Application of the theory of games for selection of effective defense

Damir KULBAEV, A.Z. ABDENOV

Faculty of Informational Systems, Eurasian National University, Astana, Kazakhstan
E-mail: damirkaz@mail.ru

Abstract: This article aims to prove that the use of games theory in decision making can aid in choosing the best methods of defense against attack weighed against the possible costs of such methods. Decision making in games theory assumes interaction between the seller or buyer with the environment as the environment fluctuates and the outcome is the expected payoff for such decisions. The decision maker makes decisions based on the possibility of risk and the expected payoff and whether or not the risk will be advantageous. The Wald Test is justified in situations where the possibility of environmental health is unknown, the solution occurs only once, and there is no risk taken. The Hurwitz pessimism-optimism theory is used when environmental information is missing or unreliable, recalculations must be made for each state of the environment, the number of implemented solutions is small, and some risk is allowed. Integrating these methodologies into the possible attacks and protections, we can evaluate the methods of protection in theory and in practice. Given the possible methods of defense being none, firewall, intrusion detection tools, and link redundancy, we can evaluate each method individually and in combination. Although the most effective method in theory would be to use firewall, intrusion detection tools, and link redundancy together, in practice the cost is prohibitive. If cost is factored into the equation, then the most effective method in theory is a firewall, however this fails to take into account the possible loss if an attack is successful. Taking into account this factor as well, a firewall works in a limited number of attacks, link redundancy for higher, and the most effective is to use all three methods in combination (firewall, intrusion detection tools, and link redundancy).

Keywords: game theory, Wald test, Hurwitz pessimism-optimism theory, security threat, firewall, link redundancy, intrusion detection tools, effective defense

References

[1] Owen G. Games theory. - .: World, 1971.
[2] Gordon L.A., Loeb M.P, Lucyshyn W., Richardson R. 2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY. - San Francisco: Computer Security Institute, 2006. - 29 p.

[3] Shun-Chieh Lin and Shian-Shyong Tseng. Constructing detection knowledge for DDoS intrusion tolerance. Expert Systems with Applications. - Atlanta: Expert Systems with Appli-cations, 2004. - Volume 27, Issue 3. - P. 379-390.