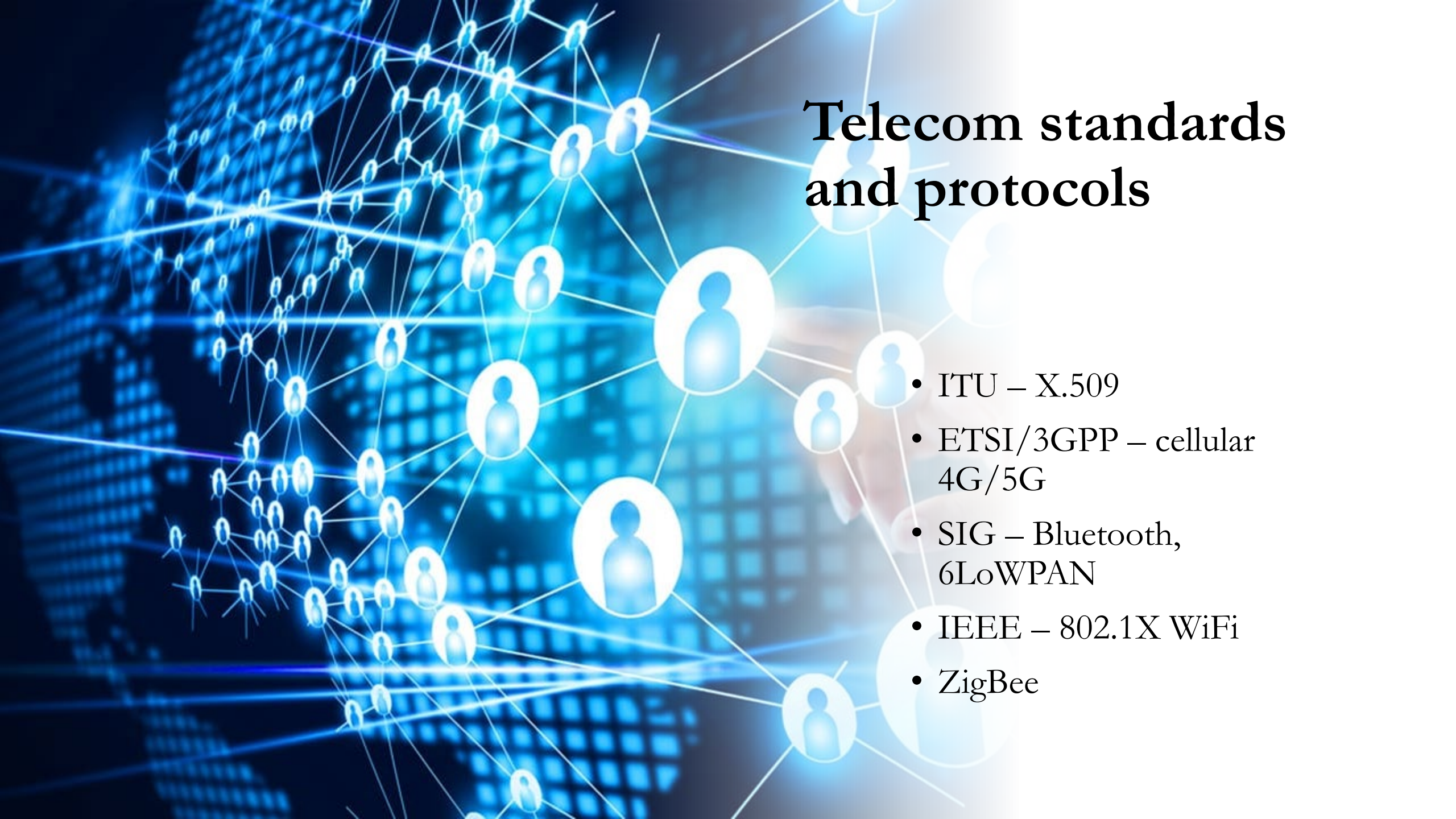
Application of IoMT devices

- ENISA 2004: definition of smart-Hospitals

…aims to improve existing patient care procedures and introduce new capabilities.

- **IoMT ecosystem's structure, 3 domains:** sensors, network(s), applications
- **Participants:** patients, healthcare service providers, telecom service providers, manufacturers, distributors, backoffice/support, regulatory authorities, research organizations





Telecom standards and protocols

- ITU – X.509
- ETSI/3GPP – cellular 4G/5G
- SIG – Bluetooth, 6LoWPAN
- IEEE – 802.1X WiFi
- ZigBee

Rules and Standards

- HL7 (Health Level 7)
- FHIR (Fast Healthcare Interoperability Resources)
- DICOM (Digital Imaging and Communications in Medicine)
- ISO/IEC 80001
- AAMI TIR57

National and international regulations

- 1997. XLVII law (Eüak.);
- 1997. CLIV. law (Eütv.);
- 62/1997. (XII.21.) NM decree;
- 1997. LXXXIII. law;
- 39/2016.(XII. 21.) EMMI decree;
- 2013. V. law (Ptk.)
- 1996 évi XX. law;
- 1992. XXXIII. law (Kjt.),
- 2012. I. law (Mt.).
- 516/2020. (XI. 25.) government decree
- 2023. XXIII. law: Cybersecurity Certification and Cybersecurity Supervision
- 910/2014/EU, (EU) 2018/1972 , NIS2, etc.

Security of Medical IoT

NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

- Measure 1.: determining the most likely use cases, identification of expected users and determination of expected ways of use
- Measure 2.: determining customer cybersecurity needs and goals
- Measure 3.: customer needs and goals must be assessed and determined
- Measure 4.: designing support according to the needs and goals of the customers
- Measure 5.: all actions taken by the manufacturer with the IoT device after the sale
- Measure 6.: method of communication with customers and its content

Security analysis of IoMT device networks

Threat modelling methods: DREAD, OCTAVE, PASTA, **STRIDE**

- Device level threats
- Network threats
- User level threats
- Failure Mode and Effects Analysis

IoMT Ecosystem Security Recommendation

- In accordance with the NIST Cybersecurity for the Internet of Things (IoT) and NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations
- IoMT logical protection: **device configuration**, data protection, **access management**, software update, security supervision, device security, regulation, **documentation**, manufacturer device monitoring and information distribution, **training and awareness**

SSNS aspects, utilization

- A "complete" picture of the current situation of IoT devices - with a focus on security,
- In general: ecosystem catalog, security situation picture, test methodology,
- NL utilization: in cooperation with SZTFH, EÜ IoT system certification

infolab@nbsz.gov.hu

infolab.nemzetilabor.hu

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Thank you for your attention!

INFOKOMMUNIKÁCIÓS ÉS INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

Orosz Péter Pál

email: orosz.peter@nbsz.gov.hu

infolab@nbsz.gov.hu

mobil: +36-30-563-0616