CYBERSECURITY AUTOMATION VIDEO DEMONSTRATION

Duncan Sparrell, CISSP, CSSLP, CCSK, Senior Member IEEE; sFractal Consulting

EXTENDED ABSTRACT

Cybersecurity has safety implications in the Fourth Industrial Revolution [1,2]. To best thwart cyber-attacks, Industry 4.0 must respond at machine speed, which requires automation [3]. On 28-October-2020, various organizations met virtually for a cybersecurity automation mashup of meetups [4] combining a plugfest with a hackathon with a proof-of-concept to demonstrate use cases showing the value of automated defense. There were over 40 participants from 7 countries on 5 continents, with representation from government, academia, and industry.

The focus was on the comply-to-connect use case; i.e. don't allow access unless the connecting device is in compliance with enterprise policies. A software bill of materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software [5] , and is crucial to the use case. OASIS open command & control (OpenC2) is a standardized language for the command and control of technologies that provide or support cyber defenses [6-10]. OpenC2 was demonstrated to obtain SBOMs and to control security devices based on the analysis of the SBOMs. CACAO playbooks [11] were used in the workshop to describe scenarios. Applicability to the Open Cybersecurity Alliance [12], Integrated Adaptive Cyber Defense [13], and Secure Content Automation Protocol [14] was demonstrated.

The workshop was a success. The workshop proved the concept of comply-to-connect, proved that SBOMs can be created, and that SBOMs can be analyzed for use in the comply-to-connect use case. Interworking was demonstrated in the plugfest portion of the workshop between many organizations and between ecosystems. The hackathon was a success with new software created [10] and existing software enhanced, including live coding at the workshop. Keynotes by senior government and industry officials highlighted the need for automation for speed and scale, the value of SBOMs, the value of open standards, and the tremendous accomplishments demonstrated at the workshop.

More work is still needed in cybersecurity automation - in research, in standards, in technology, and showing the business value. The next workshop will be in February 2021.

REFERENCES

[1] H. P. Breivold and K. Sandstrom, "Internet of Things for Industrial Automation -- Challenges and Technical Solutions," in 2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS), Sydney, Australia, 2016, pp. 532-539.

[2] D.K. Sparrell, "Cyber-safety in healthcare IoT", Proceedings of ITU Kaleidoscope 2019: ICT for Health: Networks, standards and innovation; pp 163-179.

[3] D.K. Sparrell, "IoTsm Response at Cyberspeed to Attack", Sep 6, 2018; Proceedings of the International Conference on Industrial Internet of Things and Smart Manufacturing.

[4] TDD-Plugfest-Hackathon, https://github.com/oasis-tcs/openc2-usecases/tree/master/TTD-PlugfestHackathon

[5] "Software Bill of Materials", https://www.ntia.gov/sbom

[6] "OpenC2", https://openc2.org/

[7] "Open Command and Control (OpenC2) Language Specification Version 1.0", https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs02/oc2ls-v1.0-cs02.html

[8] "Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0", https://docs.oasis-open.org/openc2/oc2slpf/v1.0/cs01/oc2slpf-v1.0-cs01.html

[9] "Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0", https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html

[10] "OpenC2 DXL Python Client Library", https://github.com/opendxl/opendxl-openc2-client-python

[11] "OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC", https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao#technical

[12] "Open Cybersecurity Alliance", https://opencybersecurityalliance.org/

[13] "Integrated Adaptive Cyber Defense", https://www.iacdautomate.org/

[14] "Security Content Automation Protocol Version 2 (SCAPv2)", https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol-v2