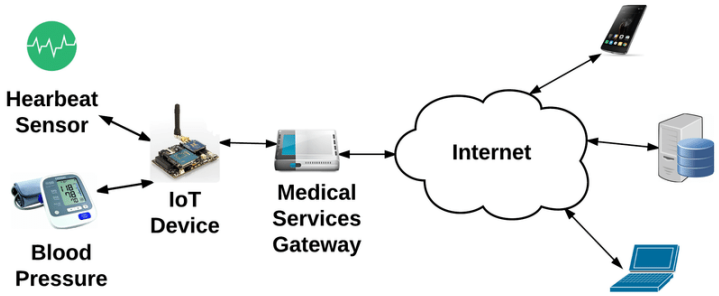
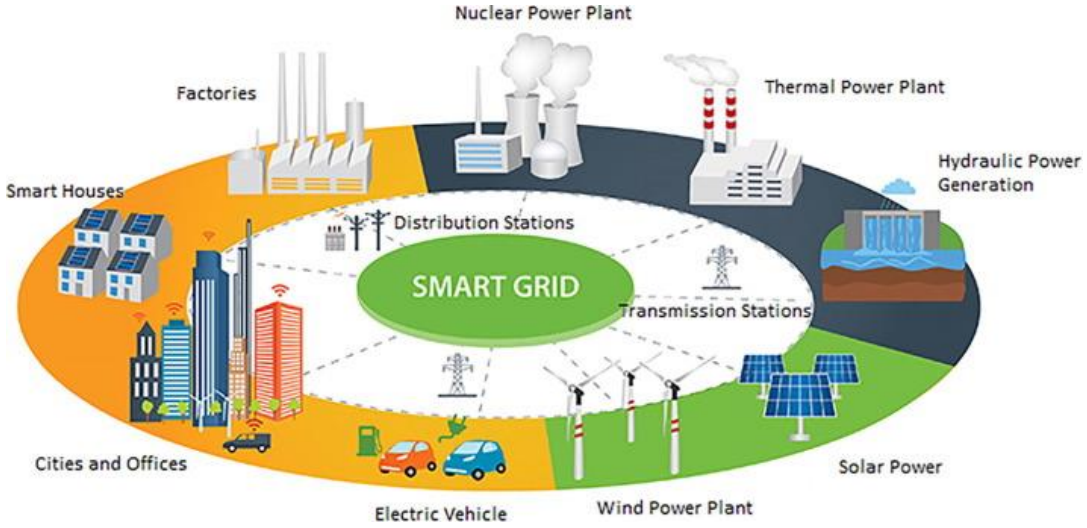
Bezpečnostní rizika IoT

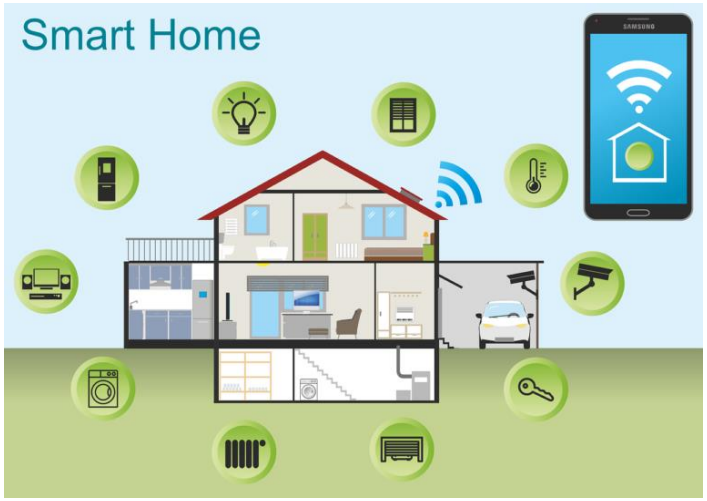
Petr Matoušek

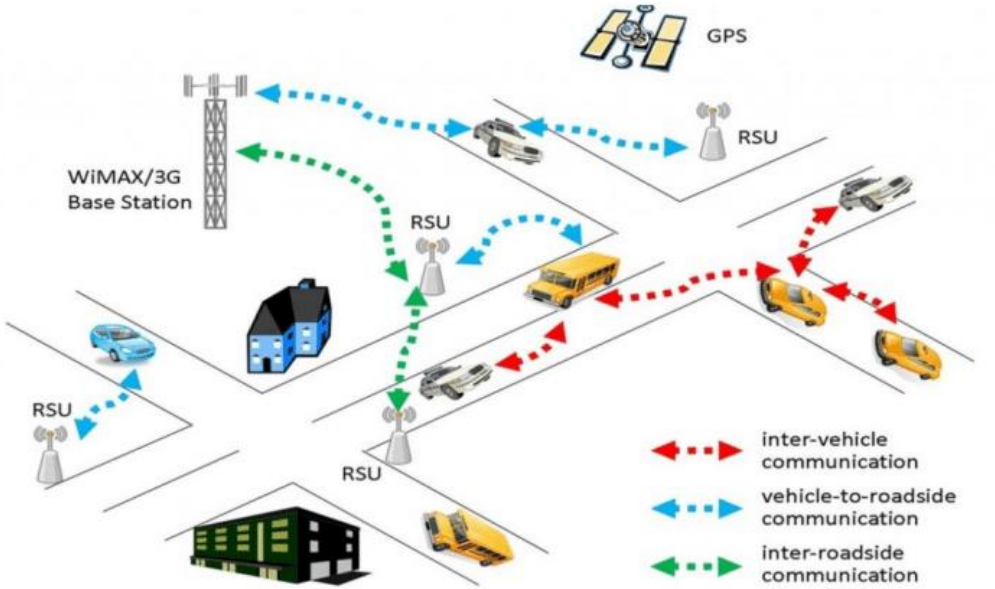
Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 1/2, 612 66 Brno - Královo Pole
matousp@fit.vutbr.cz

Co je Internet věcí?









Co je Internet věcí?

„A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies“ [1].

Základní vlastnosti IoT

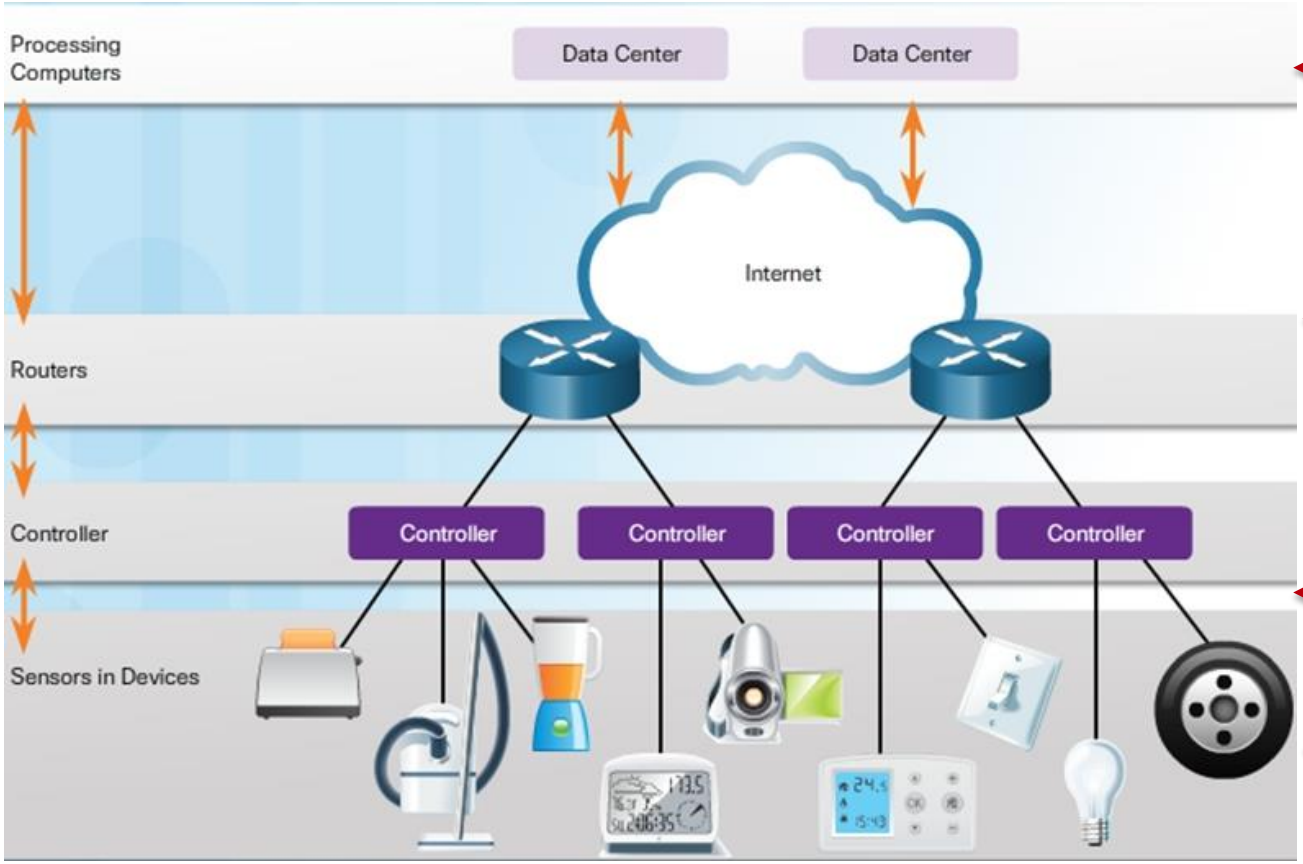
- IoT síť propojuje fyzická zařízení, senzory, objekty denního používání.
- IoT zařízení generují data, komunikují, vykonávají příkazy bez zásahu člověka.
- IoT zařízení jsou většinou jednoúčelová, s omezenou výpočetní a úložnou kapacitou.

Rozdělení IoT

- Průmyslové sítě IoT (Industrial IoT): automatizace, doprava, zdravotnictví
- Domácí sítě IoT (Home IoT, Consumer IoT): domácí zařízení, chytré přístroje

[1] Recommendation ITU-T Y.2060: Next Generation Networks – Overview of the Internet of things, 06/2012.

Koncová zařízení (IoT things) -> Kontroler/brána -> IP síť -> Cloud



Web API, mobile App

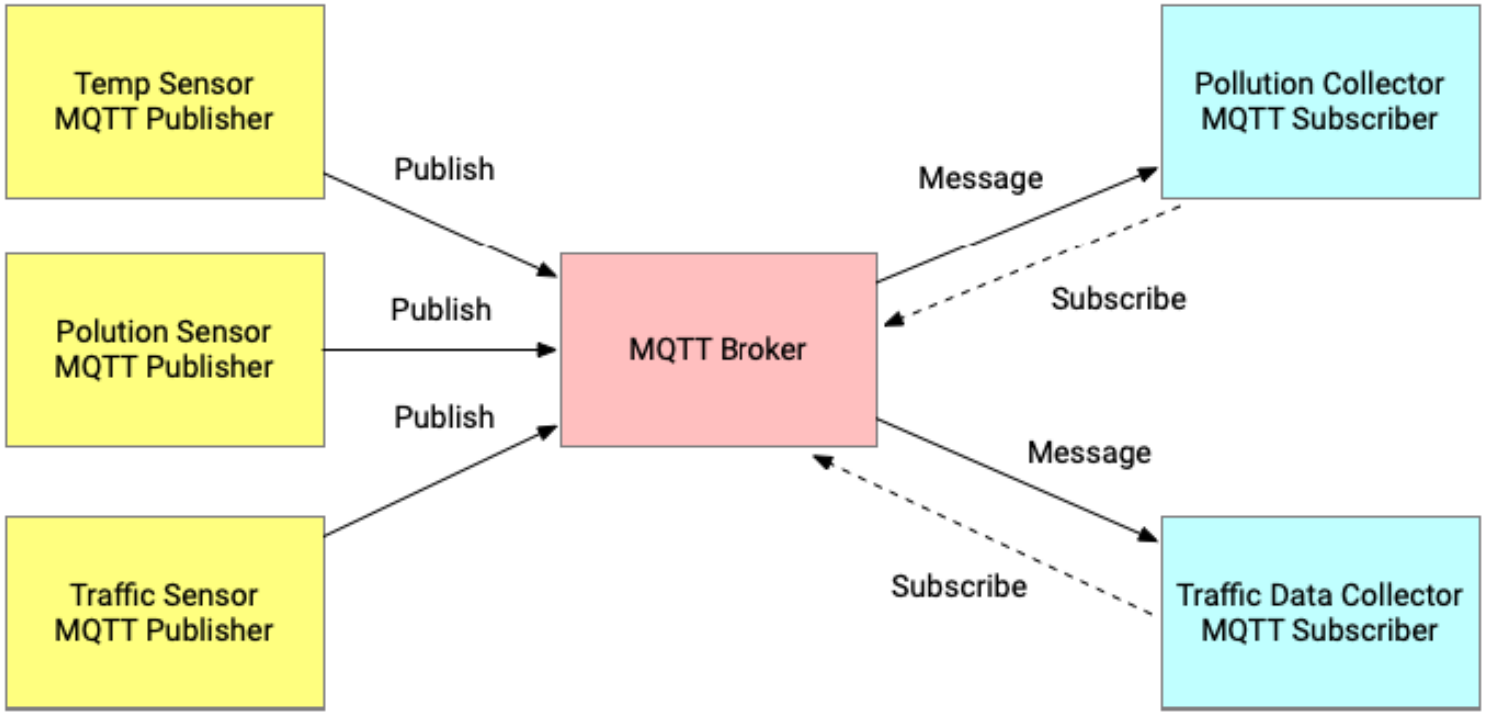
Ethernet + TCP/IP
+
MQTT, CoAP, HTTPs

WiFi, Bluetooth, ZigBee, Z-Wave, 6LoWPAN, Wireless M-BUS, ...

senzory, regulátory, kamery, chytrá zařízení

Příklad komunikace MQTT [2]

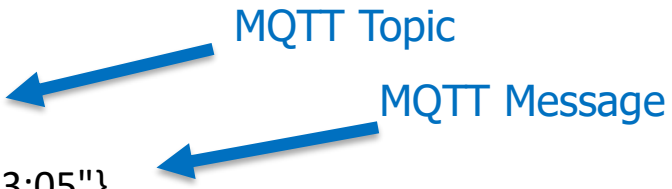
- Komunikace typu publish – subscribe (zasílání – odebírání)
- Zprávy Ping, Connect, Publish, Subscribe, Unsubscribe, ...



- Komunikace MQTT je nezabezpečená. Co nám může prozradit?

[2] Message Queuing Telemetry Transport (MQTT), ISO/IEC 20922:2016, 06/2016

Co nám prozradí MQTT?



22:01:59: 192.168.1.127 -> 192.168.1.200 tele/hifi/UPTIME
{"Time":"2018-09 11T21:02:00","Uptime":"9T10:13:05"}

22:02:48: 192.168.1.248 -> 192.168.1.200 bedlights/binary_sensor/bedlights_motion_1/state: ON

22:02:48: 192.168.1.200 -> 192.168.1.248 bedlights/light/bedlights/command: {"state":"ON"}

22:02:49: 192.168.1.248 -> 192.168.1.200 bedlights/light/bedlights/state:
{"effect":"None","state":"ON","brightness":166,"color":{"r":255,"g":255,"b":255}}

22:02:52: 192.168.1.248 -> 192.168.1.200 bedlights/binary_sensor/bedlights_motion_1/state: OFF

22:03:19: 192.168.1.200 -> 192.168.1.248 bedlights/light/bedlights/command: {"state":"OFF"}

22:03:19: 192.168.1.248 -> 192.168.1.200 bedlights/light/bedlights/state:
{"effect":"None","state":"OFF","brightness":166,"color":{"r":255,"g":255,"b":255}}

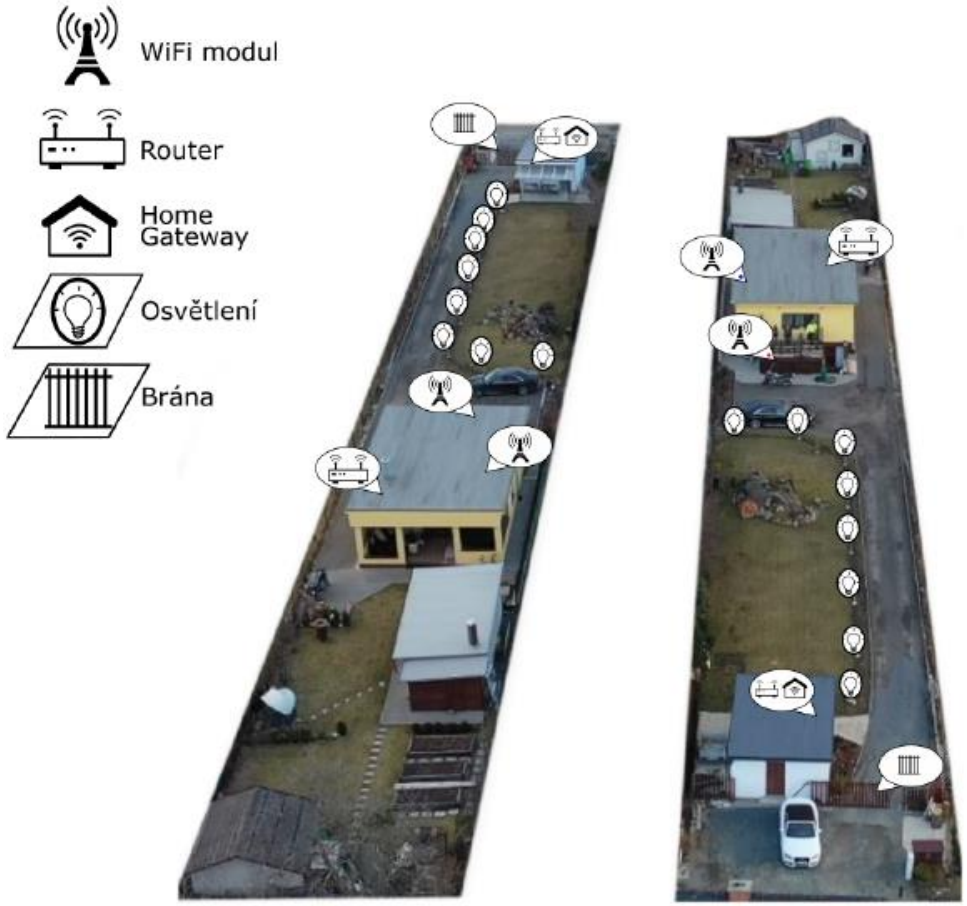
22:03:25: 192.168.1.127 -> 192.168.1.200 tele/hifi/STATE: {"Time":"2018-09-
11T21:03:26","Uptime":"9T10:14:31","Vcc":3.246,"POWER":"OFF","Wifi":{"AP":1,"SSId":"Petr-
IoT","RSSI":48,"APMac":"16:CC:20:EC:71:05"}}

22:07:30: 192.168.1.200 -> 192.168.1.244 cradlelights/light/cradlelights/command: {"state":"ON"}

22:07:30: 192.168.1.244 -> 192.168.1.200 cradlelights/light/cradlelights/state:
{"effect":"None","state":"ON","brightness":102,"color":{"r":255,"g":236,"b":218}}

Příklad chytrého ovládání světla a brány [3]

- Systém umožňující z chytrého zařízení (chytrý telefon, chytré hodinky) ovládat vstupní bránu a osvětlení domu.



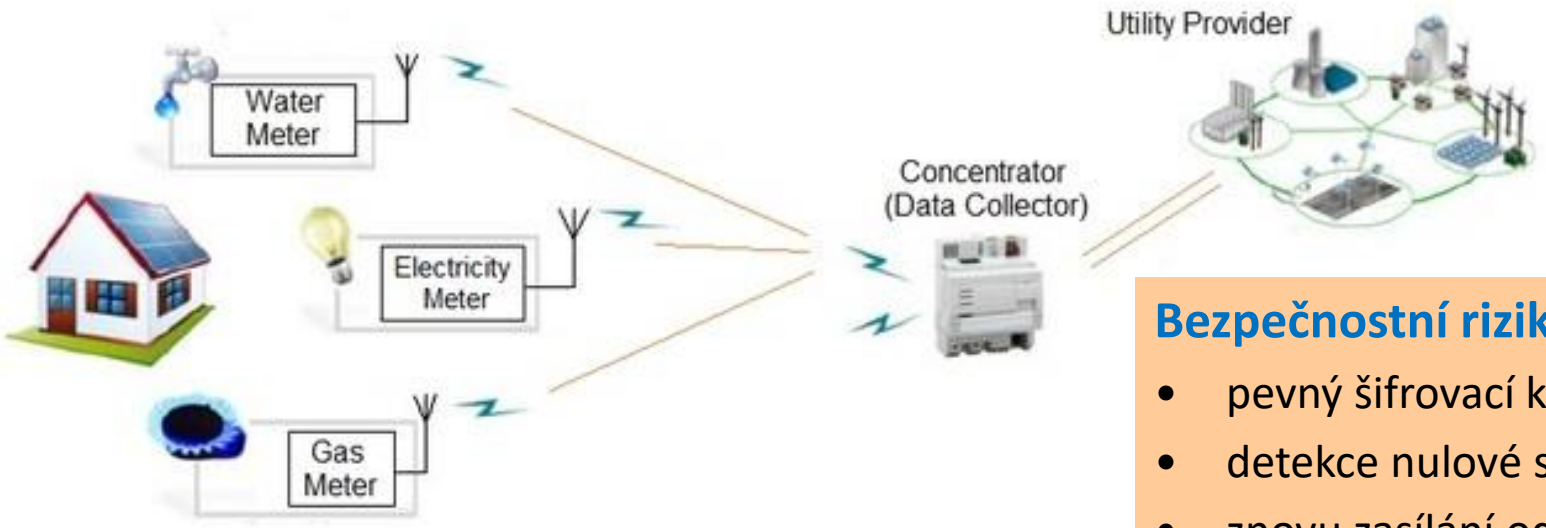
Zranitelnost systému:

- bezdrátová síť
- protokol MQTT
- domácí směrovač
- IoT brána
- mobilní aplikace

[3] J. Koudelka: IoT s Raspberry Pi, telefonem a hodinkami Samsung Galaxy Watch, Diplomová práce, FIT VUT v Brně, 2021

Příklad dálkových odečtů energie, vody, tepla [4]

- Dle směrnice EP a Rady č. 2018/2002 [5] o energetické účinnosti musí být měřiče a indikátory pro rozdělování nákladů na vytápění nainstalované po 25. říjnu 2020 dálkově odečitatelné. Stávající musí být nahrazeny dálkově odečitatelnými přístroji do 1.1. 2027.
- Používá se například bezdrátová komunikace Wireless M-BUS.



Bezpečnostní rizika [6]:

- pevný šifrovací klíč
- detekce nulové spotřeby
- znovu zasílání odečtu
- ...

[4] L. Polčák: Wireless M-Bus: Kdo ví, že perete?, Data Security Management, vol. 2019, no. 4, ISSN 1211-8737.
[5] Směrnice Evropského parlamentu a rady (EU) 2018/2002, Úřední věstník EU č. L 328/210, 2018.
[6] CVE-2021-34571, CVE-2021-34572, CVE-2021-34573, CVE-2021-34576

Požadavky na bezpečnost IoT a jejich implementace

- Ochrana dat (Confidentiality)
- Zabezpečení přístup (Access)
- Autentizace (Authentication)
- Soukromí (Privacy)
- Spolehlivost (Reliability)
- Škodlivý software, vyděračské aplikace (Malware, Ransomware)

	Conf	Access	Authen	Priv	Rel	Malw
IoT zařízení		✓	✓		✓	✓
Komunikace IoT zařízení ⇔ IoT brána	✓		✓	✓	✓	
IoT brána		✓	✓		✓	✓
Komunikace IoT brána ⇔Cloud	✓		✓	✓	✓	
Aplikace v cloudu		✓	✓	✓	✓	
Mobilní aplikace		✓	✓	✓		✓

Co nás (asi) čeká?

1. Postupné rozšiřování IoT zařízení a IoT sítí
   - Chytrá zařízení, domy, budovy, nemocnice, automobily, ...

2. Nové výzvy na bezpečnost provozu IoT
   - Ochrana soukromí (privacy)
   - Škodlivý software (malware) + vyděračské aplikace (ransomware)
   - Požadavek na spolehlivost a robustnost (reliability, redundancy)
   - Monitorování provozu IoT zařízení + detekce chyb/útoků [7,8]

3. Implementace základních bezpečnostních prvků v IoT zařízeních
   - Hardwarové nároky vs. cena
   - Nezbytné aktualizace firmwaru/softwaru
   - Ochrana zákazníků – regulace ze strany provozovatelů, státu, apod.

[7] Matoušek P., Ryšavý O., Grégr M.: Security Monitoring of IoT Communication Using Flows. ECBS '19. New York: ACM, 2019.

[8] Matoušek P., Ryšavý O., Polčák L: Unified SNMP Interface for IoT Monitoring. IEEE/IFIP International Workshop on Internet of Things Management. Bordeaux, 2021

Kde hledat doporučení ohledně bezpečnosti IoT?

- National Institute of Standards and Technology (NIST), U.S. Dept. of Commerce:
  - Fagan M., et al.: IoT Device Cybersecurity Guidance for the Federal Government. Establishing IoT Device Cybersecurity Requirements, NIST SP 800-213, 12/2020.
  - Fagan M., et al.: Foundational Cybersecurity Activities for IoT Device Manufacturers, NISTIR 8259, NIST, 05/2020.
- Dokumenty EU:
  - Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života v elektronických komunikacích, 2017/0003, stanovisko Rady ze dne 10.2.2021.
  - Nařízení EU 2019/881 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (Cybersecurity Act), 17.4.2019.
- Standardy ETSI:
  - Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI EN 303 645, v2.1.1, 06/2020.
- Průmyslové standardy:
  - IoT Security Guidelines. Overview Document, version 2.2, CLP.11, GSM Association, 29.2.2020.

Děkuji za pozornost.

Kontakt:
Petr Matoušek, FIT VUT, Božetěchova 2, Brno
E-mail: matousp@fit.vutbr.cz