Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

Evolutionary Systems: Applications to Cybersecurity

David Gould
City University of Seattle, dagould@cityu.edu

Simon Cleveland
City University of Seattle, simoncleveland@cityu.edu

Evolutionary Systems: Applications to Cybersecurity

David Gould
City University of Seattle
dagould@cityu.edu

Simon Cleveland
City University of Seattle
simoncleveland@cityu.edu

ABSTRACT

Evolution is a well-known biological theory; however, there is a gap in literature that examines how evolutionary principles can be applied to other natural as well as artificial systems. This paper includes an extension to the general evolutionary algorithm to showcase how evolutionary principles can be applied through technology evolutionary models and tools to identify and prevent cyber threats.

Keywords

Evolutionary systems, general evolutionary algorithm, cybersecurity, viruses, SCAMPER

INTRODUCTION

Arthur (2009) argued that technological evolution occurs exogenously as technologies combine or recombine to form new products or technologies. This process, termed combinatorial evolution, can create almost any number of identical copies given sufficient resources. Over time, one or more of these technologies can be combined with other technologies to create yet new technologies. Presently, there is gap in research that applies combinatorial evolution to the field of cybersecurity. To address this gap, the present study examines a substrate-neutral model of evolution along with its applications to cybersecurity. The model presented in this paper is based on the limits-to-success systems archetype and expands the general evolutionary algorithm to include additional factors driving and limiting evolutionary systems.

EVOLUTIONARY SYSTEMS

Forrester (1971) argued that a system is a set of components that function together to achieve some purpose. Mobus and Kalton (2015) offered a more formal definition of a system as a 6-tuple, described by a set of subsystems, a network or networks, the set of nodes inside and outside the system, the boundary conditions, the interactions among the nodes, and the history of the system. An evolutionary system is one that exhibits differentiation (variation), selection, and amplification (reproduction, replication, or recombination).

Furthermore, evolution is ubiquitous; not only in natural systems such as biological systems, but also in social and artificial systems. Solar systems, organizations, economies, and technology are examples of evolutionary systems. Abstracting key principles of biological evolution "differentiate, select, and amplify" generates an algorithm as Beinhocker (2006, p. 12) observed. Fichter, Pyle, and Whitmeyer (2010) referred to these steps as the general evolutionary algorithm. Yet, as Berlinski (2000) noted, "an algorithm is a finite procedure, written in a fixed symbolic vocabulary, governed by precise instructions, moving in discrete steps 1,2,3, …., whose execution requires no insight, cleverness, intuition, or perspicuity, and that sooner or later comes to an end" (p. xvii). Buenstorf (2006) noted that if selection and inheritance concepts are too close to biology, then they are of limited usefulness when applied to other disciplines.

A network is commonly thought of as a set of nodes and links. A system can be viewed as a network with interactive nodes also known as agents. These agents interact with each other as well as with their environment. Relationships between agents may be strong, weak, or null; with multiple other descriptions possible as well. The type of network or networks illustrates systems structure: matter, information, or energy flows through the system are processed; the system as a whole exhibits behavior, and some systems exhibit some form of dynamics over time such as transitional, transformational, adaptation or learning, or evolutionary.

Figure 1 illustrates a substrate-neutral model of evolution linking three principles: variation (differentiation), selection, and replication (amplification). These principles, abstracted from biological evolution, can be applied to other systems that evolve as well, although by other mechanisms than biology. From the positive feedback loop perspective, once a system is initialized to the point of being able to replicate with variation, diversity will continue to increase, and this cycle will continue until something slows or stops it. This is where the negative feedback loop is important. Selection reduces variety or diversity and some level of capacity provides a limit or limits to success or growth.

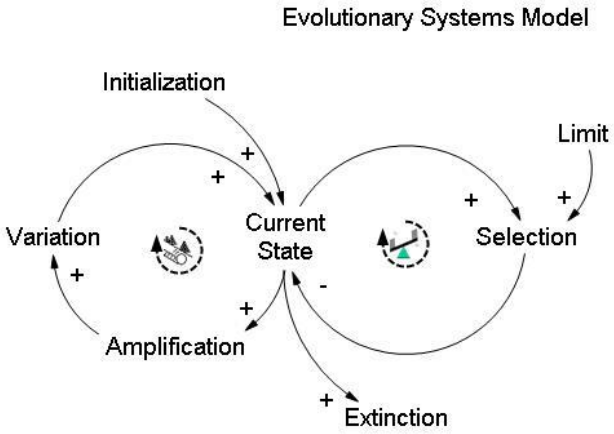

Figure 1: A substrate-neutral model of evolution

Various forms of reproduction or replication have been observed and studied. Ziman (2000) examined innovation as an evolutionary system and noted that there are "structural analogies to certain biological processes and processes involved in technological innovation" (p. 4). In addition, Ziman noted "less tangible cultural entities, such as scientific theories, social customers, laws, and commercial firms undergo variation by mutation or recombination" (p. 4). Arthur (2009) explored technology as an evolutionary system and noted many of the same points as Ziman. For example, consider computer viruses. Wilson and Kiy (2014) argued that computer viruses, just like their living counterparts, evolve and replicate. Viruses can take aim at changing the functions of a system, such as the degradation of a software function to prevent users from the functionality of the system. Furthermore, through innovative malicious logic, the virus can replicate into multiple various forms and extend with rapid speed to remote nodes on a network as noted in figure 2.

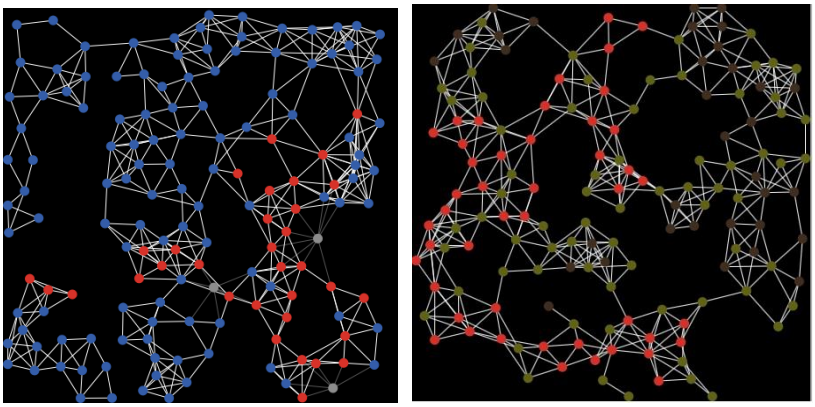

Figure 2. Simulation of Network Viral Infection (adapted from Netlogo.com)

The evolution of cybersecurity threats occurs exogenously as new techniques and technologies combine or recombine to form new products or technologies. That is, evolution by combination or "combinatorial evolution" (Arthur, 2009, p. 22). Viruses can create almost any number of identical copies given sufficient time and human behavior. Over time, this threat can be combined with other threats (e.g. piracy, or reverse engineering) to create greater risks to the system.

Variation constraints exist. For example, there are clear limits to variation or differentiation as new systems or agents cannot violate the laws of physics. The time element is frequently important. For example, does sufficient time exist for evolution of the system or agent to take place? Technologies may take considerable time to evolve. A new operating system or version of an operating system may take months to years to evolve; yet, a reverse engineering technique can only take days and have devastating effects on a company.

There are several forms of selection. In biology, there exist natural, sexual, and artificial selection; and in the cybersecurity world, there is marketplace selection, for example, where choice is the selection mechanism. Selection operates as a filter of sorts, screening out some systems or agents, while letting other systems or agents through. Extinction occurs when all systems or agents of a certain type are screened out. For example, changes in rules may cause some companies to succeed while others go extinct. Additionally, organizations with strong prescriptive security analytics in place can protect themselves from malware through the use of diagnostics and 'predictive outputs' (Grahn, Westerlund & Pulkkis, 2017), while the ones without suffer network meltdown.

The state of the system is a point in time, from which we can observe the size of a system or systems, an agent or set of agents, and the various interactions among them such as competition, predator/prey, cooperative, synergistic, or some other relationship. The behavior of a system or systems can be noted as such: increasing, decreasing, flat line, collapse, oscillation, or other. The state of the system is an accumulation of the events and activities of the system throughout the previous cycles of reproduction/replication, variation, and selection with the various influences already noted, plus any limiting influences from the negative feedback cycle. The state of the system may be measured in terms of wealth, numbers of populations, the size of populations, the health of an industry, or a variety of other measurements depending on the type of system being measured.

The limit constraints in a system represents a fundamental limit to the success or growth represented by the positive feedback loop in the model. The availability of a limit and its value or values indicates the limit of the resource and the overall influence of the limit on the system performance. This limiting constraint applies not only to biology, but also to cyber threat prevention. For example, consider the anti-tampering techniques that are successful in preventing network attacks. These include "secure loaders, integrity checks, self-healing that can automatically reverse some hacks, and the use of a secure development environment (SDE)," (Wilson & Kiy, 2014, pp 118).

In companies with resources who employ protection techniques, cyber threats will diminish. In contrast, companies with limiting constraints, such as physical capacity; capabilities such as mental models, skills, or intelligence; or the availability of resources such as time, materials, talent, expertise, education, space, tools, technology, finances, and such, the cyber threats will flourish with devastating outcomes. This limited availability will affect or influence the state of the system in a limiting or dampening way.

APPLICATION OF SCAMPER TO CYBERSECURITY THREATS

Security teams can leverage a variety of tools to prepare for cyber threats. One tool called SCAMPER (figure 3) has been used to generate architectural innovations (Daru et al. 2000). It is a structured tool used to arrange thinking processes to generate rapid innovative solutions. SCAMPER stands for Substitute, Combine, Adapt, Modify, Put, Eliminate, and Reverse (Eberle, 1996). To illustrate the approach, an examination of a cybersecurity defense is performed to demonstrate the application of the tool.

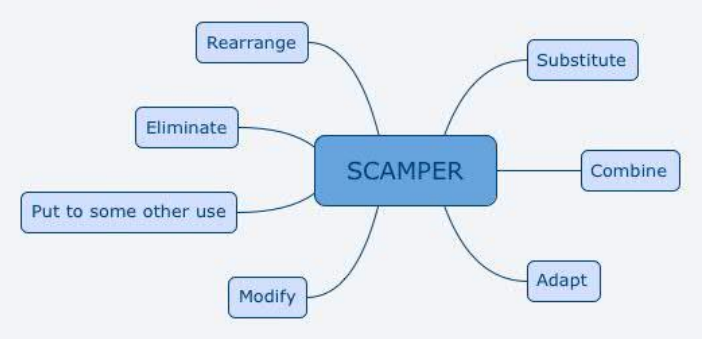

Figure 3. SCAMPER Tool

During the Substitute state, the security team will ask questions to determine whether part of the system can secured without affecting the whole system. Furthermore, the team will decide who or what can be substituted as well as better alternatives that the initially proposed solutions. During the Combine state, the team will look for ways to eliminate redundant steps, or ways to apply multiple solutions at the same time. The team will also combine resources with other partners to combat the attack, or leverage multiple technologies to solve the problems.

During the Adapt stage, the security team will look for ways to change existing approaches in order to obtain better results. They will look for innovative new ways to adjust existing solutions, make the approach more flexible, or additional methods to perform a specific solution. During the Modify stage, the team will explore more efficient and innovative ways to secure the system. Next, during the Put to another use stage, the team will examine whether the existing solutions can be leveraged in a different area of the organization (e.g. security policy to be applied to recently acquired organization). During the Eliminate stage, the security team will examine the impact of removing specific existing security measures. Some of the questions asked here include whether the same security output can be achieved without such measures: are the same amount of resources required to secure the system, or can this be done with half of these resources? Finally, during the Reverse (Rearrange) stage, the security team will assess whether reversing the existing security measures can produce a more desirable outcome.

New cybersecurity prevention techniques can be derived from existing solutions using the basic evolutionary algorithm—variation, selection, and replication with innovation playing a major exogenous role in variation. Once SCAMPER has been applied, it is necessary to test the variation for fitness (e.g. how useful a change is); at this stage selection is the principle to use, and choice is the mechanism of selection for the cybersecurity approach. Other metrics that could be considered include business value and computation time.

CONCLUSION

Biological evolution provides an algorithm to search through a design space of possibilities, and these concepts can be used to improve the capability for designing and developing new cybersecurity solutions. Challenges with cyberattacks can be addressed if they are examined as evolutionary systems that follow similar patterns of behavior. In term, security teams can leverage tools such as SCAMPER to develop innovative solutions for such attacks. Future research will validate the SCAMPER approach in a live cyberattack scenario.

REFERENCES

1. Arthur, W. B. (2009). *The nature of technology: What it is and how it evolves.* New York, NY: Free Press.
2. Beinhocker, E. D. (2006). *The origin of wealth: Evolution, complexity, and the radical remaking of economics*. London, England: Random House.
3. Beinhocker, E. D. (2010). Evolution as computation: Implications for economic theory and ontology. Retrieved from http://www.santafe.edu
4. Berlinski, D. (2000). *The advent of the algorithm*. New York, NY: Harcourt.
5. Buenstorf, G. (2006). How useful is generalized Darwinism as a framework to study competition and industrial evolution? Journal of Evolutionary Economics, 16, 5, 511-527. doi:10.1007/s00191-006-0035-3
6. Daru, R., Vreedenburgh, E. and Scha, R. (2000). Architectural innovation as an evolutionary process. Abstract of paper presented at the Generative Art Conference, Politecnico di Milano, Italy, 14-16 Dec 2000. Retrieved from www.generativeart.com/abst2000/abst77.htm
7. Eberle, B. (1996). *Scamper on: Games for imagination development*. Prufrock Press Inc.
8. Fichter, L. S., Pyle, E. J., & Whitmeyer, S. J. (2010). Strategies and rubrics for teaching chaos and complex systems theories as elaborating, self-organizing, and fractioning evolutionary systems. *Journal of Geoscience Education*, 58, 2, 65-85. doi:10.5408/1.3534849
9. Forrester, J. W. (1971). *Principles of systems*. Portland, OR: Productivity Press.
10. Grahn, K., Westerlund, M., & Pulkkis, G. (2017). Analytics for network security: A survey and taxonomy. In *Information fusion for cyber-security analytics.* 175-193. Springer, Cham.
11. Mobus, G. E., & Kalton, M. C. (2015). *Principles of systems science*. New York, NY: Springer.
12. Pearce, J. A., & Robinson, R. B. (2017). *Strategic management.* New York, NY: McGraw-Hill.
13. Wilson, K. S., & Kiy, M. A. (2014). Some fundamental cybersecurity concepts. *IEEE access*, *2*, 116-124.
14. Ziman, J. (Ed.). (2000). *Technological innovation as an evolutionary process*. New York, NY: Cambridge University Press.