A Frame Problem Approach for Adaptive Cyber Security Design

R. Shaikh, T. Bryla, and S. Ahmed

Pace University Seidenberg School of CSIS, White Plains, NY 10606, USA
{rs95452w, tb13382n}@pace.edu, syedhammadahmed@gmail.com

Abstract

This paper is about efforts to create a Frame Problem based network security solution. The paper entails the motivation and efforts to integrate the Frame Problem approach to the distributed cyber-defense mechanisms against network attacks. This paradigm is further tested using a simple simulation of cyber-attacks detection and cyber-protection mechanisms validating posit that combining the Frame Problem efficacy with the network discrete-event antecedent can produce remarkable network security solutions. The paper describes the effectiveness of the underlying principles used to solve the Frame Problem in the context of network security counteraction against cyber-attacks. A simple simulator is designed and experimented to support the proposed FP based network security model coined as the Frame Problem Autonomous Network Security (FPACS). The paper characterizes some framework and implementation parameters of the simulation environment. The paper concludes with highlighting the advantages, illuminating potential drawbacks, and recommending a broad research agenda toward realizing the theoretical and practical extensions of this work.

Key words: Frame Problem; Cyber-security

Introduction

With the growing popularity of cloud computing technology organizations find it enticing to outsource their IT requirement and focus to their core business competencies. In this motif, network security services such as anti-spam, antivirus, automated vulnerability detection and mitigation, and filtering as a comprehensive outsourced managed solution has been gaining momentum recently. However, the existing paradigm of outsourced managed service providers does not meet the security standards for many public and private sector large organizations and risks long term customer-vendor commitment making it difficult to acclimatize [1].

At the infrastructure level, the widespread use of wireless and mobile networks has further complicated the cyber-defense challenges. There is strong evidence that smart cyber-attack systems can be produced by integrating artificial intelligence with wireless networks [2].

The traditional approach to address network security has been confined, mostly on classical models of safeguarding assets in a proactive mode. Except for Intrusion Detection Systems (IDS) which wait for something to happen, most security systems - Fire Walls, VPN, Anti nefarious software, etc. - all rely on a proactive defense approach. While this approach is costly in pure dollar terms, offers reduced network efficiency and onerous management. There is no clear alternating solution available either.

However, the Frame Problem (FP) does offer an "out-of-the-box" promising solution that is worth exploring to find more economical cyber security solutions. FP was first identified by John McCarthy and Patrick J. Hayes, almost around the same time when TCP/IP was incepted. Since publication of the McCarthy & Hayes articles [3], hundreds, if not thousands of hypothetical scenarios have been constructed by researchers in the fields of AI, cognitive science, philosophy, and elsewhere, in furtherance of our understanding of the frame problem and its application in the wider world, e.g., illustrations of the difficulties known as the Yale Shooting Problem, Traveling Salesmen Problem, etc. [4]. While FP does not explicitly deal with network security solutions, a careful study of FP will reveal that the theoretical and logical principles of FP may prove to be strong enablers for discovering proficient cyber security solutions. Just as the TCP/IP lead the world from costly proprietary to cost effective open systems, with sufficient research and development efforts FP may also lead to cost effective and efficient cyber security solutions. Drawing on fundamental FP axioms it is possible to design autonomous cyber defense mechanism that learn to ignore “unknown” in providing ideal solutions from just what is “known”.

Related Work

While the application of FP in this research is mostly independent of its connection with the AI domain, it is worthwhile to point out that there is a significant amount of recent work that deals with identifying changes over the network in real time. Following the work of McIntire et al., Coates et al., Von Ahn et al., and others [5, 6, 7], we apply the FP to first identify whether a change of network state from its baseline “normal” has occured and then select appropriate defense tactics.

FP has exhibited to solve many problems from a wide variety of domains such as, Web Services Specs demonstrated by Barynnis et al. [8], Software Development Problems as depicted in the Case of the Multi-translation by Reggioby et al. [9], regarding Morality & Ethics as shown by Horgan, et al. [10], in the Analysis of Dynamic Systems as proposed by Stephens, et al., at the Concordia University (Canada) [11], etc. In “Cognitive Wheels: The Frame Problem of AI”, Daniel C. Dennett’s narrative of the cognitive evolution of fictitious robots R1, R1D1, and R2D1 illustrate, in both amusing and instructive ways, the crux of the Frame Problem (FP) [12]: what elements change when actions are performed within a dynamic system, and what elements remain unchanged as a result of those same actions? Or, put rather more specifically, how do we create intelligent dynamic systems that understand “intuitively” the ramifications of both action and inaction – or, change and non-change – within and around the environment of a system?

John McCarthy and Patrick J. Hayes identified the frame problem in their 1969 article, *Some Philosophical Problems from the Standpoint of Artificial Intelligence* [13]. The problem of formulating the commonsense law of inertia – the supposition that “everything is presumed to remain in the state in which it is” unless there is evidence to the contrary – is considered the logical or technical aspect of the FP [14].

Frame Problem as Applied to Cyber Security

The potential utility of the FP approach in providing improved security solutions would seem to relate largely to quantitative elements: data throughput volume, communication bandwidth, and computing power as determinants of system accuracy, with cost considerations coming into play in certain cases. In some instances a high degree of technical knowledge is necessary for a thorough successful application of the FP approach, while in others a good result could be achieved with significantly less efforts.

Designing the FP Model

As noted above, from a theoretical perspective, although FP has been touted to solve many problems [18], however from an engineering perspective designing a network security model which integrates FP as its core can be a challenging tas. The main engineering aspect that differentiates the proposed design from the rest of network security models is the innovative use of FP as a pragmatic manifestation of a mostly theoretical concept in logic.

From a practical point of view, it is needless to say that the possibility of such a design could not have been materialized without modern technological innovations. Today, it is possible to build systems with giga bits of Static Random Access Memory (SRAM) and multiple access ports into very small chips. Most of the modern Field Programmable Gate Array (FPGA) devices may contain multiple such systems well suited for use in networks of any size and scope [19]. The design proposed in this work relies on the fundamental assumption that the technical capabilities of the high lookup capacity offered by such memory blocks are readily available.

The Initial model, coined as The Frame Problem Based Adaptive Cyber Security System (FPACS), as shown in Figure 1, can best be described as an integrated solution comprising of the following three modules:

1. Monitoring FPACS Protocol (MFP)
2. Fast Frame Tables (FFT)
3. Experience Pages (EP)

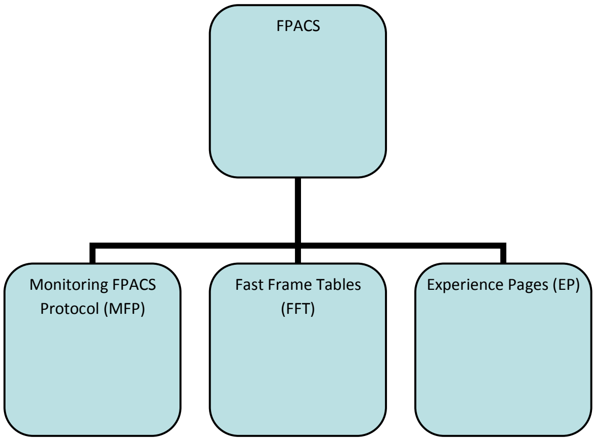


Figure 1 - FPACS

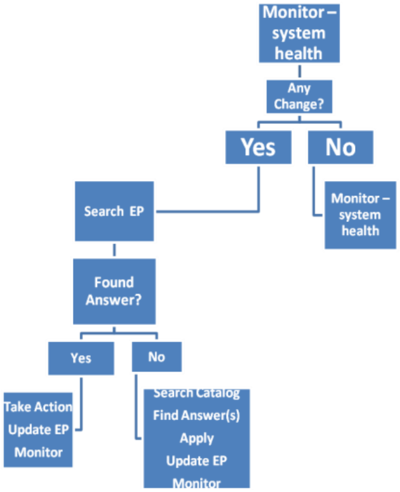


Figure 2 - MFP

Monitoring FPACS Protocol (MFP)

As shown in Figure 2, MFP describes a process of identifying a change in the network conditions and then taking some action if a state change is detected. The initial basic assumption is that the principle of inertia allows us to consider no change is taking place under "normal" conditions. At least two rudiments of this protocol is developed here:

What constitutes a "normal" state?

The design permits variables and their corresponding parametric values to be changed to represent specific size and scope of a network. For the purposes this model we design a "normal" state of the network from the following assumptions. We represent the network in the following way:

World of system events = W_t [$e_1 \ldots e_x$] ---(1)

Threshold for depicting "normal" to "change" state = T_t[$v_1 \ldots v_x$] ---------- (2)

Indication of "change" state as identified by FFT = C_t . $\sum$($v_1 \ldots . v_x$) -------------- (3)

Further explanation of FFT is deliberated separately under Fast Frame Tables, later in this paper.

Action suggestion & learning out put after a change is indicated = A_t . $\sum a_1 \ldots a_x$ ---- (4)

Search criteria for identifying appropriate action once change is detected= S_t [$s_{1.}s_x$] .(5)

Quantifying MFP output as a function for triggering actions =

[M_t = f(x)$_t$ ∫ W_t [e1…ex]. ∫ T_t[$v_1 \ldots v_x$] . ∫ C_t . $\sum$($v_1 \ldots . v_x$)] U [T_t[$v_1 \ldots v_x$]] (6)

The above can be further supported by the narrative that if MFP determines a change in the monitoring network conditions to an extent that the threshold is crossed a triggering mechanism may justify actions based on appropriate searches returned by the EP, so that:

A_t = [S_t [$s_1 \ldots s_x$] / $\sum a_1 \ldots a_x$] = < 0 or null ---------------------------------- (7)

Then, S_t [$s_1 \ldots s_x$] . C_t . $\sum$($v_1 \ldots . v_x$) = < 0 or null ------------- (8)

The algorithm should test for the above equation. Only if (8) is true, find and learn new answers.

Fast Frame Table (FFT)

FFT maintains a log of events and states for MFP. Additionally, FFT provides flags and action plans for FPACS to use EP. The development of FFT is based on an advanced version of commonly used hash tables for the monitoring of network conditions, known as Fast Hash Table with Bloom Filter [22] (FHTBF).

Extending the work done on FHTBF, a simple FFT consists of an array of y containers with each container pointing to the list of objects hashed into it. Consider the following operations for FFT:

Let,

B = Set of objects to be inserted in the FFT

Bk = List of objects hashed to container k and (Bm)k = m-th object in the k-th list

Thus,

Bk = {(B1k, B2k, B3k, ……, Bxkk} , where xk =Total number of objects in the container, and

B = ŪTk=1 . Bk , where T = Total number of lists present in the FFT

This is best explained in Figure 3. Thus, B13 = G, B23 = H, T = 3, and x3 = 3

G, H, J	B3
--	
--	
--	
N	B7
--	
--	
--	
--	
P	B13

Figure 3

Using the optimal configuration for the Bloom filter for minimizing the false probability we can map the same for FFT for reducing the cost in access and update time of event states. Thus the expected number of Hash functions for FFT may be shown as: $K = (c / xk) . T (xk)^2$, where c = Total number of containers.

Experience Pages (EP)

This is the repository of domain knowledge which is accessed by FPACS once the MFP triggers an action. The organization of EP is drawn from the commonly used principles of Ontology [23]. As the system learns by experience security solutions and action plans are added to the EP as representation of reusable security patterns. Except for few examples of categorizing the knowledge in EP, most of the EP work is left to be carried out in future.

EP contains Categories, Objects, and State Values. In our model, Categories can be classified by common classification patterns: A, B, etc. Objects are flagged by unique index ratings: 1-10, and Values determine the scalar magnitude as well as the vector indicating one of two states: Active, Passive.

For example, an initial set of categories can be programmed as under:

Categories:

A: (Criticality Index 1-10) - Vulnerabilities, Risks, Damage.

B: (Damage Index 1-10) – Successful Attacks, Failed Attacks, Total Attacks.

C: (Cost Index 1-10) – Solutions, Applied Solutions, Skipped Solutions

D: (Knowledge Index 1-10) – Known, Unknown, Hybrid

E: (Repeatability Index 1-10) – D = [A Ū B Ū C Ū D]

The Ontological representation is shown in Figure 5.

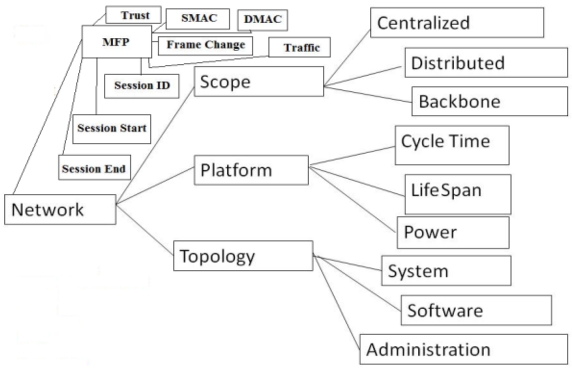
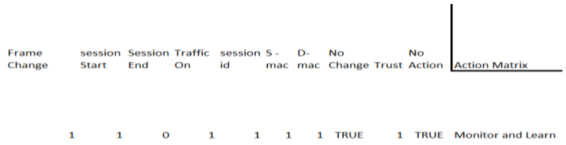


Figure 5 – EP Ontology

Simulation and Analysis

A simple simulator is created to test the performance of MFP (Figure 4). The FFT simulator was used on randomly generated continuous 24-7 network traffic with peek traffic depicting a typical 9-5 office environment of a 15-node network with a mix of mobile and fixed station equipments, all connected to the Internet via broadband high speed (1MB) multiple connections. As expected, Frame Change and Session Starts were easily singled out by MFP, as shown in Figure 6.



Frame Change	session Start	Session End	Traffic On	session id	S - mac	D- mac	No Change	Trust	No Action	Action Matrix
1	1	0	1	1	1	1	TRUE	1	TRUE	Monitor and Learn

Figure 4 - FFT Simulator

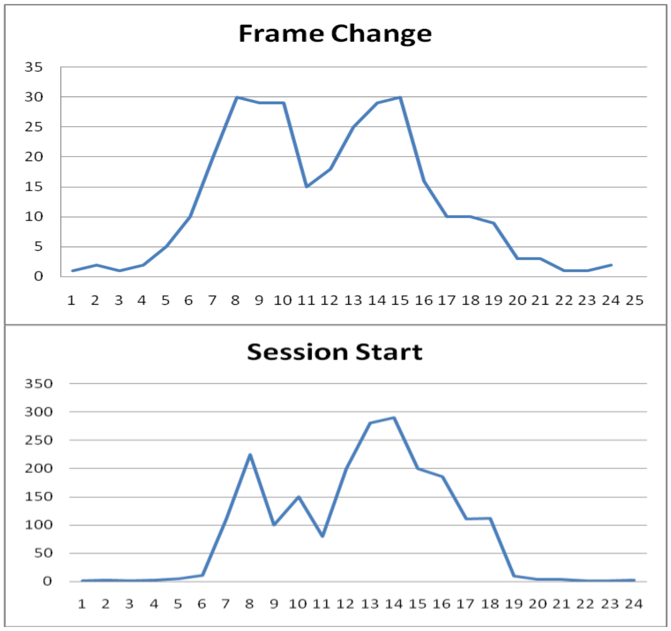


Figure 6 – Frame Changes & Session Starts

Conclusion

The FPACS model proposed in this paper and tested by a simulator exhibits sufficient confidence in validating a novel approach in combining the Frame Problem efficacy with the network discrete-event monitoring to produce economical network security solutions. The paper characterized framework and implementation parameters of the simulation environment. The paper also provided advantages and shed light on potential drawbacks that need to be considered with regards to the applicability of FPACS.

The solution presented here is not proposed to be a substitute of existing security measures. It is recommended to be a complimentary solution to work with existing security solution systems. Just like IDS, the proposed design of FPACS can only be useful if and when an event actually takes place. The utility of the proposed model lies in the fact that a cyber security event is detected which may or may not require subsequent defense tactical response. In this work it is demonstrated, in a simulated environment that the proposed model can launch appropriate security response to a cyber attack via the EP module of the design. However, more work is required to expand further applicability of FPACS using EP. Suggested areas include:

- Design and development of EP taxonomy for using comprehensive Expert Systems to deliver just the right cyber security defense for an attack identified by MFP/FFT paradigm.
- Development of the next version of FFT simulator with many more parameters possibly expanding the scope beyond security domains, such as performance and efficiency.

References

[1] Mediated overlay services (MOSES): Network security as a composable service, Sarnoff Symposium, 2007 IEEE, April 30 2007-May 2 2007, Print ISBN: 978-1-4244-2483-2

[2] T.Charles Clancy, Nathan Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, Laboratory for Telecommunications Sciences, US Department of Defense, November 2008

[3] John McCarthy and Patrick J. Hayes, Some Philosophical Problems from the Standpoint of Artificial Intelligence, 1969

[4] The Temporal Projection Problem, http://ejap.louisiana.edu/EJAP/1997.spring/copeland976.2.html

[5] McIntire, J.P.; McIntire, L.K.; Havig, P.R., A variety of automated turing tests for network security: Using AI-hard problems in perception and cognition to ensure secure collaborations, Collaborative Technologies and Systems, 2009. CTS '09. International Symposium, Print ISBN: 978-1-4244-4584-4

[6] Lu Simei, Zhang Jianlin, Sun Hao, Luo Liming, "Security Risk Assessment Model Based on AHP/D-S Evidence Theory," Information Technology and Applications, International Forum on, vol. 2, pp. 530-534, 2009 International Forum on Information Technology and Applications, 2009.

[7] Kotenko, I, Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security, Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007. IDAACS 2007. 4th IEEE Workshop, Print ISBN: 978-1-4244-1347-8

[8] The frame problem in Web service specifications, George Baryannis, Dimitris Plexousakis, Proceeding PESOS '09 Proceedings of the 2009 ICSE Workshop on Principles of Engineering Service Oriented Systems, IEEE Computer Society Washington, DC, USA ©2009 - http://dl.acm.org/citation.cfm?id=1564720

[9] A Problem Frame-based Approach to Evolvability: the Case of the Multi-translation Gianna Reggio, Egidio Astesiano, Filippo Ricca, and Maurizio Leotta, 2007, DISI, Universita di Genova, Italy.

[10] What Does the Frame Problem Tell us About Moral Normativity? Terry Horgan & Mark Timmons, December 2008, *Springer Science + Business Media B.V. 2008*

[11] How to stop thinking: A massively modular response to the frame problem, by Stephens, Robert, M.A., Concordia University (Canada), 2008, 101 pages; AAT MR45505

[12] http://www.cs.sfu.ca/~vaughan/teaching/415/papers/dennett-cognitivewheels.html, accessed Oct, 2011

[13] http://www-formal.stanford.edu/jmc/mcchay69/mcchay69.html

[14] Gottfried Leibniz's note in the margin of his Introduction to a Secret Encyclopdia, 1979.

[15] http://www.biometrics.gov/Documents/FingerprintRec.pdf, accessed Oct, 2011

[16] Xilinx Inc. Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet, November, 2004.

[17] Shaikh, R, A Security Architecture for Multihop Mobile Ad hoc Networks with Mobile Agents, Dec 2005, IEEE – INMIC Conference, Karachi, Pakistan

[18] Shaikh, R, The Frame Problem: Description & Study of Simple Solutions, April 89, Polytechinc University, New York, and USA.

[19] Xilinx Inc. Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet, November, 2004.

[20] Alex C. Snoeren†, Craig Partridge, Luis A. Sanchez‡, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, "Hash-Based IP Traceback", SIGCOMM'01, August, 2001, San Diego, California, USA.

[21] http://www.projecthoneypot.org/

[22] Haoyu Song, el, "Fast Hash Table Lookup Using Extended Bloom Filter", Applied Research Lab Washington University in St. Louis, SIGCOMM'05, August, 2005, Philadelphia, Pennsylvania, USA.

[23] http://wolandscat.net/2011/05/24/ontologies-and-information-models-a-uniting-principle/

[24] http://download.cnet.com/Network-Traffic-Generator-and-Monitor/3000-2085_4-10668961.html#ixzz1haWWiVLU

[25] IP Traffic Generator & QoS Measurement Tool for IP Networks (IPv4 & IPv6) from ZTI. http://www.zti-telecom.com/EN/IPTraffic_TM_KeyFeatures.html

[26] http://www.gl.com/ipnetsim.html?gclid=CPWkpM-znq0CFcfe4AodOF68OQ