Chapter 5
Symbiotes and defensive Mutualism: Moving Target Defense

Ang Cui and Salvatore J. Stolfo

Abstract  If we wish to break the continual cycle of patching and replacing our core monoculture systems to defend against attacker evasion tactics, we must redesign the way systems are deployed so that the attacker can no longer glean the information about one system that allows attacking any other like system. Hence, a new poly-culture architecture that provides complete uniqueness for each distinct device would thwart many remote attacks (except perhaps for insider attacks). We believe a new security paradigm based on perpetual mutation and diversity, driven by symbiotic defensive mutualism can fundamentally change the ‘cat and mouse’ dynamic which has impeded the development of truly effective security mechanism to date. We propose this new ‘clean slate design’ principle and conjecture that this defensive strategy can also be applied to legacy systems widely deployed today. Fundamentally, the technique diversifies the defensive system of the protected host system thwarting attacks against defenses commonly executed by modern malware.

5.1 Introduction

We propose a host-based defense mechanism that we call Symbiotic Embedded Machines (SEM). SEM, or simply the Symbiote, is a code structure inspired by a natural phenomenon known as Symbiotic Defensive Mutualism. This phenomenon generally refers to any short- or long-term association between populations of different species where the survival or ‘evolutionary fitness’ of one or more population partners is enhanced by the association. Mutual benefits are often the result of some emergent behavior between two or more vastly different biological systems. This synergistic dynamic is observed across the spectrum of living things, from microbes

Ang Cui
Columbia University, e-mail: ang@cs.columbia.edu
Salvatore J. Stolfo
Columbia University e-mail: sal@cs.columbia.edu
like viruses and bacteria to fungi and to flora and fauna. When considered within
the digital realm, Symbiotic Embedded Machines can be thought of as digital ‘life
forms’ which tightly co-exist with arbitrary executables in a mutually defensive ar-
rangement, extracting computational resources (CPU cycles) from it’s host while
simultaneously protecting the host from attack and exploitation. Furthermore, the
diverse nature of symbiotes provide inherent protection against direct attack by ad-
versaries that directly target host defenses. Hence, defenses are defended by the
principle of defensive mutualism.

We envision a general-purpose computing architecture consisting of two mutual
defensive systems whereby a self-contained, distinct and unique Symbiote machine
is embedded in each instance of a host program. The Symbiote can reside within
any arbitrary body of software, regardless of its place within the system stack. The
Symbiote can be injected into an arbitrary host in many different ways, while the
code of the Symbiote can be ‘randomized’ by advanced polymorphic code engines.
Thus, a distinct defensive Symbiote can be used to protect device drivers, the kernel,
as well as userland applications. The combination of Symbiote with host program
creates a unique executable different from any other instance, and thus breaks the
mono-culture by creating a plethora of ‘moved targets’.

Once the Symbiote injection process is complete, it will execute along-side it’s
host program. Since the Symbiote is a self-contained entity, it is not installed onto
the host program in the traditional sense. Current anti-virus and host-based defenses
must be installed onto or into an operating system, which places a heavy dependence
on the features and integrity of the operating system. In general, this arrangement re-
quires a strong trust relationship with the very software (often of unknown integrity)
it tries to protect.

In contrast, the Symbiote treats it’s entire host program as an external and un-
trusted entity, and therefore eliminates this unsound trust relationship. Much like
how certain ants reside within the Bullhorn Acacia tree and acts as a natural defense
mechanism against harmful insects, Symbiotic Embedded Machines reside within
its host executable, protecting it against exploitation and unauthorized modification.
Just as the ants are unfamiliar with the inner workings of the Acacia tree, and as the
Acacia tree is unaware of the existence of the ants, SEM’s reside within the target
binary in a similar arrangement. At runtime, the host program requires the Symbiote
to successfully execute in order to operate. The Symbiote monitors the behavior of
its host to ensure it operates correctly, and if not, stops the host from doing harm.
Removal, or attempted removal, of the Symbiote renders the host inoperable.

5.2 Related Work

Symbiotic Embedded Machines can be thought of as a generic way of injecting
host-based defenses into arbitrary host programs. Traditional host-based defenses
are typically installed into well-known operating systems to fortify the entire OS
from various types of exploitation. For example, numerous rootkit and malware de-