# Secure Multiparty Computation for Cooperative Cyber Risk Assessment

Kyle Hogan, Noah Luther, Nabil Schear, Emily Shen, Sophia Yakoubov, Arkady Yerukhimovich
MIT Lincoln Laboratory
Lexington, MA
Emails: {kyle.hogan, noah.luther, nabil, emily.shen, sophia.yakoubov, arkady}@ll.mit.edu

## ABSTRACT

A common problem organizations face is determining which security updates to perform and patches to apply to minimize the risk of potential vulnerabilities in their infrastructure. Limited budgets and resources constrain organizations to select a set of the most security critical updates that they can afford to perform; thus, it is very important for vulnerability risks to be computed accurately [5]. The accuracy of these risk assessments improves with the scope of data available; the more attacks that are represented in the dataset the easier it will be to determine which vulnerabilities are most likely to be exploited and how much damage an exploit is likely to cause [4].

In particular, organizations can improve the accuracy of their cyber risk assessments by pooling their data, as a dataset that covers the infrastructure of multiple institutions would allow each of them to account for attacks that others had experienced [4]. Sharing information to produce a broad dataset would greatly improve the ability of each organization involved to make value assignments, but is impractical due to the sensitive nature of the data involved. Organizations are understandably unwilling to publicly reveal information pertaining to current vulnerabilities or past attacks as it could be damaging to both their security and reputation. These privacy concerns may prevent organizations from sharing their datasets to obtain a more accurate risk assessment.

To address these concerns, we propose the use of secure multiparty computation (MPC) to allow organizations to perform joint analytics while maintaining the confidentiality of their own data (e.g. [6], [3], [1]). MPC enables mutually distrusting parties to compute on their private data without revealing their inputs or outputs of the computation. More formally, using MPC, $n$ parties $P_1, \ldots, P_n$ having private input data $x_1, \ldots, x_n$ can compute a function $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ so that each party $P_i$ learns only its intended output $y_i$ and nothing more. Specifically, in the setting of cyber risk assessment, this means that the organizations can compute relevant statistics and analyses on the global infrastructure while still keeping the details of their local infrastructure and vulnerabilities private. Moreover, this privacy guarantee holds even if some bounded number of the organizations collude or share data in an effort to learn details about a specific organizations infrastructure. Thus, MPC enables the desired level of collaboration while overcoming the privacy concerns that have previously prevented data sharing in this application scenario.

While MPC allows new collaborative capabilities, it also incurs performance overheads, primarily from communication costs. The performance overheads depend significantly on the function to be computed and the specific protocol design and implementation. In this talk, we will describe the design, implementation, and evaluation of MPC protocols for cooperative cyber risk assessment. We first identify computations relevant to this application. We then design and implement MPC protocols for these computations using on top of building blocks in VIFF, an open-source MPC framework [2]. We evaluate performance of these protocols and identify bottlenecks. We will also discuss the security, flexibility, and scalability of our protocols in terms of number of organizations participating in the computation and input sizes.

This work is sponsored by the Assistant Secretary of Defense for Research and Engineering (ASDR&E) under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

## REFERENCES

[1] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, 1988.

[2] Ivan Damgård, Martin Geisler, Mikkel Krøigaard, and Jesper Buus Nielsen. Asynchronous multiparty computation: Theory and implementation. In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09*, pages 160–179, 2009.

[3] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, 1987.

[4] Arjen Lenstra and Tim Voss. Information security risk assessment, aggregation, and mitigation. In *Australasian Conference on Information Security and Privacy*, pages 391–401. Springer Berlin Heidelberg, 2004.

[5] Fabrizio Smeraldi and Pasquale Malacaria. How to spend it: Optimal investment for cyber security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity*, ACySE '14, pages 8:1–8:4, 2014.

[6] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *FOCS*, pages 162–167, 1986.