POSTER: Blackboard-Based Electronic Warfare System

Jeremy Straub
University of North Dakota
3950 Campus Road, Stop 9015
Grand Forks, ND 58202 USA
+1 (701) 777-4107
jeremy.straub@my.und.edu

ABSTRACT
With internet-connected, SCADA and cyber-physical systems becoming the next battlefield for crime and warfare, technologies for defending and attacking these systems are growing in prevalence. For entities with significant asset collections that are prospectively vulnerable to this type of an attack, autonomous response, retaliation and attack capabilities are necessary to respond to a growing threat from numerous sectors. This paper presents a command and control technique for cyberwarfare based on the Blackboard Architecture. It discusses the utility of this approach and proposes a distributed command system that can run across multiple nodes of various types.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *authentication, invasive software, unauthorized access.*

General Terms
Algorithms, Management, Performance, Reliability, Security, Verification

Keywords
Autonomous attack and defense; Blackboard Architecture; cybersecurity; command and control; cyberdefense; cyberwarfare

1. INTRODUCTION
Technological capabilities that were the province of imagination 50 years ago and science fiction ten years ago have become and are becoming reality. Many of these technologies are network connected and rely on access to remote data and utilize local and remote computational capabilities to deliver their function. Some technologies, like those used for remote surgery [1], remotely piloted aircraft [2], national security applications and many cyberphysical systems need to be protected from data theft and denial of system operation and access to requisite data streams.

While defensive technologies are required for all applications and may represent a complete solution for some where temporary denial of service is acceptable, for other applications an active response is required. State actors may also seek to engage in (and/or offensively defend against) cyberwarfare, for which defensive-only technologies are not suitable.

This paper presents a distributed command and control architecture for the operation of the weapons of cyberwarfare, cyberdefense and cybersecurity. The proposed approach utilizes a distributed Blackboard Architecture capable of operating across numerous configurations to support a multitude of prospective applications. The technology is designed to support operations from both owned/controlled hardware and the use of temporary adversary network-homed 'forward operating locations'.

This paper continues with an overview of prior work that provides a foundation for the work presented herein. Then, the proposed system is described.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.
ACM 978-1-4503-3832-5/15/10.
DOI: http://dx.doi.org/10.1145/2810103.2810109

2. BACKGROUND
The sophistication of cyberspace threats is growing: moving from discrete categories of attack to merged "more damaging forms" [3]. Attack quantities are also increasing: for example, between 2000 and 2009, the number of reported incidents targeting the U.S. Department of Defense grew fifty-fold.

Actors range from cybercriminals (who have a variety of motivations and prospective targets [4]) to perpetrators of so-called 'hactivism' [5] to state actors to terrorists (who may target critical infrastructure, a "target ripe for terrorism" according to Pedersen [6]). A multitude of prospective targets exist, ranging from point of sale systems to cyber-espionage. Special concern exists, however, with regards to systems that interact with the physical world such as remote surgery systems [1], remotely piloted aircraft [2], "smart grid" power systems [7] and other supervisory control and data acquisition (SCADA) systems. Concern also exists regarding technologies that could be used to track citizens' location and characteristics [8] or impair emergency response mechanisms [9].

The prospective involvement of state actors raises special considerations. These range from questions of who acts on behalf of a state and what constitutes an act of war to what involvement national defense entities should have in cybersecurity.

A wide variety of attacks have been implemented by various attackers. Attack types have included denial of service attacks, ARP poisoning, unauthorized access (including hypervisor attacks, rootkits and "VM escape" attacks) [10], code injection, "drive by exploits" and insider and other targeted attacks [11].

A variety of defense and response techniques have been developed in response to this growing threat. Atoum, Otoom and Ali [12] present a holistic cyber security framework; however,

many others focus on specific component technologies. One area where autonomy has been used frequently is intrusion (and more broadly, attack) detection systems. Techniques utilized have included network visualization, active learning, Bayesian networks, genetic algorithms, nature-inspired algorithms and various combinations such as the genetic fuzzy and pairwise learning-based system developed by Elhag, et al. [13]. Systems have had goals ranging from detecting unauthorized changes to using mobile phone carrier networks to characterize criminal entity participation [14] to identifying and preventing so-called "identity theft attack" on social networks [15].

3. PROPOSED SYSTEM

The proposed system is based on a distributed blackboard which collects (or is supplied) information, makes decisions based on this information and triggers actions (in some cases) based on those decisions. It operates based on a rule-satisfaction principle, where it is tasked with one or more high-level goals and an augmentable fact-rule-action network which defines how the system operates. Several different aspects of the system are now described. First, the distributed control approach is presented. Then, the communications model is presented. Next, system operations are discussed. Distributed Control Approach

The distributed control approach for the proposed system utilizes a modified version of the Blackboard Architecture [16] in a (backwards) problem-solving mode (discussed in [17]). While, in many cases, it has a single-goal solution (e.g., a particular objective), multi-goal support (see [18]) is also included.

This control approach is very versatile and can be adapted to a variety of usage scenarios, each of which would result in a somewhat different rule network. For example, a system developed to attack a target might have the destruction (or impairment, etc.) of the target as a single goal and the rule / action / fact network would be designed to provide multiple prospective pathways to this goal. Alternately, a system designed to take offensive actions to protect a cyberasset might have asset protection as a goal and a network of rules, facts and actions designed to represent multiple pathways to the impairment / compromise / damage / destruction of this asset, which must be prevented. A variety of other applications and corresponding rule / action / fact networks are possible to support other needs.

The system has a mechanism to develop additional rules, facts and actions, based upon changing conditions. In particular, an application-specific classifier mechanism can be used to identify additional assets of an entity-target and, based on the type of systems detected, new rule / fact / action chains are built to represent the prospective new targets and attack vectors to target systems or systems under protection.

A boundary object-based Blackboard modification (described in [19]) is utilized to coordinate between the various parts of the multi-homed system. Figure 1 presents the logical architecture of the system. It is comprised of numerous local blackboards which share boundary facts with a global virtual blackboard. This virtual blackboard is shared between all of the local blackboards and may, in some applications, also have a centralized repository (in addition to the shared copy). When a fact is changed on this shared virtual blackboard, it is made available to all local blackboards. Rule processing and action triggering (which is intentionally minimized in this design) for the central blackboard can be processed by any of the parts of the multi-homed system.

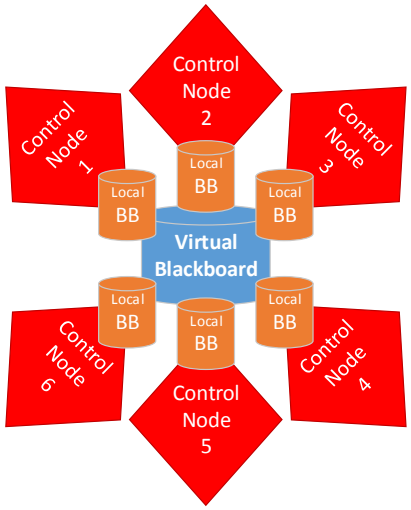

Figure 1. Logical diagram of the proposed system.

It is important to note that this logical model can be represented in multiple different ways in physical implementation. The central virtual blackboard approach intentionally supports operations across security perimeters and on untrusted (in addition to trusted) hardware. The logistics of the physical implementation are discussed subsequently.

3.1 Communications Model

There are two components to the communications logistics: the data transfer mechanism and the re-convergence mechanism. Effectively, the Blackboard Architecture is implemented using non-owned/operated data stores with hypertext transfer protocol (HTTP) as the communications mechanism. The majority of the elements of the data model are not transferred between nodes. The data that is transferred (except during new node creation) falls into two categories: boundary object changes and entity / connector / protector (and associated attribute data) network updates. Multiple transmission approaches can be used, depending on the sensitivity of the application.

3.2 System Operations

This section provides an overview of the operations of the proposed system. A wide variety of node configurations are possible given the nature of the system. One example configuration is shown in Figure 2.

Fundamentally, the system has three modes: inert, network building and active. In the first mode, nodes are waiting and regularly checking to determine if they have been triggered. Re-convergence activities will occur, if needed; however, no network expansion or attack / defense activities are conducted. The system also scans network traffic to augment the topology data store.

The second mode, network building, involves the system identifying other prospectively useful entities to place system nodes on. It will use offensive capabilities to compromise systems, as necessary, to place the control software; however, it will not conduct attacks in furtherance of goals. Like in the inert mode, the system is waiting for activation instructions and will engage in re-convergence activities, if required. It also scans network traffic to expand the topology data store with any new

information detected. For example, in the system shown in Figure 2, the gold-colored computers are system nodes. The system would, thus, identify the need to compromise and load itself on to one of the grey-colored servers to have direct access to the target network to attack the other servers.

In the third mode, active, the system utilizes its offensive capabilities to achieve the objectives dictated by its network of rules, actions and facts and the topographical information stored within the system's data stores. Continued passive scans of network traffic (and, potentially, depending on obfuscation and stealth requirements, active probing) is used to expand the topology data store. The data store is also updated with information about changes caused by system operations (computers that host a control process, computers disabled, etc.).

Once placed in active mode, the system will continue to seek to achieve its goals until it receives a command to return to the inert or network building modes. As newly deployed system nodes are always deployed in the same mode as their deploying node, all nodes that it deploys will also be in active mode. Even if cut off from other nodes, if a pathway towards goal attainment exists, it will be pursued. Thus, if a node gets proverbially 'trapped behind enemy lines' it can continue to operate until instructed to stand down to another mode, a final goal is achieved or no pathway that advances the system towards goal attainment can be identified.

The exact arsenal of attack capabilities available to the system is a deployment-specific consideration. This is based on the system owner's objectives and what types of collateral damage it considers acceptable. Limitations on attacks can be imposed through both the tools provided as well as the configuration parameters that associate particular tools with particular system types. Limiting the scope of attack takes two forms: first, if a type of system is not included, it will not be attacked. However, as some deployments may include generic attacks (that match any system) or operating system level attacks, a more specific rule can be employed that associates a system with a non-attack tool.

Human operator control over the system is achieved via the same communications mechanism used by the system nodes. A control computer (highlighted in red in Figure 2) can be located anywhere with the requisite connectivity. It will communicate with the system via the mechanisms discussed previously and perform re-convergence as required.

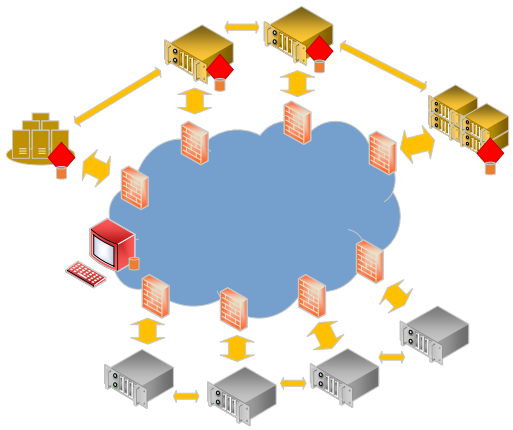

Figure 2. Example physical diagram for the proposed system.

4. REFERENCES

1. Marescaux, J.; Leroy, J.; Rubino, F.; Smith, M.; Vix, M.; Simone, M.; Mutter, D. Transcontinental robot-assisted remote telesurgery: feasibility and potential applications. *Ann. Surg.* **2002**, *235*, 487-492.
2. Kim, A.; Wampler, B.; Goppert, J.; Hwang, I.; Aldridge, H. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. *The American Institute of Aeronautics and Astronautics: Reston, VA, USA* **2012**.
3. Choo, K. R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719-731.
4. Kshetri, N. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research* **2013**, *13*, 41-69.
5. Raiu, C. Cyber-threat evolution: the past year. *Computer Fraud & Security* **2012**, *2012*, 5-8.
6. Pedersen, C. Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security. *Pepperdine Policy Review* **2014**, *7*, 3.
7. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Computer Networks* **2013**, *57*, 1344-1371.
8. Elmaghraby, A. S.; Losavio, M. M. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research* **2014**.
9. Loukas, G.; Gan, D.; Vuong, T. A review of cyber threats and defence approaches in emergency management. *Future Internet* **2013**, *5*, 205-236.
10. Abouzakhar, N. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. **2013**.
11. Ugorji, B.; Abouzakhar, N.; Sapsford, J. In *In Cloud Security: A Review of Recent Threats and Solution Models;* Procs Int Conf on Cloud Security Management; Academic Conferences Ltd.: 2013; .
12. Atoum, I.; Otoom, A.; Abu Ali, A. A holistic cyber security implementation framework. *Information Management & Computer Security* **2014**, *22*, 251-264.
13. Elhag, S.; Fernández, A.; Bawakid, A.; Alshomrani, S.; Herrera, F. On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. *Expert Syst. Appl.* **2015**, *42*, 193-202.
14. Ferrara, E.; De Meo, P.; Catanese, S.; Fiumara, G. Detecting criminal organizations in mobile phone networks. *Expert Syst. Appl.* **2014**, *41*, 5733-5750.
15. He, B.; Chen, C.; Su, Y.; Sun, H. A defence scheme against Identity Theft Attack based on multiple social networks. *Expert Syst. Appl.* **2014**, *41*, 2345-2352.
16. Hayes-Roth, B. A blackboard architecture for control. *Artif. Intell.* **1985**, *26*, 251-321.
17. Straub, J.; Reza, H. A Blackboard-Style Decision Making System for Multi-Tier Craft Control and its Evaluation. *Journal of Experimental & Theoretical Artificial Intelligence* **In Press**.
18. Straub, J. Evaluation of a Multi-Goal Solver for Use in a Blackboard Architecture. *International Journal of Decision Support System Technology (IJDSST)* **2014**, *6*, 1-13.
19. Straub, J. A Distributed Blackboard Approach Based Upon a Boundary Node Concept. *Intelligent & Robotic Systems* **Submitted to**.