AIVRTEK Autonomic Cyber Security (ACS): The Next Generation Paradigm to Secure and Protect Computers, Networks, Applications and DATA

www.avirtek.com

Problem Statement

The current cybersecurity techniques are mainly labor intensive (e.g., patch update), signature based, and not flexible enough to handle the current cyberspace complexity, dynamism, and epidemic-style propagation of attacks. Furthermore, the organization boundaries are gradually disappearing so that the idea of creating a defendable perimeter becomes useless and, on top of that, the cyber-attackers that we need to protect against can be insiders who are trusted and have full access to computing system resources and services. Consequently, it is not feasible anymore to rely on human-manual-intensive management tasks that have failed to promptly secure our cyber systems and services. It is critically important that we develop an autonomous decision making system that can adapt, react, and learn from real-time computer systems.

Limitations of Current Cyber Security Solutions

Current cybersecurity technology and tools have failed for many reasons, some of which are:

- They are mainly signature based solutions that cannot detect new and novel cyber-attacks
- They use many isolated and heterogeneous tools for monitoring performance, fault, and security that make it extremely difficult for human to comprehend and manage in a timely manner
- They are typically developed as threat response (defensive) technologies that inherently cause operational issues as they 'respond and repair' attack damages.
- They are manually intensive activities that make them too slow to respond and act in a timely manner against malicious threats (e.g., according to a recent survey of 50 benchmark companies, the average detection of a cyber-attack is 18 days and more than 200 days for detecting an insider threat if successful).

AVIRTEK Autonomic Cyber Security (ACS)

The human immune system is incredibly efficient in detecting self- and non-self entities in our bodies. Once a non-self entity is identified, it will immediately by certain types of cells to remove the intruder entity before it can cause damage. Our immune system has components that not only identify non-self entities, but also recall old recognized non-self entities that may not have been encountered for a very long time. The AVIRTEK ACS architecture is motivated by principles of the natural immune systems and a computational understanding of such systems. The simplified schematic of a biological immune system is shown in Figure 1 and it highlights the key functional elements of such a system with: (i) Dendritic cells – that devour intruders to activate the immune system; (ii) B-Cells – that search for antigens (attacking elements) and lead to producing antibodies (via cloning of plasma cells) that can seek intruders and help to destroy

them; (iii) memory-cells cloned from B-cells lead to learning attacks for future response, and (iv) T-cells – that includes helper cells to trigger and coordinate B-cell activation and killer T-cells that destroy intruders. It only seems natural that a similar approach would be useful for identifying and fending off intruders in a computer network.

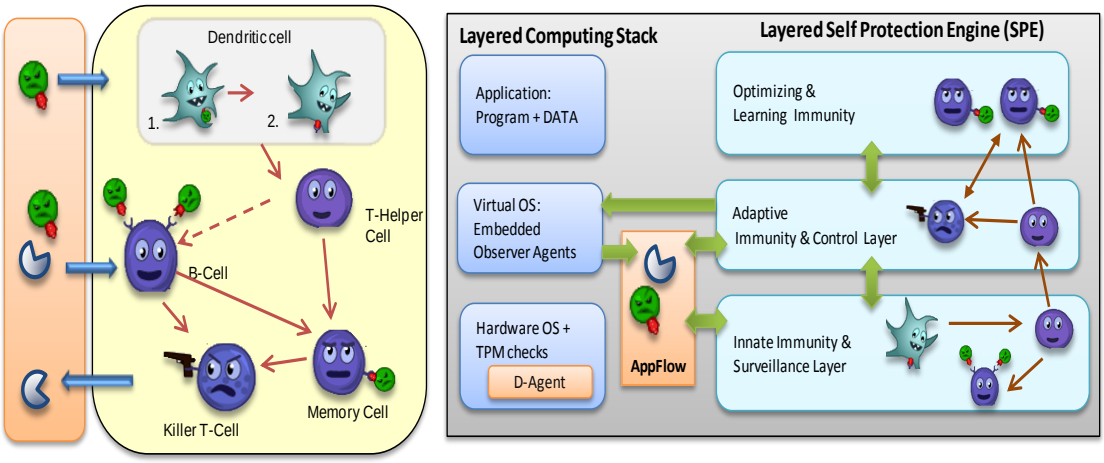

Figure 1: Human immune system

The domain of cybersecurity can significantly benefit from having a framework that is able to self-identify, self-react and self-adapt to malicious behaviors. AVIRTEK ACS technology is inspired by our immune system that leverages machine learning and Artificial Intelligence (AI) techniques to immediately identify malicious behaviors that are threats to users, computers, applications and data.

AVIRTEK has developed an innovative Autonomic Cyber Security (ACS) technology that is a true alternative to the existing cyber security technologies. ACS will revolutionize the way we secure and protect our cyber resources and services. It can efficiently and cost-effectively address the current and future challenges of cybersecurity. Like our immune system, AVIRTEK ACS continuously monitors the managed cyber resources or services and selects appropriate features to perform real-time anomaly behavior analysis so that it can take proactive actions to bring the system into normal operational regions once an anomaly is detected due to intrusions (known or unknown), faults, or accidents (malicious or natural) without the conscious involvement of users or system administrators. The ACS will provide the following innovative capabilities:

- *Self-Recognition Flows (SRFs):* These data strutures can be programmed to collect information about any cyber system or user to build the required SFR data structures that will be used to identify any non-self-behavior by the monitored systems or users.
- *Self-Recognition Agents (SRAs):* These agents will perform innovative data analytics algorithms to build self-behavior models for computers,

applications, and users. The SRAs will proactively detect any anomalous behavior (non-self behavior) by computers, users, and applications that might have been triggered by malicious actions.

- *Self-Protection Agents (SPAs):* These agents will provide automated/semi-automated actions to proactively protect computers, users, and applications against malicious attacks, and recommend actions that can be taken to resume normal operations or mitigate their impacts.

ACS Platform Architecture

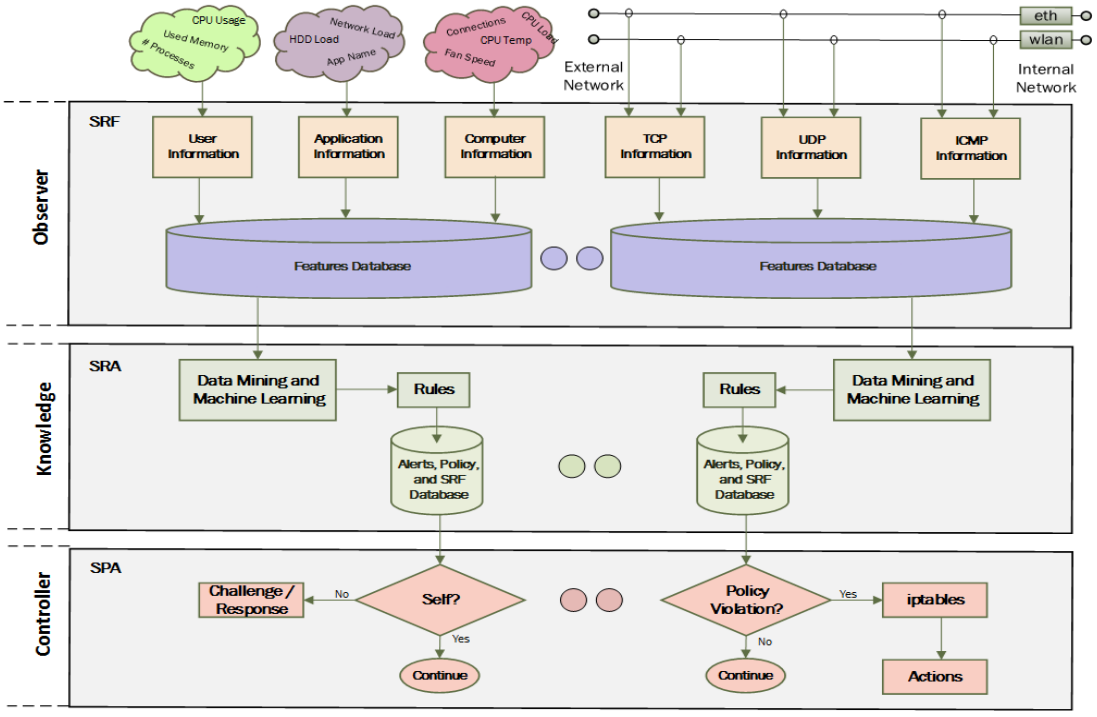

Figure 2: Autonomic cyber security development approach

Figure 2 shows the ACS architecture that has been developed by AVIRTEK. Working from top down, the software monitoring agents collect raw data that are used to build the *Self-Recognition Flows (SRFs)*. User, Application, Computer, TCP, UDP, and ICMP SRFs are inserted into the Features Database. The information gathered by the Observer module is passed to the Knowledge module in which data mining and machine learning tasks are performed. These tasks will produce specialized *Self-Recognition Agents (SRAs)* to detect any "non-self" behavior of the objects being monitored and analyzed, and alerts will be generated that are then stored in the Alerts and policy database. The *Self-Protection Agents (SPA)* will use the alert and policy information in this database to determine the appropriate recovery actions to be taken in response to each alert. To reduce the false alarms, especially for "non-self" user behavior, the SPA will launch the Challenge/Response application that forces the user to prove "Self". In the case of a

network protocol policy violation such as TCP, UDP, or ICMP, the SPA can modify the firewall to block the network port and deny access to resources on this system.