Cyber-Security Threats and Threat Actors Training

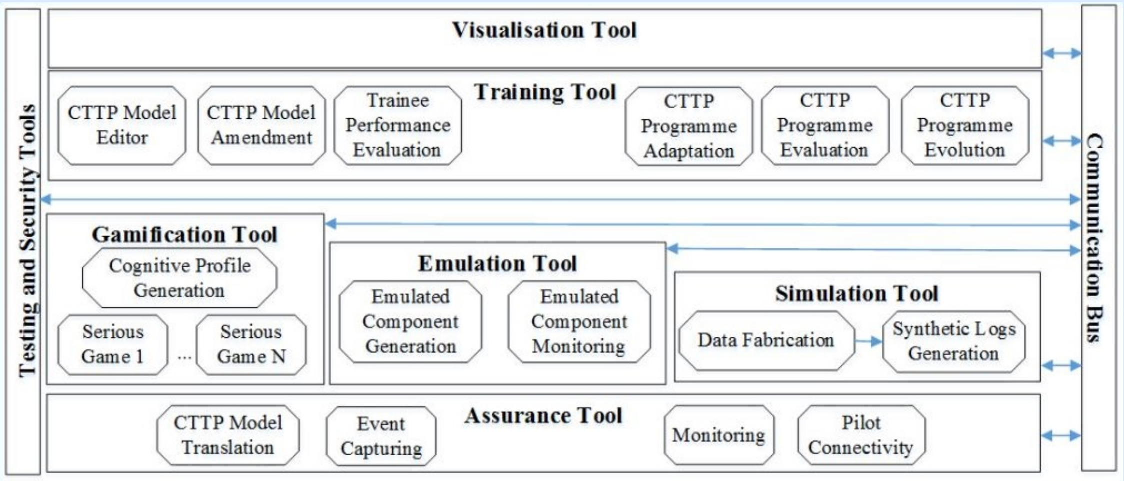
Assurance Driven Multi-Layer,

end-to-end Simulation and Training

MAY 2019 – ISSUE 2

Newsletter

Progress



The THREAT-ARREST platform

CTTP models/programmes creation: Definition/refinement of Cyber Threat and Training Preparation (CTTP) language requirements, for each of the different sub-models (Core Assurance, PAL, SAL, Deployment, Simulation/Emulation, CTTP Training programme). Definition/ refinement of areas of focus and scope of the training programs. Expansion of cyber system model (CSM) to cover physical, hardware and software parts of the cyber system, as well as information regarding their deployment. Addition of elements of the Assurance Model as part of the main CSM, depicting the relationship between threats, assets, vulnerabilities and the associated risk, as well as the controls that may be used to mitigate said risk. Development of parts of the Training, Simulation and Emulation sub-models, considering the training scenarios that will have to be covered, as well as the involved simulated and emulated assets. Initial sketching of an elementary training scenario featuring an email phishing attack, and how this scenario would be implemented and carried out within the THREAT-ARREST platform. Production of a first draft of the CSM (including SAL, PAL, and Deployment sub-models).

Emulation tool: Definition of the emulation tool, its architecture and its interfaces with the rest of the platform. Definition of its requirements. Decomposition into sub-components and modules: (a) Emulation Compiler - translation of the CTTP Emulation sub-model in actual configurations, (b) Emulation Engine - application of configurations on target architecture, (c) Emulation Repository – storage for images of generic operating systems, pilots nodes and specific simulation machines to instantiate in order to deploy the emulation environment. Deployment of a simple infrastructure on the platform based on XML–type configuration derived from the CTTP Emulation sub-model. Simple network setup by (a) based on the network connection specified in the provided configuration.

In this issue:

Training and Visualization tools: Specification of the overall architecture and identification of an initial set of components/elements to be supported. Partners coordination regarding the integration of serious games into the THREAT ARREST platform. Initial analysis on the tools' communications and data flow, the data formats and the need for secure communications. Development of the first architectural concepts for visualization. Definition of possible threat scenarios of the pilot users. Development of the technical design and implementation of visualization and simulation including the integration of the training platform. Refinement of communications and data flow between the Assurance tool and the Simulation and Emulation tools. Introduction of a new component, Dashboard, to integrate in a unified and user-friendly way the various functional and management interfaces envisaged in the platform. Agreement on several requirements and features of the Communication Bus component. Refinement and integration of the Identity & Access Management component. Agreement on stronger integration of the Gamification tool in the platform: (a) how to enable finer-grained configuration of the serious games and use them for non-social-engineering attacks training, (b) how to use the CTTP models as input to such games' configuration and the need to provide additional configuration details with respect to trainees' performance/profile, (c) how to enable the Gamification tool provide results on the trainee's progress during a serious game round and not only at the end of the game with the overall results. Clarification of the training and visualization components' structure. Initial discussions on the integration of synthetic and real event logs to be used by the simulation.

Simulation Environment: Identification of several communication aspects, (e.g., publish/subscribe mechanisms for selective and asynchronous data communication). Research on existing solutions of network security simulations. Definition and creation of the concept and high-level architecture of the technology for synthetic security events fabrication. Further detailed discussions on the usage of a message broker for asynchronous communication and the integration between the emulation and simulation components. Development of an initial version of the CTTP sub-model for instantiating a simulated scenario. Initial design and implementation of the real event logs statistical profiling module. Interconnection of the Data Fabrication Platform with the with Assurance, Training, Gamification and Emulation modules. Provision of details about the architecture of the simulation components, especially on how to integrate them with the visualization components. Definition of the simulated components and their desired behaviour needed for pilot scenarios.

Legal framework: Continued definition of the basic legal and security requirements of the platform and analysis of the entire project's requirements focusing on the privacy and security aspects.

Publicity

- Submission and acceptance of a proposal for the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC) workshop in conjunction with the ESORICS 2019 conference
- Dissemination of the workshop at several platforms (Facebook, LinkedIn, Twitter, HiPEAC community)
- A series of articles on the legal and ethical issues and opportunities of Big Data, in particular cybersecurity and data breaches, posted on several platforms (link 1, link 2, link 3) (Bird & Bird)
- Presentation on the EU Data Economy: "Data Law – Why It Matters to Business" at Vesalius College (Bird & Bird)
- Talk on "Data Breaches at the Crossroads of Privacy, Fintech and Corporate Law" at Data Law Camp: Construire un droit des données, Designing Data Law (Benoit Van Asbroek, Julien Debussche, Jasmien César – Bird & Bird)

Publications

F. Marcantoni, M. Diamantaris, S. Ioannidis, J. Polakis, **"A Large-scale Study on the Risks of the HTML5 WebAPI for Mobile Sensor-based Attacks"** in The World Wide Web (WWW'18) Conference, May 2019

G. Hatzivasilis, O. Soultatos, P. Chatziadam, K. Fysarakis, I. Askoxylakis, S. Ioannidis, G. Alexandris, V. Katos, G. Spanoudakis, **"WARDOG: Awareness detection watchdog for Botnet infection on the host device"** in IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, May 2019

G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. I. Tsatsoulis, **"Review of Security and Privacy for the Internet of Medical Things (IoMT)"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

G. Hatzivasilis, N. Christodoulakis, C. Tzagkarakis, S. Ioannidis, K. Fysarakis, G. Demetriou, M. Panayiotou, **"The CE-IoT Framework for Green ICT Organizations"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

Follow us