Defense as a Service Cloud for Cyber-Physical Systems

Mohamed Azab
Bradley Department of Electrical
and Computer Engineering, Virginia Tech
Email: mazab@vt.edu

Mohamed Eltoweissy[1]
Pacific Northwest National Laboratory
Email: mohamed.eltoweissy@pnnl.gov

Abstract— Modernizing our critical infrastructure often involves upgrades with Cyber-Physical Systems (CPS) to enhance efficiency, safety and reliability. New security and resilience requirements and challenges arise given the mission- and time-critical nature of CPS applications. These applications are always targeted by sophisticated persistent attacks exploiting potential cyber-physical integration vulnerabilities. In this paper, we present CyPhyCARD (Cooperative Autonomous Resilient Defense "CARD" platform for Cyber Physical Systems) as a resilient and secure defense cloud. The foundation of CyPhyCARD is our Cell-Oriented Architecture (COA) that enables distributed, dynamically configurable, and runtime-programmable platforms. COA comprises composable intrinsically resilient, active components termed "Cells" that dynamically manage heterogeneous resources and executable software code variants to execute CyPhyCARD defense missions. CyPhyCARD uses our generic Evolutionary Sensory system (EvoSense) to circulate context-driven, functionally customizable sensors and effectors through the target of defense. EvoSense provides cooperative autonomous control and sharing amongst interconnected defense service providers (CyPhyCARD) and/or their target of defense to enhance attack detection and deterrence. Further, CyPhyCARD uses our ChameleonSoft system to secure its infrastructure of cells. ChameleonSoft is a multidimensional software diversity system that autonomously induces runtime confusion and diffusion thereby, in effect, encrypting the spatiotemporal software behavior and realizing a moving target defense. Both EvoSense and ChameleonSoft are built using the COA. CyPhyCARD is designed to increase the cost for the attacker at all times through persistently asymmetric operations achieved, in part, using a moving target defense construction and automated recovery provided by ChameleonSoft; rabid global attack detection and mitigation through EvoSense; and Operation resilience in presence of attacks using attack containment and honeypots defense missions. We demonstrate, using an attack scenario, how our proposed solution reacts to threats targeting CyPhyCARD and/or its target of defense systems.

***Keywords*—Cyber Physical Systems, Security, Resilience, Cloud Computing, Autonomic Management.**

I. INTRODUCTION

Cyber Physical Systems (CPS) are increasingly becoming indispensible to our critical infrastructure and defense domains, ranging from smart grids and smart healthcare to smart cities and smart warfare. CPS come with large-scale heterogeneous compositions of interacting cyber and physical devices with differing capabilities and requirements. Securing these heterogeneous compositions remains a challenge especially with the significant increase in cyber-physical attacker/attack sophistication. CPS attacks usually target valuable infrastructure assets taking advantage of potential weaknesses in their defense systems. Such weaknesses might arise from the exponential increase in the volume of information flowing between cyber and physical processes that exceeds the analysis and investigation capabilities of the current defense solutions [1,2]. Further, these solutions mainly employ different approaches in provisioning security to the cyber and physical components of the CPS. Isolating the cyber and the physical defenses leads to unjustified waste of resources that might result from duplicating security measures. Additionally, it increases the possibility of conflicts between security commands. An adversary might induce such conflicts to facilitate system penetration. These ad hoc mixtures of security tools have negative impacts not only on security aspects but also on related system qualities like performance, management and resilience.

Recent research argued against the suitability of the current security solutions to CPS environments [1, 2]. We assert the need for new defense platforms that efficiently coordinate defense missions and tools in real-time.

In this paper we present CyPhyCARD (Cooperative Autonomous Resilient Defense platform for Cyber-Physical Systems) - a biologically-inspired distributed, dynamically configurable, runtime programmable platform that manages a large number of cyber and physical resources and service upon which evolutionary defenses can be built to protect participant organizations. CyPhyCARD is founded on our Cell-Oriented Architecture (COA).

COA entails a biologically-inspired, distributed construction of composable basic building components termed "cells". Cells are dynamically configurable and runtime-programmable active components with self-monitoring, context-aware adaptation capabilities. Cells adapt to changing internal and external conditions and acquire resources on demand based on the dynamics of the task on hand. Cells are composed into dynamic structures, termed organisms. An Organism binds to defense mission/application role(s) at runtime and recruits cells running on one or more host machines for its operation. Application roles are defined into different software variant sets targeting different system quality attributes. The key principles are decoupling functional roles and runtime role players; separating logic, state and physical resources; and employing functionally-equivalent, objectively-different code variants sets targeting different quality attributes. Cells regularly change their targeted quality attribute by changing their current active variant set in order to match the frequent change in their working context.

[1] The author is also affiliated with the Bradley Department of ECE at Virginia Tech and the ECE Department at University of Arizona

COLLABORATECOM 2011, October 15-18, Orlando, United States

DOI 10.4108/icst.collaboratecom.2011.247118

In addition, CyPhyCARD uses our generic Evolutionary Sensory system (EvoSense) to facilitate pervasive monitoring and analysis as well as early attack alert. EvoSense realizes early attack alert by enabling trustworthy cooperative control and sharing of defense intelligence amongst interconnected CyPhyCARDs and/or Target of Defense systems (ToDs). The goal behind that is to enhance attack detection and deterrence. EvoSense emphasizes privacy preservation by employing inspection organisms to autonomously check organization border crossing data against applicable privacy policies. EvoSense induces bloodstream effect by circulating elastic context-driven, functionally customizable sets of sensors and effectors "like white blood cells" throughout the target system. EvoSense intelligently manages and controls the current conventional attack detection (sensing) and resolution (effecting) tools for the purpose of mixing theses tools into different blends composing new sensing and effecting tools with appropriate features.

Further, CyPhyCARD uses our ChameleonSoft software defense system to secure its infrastructure of cells. ChameleonSoft employ runtime multidimensional software diversity to induce confusion and diffusion to, in effect, induce spatiotemporal software behavior encryption (ChameleonSoft Behavior Encryption (or CBE)) and a moving target defense. In time ChameleonSoft shuffles functionally-equivalent, behaviorally-different code variants to encrypt the execution behavior in order to hide software flaws. In space ChameleonSoft distributes shuffling commands through the network in a way that makes the attack target (possible flaws) in a continuous random motion. ChameleonSoft can autonomously mange runtime cell migration between remote hosts to induce more space diversity.

ChameleonSoft is also equipped with an autonomic multimode failure recovery mechanism for enhanced resilience. Recovery modes include a coarse grained failure recovery for resource constrained environments, and a fine grained failure recovery for mission critical applications. Nodes employing ChameleonSoft autonomously and cooperatively change their recovery and encryption policy both proactively and reactively according to the continual change in context and environment. CyPhyCARD is designed to provision defense services without sharing the Target of Defense (ToD) network or resources. The reason behind that is to isolate defense provisioning workload from the ToD network. Additionally, this isolation complicates defense system penetration using compromised ToD hosts.

CyPhyCARD provides a distinct CPS security solution through its high situational awareness capability. The decision making process in CyPhyCARD is primarily based on the dynamic evaluation of the current situation at the event point. Further, the system considers historical events locally within the event enclave and globally over multi enclaves' history of events with similar event context.

The main contributions in this paper are outlined as follows:

- A biologically inspired cloud architecture supporting mission-oriented application design and inline code distribution to enable adaptability, dynamic re-tasking, and re programmability;
- Target of defense isolated, unified, intrinsically resilient adaptive defense service provisioning for enhanced security, optimized performance and resilience targeting multi enclave heterogeneous CPS platforms;
- Persistently asymmetric defense (high cost to attacker at all times);
- Enabling trustworthy cooperative autonomous control and sharing;
- Multi-organization situational awareness for intelligent decision-making.

The remainder of this paper is organized as follows. Section II describes an attack scenario on a ToD system. Section III presents our CyPhyCARD platform project. Section IV discusses CyPhyCARD response against the presented attack in Section II. Section V explains the evaluation of CyPhyCARD from the performance and security perspectives. Section VI discusses related work. Finally the paper concludes in Section VII outlining ongoing and future work.

II. ATTACK SCENARIO: THE BLACKWIDOW WORM

In this section we present a synthetic attack scenario on a CPS protected by conventional defense systems. The rationale is to demonstrate weak points in current defense systems that might facilitate penetrating their target of defense. After describing CyPhyCARD in Section III, we will revisit the scenario and show how CyPhyCARD may mitigate such attack in Section IV.

Attacker tools and capabilities

- Zero-day system exploits
- Social engineering methods to recruit insider agents via social networks
- Well trained and funded attackers
- Stolen certificates and digital keys
- Small lab to mimic the attacked system and its defense system

Design aspects

The attack is designed to be stealthy by hiding from the defense system sensors searching for attack signatures. The attack will target an intermediate host machine that will contain the worm and command and control channel communications.

In order to do so, the worm is designed to not harm the host or change any of its settings that might raise the Anti-Malware (AM) alerts. The malware will use minimal resources and will work in a very slow fashion not to alert the network defense systems by its existence.

The only way to detect this malware is through deep analysis of the logs of all the communicating nodes, which is computationally very costly to the current systems that share the same host machines. Further, in order to deeply analyze and correlate strange communications patterns spreading all

over the network, a global view for all the communicating entities within the network will be needed.

The worm is later updated to use stolen digital certificates to authenticate its existence in the host machine in the form of drivers.

The malware is intended to be targeted, but due to the intentionally random deployment method, the code works in two modes as follows: (1) Benign mode where the malware infects other machines that do not belong to the target space. The machines might be used later in case of target change, or as a base for future attacks; and (2) Malicious mode, where the worm works only on the target host systems. The attacker feedback can determine the mode. The default will be benign unless the attacker changes that or predetermined targets have been programmed.

Attacker assumptions:

- The defense system shares the same network or host with the target of attack/defense system.[Note: defense system might be exposed to attack by compromising the ToD.]
- The attack target defense system, or major parts of it, uses COTS security products.[Note: A majority of defense systems are signature based, so that is probably easily to bypass with custom code.]
- The system is not capable of being fully situation aware of all its components in a massive-scale network in real time.
    - Building a very slow motion worm will increase the log file sample size needed to detect it.
    - Spreading the attack in small parts hosted in geographically remote hosts makes it more difficult to detect attacker activity unless a deep nearly network-scale analysis can be conducted to correlate all disparate logs.
- The defense system management workstations (that the administrators use) share the same network with the target of defense. [Note: Stolen passwords can simply be used to modify rules of IDS, routers, switches, firewalls, proxies, etc.]
- It is not feasible to monitor all the host behavior patterns while sharing the same workstation that is performing user tasks.
- Defense systems are not resilient against attacks, and have weak recovery mechanisms. [Note: most of them assume that they will not be the target of an attack as long as they were able to secure their ToD. Additionally, usually they have no intrinsic failure recovery.]
- Cyber security is oblivious of and is not coordinated with physical security to protect the target cyber-physical system. Human intervention is need to facilitate such coordination.[Note: the attack can make them conflict with each other to bypass both of them.]

Players:

The attacker is a sophisticated hacker group hired by XYZ, Ltd. to conduct industrial espionage and stealthy denial of service against ABC, Inc. and related firms. XYZ has two goals: foremost it wants to steal proprietary information from ABC. Second, it wishes to disrupt ABC's operations giving XYZ a competitive advantage.

The victim is ABC, Inc. and its competitors and business partners. ABC is a multinational organization. It has a well-connected set of branches that are distributed over multiple countries. These branches contain interconnected cyber and physical components.

The(synthetic) **Black Widow malware** (BlackWidow for short) is an attack that is designed to split into a set of parts and spread in different directions and locations to decrease the probability of detection and increase the probability of success. The distribution of parts and the interconnection between parts in different hosts forms a large spider-web, this web is bi-directionally traversed to send any harvested data to the attacker, and to update the malware with new tools and missions.

Attack procedure (on Air-gapped Target)

The attacker uses phishing attack that targets users' emails and social network personal pages. The attacker uses social networks as a source of information to generate more convincing phishing emails. These emails will be directed from one of the closely related contacts to the victim.

The attacker selects a group of employees working in different branches of ABC. These branches are distributed in various geographical locations, and the victims that will be the malware couriers have no direct relation with each other. This will increase the chance of the attack's success in case that the same phishing technique is used with different targets.

The attack victims will receive parts of the malware. Each of these parts will contain a fraction of the designated mission and a simple communication module. The communication module will be used to open direct channel with the attacker and to search and establish communication with other parts. Directions to other parts' locations might be sent by the attacker to minimize the search time.

The attacker uses malware fractions to construct logical executable entities in the form of mobile software agents targeting different objectives. The first objective will be to search and infiltrate the network for data stores.

The malware will sniff network traffic searching for predetermined signatures for such locations. The second objective will be to attack such data stores using the zero day exploits and the stolen certificates to locate targeted industrial secrets, and any available access keys to the protected area behind the air gap. The malware will frequently update the attacker of its findings based on a predetermined update methodology.

After successful reception of this data, the attacker will use it to generate legitimate keys to access the air gap.

The attacker will use the malware to locate the workstations controlling the surveillance cameras. In locations with no surveillance cameras the malware might use any available user connected web camera. The malware will record periodic video feeds to be sent to the attacker. These videos with the help of the attacker generated access keys will guide a recruited insider into infecting the air gap with a copy of the BlackWidow.

The malware controlling the video cameras will make sure that this process will not be recorded on any of the cameras to protect the recruited insider.

The air gap malware is programmed to increase the operational hours of certain machines that use specific raw materials manufactured by XYZ to increase XYZ profits. The malware can easily identify such machines by searching a predetermined fixed identifier that must be added to all the programming files targeting such machines. Further, the attacker will use the stolen secrets and designs to equip the malware with the needed logic to randomly manipulate the operational motors frequency in the production machines to induce random defects in the output products to lower its quality. Doing so shall cause multiple financial problems to ABC. XYZ shall benefit from ABC's loss due to its low quality products. Additionally XYZ will maliciously gain both financially and more control over ABC's production lines by, for example, carefully adjusting the amount of consumed and supplied raw materials.

III. THE CYPHYCARD DEFENSE CLOUD

CyPhyCARD is a distributed, dynamically configurable, runtime-programmable platform that manages heterogeneous resources (software and hardware) shared among multiple evolving applications representing defense missions. CyPhyCARD is designed to work in total isolation from the target of defense.

CyPhyCARD aims to achieve the following goals:

1. Achieve asymmetric advantage to CPS defenders, prohibitively increasing the cost for attackers;

2. Ensure resilient operations in presence of persistent and evolving attacks and failures; and

3. Facilitate defense alliances, effectively and efficiently diffusing defense intelligence and operations transcending organizational boundaries.

To attain these goals, CyPhyCARD adopts a novel biologically inspired construction of adaptive system building components, namely the cells. Cells are the basis of our Cell-Oriented Architecture (COA) that enables CyPhyCARD's online programming, adaptive resource allocation and dynamic re-tasking.

CyPhyCARD Apply ChameleonSoft to secure its infrastructure. ChameleonSoft employ spatiotemporal diversity to hide software flaws from attacker reach. Further, it enhances the platform resilience by multimodal automated recovery.

CyPhyCARD uses EvoSense circulatory system of lightweight virtual sensors and effectors to monitor and configure the target of defense and to interface with other CyPhyCARDs. The next subsections overview the COA followed by a description of the CyPhyCARD architecture, EvoSense , and ChameleonSoft.

A. *The Cell-Oriented Architecture (COA)*

The COA employs a mission-oriented application design and inline code distribution to enable adaptability, dynamic re-tasking, and re-programmability. The cell, is the basic building block in COA, it is the abstraction of a mission-oriented autonomously active resource. Generic cells are seamlessly created by the middleware. Then, they participate in varying tasks through a process called specialization. Stem cells are generic, unspecialized cells that abstract cloud nodes' resources, and they can encapsulate any of these resources to represent a component in a dynamic structure termed organism.

Once specialized, cells exhibit application-specific behavior. Specialized cells have mission objectives that are being continuously sought. The cell monitoring and analysis components are used to monitor performance parameters, mission objectives, and other phenomena of interest to dynamically adjust the cell performance parameters inducing better self and situational awareness.

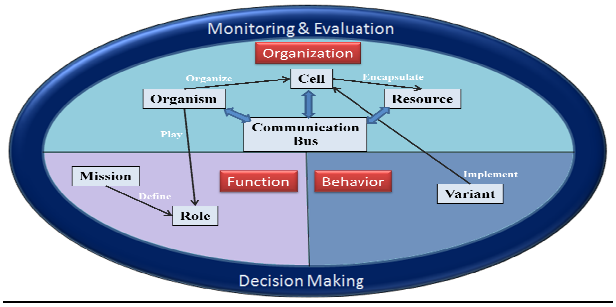

Figure 1: Components of the COA

We visualize applications built over our COA as a group of cooperating roles representing a set of objectives. An organism represents a role player that performs specific mission tasks. An organism is bound to a functional role at runtime. An organism might be composed of a single cell or multiple cells based on its objectives.

The system components are under fulltime monitoring and evaluation for situational awareness and automated failure recovery. Fig. 1 illustrates the COA components.

B. *The CyPhyCARD Architecture*

CyPhyCARD is a Biologically-inspired Autonomic Resilient Cloud platform inspired, in part, by biological organisms that use a variety of techniques to tolerate environmental changes and avoid and mitigate attacks from microorganisms and predators. CyPhyCARD cloud can be expressed as a Defense as a Service (DaaS)_cloud, where the service providers provision defense services to their clients.

The CyPhyCARD cloud uses a customized mission

interpreter to generate a set of manageable mission specific applications executing over our middleware installed on the cloud nodes. The middleware expresses these missions in the form of a set of interacting roles executed ubiquitously on top of a set of role-playing organisms.

CyPhyCARD leverages the COA efficient dynamic reconfiguration ability to achieve high degree of decoupling between functional roles and the underlying active resources (cells). This decoupling enables runtime reassignment of roles for better resource sharing, and platform-managed services like replication, dynamic resource-allocation, and re-tasking. The runtime binding of cells is facilitated by contracts. A cell begins its functionality by loading one or more implementation variants that carry out the cell contracts.

CyPhyCARD comprises two major components namely, programming framework that is responsible for defense mission interpretation to defense roles, and a middleware that facilitates cell hosting over cloud and ToD nodes. On the ToD side, the middleware facilitates ToD-based cell composition of logical sensors and effectors. These ToD-based cells cooperate with CyPhyCARD cells to execute defense missions.

C. The CyPhyCARD programming framework

CyPhyCARD exploits COA to enable the construction of platform applications from loosely coupled elements, in the form of roles. The framework separates the functional design aspects from the structural and behavioral aspects. The framework enforces strict separation between functions and processes (roles and their players). Roles define responsibilities and plans, while organisms claim the responsibilities and execute the plans. The dynamic role/organism assignment provides functional elasticity and promotes reusability of role-plans. It also promotes structural plasticity of the software components facilitating evolution. Further, it allows the application designers to focus on the application logic rather than the underlying available networked resources.

The application is viewed as a graph of functional roles executed by players. The binding between roles and players is managed and regulated at runtime. Such collaboration-based design suits self-managed, self-optimized distributed applications like CPS defense that might involve network health monitoring, accounting, resource management, and progressive software updating.

The **Middleware** functionality is split among a minimalistic kernel installed on all platform nodes and ToD nodes. The middleware is designed to facilitate dynamic deployment of roles at runtime. The middleware kernel, referred to as CC-DNA, is concerned with the essential functionalities required for a node to participate in the CyPhyCARD cloud. CC-DNA realizes another layer of CyPhyCARD intrinsic separation of design concerns by autonomously resolving host heterogeneity issues. CC-DNA constructs a uniform platform for hosting CyPhyCARD cells on cloud nodes, and EvoSense sensor and effector cells on ToD host nodes. CC-DNA functionalities include communications, acquisition and execution of roles, and profiling of the available resources that the node is willing to share with the cloud. CC-DNA is the only piece of software that is required to be preinstalled on platform or the ToD nodes. The rest of the middleware services are implemented as functional roles. The middleware roles adapt and evolve in a similar way to the application roles.

CyPhyCARD uses EvoSense bidirectional streams of logical sensors and effectors to execute defense missions. The CC-DNA installed on the ToD hosts enables EvoSense to deploy sensors and effectors cells. These cells shall abstract the host resources to sense certain phenomena of interest or to execute a set of commands.

CyPhyCARD defense missions use EvoSense sensors to collect status reports from the ToD cyber and physical components. These reports are autonomously analyzed at runtime for malicious behavior. In case of attack detection, defense missions use effectors to reconfigure the host, host network, and digitally controlled physical components for attack mitigation, containment, and deception.

Fig. 2 shows CyPhyCARD defense cloud using EvoSense circulating sensors and effectors to provide defense services to multi-enclave CPS.

Figure 2: CyPhyCARD

D. EvoSense: Evolutionary Sensory System

EvoSense is designed to enable CPS defense platforms to apply real-time pervasive monitoring and analysis techniques along with autonomous context-aware defense service provisioning. EvoSense circulates defense tools, similar to "white blood cells", through the ToD to detect, contain and resolve possible attack attempts.

EvoSense leverages the conventional defense tools - (ToD immune system) along with customized evolutionary defense and control tools (or vaccine) to enable what we call "immune

system vaccination" effect. EvoSense autonomously updates the conventional defense tools databases with the newly generated vaccines to produce long lasting defense. This is similar to the biological vaccination process; where vaccines are used to update the biological immune system database with long lasting new defense tools.

The goal of this vaccination process extends beyond immunizing a single body to immunizing the whole community of systems. EvoSense is designed to enable autonomous trustworthy information sharing between the defense community members "cooperating defense systems". EvoSense trustworthy information sharing mechanism will distribute vaccines between cooperating community members in order to create and maintain a healthy community.

EvoSense uses its lightweight sensing elements to collect all the needed information from the ToD network and to post this data to CyPhyCARD for deep analysis and investigation. This makes it much easier to work with resource-constraint environments and legacy systems.

In situations where the ToD data is so sensitive to be moved over unsecured communication lines or if the ToD organization's privacy policy restricts moving data outside the organization premises, EvoSense leverages its unified sensing and defense provisioning platform to deploy a group of contracted agents over the ToD network to facilitate local data analysis and investigation.

At successful detection of an attack event EvoSense profiles the attack event to be shared with other cooperating CyPhyCARDs. EvoSense shares only sensors and effectors with event profiles. These shared materials may not contain any private information about the source, only directions, methods, and needed tools for attack detection and mitigation. CyPhyCARD organisms playing clearinghouse roles must authorize such information sharing in order to assure organization's privacy policy preservation. Each cooperating CyPhyCARD have to ask their clearinghouse organisms for permissions before sharing or even employing any shared materials. The clearinghouse organisms will check the shared data against the ToD privacy policy rules. Sharing will only be permitted in case of no privacy violation detected.

E. ChameleonSoft for platform intrinsic failure resilience

ChameleonSoft intrinsically exploits software diversity, runtime code variant shuffling, and fault recovery to achieve the necessary security and resilience for defending mission critical systems. ChameleonSoft uses runtime hot shuffling of similar function different behavior software variants to encrypt the software execution behavior by hiding possible software flaws. This process aims to induce a moving target (a specific software flaw) defense and to dynamically control the system targeted quality attribute (performance, security,..) to match the varying context. ChameleonSoft improves platform availability by providing means of runtime graceful failure recovery. In the next paragraphs we shall give a quick overview on CyPhyCARD's moving target defense system, and the multimodal automated failure recovery mechanism.

The moving target approach:

CyPhyCARD is a software-based defense cloud designed to provision defense services to mission critical CPS. Software attacks are imminent threats to such vulnerable base and sensitive application. Our defense provisioning platform has to be resilient against such threats. CyPhyCARD uses ChameleonSoft to provision such resilience to its security platform. ChameleonSoft leverages the platform loosely coupled, dynamic construction combined with the cell intrinsic separation of design concerns to enable what we term as "ChameleonSoft Behavior Encryption (or CBE)" akin to message encryption.

CBE leverages the COA features to shuffle, at runtime, different functionally-equivalent, behaviorally-different software variants to hide software flaws that attackers target. COA divides the large missions of a huge software program into smaller tasks. Each of these tasks is assigned to one or more COA cells in the form of manually or automatically generated sets of similar function and different behavior executable variants. These sets might have different objectives targeting different quality attributes.

Each cell independently decides its shuffling criteria regarding when to shuffle and the variant/set selection for the next shuffle. Such independent decision making makes the attack target (the buggy variant) appears to be moving all over the network in a flashy look each time a cell selects executing it. In doing so, we induce confusion and diffusion along multiple dimensions. The shuffling scheme, the level of shuffling granularity, and the autonomous decision to shuffle are three of such dimensions.

The scope of shuffling might extend beyond security goals to other quality attributes like reliability, performance, robustness, mobility, etc. The system might shuffle to a variant that aims at high system performance in overloaded but low security risk situations. Alternatively, the system would resort to a higher security, perhaps lower performance variant in higher risk situations.

ChameleonSoft automated failure recovery mechanism

Diversity was widely investigated in the literature. Multi-variant approach without appropriate recovery mechanism might face a larger number of coincidental failures [2]. Further, defense platforms should always expect multiple induced failures as a result from attack attempts. Therefore, CyPhyCARD uses ChameleonSoft autonomous, dynamic, situational aware, multi mode failure recovery mechanism to resolve possible failures. A major outcome of this recovery mechanism is the failure resilience enhancement not only against coincidental failures, but also against malicious induced failures by adversaries.

ChameleonSoft can dynamically and autonomously change the cell recovery policy to cover different fault tolerance granularity levels. Such levels might target reliability, survivability and resource usage optimization. For fine grained recovery against logical failures, a cell can have one or more replicas on the same physical host. Further, for more fine grained recovery against logical or physical node failure, a cell might have one or more replicas on different physical hosts.

In a resource constrained environment, ChameleonSoft can follow a more coarse grained recovery that might save some of the resources used by replicas while compromising some of the execution states. The cell is designed to send a periodic behavior change beacon messages containing its sensitive data, the currently executing set, variant, and the last executed state to be saved on a secure remote data store. In case of failure ChameleonSoft retrieves the last stored message for the failed cell. It leverages the message content and any available communication logs to restore the failed cell to its prior state before failure.

The coarse-grained recovery mode is always on by default enabling the support of multiple concurrent recovery policies. The remote safe store is updated regularly with beacon messages from all working cells. Each cell will independently and dynamically set its own message update frequency. Such update frequency could be influenced by the change of the current recovery policy. The update frequency might decrease in fine grained recovery mode; while they should increase with lower granularity recovery.

ChameleonSoft can change cell recovery policy at runtime to respond to changes in the surrounding environment. For example, in a resource constrained situation, the system might choose the coarse grained mode until more resources are available at which time the system could go for the finer grained mode.

Fig. 3 shows a multi-cellular organism composition. The organism cells are hosted on different physical hosts communicating through an associative communication bus connecting the cell's input and output ports. Based on the cell working context and the criticality of its dedicated task some of the cells are replicated on the same host machine (cells 4 and 9), or different host machines(cells 1 and 8) representing multimode fine grained recovery. In a less hazardous context, particularly with more resource constrains; cells might prefer the coarse grained recovery with no replicas (cells 5, 6 and 7).

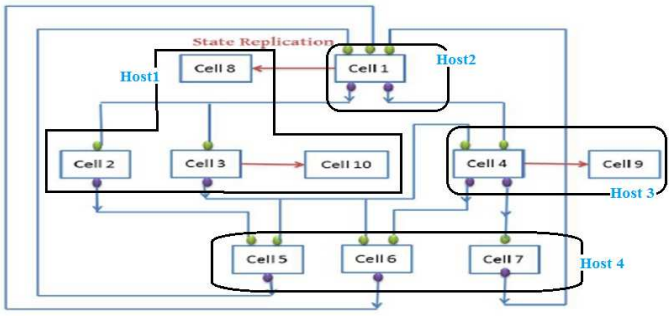

Figure 3: Multi-Cellular Organism

F. Defense provisioning workflow

CyPhyCARD programmers define defense missions in terms of a set of tasks that involve different processes. Data collection, analysis, consulting, sharing, and host configuration for deception, containment, and resolution are examples for such processes. CyPhyCARD represents defense mission as a set of similar function different behavior software variants. Variant generation can be automated; where the interpreter will generate different behavior variants for the same input logic from the programmer. It can also be manually constructed for more induced behavior deviation between variants.

CyPhyCARD programmers leverage the CC-DNA features to deploy EvoSense sensor and effector cells over the ToD host. These sensors and effectors shall be used by defense missions for purposes of monitoring, evaluation, and configuring of the host.

The CC-DNA installed in the host holds different sets of sensors and effectors APIs. These APIs combined with any other needed resources (physical resources, conventional defense tool etc.) is abstracted at runtime to construct the sensor and effector cells. Programmers will use a customized programming language to define the workflow of these cells and the needed sensors and/or effectors to execute its task. EvoSense will receive the sensors and effectors logic from CyPhyCARD cells and interprets this logic to construct the sensor or effector cells. In COA, resources can easily be acquired when needed. EvoSense might ask the logic reservoir for some sensor or effector APIs that are required to execute a designated sensing or effecting mission in case they were not already available on the targeted host.

In case of successful detection of a malicious act, EvoSense shall profile the sensing and effecting logic used for such detection and resolution to be shared with other cooperating CyPhyCARDs. Similarly, CyPhyCARD might ask other cooperating CyPhyCARDs for a specific resolution methodology (sensors or effectors APIs, resolution tools,...) for a newly detected malicious behavior with no available resolution tools.

In CyPhyCARD, sharing or employing shared materials will be permitted only if no violation of the ToD privacy is detected. CyPhyCARD takes that permission by consulting its clearinghouse organisms that will inspect the shared materials against any possible privacy policy violations. Enabling such trustworthy information sharing enhances the detection quality, and minimizes attack dispersion, and detection and resolution time.

```
//sensor 1
For i 1:10
Monitor memory usage (100 ) ->tmp[i]
Delay(10)
End
If (max(tmp)>10)
//sensor 2
        For i 1:10
        Get the maximum memory usage process (100)
        ->tmp2[I,usage]
        Delay(10)
        End
End
//effector 1
Terminate (max_repeated_incident[tmp2])
```

Figure 4: Sensor and effector logic

Fig. 4 illustrates a sample code sent from CyPhyCARD defense mission to EvoSense to construct sensor and effector cell. The cell will wait for threshold crossing and starts searching for high memory usage processes in a 100 sec samples for the duration of 10 mints. The cell will terminate the process with maximum number of occurrence in the high

memory usage processes list.

The next section will present CyPhyCARD's response to the proposed attack in section II.

IV. CyPhyCARD Defense in Action

In this section we shall discuss CyPhyCARD response to the BlackWidow attack presented in Section II. We illustrate how CyPhyCARD will detect, resolve, contain, attribute, and share information of the attack.

Detection: As mentioned before the BlackWidow worm is designed to be stealthy and tricky to deceive the conventional AM programs that detect attacks based on a predetermined behavior pattern or by detecting unjustified actions violating one of the AM rules. The BlackWidow is a custom-made worm with no pre-recorded signatures having no intention of harming or even changing the configuration of the host. A conventional defense system with most resent updates most probably will not detect or suspect the existence of the BlackWidow.

CyPhyCARD is designed to put the whole system under full supervision and periodic investigation. EvoSense circulating streams of sensors regularly scan the ToD hosts, internal, external communications, and physical properties. The sensors collected data from all over the ToD network constructs the raw material for CyPhyCARD deep investigation organisms. Such organisms can construct a global view of the whole system searching for possible indications for malicious behaviors. Such indications will direct EvoSense sensors to collect more information about such strange phenomena. For example, communication-logs-inspection sensors might report the incident of multiple transfers of a single file locally within the network, or the establishment of a communications path between the ToD workstations and unknown source. Another sensor that investigates the state of the supervision cameras will notice the manipulation and control attempts to these cameras, which will raise alerts asking for deeper investigation.

Resolution, containment and attribution: CyPhyCARD detected suspicious data will raise alerts for more deep investigation to track the source behind such suspicion. The tracking process might be as simple as a deep analysis of multiple log files or as complex as applying deception measures to uncover the sources of such actions. After identifying the possible area of threats, CyPhyCARD starts the isolation and containment procedure. Through this process CyPhyCARD uses EvoSense effectors to control the infected hosts, and communications elements to block or redirect communications away from the infected area. CyPhyCARD might use EvoSense effectors to reconfigure the infected hosts and even the physical properties to construct honeypots for attacker attribution. In mission critical applications, CyPhyCARD can maintain operation by means of replication, communication and execution filtration, and workload redistribution to healthy machines. The resolution process might be as simple as rolling back any delectated commands issued by the worm to a full system restore.

Sharing attack profile: After successful attack detection or at times of reasonable suspicion, EvoSense generates records for the attempted attack, any useful sensors and effectors used for detection or resolution, and the detection and resolution procedure. CyPhyCARD clearinghouse organisms will examine such information for possible ToD privacy policy violation. In case no violation is determined, CyPhyCARD will share these records with other cooperating CyPhyCARDs. The receiving party's clearinghouse organisms will check these records against their respective privacy policy rules. In case of no violations, the records are used to guide the detection and resolution process of the BlackWidow worm in their respective ToDs.

Platform resilience: CyPhyCARD works in total isolation from the ToD communicating only through sensor and effector streams. Such isolation makes CyPhyCARD virtually immune against ToD infections. An attacker targeting CyPhyCARD itself should face its moving target security mechanism. Further, the attacker must disable or disrupt the intrinsic automated failure recovery mechanism in order to launch a successful attack.

Conclusion: The bottom line is that CyPhyCARD defense cloud has virtually unlimited resources that can investigate and analyze, even control the whole CPS at runtime. CyPhyCARD has the tools to dynamically compose and apply different compositions of sensors and effectors to maximum detection and control capabilities. CyPhyCARD limits attack dispersion locally by applying local isolation and containment measures and globally by the trustworthy information exchange. CyPhyCARD itself is virtually immune to attack as it is isolated from the ToD network in addition to its self-defense and recovery mechanisms.

V. Evaluation Issues and Perspectives

In this section we discuss the performance and security issues regarding the use of a conventional CPS defense system against using CyPhyCARD. In a sequel to this paper, we will provide quantitative analysis. We have built a preliminary prototype and simulator for this purpose that will also be presented in the sequel..

Performance

Current CPS security provisioning involves usage of **multiple isolated layers** of security. Conventional defense systems do not involve **any cooperation between physical and cyber security** provisioning. This isolation leads to possible duplication of security measures that might waste considerable amount of resources.

The cyber part of the CPS is usually protected by anti-worms/viruses, firewalls and intrusion detection systems. These defense mechanisms, usually **share the same resources with the target of defense**. This sharing may lead to difficulty in maintaining execution timeliness due to the overhead of security provisioning. Further, the defense systems regularly work in total isolation from each other. The **lack of cooperative processing** usually consumes more resources as a result of duplicating security measures. Additionally, CPS usually involve huge data processing and exchange. Traditional centralized defense systems **cannot deeply inspect**

such data in real-time without negatively affecting the ToD performance. Many contemporary defense systems use hardware-based security modules to overcome these problems. The fact that such modules still share the same network with the ToD does not completely waive the negative impact of the security provisioning over the ToD performance. Further, it is not easy to maintain updates for such hardware modules.

Also, conventional CPS defense systems usually apply preconfigured customized defense missions over the ToD. This customization **limits the defense provisioning capability to a specific target** with very limited reusability with other systems.

CyPhyCARD is designed to **work in total isolation** from the ToD to minimize the effect of security provisioning workload over the ToD operational workload. CyPhyCARD uses **unique communication streams** of lightweight sensors and effectors to **sense and configure both the cyber and physical parts** of the CPS. CyPhyCARD treats the CPS system components as a single body; where parts are continuously affecting each other. **The collected information from all the system parts is used to better serve the whole system defense**. The security provisioning tools used to defend the system components are in full cooperation. This **cooperation optimizes the resource usage** by minimizing replications of security commands. The distributed nature of CyPhyCARD processing elements "the cells" enables CyPhyCARD to **process tremendous amounts of data in real-time with minimal impact on the ToD** performance. CyPhyCARD platform enhanced resilience guaranties an adequate level of defense system survivability, which positively affects the survivability of the ToD.

Importantly, the **Defense as a Service cloud construction** of CyPhyCARD provides an on-demand pool of resources that can shrink or grow based on the situation on hand.

Security

A defense system that **shares the host network with the ToD** is an easy prey for attackers. An attacker can easily target the defense system after a successful compromise of one of the hosts. A successful attack on a **centralized defense** system may expose both the physical and the cyber components of the CPS to attacker reach. On the other hand, **isolating security provisioning** between interacting system components might induce some conflicts that facilitate system penetration or disrupt normal operation.

CyPhyCARD is a **comprehensive defense** system that provides defense services while **considering the interaction** between system components. This comprehensive defense provisioning **eliminates any possibility of conflicts** between security commands. Further, CyPhyCARD interaction with the ToD through only one **unified communication stream of sensors and effectors without sharing the host network** keeps it away from attacker reach. CyPhyCARD is **built over ChameleonSoft secured resilient infrastructure** to complicate attacking the defense system. CyPhyCARD cloud construction increase the capability of the defense provisioning by **enabling deeper real time investigation of system components.** The elastic nature of CyPhyCARD defense missions and its intrinsic separation between security provisioning and private system configuration makes it **fully reusable between multiple systems.** This reusability comes **without violating the ToD privacy policies**. Conventional defense systems mainly focus on stopping attacks; while CyPhyCARD aims **to block attack attempts while increasing the cost of further attacks.** CyPhyCARD manages to achieve that by means of **attacker attribution, attack containment, and honey-pots**. CyPhyCARD **uses trustworthy information sharing** techniques to share defense experiences with other cooperating CyPhyCARDs. This information sharing enhances the defense capability of cooperating systems, and minimizes attack detection and resolution time.

VI. RELATED WOK

An overview of CPS security challenges appeared in [1, 2], where the authors stated that securing future CPS should depend on attack early detection and alarm techniques. Such techniques should incorporate automated mechanisms to investigating massive volumes of collected multimodal data searching for attack indications. Current solutions mainly utilize data visualization and visual analytics to handle such large volumes of data[14]. Unfortunately these mechanisms have not addressed uniform knowledge representation and reasoning mechanisms for defense covering both cyber (e.g., hosts and networks) and physical (e.g., devices and plants) aspects of the CPS. Further, they fail to support different types of concurrent workflows and operational goals (e.g., control and business). CyPhyCARD uses a unified sensing stream to sense such heterogeneous cooperating compositions of CPS components. This unification of sensing, and data representation makes it easy for the analysis and investigation mechanisms to process their tasks. Further, CyPhyCARD sensing and control ability for the whole system through the same platform facilitates directing data fusion towards meaningful conclusions.

Securing information and control sharing among multi enclave organizations is a major challenge in the field of CPS security. Federated [9] and cross-domain solutions [10] are presented to address analogous issues in the cyber realm. It is envisioned that these solutions shall be applicable in the CPS context. One of the major limitations is that those solutions were mainly concerned about information management in the cyber domain with no consideration of control. Similarly, the existing cross-domain solutions assume a fairly restrictive environment in terms of interconnections availability among domains. CyPhyCARD cloud infrastructure is designed to be is scalable enough to provision defense services to multi- enclave multi-organization clients having heterogeneous compositions of cyber and/or physical devices. CyPhyCARD's trustworthy information sharing mechanism facilitates information and control sharing while enforcing privacy policies. Clients can permit sharing of control and information only within a specific region of their organization, within their organization's borders or with other cooperating organizations CyPhyCARD autonomously and seamlessly manages such operation with minimal human intervention.

Attack containment is a high priority goal of adequately defending CPS systems,. Research work in [11, 12, 13]

proposed solutions incorporating multiple overlapping detection capabilities and containment regions with potentially overlapping control hierarchies. These solutions have not considered the possible transitive reach of an attack into the physical realm from the cyber realm. Further, detection and containment mechanisms and semantics used in such architectures need to be extended in order to cover the system's physical aspects. CyPhyCARD leverage its capability to sense and control both the cyber and physical parts of the system using its unique construction of elastic sensor and effector streams to enable intelligent attack containment. CyPhyCARD can control the managed system cyber and physical devices to construct a quarantine area for the attack. Intelligent deception techniques can be applied to preserve the attack in an active harmless mode for deep investigation and further containment assurance. CyPhyCARD can autonomously restore operation of the quarantined area by leveraging backup images of prior attack detection and workflow redirection mechanisms to safely transfer the workflow to another remote location with similar physical capabilities.

Other solutions such as [3,6,7,8] have been presented to address other CPS security challenges mentioned in [1,2]. However, all these solutions focus only on a subset of the CPS security challenges in application specific domains. Those solutions have no consideration of the fulltime interaction between different CPS layers like management, security, etc. This inhibits such systems from being comprehensive enough to present a scalable general-purpose solution addressing the different CPS security challenges. Up to our knowledge, a synergistic, systemic and structured integration of defense solutions for CPS has not been proposed prior to our work.

VII. CONCLUSION

We presented CyPhyCARD, a biologically-inspired defense cloud that provides right-sized resources on-demand to effect comprehensive defense for CPS. CyPhyCARD is a customizable platform that facilitates proactive intelligent defense that, by construction, aims not only to defend but also to enhance resilience and increase the cost to attacker through attack containment, moving target defense, cooperative detection and deception, and automated recovery. The proposed solution is suitable for both cyber and cyber-physical systems. We presented a scenario-based qualitative analysis of CyPhyCARD's response against a synthetic worm (BlackWidow). CyPhyCARD has demonstrable advantages over the current solutions. The CyPhyCARD construction as a self-managed, autonomously controlled resilient cloud combined with its global situational awareness and control over the ToD would enable automated real-time, deep system analysis and configuration. These features, in turn, would facilitate attack detection, containment, deception, and resolution while preserving continuity of service operations. Additionally, CyPhyCARD defense operating in isolation from the ToD minimizes the overhead impact of security assurance on the ToD system performance. Moreover, CyPhyCARD's trustworthy early warning mechanism across organizations facilitates the secure exchange of information and knowledge between organizations in order to enhance detection and response without violating individual privacy policy.

Ongoing research includes formalizing the COA, refining the architecture and prototype of the CyPhyCARD defense cloud, and formalizing and implementing EvoSense sensors and effectors generic conduit. Rigorous quantitative experimental and simulation results are planned for a sequel to this paper.

There are several interesting challenges to be addressed. We are exploring autonomously coordinating defense missions and dynamically allocating relevant resources and services. Also, we will devise a deception mechanism to autonomously configure the cyber and physical components of the system for attack containment. Finally, privacy preservation remains a formidable challenge that will require us to demonstrate provable privacy preservation to obtain the needed buy-in from both the public and private sectors as well as the consumers.

VIII. REFERENCES

[1] Partha Pal, Rick Schantz, Kurt Rohloff and Joseph Loyall., "Cyber physical Systems Security Challenges and Research Ideas" Workshop on Future Directions in Cyber-physical Systems Security, July 2009.

[2] Clifford Neuman., "Challenges in Security for Cyber-Physical Systems", DHS Workshop on Future Directions in Cyber-Physical Systems Security, 2009.

[3] J. Haack., G. Fink, E. Fulp, and W. Maiden,. "Cooperative Infrastructure Defense", Workshop on Visualization for Computer Security, 2008.

[4] W.M. Maiden, "DualTrust, A Trust Management Model for Swarm-Based Autonomic Computing Systems", Master's Thesis, Pullman, WA: Washington State University, 2010.

[5] W.M. Maiden, I. Dionysiou, D.A. Frincke, G.A. Fink, and D.E. Bakken., "DualTrust: A Distributed Trust Model for Swarm-Based Autonomic Computing Systems", Data Privacy Management and Autonomous Spontaneous Security, 2010.

[6] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta., "Green and sustainable cyber physical security solutions for body area networks", International Workshop on Body Sensor Networks, 2009.

[7] J. Hu and A. C.Weaver., "A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications". Pervasive Security, Privacy and Trust,2003.

[8] K. Ouchi, T. Suzuki, and M. Doi., "Lifeminder: A wearable healthcare support system using user's context", 22th International Conference on Distributed Computing Systems Workshops, 2002.

[9] G. Mitchell, J. Loyall, J. Webb, M. Gillen, A. Gronosky, M. Atighetchi, A. Sinclair, "A Software Architecture for Federating Information Spaces for Coalition Operations," MILCOM 2008, San Diego, CA, November 17-19, 2008.10

[10] Defense Information Systems Agency (DISA). (2011,Aug). DoD cross-domain solutions access controlled. Available: http://iase.disa.mil/cds/index.html

[11] P. Pal, F. Webber, R. Schantz, "Survival by Defense-Enabling", Foundations of Intrusion Tolerant Systems (Organically Assured and Survivable Information Systems), IEEE, 2003, pp 261-269. 7

[12] P. Pal, F. Webber, R. Schantz, "The DPASA Survivable JBI- A High-Water Mark in Intrusion-Tolerant Systems," EuroSys Workshop on Recent Advances in Intrusion-Tolerant Systems, Lisbon, March 23, 2007.

[13] Kurt Rohloff, Richard Schantz and Yarom Gabay. "High-Level Dynamic Resource Management for Distributed, Real-Time Embedded Systems." 5th Symposium on Design, Analysis and Simulation of Distributed Systems (DASD), San Diego, CA, 2007.

[14] P. Benjamin, P. Pal, F. Webber, P. Rubel, M. Atighetchi. "Using A Cognitive Architecture to Automate Cyberdefense Reasoning," ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security (BLISS 2008), IEEE Computer Society, August 4-6, 2008.