Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Active Defence: An Evolving Gaming Strategy for Attacker Defender in a Network Environment

Waziri, Victor Onomza, Anuonye, Stanley Obinna, Morufu Olalere, Ismaila, Idris
Cyber Security Science Department, School of Information and Communications Technology, Federal University of Technology, Minna, Niger State, Nigeria

Abstract: This paper uses active defense mechanism to determine appropriate strategies for attackers and defenders in a simple network security game, using a method which is generic to many other security games. The largest problem facing active defence is determining what actions to take and when to take them given the risks of the actions and the risk of the threats. This leaves only one choice: to implement a defence that can mitigate a threat in real-time that it is detected and the time that it would achieve its goal. This is the essence of active defence. This presents the concept of computing the risk available to the process proactively. Due to resource constraint in time, we will not build a heuristic model for a simulated Game theory that could be set up to give detail experiment; but this paper will expose and stress on the concept of predicting an attacker technique theoretically that could be applied to develop an active defence strategy by evolving an attacker and defender population in parallel and then testing them against each other by considering a prototype generic algorithm for the simulated environment.

Keywords: Active defence, Security, Game Theory, Risk and Simulation

I. INTRODUCTION

Malicious activity on the Internet is a significance and growing nefarous epidemic. The spectrum of threats includes Denial-Of-Service (DoS) attacks, self-propagating worms, spam, spyware, and botnets [10, 20] that are growing destructive impunities in both political and commercial institutions. Malicious parties (Black Hats) are constantly looking for new potential victims' systems, which are typically identified by scanning across large portions of the Internet address space in devious dexterity around the world. Many tools [8] have been developed to facilitate the mitigation these hazardous machineries; and researchers describe and evaluate the magnitude of the threat posed by utilizing highly efficient computational scanning strategies that are inefficient to zero-day malware detections. Hence, there is no doubt in postulating that providing a strong and unbreakable defense over a network of computers is becoming increasingly complex that need new more ingenuous computing approaches and mitigating technologies. A network administrator needs to have an in-depth understanding of server configurations, Internet Protocols, access controls, data storage shrewdness etc. However, one of the key criteria of being a good Cyber Security Manager (CSM) or Chief Information Security Officer (CISO) simply understands that much effort and time is required in securing systems and where to focus that effort and time. It is of no surprise to the security community that the numbers of attacks on computer systems have been steadily in the increase over the past several years. This pattern is more disturbing as the number of national infrastructure systems that are accessible over the Internet is also growing [9] and overstretching due to the ever growing wisdoms of the nefarious communities around geographical regions in the world. Not only are Government critical infrastructures put under threat, other infrastructures such as medical and financial systems are equally vulnerable and accessible using technical computing technologies, placing life-critical systems in danger.

There is no question that these systems are being protected by extensive security measures such as firewalls and intrusion detection systems. However, what happens if an intruder were to bypass those defences? Sergio [19] intelligently liken this as a complete catastrophic phenomenon for it would be like having a castle with very thick and tall walls, but having no security force inside. That if an attacker were to tunnel under the walls, he would have full and complete access to full acquisition of the critical infrastructure until he chooses to leave. The defenses on the modern critical systems are good, but not sufficient enough to protect against the level of sophistication that intruders are reaching by the day. Additionally, these defenses cannot be maintained fast enough to keep up with the number of vulnerabilities discovered instantly, daily, weekly or monthly; thereby providing attackers with complete laxity in time between when the vulnerability is discovered, and when a vulnerability can be protected against [7]. Preventative defenses are no longer sufficient, especially for national infrastructure and life-critical systems.

This leaves only one choice: to implement a defense that can mitigate a threat between the time it is detected and the time that it would achieve its goal. *This is the essence of active defense;* which is another conception outline of being potentially alert or a state of being proactive-*stitch in time saves nine.*

Active defense is an area that most security researchers usually would always want to work on because it provides an avenue for real-life time mitigation resistance. However, Active defense actions are varied in scope; from the notification of appropriate personnel, to the notification of authorities, to rewriting firewall rules, to initiating a denial of service attack against the attacker [19]. An active defense is any set of actions taken to mitigate a threat against an asset between

the time the threat is detected until the time it has completed its objectives. There have been very few published instances of active defense actually being utilized. Some famous cases involve Cliff Stoll [11] tracking German hackers in the early 80's and the US Department of Defense initiating an attack against a group attempting to use a Distributed Denial of Service Attack (DDoS). However, certain companies have recently begun to include 'response' technologies in their firewall and intrusion detection systems [6]. These 'responses' limit themselves to rewriting firewall or routing rules in an attempt to block an emerging threat. Yet although the technology now allows us to undertake active defense action, there is still no clear method of creating and evaluating the effectiveness of an active defense strategy. An active defense strategy is the ordered set of actions that will be taken in response to the detection of a threat.

This paper will describe steps theoretically that could facilitate in the development of the derivation of active defense strategies using evolutionary techniques and genetic algorithms. While active defense strategies can be derived in deviant ways, an evolutionary environment can provide a unique setting where the strategies are not determined solely by calculated risk and success, but by which strategies perform best against an attacker's strategy or strategies. Many artificial strategies abound that could fasten the development of the heuristic strategies such as Clonal Particle Swarm optimization, Support Vector Machines, Artificial Immune, genetic algorithm, neural networks, ant colony etc. These strategies could be hybridized to develop more efficient strategies that could improve active defend strategies.

In particular, competitive evolution could be be utilized so that both an attack and defend strategy are simultaneously coevolved. The strategies are then evaluated based on their performance against their evolved counterparts. In this way, we hypothesize, that using evolutionary strategies to derive active defense strategies will yield results that are reasonable based on a commonsense understanding of security and on the application of active defence models. The structure of the remaining part of the works are as follows: Section 2 reviews the literature on ground; the structure of section 3 deals with these: Information warfare, Active Defence, Generic Algorithms and Co-Evolution, Section 4 presents the Parameters Involved in Modelling Active Defence, section 5 gives detail theoretical experimental frameworks; while section 6 discusses, concludes and provides suggestions for further future research works.

II. RELATED WORKS

Pavan Vejandla et al. (2010) [1] implemented a memory based multi –objective evolutionary objective algorithm (MOEA) in an Anticipation game framework to generate action strategies and experiments were performed in a simulated network. Simulations with different types of nodes and services are performed, results were analyzed and reported. This approach takes into account multiple conflicting objectives like cost, time, reward, and performance of the generated performance strategies.

Alan Nochenson and C.F. Larry Heimann (2010) [2] proposed the concept of Agent-based modeling as a fairly new approach to modeling complex systems. The key feature of an agent-based modeling scenario is the presence of a set of agents (with attributes and behaviors), relationships between and among the agents, and the environment that the agents "live" in envisioned and described being autonomy as the defining characteristic of an ABMS. This autonomy is bounded by some normative model that describes the behavior of a given agent which can be heterogeneous. This paper examined an agent-based model to simulate security scenarios to identify Nash Equilibria strategies for both attackers and defenders.

Stocco and Cybenko (2011) [4] used simulation to model various strategies in a game of High Card, which they used as a stand-in for a security investment game. This paper exposed a similar strategy with a very different game and explicitly models a network security scenario to best generalize strategies to other related scenarios. The game of High Card simulates a single round of betting in a game of poker. Stocco and Cybenko pit bots with various utility functions against each other, and concluded that the behavior of a bot using a prospect theory-based function performs better than using utility functions based on linear, sublinear and superliner functions. They then developed a modeling bot that learned from the past behavior of its opponents, which was superior.

Sergio Caltagirone (2005) [10] also viewed Active defense as a security tool that has not received much attention in research. His paper examined co-evolution that is used as a technique to develop an active defense strategy by evolving an attacker and defender population in parallel and then testing them against each other. This technique was successful and illustrated that competitive co-evolution can be a useful tool in determining security strategies.

Crosbie and Spafford (1995) [12] in a published seminar paper on the topic proposed a prototype system, where the agents on the system were taught to detect intrusive behavior using genetic programming techniques. To accomplish this, they developed a meta-language to examine specific aspects of the system such as network data and disk access. This language was used in the parse trees developed through the use of genetic programming, which were used as rules in the agents. If a rule was broken on the system, an agent raised the suspicion level and other agents began to look more closely at their own data by incorporating more strict rules. When a sufficient number of agents have raised the suspicion level, the level goes above a threshold and the security officer is notified of a potential system intrusion.

Spears and Gordon (2000) [5] published a paper regarding the evolution of finite-state machine strategies for a defender-adversary game. This work attempted to evolve strategies for a game involving two players competing for limited resources; the adversary's strategy was fixed, while the defender evolved to beat it. Their results were promising, however limited by the existence of cycles in the strategies. Their work has potential applicability in the survivability and defense of networks.

Kunreuther and Heal (2002) were some of the first researchers to look at interdependent problems in security. Interdependence refers to the idea that decisions are not made in a vacuum. The choice one agent in a network makes affects the well-being of others. This paper does not have multiple strategic defenders like in, but it does have multiple

machines which are all interconnected. Varian [2000] [6] looked at a variety of security games and acknowledges that security is a public good. Adding security to one machine in a network increases the security of the overall system.

III. INFORMATION WARFARE, ACTIVE DEFENCE, GENERIC ALGORITHMS AND CO-EVOLUTION

An active defense is any set of actions taken to mitigate a threat against an asset between the time the threat is detected until the time it has completed its objectives [3]. Although information warfare and active defence are regularly confused because of potential offensive action, there is a significant difference between the two. These include the Information warfare that is concerned with achieving a "military advantage using tactics of destruction, denial, exploitation, and/or deception." Active defence, on the other hand, is not concerned with military advantage, and only attempts to mitigate a threat until a previous security state has been reached. This difference does not mean that information warfare research is not valuable; on the contrary, information warfare research is very valuable because of the stress on offensive action – the most questionable element of active defence.

A genetic algorithm is a computation paradigm that utilizes a population of encoded chromosomes, and operations upon those chromosomes for the purpose of searching search spaces by increasing population fitness as individuals near a goal. This paradigm was first introduced by John Holland [18]. However, although his original work describes natural competitive coevolving populations, his theories and experiments are only subject to fixed environments.

"Hierarchical Co-evolution or Co-Evolution for short is defined as the environment for the first population consists of a second population and vice versa. He also describes "relative fitness," which is where an individual's fitness is determined by its performance against all of the individuals of the opposing population. He puts these into practice by attempting to evolve a game strategy using a tree structure; and succeeds in evolving the optimal strategy for each player without any direct knowledge of such strategy.

In this term paper, two topics are being combined in the hope of developing a new technique for information assurance policy and strategy creation viz; ***active defense and evolutionary computation***. Intrusion Detection Systems (IDS) as a field emanated from the combination of evolution and security, using active defence as a major weapon.

IV. PARAMETERS INVOLVED IN MODELLING ACTIVE DEFENCE

The first and initial step in developing an active defence strategy is the identification of potential actions and associated risk. In active defence strategy, some popular strategies are [13]:

1. Installation of an antivirus;
2. Shut down port at firewall;
3. Filter IP addresses at firewall;
4. Send virus against an attacker;
5. DoS attacking style;
6. Hacking the attacker;
7. Ask ISP to shut off attack;
8. Send TCP RST packet;
9. Use trace back;
10. Contact CISO; and
11. Shut down server

These actions were given a risk amount in a simulated environment, which is only relative to the other actions. Additionally, a precondition is set and if met, it would be clear that if the attacker's IP address was a necessary piece of information to carry out the action; and whether the action, if successful, would permanently stop the attacker. The table below shows the associated risks and level of defence

S/No.	Defence Strategy	Risk	IP address necessary?	Permanent Stop?
1.	Installation of an antivirus;	5	N	N
2.	Shut down port at firewall;	1500	N	N
3.	Filter IP addresses at firewall;	12	Y	N
4.	Send virus against an attacker;	15	Y	Y
5.	DoS attacking style;	900	Y	N
6.	Hacking the attacker;	2000	Y	Y
7.	Ask ISP to shut off attack;	1000	N	N
8.	Send TCP RST packet;	1250	Y	N
9.	Use trace back;	10	N	N
10.	Contact CISO; and	19	N	N
11.	Shut down server	5000	N	N

Figure 4.1: Table showing risk levels of defence actions by the defenders and probable actions Key: Y = YES; N = NO

The second step in developing an active defence strategy is the identification of potential actions and associated risk. Some offensive actions are also defined. The risks of the offensive actions are not determined by any formula, but as relative to the other actions and the value of the asset (mainly availability and integrity). These are described as follows:

1. Spoofing of IP address;
2. Porting of scan server;

3. DoS server;
4. Ping server;
5. Installation of back door on server;
6. Poison DNS;
7. Send virus against server;
8. Change records; and
9. Download record

Action	Risk
Spoof IP Address	20
Port Scan Server	30
Ping Server	22
DoS Server	800
Poison DNS	200
Install Backdoor on Server	900
Download Records	1000
Change Records	1500
Send Virus against Server	400

Figure 4.2: Table showing risk levels of offensive actions by the attacker

A table is now created that specifies which defensive actions stop which offensive actions The 'Use Traceback' defensive action plays an important role. It itself does not stop any actions, however if an attacker has used the 'Spoof IP' action, then traceback will find the IP of the attacker so that defensive actions that require a valid IP will then be effective. Additionally, the CISO actions do not do anything very valuable, but are there because in a real active defense scenario those would are required before an active defense can be initiated.

Defensive Action	Stops These Actions
Contact CISO	
Shutdown Port at Firewall	Port Scan, Ping, DoS Backdoor, Download Records, Change Records, Virus
Install Antivirus	Port Scan
Filter IP at Firewall	Port Scan, Ping, Backdoor, Download Records, Change Records
Shutdown Server	All Actions
Send TCP RST Packet	Port Scan, Ping, Backdoor, Download Records, Change Records
ISP Shut-off	Port scan, Ping, DoS, Backdoor, Download, Change Records
Use Traceback	
Send Virus Against Attacker	Port Scan, Ping, DoS, Backdoor, Download, Change Records, Send Virus against Server
DoS Attacker	Port Scan, Ping, DoS, Backdoor, Download, Change Records
Hack Attacker	Port Scan, Ping, DoS, DNS, Backdoor, Download, Change Records

Figure 4.3: Table showing mitigation matrix for defence action

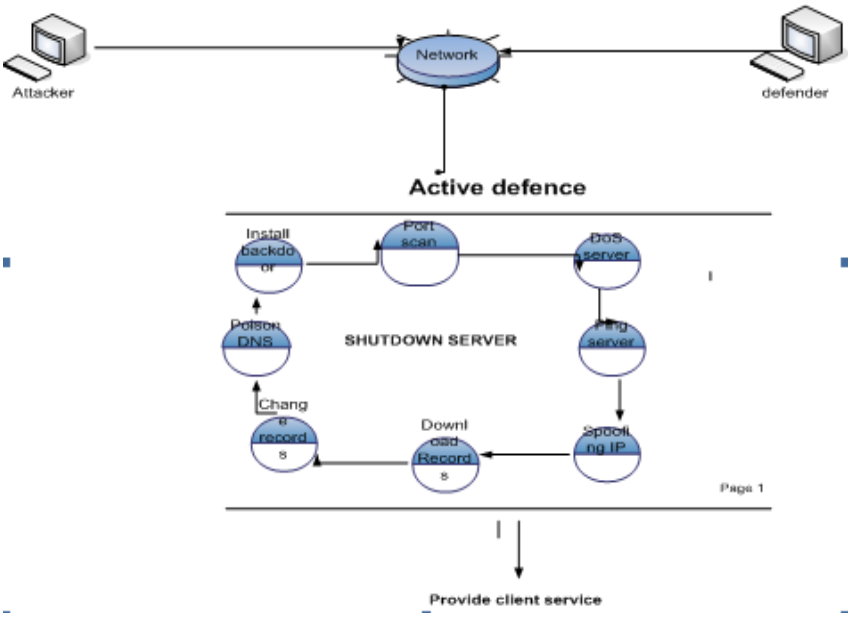

Figure 4.4: Attacker defender algorithm

The diagrammatic algorithm for attacker defender scenario for active defence is shown below:
It should be clearly stated that in an attacker defender game, each action by either the attacker or the defender amounts to risk [14]. The algorithm terminates when either of the two conditions occur:

1. Whenever there are no more defensive actions from the defender; or
2. Whenever the assumed threat is mitigated against; meaning the attacker is defeated.

From the flowchart above, the risk element [19] in an entire attacker defender session that can be explained and calculated by the algorithm below:

```
int risk = 0;
for-each(attacker Action){
boolean stopped = false;
for-each(defender Action  {
risk += risk(dAction);
if (permanent Stop(dAction,aAction)          {
return risk;
                    }
else if (stops (dAction, aAction)){
stopped = true;
                    }
          }
if (!stopped) risk += risk(aAction);
} return risk;
```

Risk management can be achieved whenever there are attack graphs [15]. Attack graphs are tools used by analysts to produce pictorial display of local vulnerability information along with other information about the network, such as connectivity between hosts. Hence attack graphs can minimize risk along the network.

V. EXPERIMENTAL RESULTS

The below example is the result of the algorithm for an attacker defender game using active defence, if carried out in a simulated environment, though a bit of competitive co-evolution may be introduced.

Attacker: (Port Scan the Server) **Defende**r: (Install antivirus) (Provide service to client);
Attacker: (Port Scan the Server, DoS Server) **Defende**r: (Dos attacking style) (Provide service to client);
Attacker: (Port Scan the Server, DoS Server, Ping Server) **Defende**r: (Send TCP) (Provide service to client);
Attacker: (Port Scan the Server, DoS Server, Ping Server, Spoofing of IP Address) **Defende**r: (Filter IP) (Provide service to client);
Attacker: (Port Scan the Server, DoS Server, Ping Server, Spoofing of IP Address, Download Records) **Defende**r: (ISP Shutoff) (Provide service to client);
:
:
:
Attacker: (Port Scan the Server, DoS Server, Ping Server, Spoofing of IP Address…) **Defende**r: (Shutdown Server).

VI. DISCUSSION, CONCLUSION AND SUGGESTION FOR FURTHER RESEARCH

The main aim of the experiment when carried out in a simulated environment is to show that active defence is a useful technique which reduces the risk element for attacker defender games. The attackers choose a strategy that inflicts the most amount of risk while minimizing the defensive actions available to mitigate the threat. As shown in the experimental results above, when the attacker ports the scan, the defender is expected to quickly install an antivirus before providing service to the client. Moreso, if it passes the "port scan" attack and moves to the "Denial of Service" attack on the server, the defender is expected to also deny the service to all attackers on the simulated environment. This strategy was developed consistently over many iterations of the experiment. The strategy produced is reasonable and effective.

Further work can be expanded in this area by considering the effect of attacking defender strategies on multiple hosts such as the attacker on Linux and the defender on windows platform. Moreso, immunity based techniques in cyber security games can be further researched into where a group of certified risk professionals mimic antibodies in their protection of physical and logical devices of a system network.

In the perennial struggle against network intruders and malicious attacks, safeguarding computer networks is becoming an urgent problem. This paper abstracts the problem of game theory then applying active defensive techniques which is modeled in a flowchart algorithmic pattern. Howbeit, active defense can be used as a security tool that is legitimate if more attack types can be anticipated and defended by the attacker. Finally since the strategies of the attacker and the defender amounts to risk, a brief algorithm is developed for the computation of total risk for the entire attacker defender process.

REFERENCES

[1] Pavan Vejandla,Dipankar Dasgupta, Aishwarya Kaushal, Fernando Nino, Evoloving Gaming Strategies for attacker – defender in a simulated network environment
[2] Nochenson, A., Heimann, C.F.L.: Optimal security investments in networks of varying size and topology. In: International Workshop on Socio-Technical Aspects in Security and Trust (2012)
[3] Pratt, J.W.: Risk Aversion in the Small and in the Large. Econometrica 32 (1964)

[4] Stocco, G.F., Cybenko, G.: Exploiting Adversary's Risk Profiles in Imperfect Information Security Games. In: Baras, J.S., Katz, J., Altman, E. (eds.) GameSec 2011. LNCS, vol. 7037, pp. 22–33. Springer, Heidelberg (2011)
[5] W. M. Spears and D. F. Gordon, "Evolving Finite-State Machine Strategies for Protecting Resources," presented at the 12th International Symposium.
[6] Varian, H.R.: System reliability and free riding. In: Economics of Information Security,
[7] Symantec, "Symantec Internet Security Threat Report," M. Higgins, Ed., 3 ed. Cupertino, CA: http://www.securitystats.com/reports/Symantec-Internet_Security_Threat_Report_vIII.20030201.pdf, 2003.
[8] CERT, "Testimony of Richard D. Pethia before the House Select Committee on Homeland Security: Cyber Security - Growing Risk from Growing Vulnerability," http://www.cert.org/congressional_testimony/Pethia_testimony_06-25-03.html, 2003.
[9] Reuters, "Computer Under Attack Can hack Back, Expert Says," http://www.usatoday.com/tech/news/computersecurity/2002-08-05-hack-back_x.htm, 2002
[10] S. Caltagirone, "ADAM: Active Defense Algorithm and Model," University of Idaho, 2004.
[11] C. Stoll, "Stalking the Wily Hacker," in *Communications of the ACM*, vol. 31, 1988, pp. 484-497.
[12] M. Crosbie and E. Spafford, "Applying Genetic Programming to Intrusion Detection," presented at 1995 AAAI Fall Symposium on Genetic Programming, Cambridge, Massachusetts, 1995.)
[13] Chapman, C., Ward, S.: Project Risk Management: processes, techniques and insights. Chichester, John Wiley (2003)
[14] CVSS (Common Vulnerability Scoring System) URL: http://www.first.org/cvss/
[15] Dantu, R., Loper, K., Kolan P.: Risk Management using Behavior based Attack Graphs. International Conference on Information Technology: Coding and Computing (2004)
[16] Hariri, S., Qu, G., Dharmagadda, T., Ramkishore, M., Raghavendra, C. S.: Impact Analysis of Faults and Attacks in Large-Scale Networks. IEEE Security&Privacy, September/ October (2003)
[17] Jha, S., Sheyner, O., Wing, J.: Minimization and reliability analysis of attack graphs. Technical Report CMU-CS-02-109, Carnegie Mellon University (2002)
[18] J. Holland, Adaptation in Natural and Artificial Systems. Ann Arbor, Michigan: University of Michigan Press, 1975.)
[19] Sergio Caltagirone (2005)+, Evolving Active Defense Strategies University of Idaho
[20] Waziri Victor Onomza, Osho Femi (2013): A conceptual Models and Simulation of Computer warms propagation; Verlag Publishers: LAP LAMBART ACadic Publising; ISBN:978-3-659-474545

Bibliography

Dr. Victor O. Waziri is an Associate Professor in the Department of Cyber Security, Federal Federal University of Technology, Minna-Nigeria. His Computational Research is based on Computational Intelligence with Applications on Cyber Security related problems. In most cases, Matlab, Maple and Mathematica are the basis for his accessory in modeling and Simulations in Modern Cryptographic analyses. His researches area also extends into Computational Optimization and in Zero-day Malware Detections. He has published many papers in reputable Journals at both International and Local Levels. He Lectures various courses in the Department that include Cryptography, Network Security, Clouds Security, Data Mining, Computational Theory, Automata and Programming Languages

Anuonye, Stanley Obinna Anuonye Stanley graduated from the Federal University of Technology Owerri in October, 2006 . His thesis was on Security of ICT systems generally with emphasis on intrusion detection and cryptographic security. His research interests include security at application and protocol levels. He is currently undergoing his masters in Cyber Security and the ICT officer in a government establishment.

Dr. Ismaila Idris is with the Deparment of Cyber Security Science. He obtain his Bachelor degree with Federal University of Technology, Minna. M.Sc. with university of Ilorin and PhD degree with University of Teknologi Malaysia. His research interest are Information Security, Data Mining, Machine Learning, Evolutionary Algorithm.

Morufu Olalere was born in Ode-omu, Osun state, Nigeria in 1980. He has B.Tech Industrial mathematics/computer science and M.Sc. in Computer science (Biometrics) from Federal University of Technology, Akure and University of Ilorin, Nigeria in 2005 and 2011 respectively. He is a LECTURER from department of Cyber Security Science, Federal University of Technology Minna, Nigeria and currently on study fellowship as a PhD student in the faculty of computer Science and Information Technology, University Putra Malaysia. His research interest includes biometric, network security, cryptography and security in Bring Your Own Devices. Mr. Olalere is a member of Computer Professionals Registration Council of Nigeria (CPN), a member of Nigeria Computer Society (NCS) and a member of Association for Information Systems (AIS). he is a certified ethical hacker.

