Návrh témat bakalářských a diplomových prací pro akademický rok 2019/20

Vedoucí práce: RNDr. Šárka Vavrečková, Ph.D.

Poslední aktualizace: 25. října 2019

Upozornění: téma musí být před vybráním konzultováno s vedoucím práce. Pokud máte vlastní nápad, je nutné s ním přijít co nejdřív.

Tento seznam je v *aktuální elektronické formě* k dispozici na
http://vavreckova.zam.slu.cz/dipl.html dole, včetně historie (témat z předchozích let).

Internet věcí z pohledu kyberbezpečnosti (Internet of Things from the Cybersecurity Perspective)

Rezervováno

Zásady pro vypracování: Autor se ve své práci bude zabývat Internetem věcí (IoT) se zřetelem na možnosti jeho zabezpečení. Popíše a srovná přenosové technologie používané v sítích IoT a při přístupu do těchto sítí (Ethernet, Wi-fi, Zigbee, Z-wave, Sigfox, LoRaWAN, apod.), typické útoky na IoT zařízení, nástroje na jejich detekci a možnou obranu.

Zdroje:

- URBANOVSKÝ, Jozef. Internet of Things (IoT) Security Risks and Threat. Bakalářská práce. Dostupné na: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=181802
- BANAFA, Ahmed. *Secure and Smart Internet of Things (IoT): Using Blockchain and Artificial Intelligence (AI)*. Gistrup, Delft: River Publishers, 2018. ISBN 978-87-7022-029-3. Většina stránek dostupná na: https://books.google.cz/books?id=aNd8DwAAQBAJ&printsec=frontcover
- PATEL, Chintan a Nishant DOSHI. *Internet of Things Security: Challenges, Advances, and Analytics*. Boca Raton: CRC Press, 2018. ISBN 978-0429-84572-7. Většina stránek dostupná na: https://books.google.cz/books?id=IwprDwAAQBAJ&printsec=frontcover
- CHERUVU, Sunil, Anil KUMAR, Ned SMITH a David M. WHEELER. *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*. Apress, 2019. ISBN 978-1-4842-2895-1. Většina stránek dostupná na: https://books.google.cz/books?id=YSKpDwAAQBAJ&printsec=frontcover
- CCNA Cybersecurity Operations Companion Guide. Indianapolis, IN: Pearson Education, Cisco Press, 2018. ISBN 978-1-58713-439-5. Dostupné také z: https://books.google.cz/books?id=FxRbDwAAQBAJ&printsec=frontcover
- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

- PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.
- GORALSKI, Walter. The Illustrated Network: How TCP/IP Works in a Modern Network. 2nd edn. Cambridge, MA: Elsevier, 2017. ISBN 978-0-12-811027-0.

Komentář: Varianty: IoT Cloud, atd.

Kybernetické útoky a jejich detekce (Cyber Attacks and their Detection)

Rezervováno

Zásady pro vypracování: Autor se ve své práci bude zabývat nástroji na detekci kybernetických útoků ve firemní síti. Popíše nejběžnější kybernetické útoky směřující na firemní sítě a dále se bude věnovat nástrojům na detekci těchto útoků (především IDS systémů), s důrazem na open-source nástroje. Vybere si několik těchto nástrojů, charakterizuje, srovná a alespoň jeden podrobně otestuje.

Zdroje:

- CCNA Cybersecurity Operations Companion Guide. Indianapolis, IN: Pearson Education, Cisco Press, 2018. ISBN 978-1-58713-439-5. Dostupné také z: https://books.google.cz/books?id=FxRbDwAAQBAJ&printsec=frontcover
- COOPER, Stephen. 2019 Best Intrusion Detection Systems (10+ IDS Tools Reviewed) [online]. *Comparitech.com* [cit. 2019-10-14]. Dostupné z: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
- SCHILLER, Jon. *Cyber Attacks & Protection: Civilization Depends on Internet & Email*. CreateSpace, 2010, 204 stran. ISBN 978-1453-60913-2. Dostupné také z: https://books.google.cz/books?id=viivLxZ7FxIC&printsec=frontcover
- SOOD, Aditya a Richard ENBODY. Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware. Waltham, USA: Syngress, 2014. ISBN 978-0128-00619-1. Dostupné také z: https://books.google.cz/books?id=hi2SAgAAQBAJ&printsec=frontcover
- KUMAR, Raghvendra, Prasant Kumar PATTNAIK a Priyanka PANDEY. Detecting and Mitigating Robotic Cyber Security Risks. Hershey, PA: IGI Global, [2017]. ISBN 978-152-2521-556. Dostupné také z: https://books.google.cz/books?id=NWtxDgAAQBAJ&printsec=frontcover
- https://www.educba.com/32-most-important-cyber-security-tools/
- https://geekflare.com/cyberattack-simulation-tools/
- https://phoenixnap.com/blog/best-network-security-tools

Komunikace v Internetu věcí (Communication in Internet of Things)

Rezervováno

Zásady pro vypracování: Autor se ve své práci bude zabývat komunikačními protokoly používanými zařízeními Internetu věcí. Nejdřív se zaměří na síťové protokoly pro bezdrátovou komunikaci používané na kratší i delší vzdálenost (například Wi-fi, BT, Zigbee, Z-wave, LoRaWAN, Sigfox) a následně na protokoly umožňující efektivní spolupráci IoT zařízení (například MQTT, Modbus TCP). Jednotlivé protokoly charakterizuje a porovná možnosti jejich využití v rámci dané skupiny.

Zdroje:

- The TCP/IP Guide [online]. [cit. 2019-09-18]. Dostupné z: http://www.tcpipguide.com/
- GORALSKI, Walter. The Illustrated Network: How TCP/IP Works in a Modern Network. 2nd edn. Cambridge, MA: Elsevier, 2017. ISBN 978-0-12-811027-0.
  Část stránek dostupná na: https://books.google.cz/books?id=6nDtNA6VJ5YC&printsec=frontcover

- HASSAN, Qusay F. Internet of Things A to Z: Technologies and Applications. Hoboken, New Jersey: John Wiley, 2018. ISBN 978-1-111-945674-2.
Část stránek dostupná na: https://books.google.cz/books?id=YmpaDwAAQBAJ&printsec=frontcover
- HORACKOVA, Maria. Linkové a síťové protokoly IoT. Praha, 2018. Dostupné také z: https://vskp.vse.cz/73304_linkove_asitove_protokoly_iot. Bakalářská práce. VŠE Praha. Vedoucí práce Felix Espinoza.
- CHAOUCHI, Hakima. The Internet of Things: Connecting Objects. London: Wiley, 2013. ISBN 11-186-0017-7.
- PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-807-2323-883.
- Technologie IoT [online]. IoT portál: brána do světa Internetu věcí [cit. 2019-10-25]. Dostupné na: https://www.iot-portal.cz/technologie/
- https://www.ekonomickymagazin.cz/2018/09/chytre-domacnosti-od-kutilova-domu-na-tlacitko-po-umelou-inteligenci/
- https://www.bydleni.cz/clanek/Jak-je-vnimana-chytra-domacnost
- https://www.root.cz/clanky/protokol-mqtt-komunikacni-standard-pro-iot/
- https://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html
- https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice
- https://www.gfk.com/landing-pages/smart-home-white-paper/
- https://www.rfidjournal.com/smart-home/whitepapers
- https://www.enocean.com/fileadmin/redaktion/enocean_alliance/pdf/Downloads/EnOcean_Alliance_White_Paper_Smart_Home_EN.pdf
- http://upnp.org/resources/whitepapers/UPnP_SmartHome_Whitepaper_2015.pdf
- https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=173800

Aplikace pro zpracování otevřených dat (Application for Open Data Processing)

Zásady pro vypracování: Cílem práce je naprogramovat aplikaci, která bude nějakým smysluplným způsobem využívat otevřená data. Student se v práci bude zabývat otevřenými daty, jejich smyslem, původem, vhodnými formáty pro strojové zpracování, publikací dat. Praktickou částí bude naprogramování aplikace využívající otevřená data publikovaná některou institucí, úřadem či organizací dle vlastního výběru (například ČOI, ČTÚ či některým evropským úřadem).

Zdroje:

- BOČEK, Jan, Jáchym ČEPICKÝ a Jakub MRÁČEK. *Jak otevírat data?* Fond Otakara Motejla, 2014. ISBN 978-80-87725-15-3. Dostupné také z: http://www.otevrenadata.cz/res/data/001/003498.pdf
- http://www.otevrenadata.cz/
- http://opendatahandbook.org/guide/en/what-is-open-data/
- http://www.ctu.cz/otevrena-data/katalog-otevrenych-dat-ctu.html
- http://www.coi.cz/cz/spotrebitel/otevrena-data/

Komentář: Toto téma vyžaduje určitou kreativitu – je třeba vymyslet nějakou smysluplnou možnost uplatnění otevřených dat. S aplikací se můžete zúčastnit některého ročníku soutěže

o nejlepší aplikaci nad otevřenými daty (http://www.otevrenadata.cz/soutez/). Každoročně se přihlásí cca 20 aplikací, tedy je celkem dobrá šance na výhru, zvláštní cena je i pro studenty.

Naprogramování modulu pro některý open-source program.

Praktickou částí práce bude naprogramování modulu pro open-source program dle vlastního výběru (Firefox, Gimp, Inkscape, OpenOffice.org, ...). V teoretické části práce autor stručně popíše princip otevřeného kódu, program, který si vybral, možnosti jeho rozšíření a dále samotný postup pro vybraný modul.

Zdroje:

- internetové stránky vybraného programu
- diskusní fóra a další stránky s informacemi programátorů (na http://google.com zadat s názvem daného programu klíčové slovo module, programming apod.)

Témata ve spolupráci se společností Red Hat

Komentář: Je možné vybírat si témata z webu https://research.redhat.com/thesis/. Informace jsou také na https://mojefedora.cz/diplomky/.

Další okruhy pro individuálně domlouvaná témata – je třeba konkretizovat:

- nástroje pro detekci útoků, metodika Cyber Kill Chain (identifikace a prevence útoků), atd.
- bezpečnost a anonymizace toku dat
- témata z oblasti operačních systémů, jádro Linuxu, bezpečnost, hardware, sítě
- LaTeX – export do/z (převod formátů), apod.
- konkrétní témata z praxe