Generalized Adaptive Security for Computer Systems

H S Srihari[1], Anjan K Koundinya[2], G N Srinivasan[3]

***Abstract*— Developing technologies like the Internet of Things (IoT) and the advent of Big Data Analytics have posed newer threats to security and consequently increased the security threat significantly and necessitated a more sophisticated approach to deal with the multitude of devices and systems which connect and communicate online. Thus, the earlier goal of building a robust security solution for a system or application is no longer a valid solution. Instead, the systems these days demand are adaptive solutions which will automatically detect and configure itself for the changing situations. The solution to this challenge needs the applications of soft computing technologies like learning systems and Artificial Intelligence to learn, predict, prevent and defend any unforeseen security threats. This is the goal of the adaptive security mechanism and this paper proposes a model to dynamically change for the security solution for the scenario and the application demand.**

***Index Term*—adaptive security; threat analytics; Machine learning security; aspect-oriented programming**

I. Introduction

The advent of interconnected systems with a multitude of devices and more importantly the connection between these IoT devices and big data has resulted in the need for a security system of incident response which must be modified to adopt the continuous evaluation method which is far more reliable than the traditional approach.

To compete with adaptive products, conventional security software requires extensive self-aware behaviour monitoring for normal system and software actions or, conversely, defining and logging them as out of the ordinary. Adaptive security provides finer-grained controls to adapt to changes in the network and computing environment, as well as dashboards for better monitoring. The software autonomously blocks behaviors but must have the ability to allow for human intervention. Security staff are notified and alerted of new behaviors, which they can selectively allow, to enable continued functioning in the changing environment.

Since many applications are too complex to be solved ad hoc, mechanisms need to be developed to deal with security as a separate aspect. However, the implementation of security mechanisms often interacts or even interferes with the core functionality of the application. This results in tangled, unmanageable code with a higher risk of security bugs. It is imperative that organizations shift their security mindset from incident response‟ to „continuous response‟, where systems are assumed to be compromised and require continuous monitoring and remediation.

H S Srihari is with Dept of Computer Science and Engineering, RV College of Engineering, Bengaluru, India (Email: hssrihari98@gmail.com)
Anjan K Koundinya is with Dept of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru, India (Email: anjank@rvce.edu.in)
G N Srinivasan is with Dept. of Information Science and Engineering, RV College of Engineering, Bengaluru, India

II. Design and Architecture

The design approach to solve an enterprise security issue can be largely done in 2 ways:

A. Use of complex adaptive system
B. Aspect Oriented Programming

A. Complex Adaptive System

The new approach to information security architecture has to try to mimic a complex adaptive system that can adjust to constantly emerging and changing security threats. This is the essence of Adaptive Security Architecture, to serve as the enterprise security immune system.

This can be achieved by developing an Adaptive Security Architecture (ASA), which aims to contain active threats and to neutralise potential attack vectors. Gartner defines an ASA along four security capabilities:

- **Preventive capability**: This is the set of policies, products and processes that prevent a successful attack. Preventive capabilities protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional.
- **Detective capabilities**: These are the controls designed to identify attacks that have evaded the preventive measures and reduce the threat amplification. Detective capabilities provide visibility into malicious activity, breaches and attacks. These controls include logging of events.
- **Retrospective capabilities**: These provide a way to shrink the attack surface, slow the rate of the attack and reduce remediation time. Response/Retrospective capabilities provide the process, procedures and technology necessary to take appropriate action in response to a variety of cybersecurity events. These include forensic investigations, network changes, remediation changes and automated response capabilities.
- **Predictive capabilities:** These capabilities enable the organisation to predict attacks, analyse security trends and move from a reactive to a proactive security posture. Predictive capabilities provide security intelligence from the monitoring of internal and external events to identify attackers, their objectives and methods prior to the materialization of attacks.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

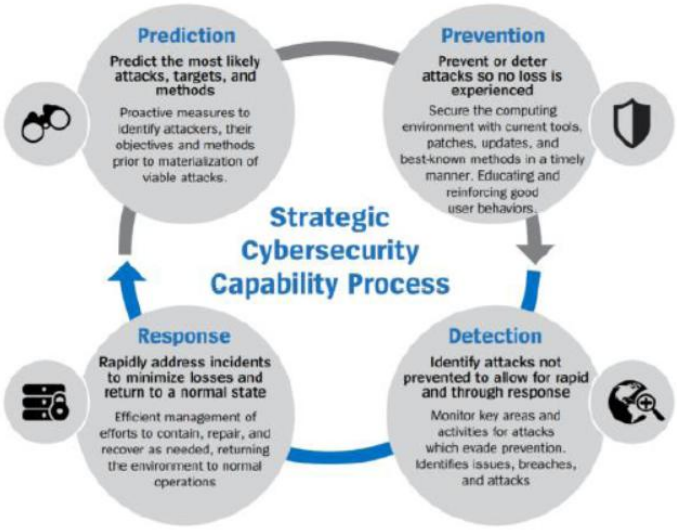

Figure 1: General Process flow for Strategic Cybersecurity

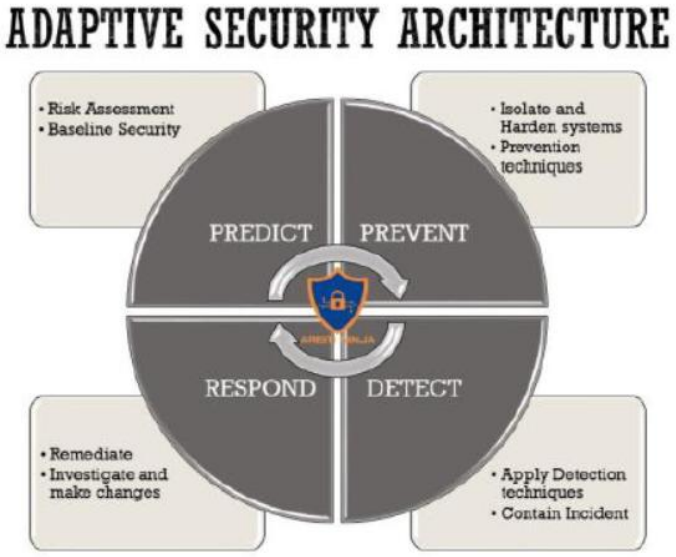

Figure 2: General Process flow for adaptive security

To this end, the key objective of an Adaptive Security Architecture (ASA) is to be able to detect, contain and respond to cyber threats before they cause damage by:

- Continuously monitoring the "entire IT stack"
- Shifting from "incident response" to "continuous response"
- Moving to a "unified" or "integrated" detection, response, prediction & protection capability
- Preventing "successful attacks"
- Reducing the surface and velocity of attacks
- The Adaptive Security Architecture is the enterprise security immune system
- Reducing the Mean-Time-To-Detect Threats (MTTD) and the Mean-Time-To-Respond to Threats (MTTR)

A. Aspect oriented Programming

Aspect-oriented programming promises to tackle this problem by offering several abstractions that help to reason about and specify the concerns one at a time. In this paper we make use of this approach to introduce security into an application. By means of the example of access control, we investigate how well the state of the art in aspect-oriented programming can deal with the separation of security from an application. We also discuss the benefits and drawbacks of this approach, and how it relates to similar techniques.

Adaptive security systems may have to use heuristics to more proactively predict, recognize and deal with threats like malware and hackers autonomously, aside from logging and alerts. Using its heuristics, the system can track its own behaviour and recognize events that are out of the ordinary, tracking the event to its source. Tracking behaviours helps protect against advanced threats far better than traditional security products can protect. Thus, adaptive security products may make virus definitions obsolete.

Intelligent systems usually require additional information not generally accepted as being a justified concern. Due to the general nature of this statement it can be applied to a wide variety of different areas of research that may fall under the general area of Adaptive Security. Such area may include adaptive access control policies where policies incorporate application specific information in policy decisions, adaptive intrusion detection systems which allow individual trust management to conserve processor resources, adaptive agents where the system itself moves between diff erent domains and has to detect and adapt to various malicious scenarios, adaptive security in resource constrained networks where appropriate security protocols are selected at runtime based on the current network conditions and threats adaptive security infrastructures (ASI) where the ASI consists of many security systems which cooperate to ensure minimal policy conflicts and many more.

By its very nature adaptive security systems must be dynamically configurable at run time. Automated runtime security adaptation has great potential in providing timely and fine-grained security control.

Aspect Oriented programming pushes this idea even further by allowing cross-cutting concerns, which could include security, logging, tracing, profiling, pooling and caching among others, to be dynamically added to objects at runtime (or compile time) without the objects needing to have any knowledge of the addition. The implications and usefulness of this paradigm is an active topic for current research.

Further, it is proposed to develop jointly an Adaptive Security methodology/ Architecture to extend non-adaptive legacy security systems with adaptive features and create a design of such an extended system to support the methodology. The study may identify and result in inventing newer additional key components necessary for the creation of an adaptive security system.

III. Adaptive Design for Computing Environment

To completely understand the adaptability of a system, we first need to evaluate the parameters that affect a general system. Some of these parameters include implementations of big data and network security analysis. These parameters include:

- Network usage
- Resource usage
- Buggy Software
- Unified data management platform;
- Support for multiple data types, including log, vulnerability and flow;
- Scalable data ingestion;

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- Information security-specific analytics tools; and
- Compliance reporting.
- update anti-virus software regularly,
- back up critical data,
- use a firewall.

Table 1: Threats can be due to the factors stated below

Behaviour	Level 1	Level 2	Level 3
Update security patches for OS	✓		
Scan with an anti-spyware program	✓		
Use a pop-up blocker	✓		
Use a spam filter	✓		
Use a firewall	✓		
Erase cookies	✓		
Update virus protection software	✓		
Update security patches for Internet browser	✓		
Scan computer with a browser hijack eraser	✓		
Carefully read license agreement before software download		✓	
Verify identity of a website		✓	
Carefully read website privacy policies before filling in online forms		✓	
Verify a website privacy seal		✓	
Change passwords		✓	
Back up files regularly		✓	
Increase privacy settings in browser		✓	
Send credit card number over an unsecure connection			✓
Open an email attachment I am not expecting			✓
Click inside a pop-up window that opens unexpectedly in browser			✓
Switch to a different OS			✓

Equations

Based on the parameters stated in the table above, we can generalize the dependency of a security system on the basis of the below formula:

$$\mu_e = Factor_1 + Factor_2 + Factor_3 + Factor_4 + \ldots.. + Factor_n$$

$$\mu_e = \sum_{i=1}^{n} Factor(i)$$

Where, Factor 1 may be resource utilization
Factor 2 may be network utilization
and so on…
Factor „i" may be a dependent parameter

The result of the above is compared with security levels defined over particular ranges. The security levels are derived from μ_e and then the resultant solution is classified into:

a) Level 1
b) Level 2
c) Level 3

After being classified as a particular security level, the adaptive security system adapts itself to intuitively tackle the security threat as per the level.

IV. Conclusion

The security adaptability is the key to the modern complex systems with heterogeneous environmental constraints. This leads to the intelligent ways of dealing with security crises or breach in any enterprise environment. The design of the adaptive layer is to be incorporated in the application as well as on the underlying network. The need of the hour is to find multiple factor of influence in the security breach and how to over-come them. This leads to perfecting the factor calculation for generic computing environments and thereby improving the adaptive security design. Covering all factors are important and challenging too.

Acknowledgement

Dr. Anjan K Koundinya would like to thank Late. Dr. V K Ananthashyana, Former Head, Dept. of CSE, MSRIT for igniting passion for research.

References

[1] D. Gollmann, "Communication'S Security on the Internet," Software Focus, 2011
[2] K. Solic and V. Ilakovac, "Security Perception of a Portable PC User (The Difference between Medical Doctors and Engineers): A Pilot Study," Mediciniski Glasnik, vol. 6, no. 2, pp. 261–264, August 2009.
[3] The National Academic Press, "Criteria to evaluate Computer and Network Security", 1991, pgs 124-128
[4] Mark S. Merkow, Jim Breithaupt, "Information Security: Principles and Practices", 2014, Chapter 6
[5] Sameer Nanda, TATA Cyber Security Community, "15 Parameters. To Evaluate A Vulnerability Management Tool", 2016
[6] Rob van der Meulen, David Cearley "Build Adaptive SecurityArchitecture Into Your Organization", 2017, 4 Stages of Adaptive Security Architecture
[7] A Shnitko, "Adaptive Security in Complex Information Systems", 2003