Barriers to Automated Threat Intelligence Sharing

Eric Burger
Georgetown University
eric.burger@georgetown.edu

The Security and Software Engineering Research Center (S^2ERC)[1] is an NSF- and industry-sponsored center that conducts a program of applied and basic research on software security, system security and software technology problems of interest to its members. The goal of this research is to enable security and software technology gains.

The Georgetown site of the S^2ERC[2] hosts the Cyber Threat Intelligence Information Sharing Exchange Ecosystem Program (CyberISE).[3] The CyberISE program has the goal of enhancing the world's network security posture through the accelerated adoption of automated threat intelligence sharing.

Completed projects in the CyberISE program include three economic studies. As the IETF's Richard Shockey would say, "Money is the answer, what is the question?" With that inspiration, we addressed the financial issues inhibiting automated threat exchange. The first examined the cyber information sharing experiences of the financial services sector in the United States.[4] The second analyzed proposed incentives being considered by the United State government to get critical infrastructure entities to adopt threat-sharing practices.[5] The final report reviewed various models for the return on investment for cyber security programs.[6]

Two companion projects in the CyberISE program examine legal barriers to intelligence sharing. Our focus has been on enterprise-to-enterprise sharing. That is, we are focusing on private sector or non-governmental organization sharing. The first of the companion projects examined the statutes, regulations, and common law around information sharing in the United States. This project was completed in March 2015. The second project is about to start. It will examine the statutes, regulations, common law, and international norms relating to multi-national, private information sharing. As an example of an issue of importance to the information sharing community is the status of an IP address. In the United States, there is no statute defining whether an IP address is personally identifiable information. However, there is case law that decided (for the Southern District of Illinois) that an IP address is not personally identifiable information. Contrast this to Germany, where there is statute defining an IP address as personally identifiable information. The impact is the regulatory regime in the United States is quite different than the regulatory regime in Germany, which impacts what data a multi-national information sharing exchange can trade, as well as limitations and expectations that may attach to that data. As well, we are assisting with the development of new laws in the United States to remove some of the legal and policy barriers to sharing.

Another completed project at in the CyberISE program created a taxonomy model for cyber threat intelligence exchange technologies.[7] There was a need for a meta-description of the various automated exchange technologies, such as OpenIOC, IODEF, and STIX. We presented this work at the Workshop on Information Sharing and Collaborative Security just a few months ago.[8]

For the CARIS Workshop, we would like to discuss our initial results examining a meta-ontology of cyber threat elements. In any information exchange, having a generally agreed ontology is critical to understanding what the exchanged information means. This is more especially so if we expect machines, not people, to understand the information. By the time of the Workshop, we expect to be able to present our mapping between the major threat exchange standards.

Given the expected audience at the CARIS Workshop, we would prefer not to give a dry lecture on results you could just as easily read. Rather, our purpose for participating is to build a dialog amongst the users of automated threat exchange (the CSIRTs), the major consumers and the first line of defense (the ISPs and security operators), as well as with other researchers in the space. The results of the discussion will have direct relevance on standards activities, as interoperability between different ontology sets will become increasingly important as the penetration of automated threat exchange increases.

[1] https://www.serc.net
[2] https://s2erc.georgetown.edu
[3] https://s2erc.georgetown.edu/projects/cyberISE
[4] https://s2erc.georgetown.edu/sites/s2erc/files/FS Incentives.pdf
[5] https://s2erc.georgetown.edu/sites/s2erc/files/Analysis of Incentives_0.pdf
[6] https://georgetown.box.com/s/i2uhqepbxvmhy3r6zuye
[7] https://georgetown.box.com/s/cfap21dxmsgr4k9hnipu
[8] https://dl.acm.org/citation.cfm?id=2663883