Cyber-Security Threats and Threat Actors Training
Assurance Driven Multi-Layer,
end-to-end Simulation and Training

SEPTEMBER 2019 – ISSUE 3

Newsletter

Progress

CTTP models/programmes creation: Adaptation and further development of the security assurance model, following internal feedback – UML Class Diagram, description of its objects. Focus mainly on the Cyber Range (CR) sub-model of the assurance model, including the Training, Simulation and Emulation sub-models. Description and illustration of one simple and one more complex phishing scenario based on the CR sub-model. Description of several smart home related scenarios covering various threats in such environments (device compromise, misconfiguration, internet exposure, etc.). Modelling of scenarios via the CR sub-model. Further development of the training scenarios defined for the maritime and healthcare use-cases.

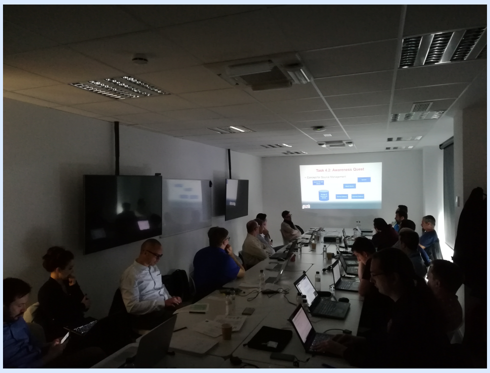
Emulation tool: Development of the Emulation Tool components. Presentation of a prototype and a first demo of the tool. XML configuration file based on the CTTP emulation concepts, containing the description of the emulated architecture, as input for the Emulation Controller REST interface and deployment of the emulated architecture as well as setup of the SSH connections with the user and each virtual machine. Discussions concerning the tools' interconnection. Work on the correlation of the CTTP sub-models for deploying emulated components. Work on the inter-platform communication of the various modules through the RabbitMQ broker.

Training and Visualization tools: Further work on the design of the training tool, focusing on the structure of the Dashboard. Aggregation of technologies used in other modules, ensuring proper communication with the Dashboard and all the pilot-specific requirements for the Dashboard's functionalities. Update and finalizing of the sequence diagram for the training tool, depicting all activities (actors, classes and message exchanges) and describing all communications with the rest of the tools. Further development of the first version of the visualization module. Improvement of the gameplay for the gaming tool PROTECT. Evolving of the communications and data flow between the Training and Visualization Tools and the rest of the platform's tools.

Simulation Environment: Further discussions detailing the integration of simulation, the Data Fabrication Platform and the statistical analysis tool into the overall THREAT-ARREST platform architecture. Usage of a message broker for the asynchronous communication and integration between the emulation and simulation components. Implementation of an initial set of simulation components required for the pilots. Development of the first version of the simulated components and their connection to the first prototype of the visualization component. Further development of the module for statistical profiling of real event logs. Specification of the REST API for integrating the Data Fabrication Platform in the overall THREAT-ARREST system architecture.

Plenary meeting

The 2nd THREAT-ARREST plenary meeting was successfully held on April 10th, 2019 at the premises of ATOS in Barcelona, Spain



In this issue:

Publicity

✔ Organization of ENISA's summer school - Serious Games training session - Participation and support by consortium partners - Presentation of the project's video - Presentation of the project's poster - Flyer handout

✔ Talk hosted by Julien Debussche, Jasmien César, Simon Mortier, Alexandra Voinescu (Bird & Bird), at a company seminar, on "Dealing with data breaches: best practices", in June 2019

✔ Poster presentation at the 2nd Summer School on Industry Digital Evolution "Beyond Transformation: Evolving the Digital Enterprise" (Carovigno, Italy), in July 2019, by UMIL

✔ Talk hosted by Lara Mauri (UMIL), at the 2nd Summer School on Industry Digital Evolution, presenting the THREAT-ARREST project, in July 2019

✔ Talk hosted by George Hatzivasilis (FORTH), at the training session on business and technical personnel of the Cypriot Internet provider CABLENET, on cyber-security training for critical infrastructure owners, in August 2019

✔ Keynote talk by Prof. Vassilis Prevelakis (TUBS), at the 1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), on Cybersecurity for the Protection of Critical Infrastructures, in September 2019

Publications

G. Hatzivasilis, P. Chatziadam, N. E. Petroulakis, M. Mangini, C. Kloukinas, A. Yautsiukhin, M. Antoniou, D. G. Katehakis, M. Panayiotou, **"Cyber Insurance of Information Systems"** at the 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), September 2019

G. Hatzivasilis, P. Chatziadam, A. Miaoudakis, E. Lakka, A. Alessio, M. Smyrlis, G. Spanoudakis, A. Yautsiukhin, M. Antoniou, N. Stathiakis, **"Towards the Insurance of Healthcare Systems"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

O. Soultatos, K. Fysarakis, G. Spanoudakis, H. Koshutanski, E. Damiani, K. Beckers, D. Wortmann, G. Bravos, M. Ioannidis, **"The TREAT-ARREST Cyber-Security Training Platform"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

L. Goeke, A. Quintanar, K. Beckers, S. Pape, **"PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

I. Somarakis, M. Smyrlis, K. Fysarakis, G. Spanoudakis, **"Model-driven Cyber Range Training – The Cyber Security Assurance Perspective"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, L. Mauri, **"A model driven approach for cyber security scenarios deployment"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Vassilis Prevelakis, Mohammad Hamad, Jihane Najar and Ilias Spais, **"Secure Data Exchange for Computationally Constrained Devices"** at the International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), September 2019

Manolis Chatzimpyrros, Konstantinos Solomos and Sotiris Ioannidis, **"You Shall Not Register! Detecting Privacy Leaks across Registration Forms"** at the International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), September 2019

Follow us