Cyber Security Early Career Professionals monthly webinar and networking series

Organised by Information Security Specialist Group (BCS-ISSG)
Consist of career stories and presentations/workshops delivered by Cyber Security Early Career Professionals from around the world. The event is open for all.

July 2021 talk: Challenges of Machine Learning in Production

Speaker: Jelena Milosevic, Data Scientist, Mondi Group

Agenda:

15:00 - Introductions & Networking

15.10 - Presentation & Discussion

16:00 – Close of event

Moderators: Deepthi Ratnayake, Marie Setterfield

Challenges of Machine Learning in Production

Jelena Milosevic, PhD

Data Scientist @ Mondi Group

Outline

- About Me
- My Journey
- Technical Part – Challenges of Machine Learning in Production

About me

- Currently
  - Data Scientist @Mondi
- Previously
  - Postdoc & Project Assistant @TU Wien, Vienna, Austria
  - PhD in Informatics @ USI-Lugano, Switzerland
  - Research Internship at
    - IBM Israel
    - Intel Ireland
  - MsC and BsC Electrical and Computer Engineering @ University of Novi Sad, Serbia

My Journey

- **Malware detection**
  [C&S-19, FPS-18, DASC-16, SECRYPT-16, CCNC-16, IWSMA-14]
- **Face recognition** [arxiv-18]
  Anomaly detection [IJCNN-18]
  Failure prediction [CINC-14]

- **Attacks against ML**
- **Robust defences** [FSS-18]
- **Explainable ML**

Application Domains

Mobile systems [C&S-19, FPS-18, HST-17, DASC-16, SECRYPT-16, CCNC-16, IWSMA-14]
Embedded systems [IJCNN-18, arxiv-18, CINC-14,SECRYPT-14,SECRYPT-13]
Communication Networks [FSS-18, JISA-20]

Publications

- Iglesias, F.**, Milosevic, J.,** Zseby, T., 'Fuzzy classification boundaries against adversarial network attacks', Fuzzy Sets and Systems, Elsevier, 2019
- **Milosevic, J.**, Malek, M., Ferrante, A., 'Time, accuracy and power consumption tradeoff in mobile malware detection systems', Computers & Security, Elsevier, 2019
- Wahab, M., **Milosevic, J.**, Regazzoni, F., Ferrante, A., 'Power & performance optimized hardware classifiers for efficient on-device malware detection', Sixth Workshop on Cryptography and Security in Computing Systems, ACM, 2019
- Bianchi, F., Livi, L., Ferrante, A., **Milosevic, J.**, Malek, M., 'Time series kernel similarities for predicting Paroxysmal Atrial Fibrillation from ECGs', International Joint Conference on Neural Networks (IJCNN), IEEE, 2018

Publications

- **Milosevic, J.**, Regazzoni F., Malek M. 'Malware Threats and Solutions for Trustworthy Mobile Systems Design', Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment, Springer, 2017
- **Milosevic, J**., Malek, M, Ferrante, A. 'Runtime Classification of Mobile Malware for Resource-Constrained Devices', Lecture Notes in Communications in Computer and Information Science, Springer, 2017
- Ferrante A., Malek M., Martinelli F., Mercaldo F., **Milosevic J.**, 'Extinguishing Ransomware – A Hybrid Approach to Android Ransomware Detection', The 10th International Conference on Foundations & Practice of Security, 2017
- **Milosevic, J.,** Ferrante A., Malek M. 'Trojan Families Identification Using Dynamic Features and Low Complexity Classifiers', The 24th EICAR Annual Conference on Trustworthiness in IT Security Products EICAR-2016

Publications

- **Milosevic, J.**, Ferrante A., Malek M. 'MalAware: Effective and Efficient Runtime Mobile Malware Detector', The 14th IEEE International Conference on Dependable, Autonomous and Secure Computing DASC-2016
- **Milosevic, J.**, Malek M., Ferrante A. 'A Friend or a Foe? Detecting Malware Using Memory and CPU Features', The 13th International Conference on Security and Cryptography SECRYPT-2016
- **Milosevic, J**., Ferrante A., Malek M. 'What Does the Memory Say? Towards the Most Indicative Features For Efficient Malware Detection', The 13th Annual IEEE Consumer Communications and Networking Conference CCNC-2016
- Ferrante A., Medvet E., Mercaldo F., **Milosevic J**., Visaggio C.A. 'Spotting the Malicious Moment: Characterizing Malware behavior Using Dynamic Features', The Fifth International Workshop on Security of Mobile Applications IWSMA-2016

Publications

- **Milosevic, J.**, Ferrante A., Malek M. 'AndTrojanID: Android Trojans Detection Using Dynamic Features', Workshop on Trustworthy Manufacturing and Utilization of Secure Devices-Collocated with DATE Conference Trudevice-2016
- **Milosevic, J.**, Dittrich A., Ferrante A., Malek M., 'A Resource-optimized Approach to Efficient Early Detection of Mobile Malware', 3rd International Workshop on Security of Mobile Applications IWSMA-2014
- **Milosevic, J.**, Ferrante A., Regazzoni F. 'Security Challenges For Hardware Designers Of Mobile Systems', First Workshop On Mobile Systems Technologies MST-2015
- **Milosevic, J.**, Ferrante A., Malek M. 'Can we Achieve both Privacy Protection and Efficient Malware Detection on Smartphones?', First Interdisciplinary Cyber Research Workshop ICR-2015
- **Milosevic, J.**, Ferrante A., Malek M. 'Poster: A General Practitioner or a Specialist forYour Infected Smartphone?', IEEE Symposium on Security and Privacy S&P-2015, San Jose, CA, USA

Technical Part

Challenges of Machine Learning in Production

About Machine Learning

- Great tool
  - Entered and changed almost every area of our life
  - Used to analyze large amount of data and create insights
  - Already goes above human performance in some specific domains
- At the same time
  - Not a silver bullet
  - Has its own challenges and unique problems
  - Should be used only if really needed

Cross Industry Standard Process for Data Mining - CRISP DM

Image source: https://uwsdatamining.files.wordpress.com/2013/10/crisp-dm_process_diagram.png

Cross Industry Standard Process for Data Mining - CRISP DM

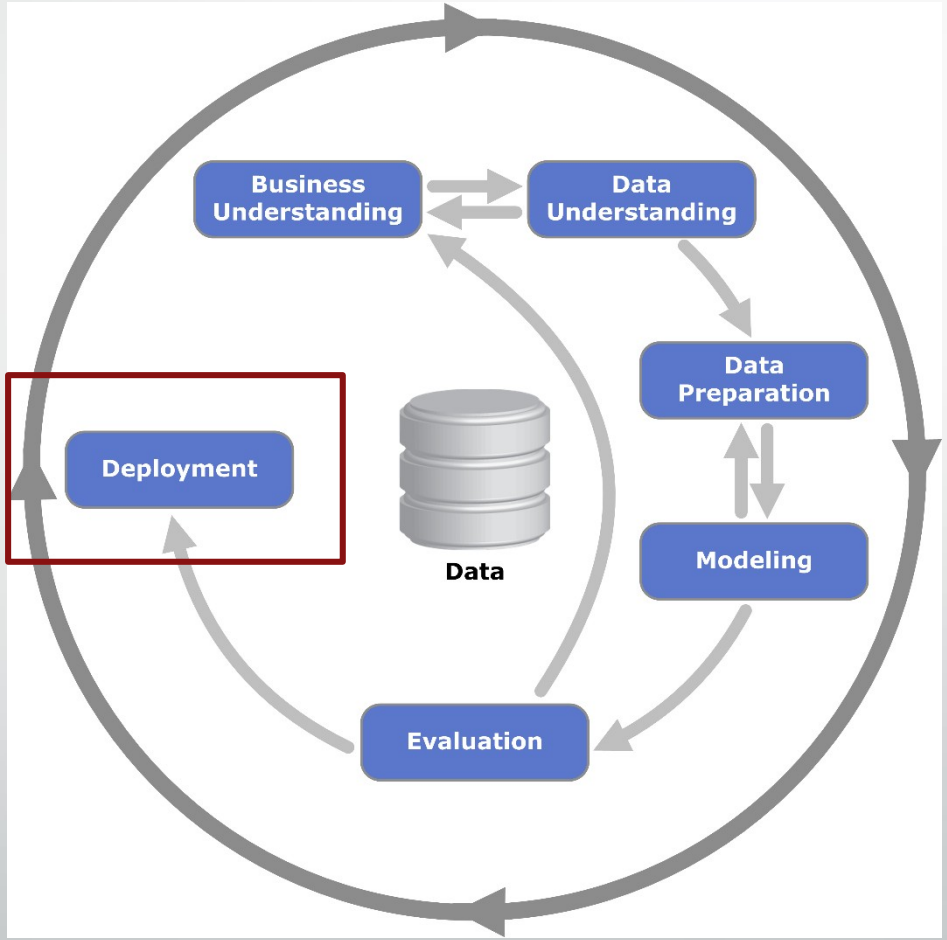
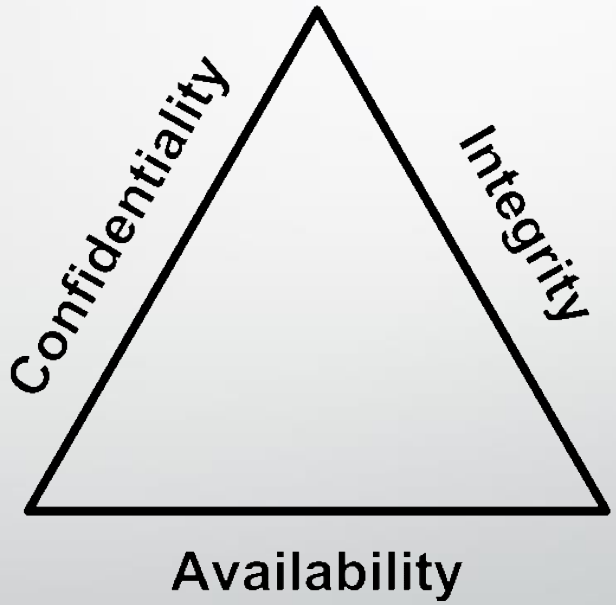


Image source: https://uwsdatamining.files.wordpress.com/2013/10/crisp-dm_process_diagram.png

Secure Deployment of Machine Learning

- Why is it a challenge?

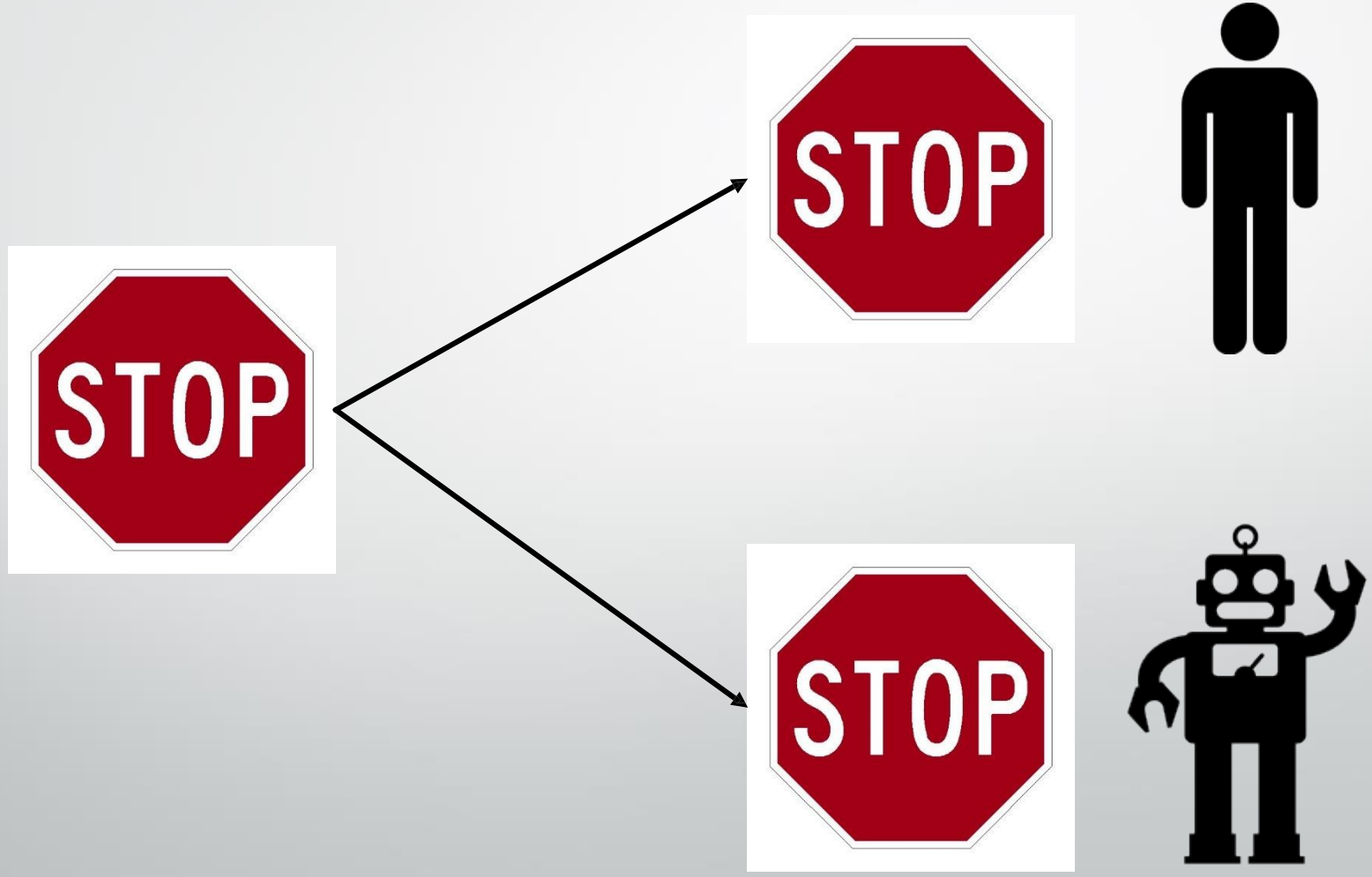
Main Security Aspects: CIA Triad



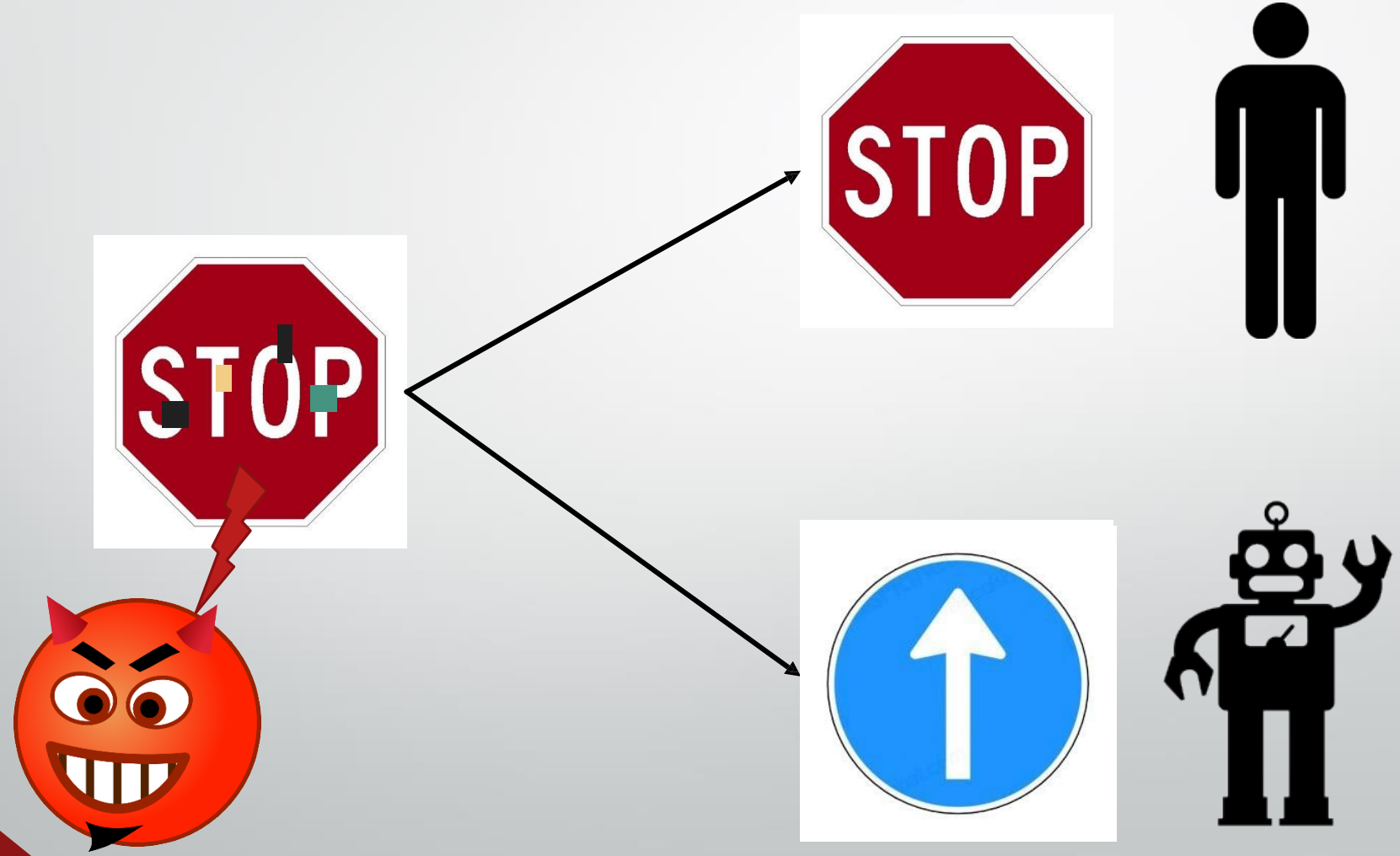
What Can Go Wrong with Machine Learning?

	Confidentiality	**I**ntegrity	**A**vailability
Deployment	Model stealing Model inversion Membership inference attack	Evasion	Increasing false positives

Evasion Attacks



Evasion Attacks



Some Defenses

- Ensemble
- Adversarial retraining
- Defensive distillation
- Dimensionality reduction
- Regularization
- Using fuzzy boundaries and membership score as a feature

Concept Drift

- Data changes over time
- Why is it a challenge?
  - Performance of ML degrades, sometimes slowly sometimes abruptly
- Some solutions to the problem
  - Occasional retraining
  - Statistical testing on changes in distributions
  - Ensemble of models
  - Monitoring performance is the key

Reusing Trained Models

- Desired property to "quickly" reuse ML model from scenario A in scenario B
- Why is it a challenge?
  - Success depends on type of tasks and amount of data
  - Not always clear if full retraining is a better option
- Some solutions
  - Transfer learning in NLP and Computer vision

Explainability

- The most accurate models are usually least explainable
  - It creates lack of trust
  - It can be the cause of bias and unfairness
  - It can make random associations
- Solutions
  - LIMO
  - Sharpley values

Some Resources

- Papers
  - https://papers.nips.cc/paper/2015/file/86df7dcfd896fcaf2674f757a2463eba-Paper.pdf
  - https://thodrek.github.io/CS839_spring18/papers/p1723-polyzotis.pdf
- Blogs
  - https://towardsdatascience.com/challenges-deploying-machine-learning-models-to-production-ded3f9009cb3
  - https://cloudxlab.com/blog/deploying-machine-learning-model-in-production/
- Books
  - MarkTreveil & the Dataiku team: How to scale Machine learning in the Enterprise
  - Geoff Hulten: Building intelligent systems

Q&A

Email: jelena@milosevic.cc

Linkedin: https://www.linkedin.com/in/milosevicjelena/

Twitter: @DrMrLena

Cyber Security Early Career Professionals monthly webinar and networking series

If you are an inspiring early career professional in Cyber Security and you would like to share your knowledge and exciting career journey story through this webinar series, please get in touch with

Dr. Deepthi Ratnayake (d.ratnayake@herts.ac.uk)

Early career professionals can be, but are not limited to graduates, and apprentices or those who have changed careers.

Cyber Security Early Career Professionals monthly webinar and networking series

Organised by Information Security Specialist Group (BCS-ISSG)
Consist of career stories and presentations/workshops delivered by Cyber Security Early Career Professionals from around the world. The event is open for all.

August 2021 talk: Cyber Security beyond classical IT

https://www.eventbrite.co.uk/e/early-career-webinar-cyber-security-beyond-classical-it-bcs-issg-tickets-160783001285

Speaker: Nacho Fernandez, Cyber Risk Manager, Lloyds Banking Group

Date and time: Fri, 6 August 2021 15:00 – 16:00 BST

Agenda:

15:00 - Introductions & Networking
15.15 - Main topic
- Academic and Professional Background
- The Case of Cyber Security in Automotive Sector
- Cyber Security experience in Banking Sector

16:00 - Close of event