A New SOA Security Model to Protect Against Web Competitive Intelligence Attacks by Software Agents

Hamidreza Amouzegar, K. N. Toosi University of Technology, Iran
Mohammad Jafar Tarokh, K. N. Toosi University of Technology, Iran
Anahita Naghilouye Hidaji, Infotech Pars Company, Iran

ABSTRACT

This article presents an automata SOA based security model against competitive intelligence attacks in e-commerce. It focuses on how to prevent conceptual interception of an e-firm business model from CI agent attackers. Since competitive intelligence web environment is a new important approach for all e-commerce based firms, they try to come in new marketplaces and need to find a good customer-base in contest with other existing competitors. Many of the newest methods for CI attacks in web position are based on software agent facilities. Many researchers are currently working on how to facilitate CI creation in this environment. The aim of this article is to help e-firm designers provide a non-predictable presentation layer against CI attacks.

Keywords: Automata, Competitive Intelligence, Finite State Machine, Interactive Model, Security, SOA, Web

INTRODUCTION

No business is an island. For success, the business will need to deal with customers, suppliers, employees, and others. In almost all cases there will also be other organizations offering similar products to similar customers. These other organizations are competitors. And their objective is the same—to grow, make money and succeed. Effectively, the businesses are at war—fighting to gain the same resource and territory: the customer. And like in war, it is necessary to understand the enemy, how he thinks, what his strengths are, what his weaknesses are, where he is vulnerable, where he can be attacked, and where the risk of attack is too great (SCIP).

And like in war, the competitor will have secrets that can be the difference between profit and loss, expansion or bankruptcy for the business. Identifying these secrets is thus crucial for business survival. But all this is not new; around
the year 500 BC, the great Chinese military strategist, Sun Tzu wrote a treatise on the Art of War. From a 21st-century perspective, many of Sun Tzu’s approaches would be viewed as barbaric today (Gordon, 1989). Nevertheless, his views on strategy are still relevant today for both military commanders and business leaders looking at how to win against competitors.

Although elements of organizational intelligence collection have been a part of business for many years, the history of Competitive Intelligence began in the U.S. in the 1970s. In 1980 Michael Porter published the study competitive strategy: Techniques for Analyzing Industries and Competitors which is widely viewed as the foundation of modern competitive intelligence (Porter, 1998).

Business competitors are:

- Other organizations offering the same product or service now.
- Other organizations offering similar products or services now.
- Organizations that could offer the same or similar products or services in the future.
- Organizations that could remove the need for a product or service.

After the web was born, the entire competitive analysis model turned to new direction which grows by search engines and measuring the competitor web sites traffic according to customer’s behavior. The big problem was how to model the web sites and customers manner which present the business intelligence of competitors (Russel & Norvig, 2002). Nowadays many researchers are working on how to facilitate CI creation in this environment and trying to use some automotive solutions with software agent approach which is used before as a method of recursive searching in e-payments.

This article will try to introduce an automata SOA based security model against competitor agent’s attacks in web environment to prevent e-firms from business model transparency.

The first section will explain CI analysis methods and their solutions in web. The second section will introduce SOA uses in web. The third section will explain the security gaps. The forth section will focus on software agent specifications. And the final part will represent the proposed model for protecting the business from attackers.

COMPETITOR ANALYSIS METHODS

Competitor Array

One common and useful technique is constructing a competitor array. The steps in web environment include:

1. Define your e-firm scope and nature of the firm.
2. Determine who your competitors are and their services URL. Divide them to two section of secure and insecure which comes from their protocol.
3. Determine who your customers are and what benefits they expect.
4. Determine what the key success factors are in your e-firm.
5. Rank the key success factors by giving each one a weighting—The sum of all the weightings must add up to one.
6. Rate each competitor on each of the key success factors – this can best be displayed on a two dimensional matrix–competitors along the top and key success factors down the side.
7. Multiply each cell in the matrix by the factor weighting.
8. Sum columns for a weighted assessment of the overall strength of each competitor relative to each other.

Competitor Profiling

Another common technique is to create detailed profiles on each of your major competitors. These profiles give an in-depth description of the
Efficient Routing Protocol for Location Privacy Preserving in Internet of Things

Modeling Processes and Outcomes From Cybersecurity Talent Gaps in Global Labor Markets
[www.igi-global.com/chapter/modeling-processes-and-outcomes-from-cybersecurity-talent-gaps-in-global-labor-markets/213443?camid=4v1a](www.igi-global.com/chapter/modeling-processes-and-outcomes-from-cybersecurity-talent-gaps-in-global-labor-markets/213443?camid=4v1a)
Risk Planning and Mitigation in Oil Well Fields: Preventing Disasters
[www.igi-global.com/article/risk-planning-and-mitigation-in-oil-well-fields/145364?camid=4v1a](www.igi-global.com/article/risk-planning-and-mitigation-in-oil-well-fields/145364?camid=4v1a)

Viruses and Virus Protection in Cybercafés
[www.igi-global.com/chapter/viruses-virus-protection-cybercafés/28536?camid=4v1a](www.igi-global.com/chapter/viruses-virus-protection-cybercafés/28536?camid=4v1a)