Evolving Sharing Strategies in Cybersecurity Information Exchange Framework*

Iman Vakilinia
Dept. of Computer Science and Eng.
University of Nevada, Reno
ivakilinia@unr.edu

Sushil J.louis
Dept. of Computer Science and Eng.
University of Nevada, Reno
sushil@cse.unr.edu

Shamik Sengupta
Dept. of Computer Science and Eng.
University of Nevada, Reno
ssengupta@unr.edu

ABSTRACT

Cybersecurity information sharing among participating organizations proactivly helps defend against attackers. However, such sharing also exposes potentially sensitive organizational information. We attack the problem of finding sharing incentives and penalties that maximize sharing utility while minimizing risk by modeling cybersecurity information sharing as an iterated prisoner's delimma-like game. A genetic algorithm then evolves potential strategies that lead to high utility for an organization participating in a Cybersecurity Information Exchange. Preliminary results indicate that the genetic algorith finds strategies better random or Tit-for-tat.

KEYWORDS

Cybersecurity Information Sharing, Genetic Algorithm, Prisoner's Dilemma

ACM Reference format:
Iman Vakilinia, Sushil J.louis, and Shamik Sengupta. 2017. Evolving Sharing Strategies in Cybersecurity Information Exchange Framework. In *Proceedings of GECCO '17 Companion, Berlin, Germany, July 15-19, 2017,* 2 pages.
DOI: http://dx.doi.org/10.1145/3067695.3075613

1 INTRODUCTION

Due to the importance of sharing cybersecurity information to prevent other organizations being exploited, governments and legislators encourage entities to share such cybersecurity data. As an example, the federal Cybersecurity Information Sharing Act (CISA) [3] was designed to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. A Cybersecurity Information Exchange Framework (CYBEX)[7] provides a platform for sharing cybersecurity information. However, several obstacles prevent easy cybersecurity information sharing. First, shared information may leak other vulnerability/threat data. Second, other CYBEX organizations might misuse such shared data. And third, reporting successful attacks may negatively affect an organization's reputation.

Cybersecurity information sharing has been extensively studied in several papers[4–8]. However, to the best of our knowledge, none of this prior work has considered the problem of finding an efficient sharing strategy that maximizes sharing utility for an organization. In this paper, we cast this problem as a repeated game of cybersecurity information sharing and investigate using a genetic algorithm to evolve sharing strategies. Drawing on Axelrod's work with the iterated prisoner's dilemna, we use a very similar encoding and compare evolved strategies against four baseline strategies [1]. Preliminary results show that the genetic algorithm evolves strategies that beat all four.

*This research is supported by the National Science Foundation (NSF), USA, Award #1528167. This work is also partially supported by the Office of Naval Research under Grant N00014-15-1-2015.

GECCO '17 Companion, Berlin, Germany
 978-1-4503-4939-0/17/07…$15.00
DOI: http://dx.doi.org/10.1145/3067695.3075613

2 METHODOLOGY

In the iterated cybersecurity information sharing game, organizations choose their strategy based on the benefits they receive from CYBEX. For simplicity and without loss of generality, we consider four types of sharing strategies ($S1$ through $S4$) and three types of organizations (*Effective*, *Moderate*, and *Small*). $S1, S2, S3, S4$ share 25%, 50%, 75%, 100% of their cybersecurity information and the payoff depends on the type of organization being shared with.

The four strategies compared against are:

• *High Rate*: Participating organizations share more than 50% information. Such organizations split their strategy between $S3(50-75)\%$ and $S4(75-100)\%$ with probability $3/4$ for $S4$.

• *Low Rate*: Participating organizations share less than 50% information. Such organizations split their strategy between $S1(0-25)\%$ and $S2(25-50)\%$ with probability $3/4$ for $S2$.

• *Random Sharing*: Participating organizations randomly choose among $S1$ through $S4$.

• *Reflective*: Participating organizations choose what the evolved strategy chose on the previous iteration.

The GA then evolves a sequence of Si where i varies from 1 though 4 (and requires two bits to represent) to compete against the four strategies above. We keep a history of past games so we can use past experience to guide our current decision. Since our payoff matrix has 16 possible outcomes for each cycle, we have 16^H different possibilities for encoding H previous cycles. If we chose to keep three game cycles of history, we have $16^3 = 4096$ possible historical decisions to encode and two bits to represent our response. Our chromosome length therefore works out to $4096 \times 2 = 8192$ to start with. This is very similar to Axelrod's representation in his early work on using genetic algorithms to evolve strategies for the prisoner's dilemma [1]. Like Axelrod, we also need to store three initial moves of history at the start, requiring $2 * 2 * 3 = 12$ more bits for a total chromosome length of 8204. Our search space for $H = 3$ is thus 2^{8204} and we use a genetic algorithm to search this space of strategies.

Table 1: Final result of the evolved strategies and their corresponding payoff

CYBEX Strategy	Organization Type	Evolved Strategy	Payoff	Random Strategy Payoff	TFT Strategy Payoff
Low	Effective	12% S1 and 88% S2	-0.23	-2.17	-0.34
	Moderate	100% S2	-0.54	-3.46	-0.78
	Small	42% S2 and 58% S4	-0.49	-3.11	-1.06
High	Effective	78% S2 and 22% S1	0.92	-0.05	0.47
	Moderate	100% S2	0.54	-1.14	0.29
	Small	82% S2 and 18% S4	0.61	-0.09	0.30
Random	Effective	46% S1, 43% S2, and 11%	0.51	-1.98	-1.17
	Moderate	57% S4 and 43% S2	0.12	-1.54	-1.61
	Small	61% S2, 21% S4, and 18% S1	0.04	-2.35	-2.14
Reflective	Effective	100% S4	1	-0.03	-0.25
	Moderate	100% S4	0.25	-1.21	0
	Small	100% S4	-0.12	-2.54	-0.37

CYBEX

O_i	S1	S2	S3	S4
S1	$(0,0)$	$(1,-1)$	$(2,-2)$	$(3,-3)$
S2	$(-1,1)$	$(0,0)$	$(1,-1)$	$(2,-2)$
S3	$(-2,2)$	$(-1,1)$	$(0,0)$	$(1,-1)$
S4	$(-3,3)$	$(-2,2)$	$(-1,1)$	$(0,0)$

O_i	S1	S2	S3	S4
S1	$(0,0)$	$(1,-1)$	$(2,-2)$	$(3,-3)$
S2	$(-1,0.5)$	$(0,-0.5)$	$(1,-1.5)$	$(2,-2.5)$
S3	$(-2,1)$	$(-1,0)$	$(0,-1)$	$(1,-2)$
S4	$(-3,1.5)$	$(-2,0.5)$	$(-1,-0.5)$	$(0,-1.5)$

O_i	S1	S2	S3	S4
S1	$(0,0)$	$(1,-1)$	$(2,-2)$	$(3,-3)$
S2	$(-1,0.25)$	$(0,-0.75)$	$(1,-1.75)$	$(2,-2.75)$
S3	$(-2,0.5)$	$(-1,-0.5)$	$(0,-1.5)$	$(1,-2.5)$
S4	$(-3,0.75)$	$(-2,-0.25)$	$(-1,-1.25)$	$(0,-2.25)$

Figure 1: Payoff Matrices

In our simulation, we evaluate the chromosome against a payoff matrix based on effects of the organization over CYBEX's payoff. Our payoff matrix is shown in Table 1.

The game is played 100 times and the accumulated payoff is calculated based on the payoff matrix and the rules of game. The GA usese CHC selection [2] where parents also compete for population slots in the next generation. The parameters of GA are as follows: Crossover = 95%, Mutation = 0.1, Population Size=100, and Generations=1000.

3 RESULTS AND DISCUSSION

We ran our experimental GAs with 5 different random seeds and provide averages over these five runs. We calculate the payoff through the payoff matrices under the rules of the game and compute utility as the average of GA's output payoff value.

Table 1 depicts the results. We compare the performance of the best evolved strategy found by the GA with the random sharing strategy and Tit-For-Tat (TFT). In the random sharing strategy, the organization chooses the sharing rate randomly for each round, and in TFT, the organization selects the same sharing amount chosen by the other organizations in the previous round. The results show that the GA evolves strategies that beat our baselines.

4 CONCLUSION AND FUTURE WORK

Cybersecurity information sharing helps organizations proactively defend against attackers. However organizations are reluctant to share security information because of the risk of leak of sensitive and secret information. A Cybersecurity Information Exchange Platform helps organizations manage risk through incentives and penalties. Modeling this risk and reward as a form of iterated prisoner's dilemna game, we use a genetic algorithm to evolve sharing strategies that optimize organizational utilities for different types of organizations. Simulation results show that the genetic algorithm can evolve strategies that outperform a purely random player as well as a player who plays Tit-For-Tat. We believe this preliminary work shows the potential for modeling and investigating multiple forms of Cybersecurity information exchanges and lead to organizational strategies for proactively managing cybersecurity threats.

REFERENCES

[1] Robert Axelrod and others. 1987. The evolution of strategies in the iterated prisonerfis dilemma. *The dynamics of norms* (1987), 1–16.

[2] Larry J Eshelman. 2014. The CHC adaptive search algorithm: How to have safe search when engaging. *Foundations of Genetic Algorithms 1991 (FOGA 1)* 1 (2014), 265.

[3] Eric Fischer, Edward Liu, John Rollins, and Catherine Theohary. 2013. The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. (2013).

[4] Kjell Hausken. 2007. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy* 26, 6 (2007), 639–688.

[5] Panos Kampanakis. 2014. Security automation and threat information-sharing options. *IEEE Security & Privacy* 12, 5 (2014), 42–51.

[6] Stefan Laube and Rainer Böhme. 2016. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* (2016), tyw002.

[7] Anthony Rutkowski, Youki Kadobayashi, Inette Furey, Damir Rajnovic, Robert Martin, Takeshi Takahashi, Craig Schultz, Gavin Reid, Gregg Schudel, Mike Hird, and Stephen Adegbite. 2010. CYBEX: The Cybersecurity Information Exchange Framework (x.1500). *SIGCOMM Comput. Commun. Rev.* 40, 5 (Oct. 2010), 59–64.

[8] Shahin Vakilinia, Behdad Heidarpour, and Mohamed Cheriet. 2016. Energy Efficient Resource Allocation in Cloud Computing Environments. *IEEE Access* (2016).