Education Materials

Akond Rahman – Tennessee Tech

* How students perceive about exercises on secure software development:

<https://akondrahman.github.io/files/papers/fie2021.pdf>

<https://akondrahman.github.io/files/papers/quatic2021.pdf>

* Use of authentic learning to teach secure development of Ansible scripts:

<https://akondrahman.github.io/files/papers/iticse2022.pdf> 

* My course website on secure software development:

<https://github.com/paser-group/continuous-secsoft> 

* Docker image that contains all exercises:

<https://hub.docker.com/repository/docker/akondrahman/sec-soft-edu-materials>

Jim Whitmore – Dickinson College

* Concepts and Tools for Security Analysis:

<https://jjwhitmore.github.io/SE-workbench/>

* Curriculum outline:

<https://www.nist.gov/system/files/documents/2020/01/30/031_NICE%20Framework%20Request%20for%20Comments_508.pdf>

* My faculty page: <https://users.dickinson.edu/~whitmorj/>

Arash Habibi Lashkari – York University

Dr. Arash Habibi Lashkari is an Associate Professor at York University and a senior IEEE member in Canada. His journey in using CAPEC, CVE, and CWE started in 2009 when he was a graduate student working on designing and developing a new [Graphical User Authentication (GUA)](https://www.amazon.ca/Graphical-User-Authentication-GUA-Algorithms/dp/3843380724) model to improve the authentication process. Since 2016, he has used CAPEC, CVE, and CWE as the standard references for all facets of course delivery, including course materials, student activities, graded assignments, and final projects on his Network Security, Digital Forensics, and Security Risk Management courses. Along with course delivery, his research teams have generated and released [sixteen cybersecurity datasets](http://ahlashkari.com/Datasets.asp) and [six cybersecurity open-source projects](https://github.com/ahlashkari) using CAPEC as the standard for creating attack scenarios to mimic the behaviour of attackers and CVE as the standard to define the target points for executing attacks and malware families in all datasets. With regard to open-source projects, to detect and prevent malicious activities, these teams have focused on extracting features which have been defined and formulated by CAPEC for threat analysis. In 2020, he and his colleagues [patented a new idea](https://patents.google.com/patent/US20200244693A1/en?oq=US+2020/0244693+A1) for determining the security risk associated with one or more users of a computer network based on the CAPEC standard for threat events and the CVE standard for asset vulnerability. In this patent, users are monitored over time to build security related profiles which are employed to assess the risk they impose on the network. To calculate the risk, they proposed a new formula *T°I≡Σ* i=1 n *t* i(Σj=1 m *CV* ij+Σk=1 P *VB* ik)+Ii, where ti is a threat event (CAPEC standard) and CVij is the asset's vulnerability (CVE standard).

For more information see <http://ahlashkari.com/>

Suzanna Schmeelk – St. John’s University

* Schmeelk, S. (2020) Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology. Proceedings of the 53rd Hawaii International Conference on System Sciences <http://hdl.handle.net/10125/64216>​
* S. E. Schmeelk, D. M. Dragos and J. E. DeBello, "ABET Cybersecurity Continual Course Improvements for Secure Software Development," 2021 IEEE Frontiers in Education Conference (FIE), 2021, pp. 1-6, doi: 10.1109/FIE49875.2021.9637296.​
* Suzanna Schmeelk, Junfeng Yang, and Alfred Aho. 2015. Android Malware Static Analysis Techniques. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR '15). Association for Computing Machinery, New York, NY, USA, Article 5, 1–8. DOI:https://doi.org/10.1145/2746266.2746271
* St. John’s University. Masters in Science in Cyber and Information Security https://www.stjohns.edu/academics/programs/ms-cyber-and-information-security ​

Drew Buttner and Larry Shields – MITRE

<https://opensecuritytraining.info/IntroSecureCoding.htm>