Workshop: CRATE as a national research infrastructure

As SWITS attendees might know, FOI operates a cyber range called CRATE. CRATE has primarily been built and financed by MSB for the purpose of hosting cyber security exercises and courses. However, in recent years, CRATE has also been used for research related to IT-security. This includes studies of vulnerability assessment methods (e.g., [1]-[3]) and research on intrusion detection (e.g., [4]-[5]). FOI believes that CRATE has an untapped potential of supporting non-FOI researchers, and research on other topics than these. The Swedish Research Council (Vetenskapsrådet) also see this potential and has provided funds so that FOI can investigate the demand for a cyber range like CRATE in the Swedish IT-security research community. If there is a strong support from the research community, CRATE may be appointed to be a national research infrastructure, with the Swedish Research Council providing financial support that makes CRATE available to researchers in Sweden.

In this workshop, the current capabilities of CRATE will be presented together with some ideas on how CRATE can be developed to offer better support to external researchers. Based on this, FOI will try to elicit opinions, thoughts and direct requirements from the attendees.

[1] H. Holm, T. Sommestad, J. Almroth, and M. Persson, “A Quantitative Evaluation of Vulnerability Scanning.” *Information Management & Computer Security*, vol. 19, no. 4, pp. 231–247, 2011.

[2] H. Holm, M. Ekstedt, and D. Andersson, “Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 825–837, Nov. 2012.

[3] Sommestad, T. & Sandström, F., An empirical test of the accuracy of an attack graph analysis tool. Information & Computer Security, in press.

[4] T. Sommestad and A. Hunstad, “Intrusion detection and the role of the system administrator,” *Information Management & Computer Security*, vol. 21, no. 1, pp. 30-40, 2013.

[5] T. Sommestad and U. Franke, ”A test of intrusion alert filtering based on network information,” Security and Communication Networks, in press