Global Journal of Computer Science and Technology
Neural & Artificial Intelligence
Volume 12 Issue 10 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Artificial Intelligence an Essential Expected Computer World Surveillance

By K.Sudheer Kumar, D.Srikar & CH.S.V.V.S.N Murthy
D.N.R College, Bhimavaram

Abstract - A position paper toward an important and urgent discussion on how best uses the potential of Artificial Intelligence in the context of Computer World surveillance. AI is often cited in papers on Computer World surveillance. But what is meant is using pre-existing AI techniques in Computer World surveillance. AI techniques are established around applications. Computer World surveillance has never been an area of deliberation in AI. In this paper we argue that Computer World surveillance calls for new and specific AI techniques developed with that kind of application in mind. In practice, this paper is based on a broad overview of different slants, which have the budding to be game changers in Computer World surveillance. This paper focuses on web solicitation security and supporters the use of Knowledge Based Systems, probabilistic reasoning and Bayesian apprising to control the probability of false positives and false denials.

Keywords : *Documentation, Security, Theory, Bayesian updating, CSRF, probabilistic reasoning.*

GJCST-E Classification: *I.2.1*

Strictly as per the compliance and regulations of:

Artificial Intelligence an Essential Expected Computer World Surveillance

K.Sudheer Kumar [α], D.Srikar [σ] & CH.S.V.V.S.N Murthy [ρ]

Abstract - A position paper toward an important and urgent discussion on how best uses the potential of Artificial Intelligence in the context of Computer World surveillance. AI is often cited in papers on Computer World surveillance. But what is meant is using pre-existing AI techniques in Computer World surveillance. AI techniques are established around applications. Computer World surveillance has never been an area of deliberation in AI. In this paper we argue that Computer World surveillance calls for new and specific AI techniques developed with that kind of application in mind. In practice, this paper is based on a broad overview of different slants, which have the budding to be game changers in Computer World surveillance. This paper focuses on web solicitation security and supporters the use of Knowledge Based Systems, probabilistic reasoning and Bayesian apprising to control the probability of false positives and false denials.

GeneralTerms : Documentation, Security, Theory.
Keywords : Bayesian updating, CSRF, probabilistic reasoning.

I. Introduction

It has been known for a long time that in Computer World surveillance, defense uses a flawed hypothesis because it leads to a strategy based on tweaking and "fixing the comprehending" with no long term vision. When new forms of attacks appear, ad hoc response are put together, which often involves making the use of the internet more cumbrous, by adding layers of authentication. "Defensive measures tend to involve complicating protocols or their implementation, making things more secure by making them more cumbersome a mentioning abstaining from using some functionality, as more often than not each new functionality provides new points of entry for malicious activities [1],[2],[3],[4]. But the introductions of new functionalities are precisely what make the internet so attractive and successful. Furthermore there is still no tolerable defence to zero day attack, as anomaly based detection has still some open problems, like the false positive probability. An ideal cyber- defense would provide full protection to users, while preserving all the functionalities. We are very far from this situation. But there is no reason why in the long run, we could not get close to such a situation.

One thing that cyber-defense can do and should is to be more intelligent. The approach to defense based on" fixing the plumbing" is inherently suboptimal. A massive paradigm shift is needed, the kind of paradigm shift that makes a much heavier use of Artificial Intelligence (AI). The idea or making heavier use of AI in Computer World surveillance is not new. In an editorial in IEEE security and Privacy [5], Carl Landwehr stated that "In their early days, computer security and artificial intelligence didn't seem to have much to say to each other. AI researchers were interested in making computers do things that only humans had been able to do, while security researchers aimed to fix the leaks in the plumbing of the computing infrastructure or design infrastructures they deemed leak proof." But the dream of retroactively make the internet secure and leak-proof, is clearly not a clever approach.

The introduction of new technologies like the proliferation of new web applications or the increasing use of wireless, have exacerbated this fact [1]. Computer World surveillance, has become the most complex threat to society. Despite years of incremental improvements in cyber-defense, it is clear that a paradigm shift is needed, but at the same time difficult to imagine.

This is even more true for web-application security and the need for AI is even more obvious and urgent there. Against web application attacks, such as Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), injection code, the present approach consists in introducing rules supposed to prevent them. This is the same kind of logic that un derived the idea of same origin policy. Over the years XSS and CSRF began to mean a variety of attacks. Some of them can be construed as direct circumvention of the same origin policy. Same origin policy looked like a simple and efficient protection.

It turned out that it could be circumvented reasonably easily and was preventing some functionality to modern websites. In the words of D. Crockford same origin policy (which is adopted by most browsers) "prevents useful things and allows dangerous ones" [7]). Today, this policy is being revisited. For example, cross-site access control [8] is an attempt to refine the security policy in such a way that one can get the benefit of cross site access without the security implications.

Author α : Asst.Professor, Department of Computer Applications, P.G.Courses & Research Center, D.N.R College, Bhimavaram.
E-mail : sudheerkumarkotha@gmail.com
Author σ : Associate Professor Department of Computer Application P.G.Courses K.G.R.L.College, Bhimavaram.
E-mail : srikar_d@yahoo.com
Author ρ : Asst. Professor, Department of IT Sri sai Aditya Institute of Science &Techonlogy, Surampalem.
E-mail : chsatyamurthy@gmail.com

In the same way, SQL injection codes were described as "extremely easy to avoid" [9]. Still recently MYSQL and Oracle, both suffered such attacks. What may be construed as mistakes is also reflection of the fact that those mistakes are not so easy to avoid in the increasingly complicated world of web applications. To detect web application attacks such as XSS, CSRF or injection codes requires more than simple rules, but the ability to some form of context dependent reasoning. Despite some work done in the past, AI does not play central role in Computer World surveillance today and Computer World surveillance has not been an area of development of AI as intensely pursued as robots, machine learning and the like. Typically, the use of AI in Computer World surveillance has consisted in using some tools developed in AI and apply them to intrusion detection or other aspects of Computer World surveillance. The approach consisting in importing some AI techniques developed in totally different areas and try to apply them to Computer World surveillance, may work in a few cases, but has inherent and severe limitations. AI has been developed and is organized around specific applications, many of them (AI is a large field). Computer World surveillance has specific needs and to be a long term contributor to Computer World surveillance, new AI techniques will have to be developed specifically.

Obviously AI has made a lot of accomplishments and there is a lot to be learned relevant for Computer World surveillance and many new techniques suited for Computer World surveillance could be inspired from existing ones in AI. In a sense this has happened already. As observed by C. Landwehr [5]: "A branch of AI that has been connected with computer security from relatively early days is automated reasoning, particularly as applied to programs and systems. [...] Although it wasn't identified as AI at the time, Dan Farmer and Wietse Venema's SATAN program, released in 1995, automated a process for finding vulnerabilities in system configurations that had previously required much more human effort." S. Forrest [10] has proposed a system of inductive reasoning, which belongs to the realm of AI. And one can interpret the work of the group of Vigna et al in UCSB [11], [12], [13], [14], [15]) as proceeding from a somewhat similar philosophy. Arguably Web application firewalls (WAFs) or more generally firewalls using deep packet inspections can be construed as a kind of instantiation of AI in security. Firewalls have been part of the arsenal of cyber-defense for many years. Although more sophisticated techniques are also used, in most cases the filtering is based on port numbers. WAFs cannot rely on port number as most web applications use the same port as the rest of the web traffic. Deep packet inspection is the only option for WAFs to be able to tell a malicious application from a legitimate one. The idea of filtering at the application layer was introduced already in the third generation of firewalls in the 1990's. WAFs can be construed as a special case of application layer firewalls. The modest success of those technologies reflects the need for far more work on AI before they can make significant difference Computer World surveillance.

But those examples show that AI has a natural role to play in Computer World surveillance. They also show that using AI is inherently difficult. Introducing tools whose reaction to attacks is not totally predictable as they involve some context dependent reasoning will force attackers to potentially change completely their strategy. The increasing role of AI is in the logic of the modernization of the web and the internet. Web 2.0, the semantic web, the use of first order logic, the development of OWL are as many evidences of that. These developments will raise the level of complexity of Computer World surveillance and force it to be much more sophisticated. Computer World surveillance may turn out to be one of the best areas of applications of AI.

a) An Illustrative Example: Cross Site Request Forgery (CSRF)

This paragraph is meant to make the following discussion a bit less "high level" or purely abstract, by providing an example around which the rest of the discussion can be organized. The example is Cross Site Request forgery (CSRF). CSRF is not new. In 1988 it was known as "confused deputy". Dubbed a "sleeping giant", it came to prominence (i.e. enter in the OWASP top ten list) in the last few years. In the same way that XSS covers a large spectrum of attacks or vulnerabilities, some of which justifies to be called "cross site scripting", CSRF has grown into an open ended class of attacks. What all these attacks seem to have in common is that they hijack some credentials from a user and use them for the advantage of the attackers. Of this large class of attacks, what follows applies only to a subclass: it is when the attack takes place within the browser of the user. In fact the following considerations would apply to all situations where the attacks take place within the browser of the user, such as the man in the browser. Would an expert monitoring each HTTP request be able in real time to realize that a CSRF attack is unfolding?

Some context dependent analysis is of essence. The decision of whether malicious activity is taking place or not does not need to be the result of only one measurement. The analysis can be protracted and based on a succession of observations. An AI machine using a Bayesian algorithm could potentially do exactly the same. It is known that in a situation where the probability of false positive and negative of individual measurements is not so small, a shrewd Bayesian algorithm, well implemented can dramatically reduce the overall probability of false positive, while maintaining the probability of false negative low [16]. In other words, it is

possible with a shrewd use of multi-observations to maintain the probability of mis-determinations very low [16].

If one takes the example of the CSRF attack described in the classic paper of Felten [17]. A user while in a trusted session with his bank goes to a malicious website and click to download an image. The HTML request is crafted in such a way that through the browser, the query ends going to the bank website and instead of downloading a picture gives instructions (like transferring money or creating a new account) to the bank on behalf of the victim user.

Figure 2.1.1 : General cyber attack

A security tool monitoring the steps would find suspicious to have to find an image at a bank using the trusted session. It would assign a reasonably small probability of false positive for that (which could have been determined statistically before). Parsing the request, it would notice that it carries an executable. This too would raise serious suspicion. Then it could figure in the executable corresponds to what the bank requests for financial transaction. The probability of those three occurrences happening within the same query is small enough to trigger an alert that has a very very small probability of being a false positive. At each step the probability of false positive will be small, but different.

The point is that the tool would have to be able to do those inferences. It should be somewhat intelligent. We now turn to the questions: How far is AI from being able to produce tools like that? And what can be done now to facilitate the development of such tools?

b) A Very Brief Discussion of AI Methods

Although AI can be called a discipline, it is so organized around many different applications that it almost looks like a vast fragmented world. The example of CSRF points toward some form of probabilistic reasoning, as being a more natural approach to deal with that kind of situation than an approach requiring a lot of data for statistical learning for example.

When it comes to probabilistic learning, it seems difficult to avoid contact with Bayesianism. Bayesian reasoning is not without pitfalls, as Judea Pearl intimated in a recent presentation: " I turned Bayesian in 1971, as soon as I began reading Savage's monograph The Foundations of Statistical Inference [18]. The arguments were unassailable: (i) It is plain silly to ignore what we know, (ii) It is natural and useful to cast what we know in the language of probabilities, and (iii) If our subjective probabilities are erroneous, their impact will get washed out in due time, as the number of observations increases.

Thirty years later, I am still a devout Bayesian in the sense of (i), but I now doubt the wisdom of (ii) and I know that, in general, (iii) is false." But (iii) may be false for humans, but not necessarily for machines, because machines do not need to be prejudiced. Algorithms based on Bayesian updating work better with machines than humans.... An additional reason to use a Bayesian approach, is that as we saw in the previous paragraph, through Bayesian updating, it is possible to reduce the probability of false positive and negative. The decision of whether malicious activity is taking place or not does not need to be the result of only one measurement. It can be the result of analyzing a succession of steps.

This vision of a system able to process fast a lot of information, maintaining the rate of false positive and false negative small, despite the fact that the individual components themselves can have a high rate of false positive or false negative is reminiscent of the original idea of von Neumann discussed in his 1956 paper entitled: "Probabilistic logics and the synthesis of reliable organisms from unreliable components" [19].

As can be seen in the CSRF example, this probabilistic reasoning supposes the ability of some autonomous context dependent decision capability, i.e. needs some form of model of the environment. In the words of Judea Pearl [25]: "An intelligent system attempting to build a workable model of its environment cannot rely exclusively on pre-programmed causal knowledge", but must be able to interpret autonomously direct observations. This is where AI differs from more traditional approach to security, which tends to be based on rules. But it is also where the use of AI looks more challenging.

The amount of knowledge virtually present is very much greater than the amount of knowledge explicitly present. The extra knowledge is the result of query-time inference, which can require a lot of computation. And yet, we humans routinely perform this kind of inference quickly and in a way that seems almost effortless." One problem is to access this "virtual knowledge".

We humans also have a remarkable ability that is central to all recognition tasks: we begin with a set of observed features, a set of expectations, and a vast collection of stored descriptions; the problem is to find the stored description that best matches these features and expectations. This is a computationally demanding task that we humans do frequently, quickly, and with no sense of mental effort," but far more challenging for

machines. This is where the AI formidable challenge of identifying algorithms and world representation enters.

The attraction of Knowledge Based systems (KBS) [21] is their ability to make context dependent inferences. KBS tends to be specialized. Knowledge (virtual or real) is acquired or introduced in a variety of ways. But a lot rides on the way knowledge is stored and represented.

Those systems can reason and make inferences. Although they have been developed with different applications in mind, in principle they could be able to make autonomous determination of whether a malicious attack is unfolding.

Computer World surveillance may in fact be an area very appropriate for the application of constructs like the KBS Scone (developed at CMU by Scott Fahlman [22]). Like other KBS, Scone provides support for representing symbolic knowledge about the world: general common-sense knowledge or knowledge about some specific application domain. But Scone is designed to be used as a component in a wide range of software applications. Therefore, a primary emphasis has been put on Scone's expressiveness, ease of use, scalability, and on the efficiency of the most commonly used operations for search and inference. A feature of Scone, which makes it attractive in the context of Computer World surveillance tools is that unlike other KBS (such as Cyc [23], Owl [24], for example, and most Description Logic systems), the emphasis is on the ability to do a lot of simple inference very quickly, not the ability to prove deep theorems or to solve complex logic puzzles. In the system of trade-offs that underlie the development of KBS's, the priority was put on "expressiveness" and "scalability". At this stage, it is far too premature to exclude or recommend any approach.

c) What AI Could Bring to Computer World surveillance

CSRF is meant only as an example. It is only one in an already large and increasing number of web-applications vulnerabilities. Many popular websites are known to have exploitable cross-site scripting (XSS) [2] or cross site request forgery (CSRF, [24], [1]), "ClickJacking" vulnerabilities[4].

Most existing defenses against CSRF are ad hoc. Since CSRF involves in general hijacking a trusted session between a user and a website, a natural approach is to make such hijacking more difficult. One possibility is to not rely excessively on cookies to build trust, but add additional identifiers, at the cost of making trusted sessions more burdensome. A minor consideration in the security community, but the cumulative effect of making every "critical" interaction cumbersome is to project the impression that the logic of the culture of security is just the opposite of the logic of the technological innovations taking place in the internet and the web.

Since users for their security should not have to rely on website designers to anticipate all forms of attacks, tools protecting directly the users are intrinsically more attractive. The user side proposals tend to be based on rules tailored for each known scenario of attack. An example is to treat HTTP POST requests as more dangerous, because they are the one that changes the state of the server and forbid them in some circumstances. In addition to interfere with some useful functionality, this is not sufficient since it is possible (using Java script code injection) to make GET requests accomplish the same thing as POST requests. Disallowing or limiting the use of Java script has been suggested. This makes sense in some specific cases, but that kind of approach is an exacerbated version of security standing on the way of functionalities.

The commercial tool Request Rodeo is a commercial tool, which precludes scenarios on the basis of rules, that could lead to CSRF attacks. Its rules are so strict that it precludes proper interactions with a large number of modern websites. Relaxing the rules on the other hand would reduce the degree of protection, demonstrating if need be that an ideal tool would have to be more intelligent than simply applying rules.

Web application security generates a very new type of challenges compared with the world of worms, buffer overflows, etc.. The two worlds overlap, but they call for very different kinds of security tools. In fact there is no good security tool or even paradigm yet for web application. From the perspective of Computer World surveillance, the world of web applications is very complicated as it seems to offer an infinite numbers of opportunities for abuse.

Some exploitable vulnerabilities are difficult to understand or anticipate as they result from technical details of protocols, implementation of application or are consequences of abusing functionalities which otherwise are very useful or valuable. This is at a time where web applications are proliferating fast and playing an increasingly central role in many critical operations performed in the internet. Some exploitable vulnerabilities are difficult to understand or anticipate as they result from technical details of protocols, implementation of application or are consequences of abusing functionalities which otherwise are very useful or valuable. Most of web application vulnerabilities stems from what makes HTTP, HTML, Java-Script and the like so efficient to support web activity. The controversy around the "same origin policy" illustrates the complication of web application security. All this to show that web application security calls for intelligent tools.

Approaches to defense deliberately relying on AI may not deliver quick results. But they offer the perspective of a future very different and far more attractive than what the present approach based on "tweaking the plumbing" offers. In the same way that the co-evolution of pathogens and defenses from biological

organisms has led to the emergence of the immune system, and AI-based approach to cyberdefense can be seen as the natural next step.

To the legitimate concern that AI-based tools may be very large and suck a lot of CPUs (the immune system has as many cells as the nervous system: it is a huge organ), one can point to the fact that there is not much alternative. One immediate predictable benefit of approaching Computer World surveillance from and AI point of view will be to raise the level of the debate. Instead of being lost in the details of the implementation of old ideas, it will be forward looking.

On the other hand, it has to be recognized also that letting security be the organizing principle of modernization of the internet, will have a stifling effect on innovations, i.e. one of the main reasons of the success of the internet. But if innovation and Computer World surveillance begin to use the common perspective of AI, both at the same time rely increasingly on AI, the logic of the interaction will be dramatically different.

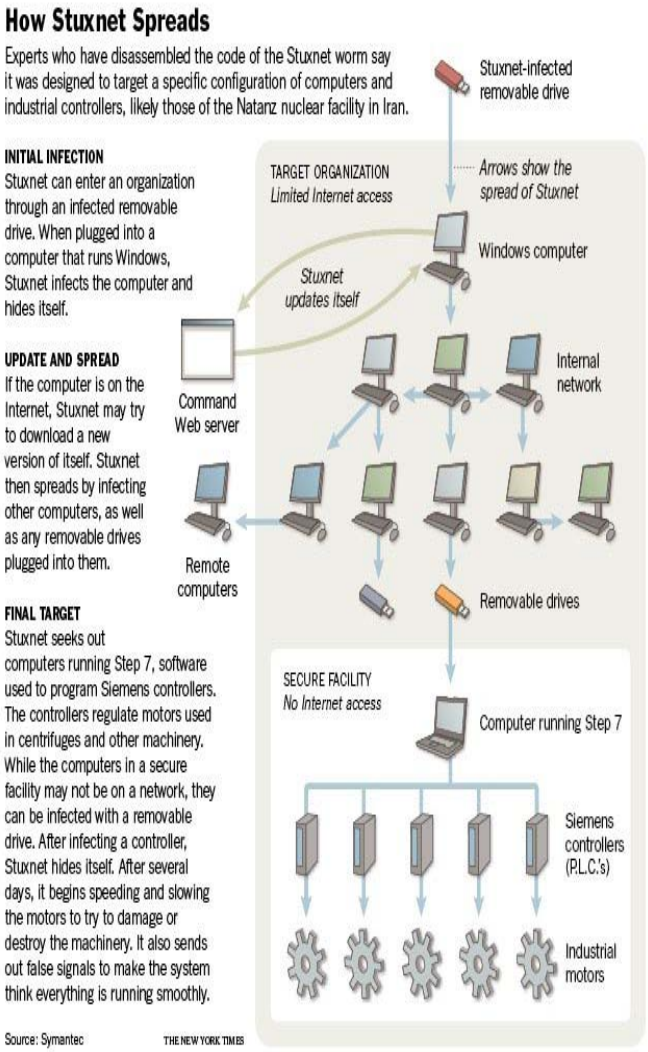

Figure 2.3.1 : How stuxnet Spreads

References Références Referencias

1. Barth, C. Jackson, and J. C. Mitchell. Robust Defenses for Cross-Site Request Forgery. In Proceedings of 15th ACM Conference, CCS, 2008
2. Seth Fogie, Jeremiah Grossman, Robert Hansen, Anton Rager, and Petko D. Petkov. XSS Attacks: Cross Site Scripting Exploits and Defense. Syngress, 2007.
3. N. Jovanovic, E. Kirda, and C. Kruegel. Preventing Cross Site Request Forgery Attacks. Securecommand Workshops, 2006, pages 1–10, Aug. 28 2006- Sept. 1 2006
4. Davide Balzarotti, Marco Cova, Vika Felmetsger, Nenad Jovanovic, Engin Kirda, Christopher Kruegel§, and GiovanniVigna,: Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2008.
5. Landwehr,Cal, Computer World surveillance and Artificial Intelligence: From Fixing the Plumbing to Smart Water, IEEE, Security and privacy, September/October 2008, p.3
6. Bruce Schneier, On Security, 2008.
7. Douglas Corckford, Ajax Security, 2006.
8. http://www.w3.org/TR/access-control/
9. http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
10. Kenneth Ingham, Anil Somayaji, John Burge, Stephanie Forrest , Learning DFA representations of HTTP for protecting web applications Journal of Computer Networks. 51:5, pp. 1239-1255 (2007).
11. Darran Mutz, William Robertson, Giovanni Vigna, and Richard Kemmerer, Exploiting Execution Context for the Detection of Anomalous System Calls, Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Gold Coast Australia, 2007
12. Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna Swaddler : An Approach for the Anomaly-based Detection of State Violations in Web Applications,
13. Robertson, Federico Maggi, Christopher Kruegel Giovanni Vigna, Effective Anomaly Detection with Scarce Training Data, Proceedings of the Network and Distributed System. Security Symposium (NDSS), San Diego, CA, February 010.
14. B. Morel, "Anomaly based intrusion detection systems", chapter in "intrusion detection systems,Intech (2011).
15. William Zeller and Edward W. Felten; Cross-Site Request Forgeries: Exploitation and Prevention, Princeton (2008); http://citp.princeton.edu/csrf/
16. L. J. Savage: The foundations of statistical inferences, 1962.

17. J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components", in C. E. Shannon and J.McCarthy,editors, Annals of Math Studies, numbers 34, pages 43-98. Princeton Univ. Press, 1956
18. Scott Fahlman: "NETL, a System for Representing and Using real World Knowledge", MIT Press, Cambridge, MA, 1979
19. R. Akerkar, P.S. Sajja, Knowledge Based Systems, Jones and Bartlett, 2009.
20. Fahlman, S.E.: The Scone Knowledge Base (homepage), http://www.cs.cmu.edu/~sef/ scone/
21. Blake Shepard et al. (2005). "A Knowledge-Based Approach to Network Security http://www.w3.org/2004/OWL/
22. Judea Pearl. Probabilistic Reasoning in Intelligent systems: Networks of Plausible Inference. Morgan Kaufmann, San Mateo, CA, 1988.