Adaptive Host and Network Security
AHANS 2012

I. Introduction
Over the past decade the threat of cyber attacks on critical commercial and government infrastructure
has been growing at an alarming rate to a point where it is now considered to be a major threat in the
world. Current approaches to cyber security involve building fast-growing multi-million line systems that
attempt to detect and remove attacking software. Meanwhile, cyber exploits continue to multiply in
number, but their size continues to be a couple of hundred lines of code. This disparity of effort means
that the current defensive approaches to cyber security can at best fight a holding action. The workshop
is intended to explore game-changing approaches to cyber security that focus on adaptation. There is a
clear need to develop systems at both the host level and the network level to actively adapt to cyber
attacks and to provide greater protection for networked computation at all levels.

The significance of this workshop is to bring together researchers from different areas such as
networking, programming languages, computer hardware, and operating systems to gain broad insights
into specific research issues related to adaptive host and network security, and to foster discussions
about ongoing research, establish directions for future research and collaborations, and identify best
practices for adaptive security.

A diverse collection of interesting papers were selected for presentation at the workshop. There are
many ways that these eight papers could be categorized and grouped, but an interesting breakout was to
consider the primary system element that was being defended: the host, the application, the network or
the system as a whole. We organized the workshop into four sessions on these topics, and two papers
somewhat naturally fell into each session.

II. Host Security
The first paper is “Hardware Support for Safety Interlocks and Introspection”, by Udit Dhawan, Albert
Kwon, Edin Kadric, Catalin Hritcu, Benjamin C. Pierce, Jonathan M. Smith, Andre Dehon, Gregory
Malecha, Greg Morrisett, Thomas F. Knight, Andrew Sutherland, Tom Hawkins, Amanda Zynxfryx, David
Wittenberg, Peter Trei, Sumit Ray and Greg Sullivan. This paper describes a novel hardware architecture
that incorporates mechanisms for pointers with manifest bounds, hardware types, processor supported
authority, gates, and dynamic tag management. More specifically, it describes an FPGA implementation
of the architecture, that includes:

- Fat pointers that contain not just objects' locations, but also their bounds.
- Hardware support for typed memory words: prevent arbitrary code from, e.g., forging fat pointers,
distinguish data from code, etc.
- Hardware representation of authority as pointers.
- Hardware support (gates) for privilege change -- this allows efficient moving from one authority
  level to another, critical for efficiently separating levels of privilege.
- Hardware support for Metadata, providing hardware enforcement of some program invariants.

The second paper on host security is “Using Concolic Testing to Refine Vulnerability Profiles in
FUZZBUSTER”, by David Musliner, Jeffrey Rye and Tom Marble. This paper describes two tools that
work together to identify and patch vulnerabilities against memory errors in C programs. The first tool,
CREST, uses CIL to track user-specified variables (with a combination of symbolic and dynamic
analysis). The second tool, Fuzzbuster, can adapt this information to generalise a specific vulnerability
into a more general test case (and hence a better patch).
CREST performs concrete and symbolic execution on the target software system. FUZZBUSTER leverages it to find symbolic constraints for fault inducing test cases. These determined constraints specify the range of values that inputs can take while following the same execution path in the code. Vulnerability profiles are refined from the extracted constraints allowing creation of more effective adaptations.

III. Application Security

The first paper on application security is "A3: An Environment for Self-Adapative Diagnosis and Immunization of Novel Attacks", by Partha Pal, Richard Schantz, Aaron Paulos, Brett Benyo, David Johnson, Mike Hibler and Eric Eide. The paper describes the A3 system, which provides a virtual machine-based architecture for supervising the execution of programs in order to protect them from cyber attacks. The architecture features:

- a sandboxing approach that is specific to each protected application, rather than generic (cf. the browser sandbox)
- crumple zones, which are intended to contain intrusion effects before they can damage neighboring systems or the overall execution environment
- facilities for replaying execution of protected systems, in order to learn from and react to, intrusions that may have occurred long before they were detected. This is called "replay with modification" or RwM.
- state management of executing programs in order to enforce invariants, etc.
- The primary focus of the paper is use of RwM in experiments to identify intrusion effects and develop countermeasures.

The second paper focusing on application security is "Exploring Compartmentalisation Hypotheses with SOAAP", by Khilan Gudka, Robert Watson, Steven Hand, Ben Laurie and Anil Madhavapeddy. This paper introduces Security Analysis of Application Programs (SOAAP), a set of tools to support semi-automated compartmentalisation (aka sandboxing) of C-language Trusted Computing Base (TCB) components such as operating systems and web browsers. SOAAP employs a variety of static and dynamic approaches, driven by source code annotations called 'compartmentalisation hypotheses', to help programmers evaluate strategies for compartmentalising existing software, before/without implementing them.

The paper champions compartmentalization for securing operating systems, libraries, middleware frameworks and applications. It explains the issues and challenges in converting existing code into compartments. One side effect of compartmentalization is that if compartments are isolated to application process' and communicate via IPC, then the compartmentalized application effectively makes good use of multi-core architectures.

IV. Network Security

The first paper on network security is "Self-Organized Mechanism for Distributed Setup of Multiple Heterogeneous Intrusion Detection Systems", by Karel Bartos and Martin Rehak. This paper proposes a technique that enables a collection of IDS nodes to modify their configurations in a collaborative manner such that each node focuses on a relatively unique set of intrusion events. The goal is to increase the overall sensitivity (true positive rate) of the IDS system to actual intrusion events. Re-configuration algorithms are local to each node, but ideally the nodes exchange event data to assess the similarity of detected events. The authors thus propose a distributed self-organizing framework for coordinating the effective recognition of intrusions from multiple IDS sensor systems located throughout a network deployment. The collaboration is done by full event report information sharing but without negotiation using a game-theoretic model.

The second paper on network security (which however might also well have been put in the category of System Security), is "Autonomous, Collaborative Control for Resilient Cyber Defense (ACCORD)", by Stuart Wagner, Eric van den Berg, Jim Giacopelli, Andrei Ghetie, Jim Burns, Miriam Tauil, Soumya Sen, Michael Wang, Mung Chiang, Tian Lan, Robert Laddaga, Paul Robertson, and Prakash Manghwani. This paper describes a Nash Bargaining-derived technique for balancing load across "micro-clusters" cloud
compute resources, motivated by the problem of distributed cloud computation in high-risk environments (e.g., battlefield). Each microcluster uses a Nash Bargaining Solution (NBS) to apportion resources within the cluster to client jobs, based on the submitted job's vector of resource requirements (cycles, memory, storage). Clients query each available microcluster for a "congestion price" and select to which cluster they submit their job based on the returned prices. A prototype implementation is discussed in the context of a Hadoop cluster, and experimental results described.

V. System Security

The first paper on system security is “STRATUS: Strategic and Tactical Resiliency Against Threats to Ubiquitous Systems”, by Mark Burstein, Robert Goldman, Paul Robertson, Robert Laddaga, Robert Balzer, Ugur Kuter, Christopher Geib, David McDonald, John Maraist, Peter Keller, Neil Goldman and David Wile. The paper describes a relatively comprehensive approach to the problem of threat diagnosis and response, including the interesting idea of strategic, proactive prediction and reconfiguration of resources to anticipate an attacker's future actions. A key element of the approach is modeling of potential attack plans, based on knowledge of current system behavior, so that actual attacks can be categorized and responded to most effectively. The STRATUS system includes: RAPPA, to generate qualitatively different candidate attacks; PAPR, for probabilistic plan recognition; MIFD for intrusion detection; DAD for maintaining a probabilistic trust network; MOTHER, for planning responses and also allocating resources towards contingency plans; CSE, a secure communications substrate that serves as both a sandboxing and a sensing mechanism.

The second paper is in this section, because it describes the trust management aspects of the above described STRATUS system. "Adaptive Security and Trust", by Paul Robertson and Robert Laddaga, discusses ongoing work in STRATUS to develop new ways of achieving cyber security. The authors describe how trust in cyber assets can be modeled and used to support self-adaptive techniques in continuing to operate important computational functions in a system that is actively under attack. In particular, the paper describes a trust modeling system that attempts to maintain a model of trust for networked resources using a combination of two basic ideas: 1) Conditional Trust based on conditional preference (CP-Nets) and 2) the Principle of Maximum Entropy. The approach treads a middle ground between recognizing the difficulty in producing more than qualitative comparisons of trust and utility, and the need to have numbers in order to adequately compare expected utility of alternatives.

VI. Summary of Workshop

This was the first meeting of the AHANS workshop, which brought security researchers up and down the computational stack (CPUs, operating systems, program analysis, applications, and distributed systems) together with researchers in self-organizing and adaptive systems for a lively discussion as to how systems might adapt (or be adapted) in the presence of malicious attackers. The workshop was keynoted by Dr Howard Shrobe (DARPA, MIT) who described how concepts of adaptivity were central to on-going DARPA-sponsored research into cyber-security.

After each group of papers was presented, the group as whole discussed both the individual presentations, and the overall topic of the group of presentations.

Robert N. M. Watson  
Computer Laboratory  
University of Cambridge  
Cambridge, UK  
robert.watson@cl.cam.ac.uk

Robert Laddaga  
Dynamic Object  
Language Labs, Inc.  
Lexington, MA, USA  
rladdaga@dollabs.com

Stuart Wagner  
Applied Communication Sciences, Inc.  
Piscataway, NJ, USA  
swagner@appcomsci.com
Chairs
Robert Laddaga
Stuart Wagner
Robert Watson

Program Committee
Jonathan Anderson
Mark Burstein
Jim Giacopelli
Robert Goldman
Robert Laddaga
Anil Madhavapeddy
Prakash Manghwani
David Musliner
Paul Robertson
Greg Sullivan
Eric Vandenberg
Stuart Wagner
Robert Watson