

Robert R. James  
Doctoral Student, Adjunct Professor  
Information Assurance: Network Research and Security  
College of Technology  
Eastern Michigan University

Network Security and Information Assurance – The development of an offensive software DNA bot network for the purpose of protecting an intranet from malicious bots, worms and viruses.

A proposal for funding under  
Eastern Michigan University's Information Assurance Research Allocation

Professor Gerald Lawver, Administrator

Professors Peter Stephenson and Ann Remp  
Faculty Sponsors

## Abstract

Current network security infrastructures comprise a defensive grid including firewalls, virus and spyware detection, and eventual removal by software executed at a given point in time. On the other hand, adversaries utilize their talents to offensively capture system resources and entangle the network into botnets, worm transmitters and virus repositories. Honey pots and honey nets were devised to trap viruses in an environment where they can await the execution of the malicious code then act upon the intruder. The major problem with the techniques is that all but the honey net are defensive in nature. The honey net waits for the malicious code to execute before taking action to correct or succumb. When these defensive measures fail to stop an attack, the malicious code enters a system fully capable of doing damage. Many of today's attacks are perpetrated by botnets. For example, denial of service attacks (Ddos) on infrastructure servers are attributed as successful by the botnet master, where thousands of systems attack at once, upon command from the main system. What is needed is a proactive system to respond to botnet attacks. This is the direction of the current proposal.

Current approaches to studying networks are multidisciplinary (see Barabasi, for example). Of particular significance in the current proposal is developing network capabilities as analogs of biological systems, particularly immune systems (see Stephenson). These discussions form a background for the current proposal.

## Introduction

I propose the research of potentially combining several theories to create an offensive botnet. This experimental botnet would be created within a research intranet and would be designed to be associated with the infrastructure of this intranet, initially with designated elements of the infrastructure and later with a broader range of components. This botnet would monitor these infrastructure element activity for potential changes to the infrastructure. The purpose of the botnet would be to detect active intrusion and subsequent attack of designated infrastructure elements and provide an immediate defense shield to these elements. A key concept in this research is using the infrastructure identity itself and its binding to the botnet as the mechanism for detecting attempts to modify the infrastructure.

The first subject to be reviewed is the initial creation of a simple robot (CadeBouBot) and its control by a single entity (a system, such as a server). Each system within the network will have its own active robot executable and thus capable of taking orders and identifying itself continuously. This is the scope of the initial research.

Following this first stage and subsequent research, the robot needs to have significant improvement in respects to an identity. An intranet DNA is created and maintained,

similar to the human genome. Once the identity is created and secured, the antibody robot can wait for an intruder to attack the system, analogous to awaiting a germ or cancer in the human body. If an intruder were to attack for the purpose of changing the identity of the CadeBouBot, the intruder would not be able to attack all of the internal bots simultaneously. Therefore, it would be unable to take over the entire network infrastructure. Since the DNA source is protected, the intruding bot would be unsuccessful in its attempt.

The robot must be able to detect attack and neutralize an attacking entity. The robot can be programmed with configuration parameters based on the system it is supporting. If an anomaly occurs to the system, the bot can transmit the attack, take action against the intruder, or shut the system down so the infected system cannot be used for further attacks within the intranet.

How does the robot know its boundaries? Firewalls, routers and switches will need to be able to detect and support the functional robot. The intranet entry point will be used as the trapping net, just as harbors utilized nets to keep enemy submarines from entering or exiting during times of war.

#### Method of study

The method of study will follow a process of systematic, critical scrutiny of previous works, in order to base the inception on sound theories and research practices.

The initial process is seen as linear, described by its main steps of:

- Select (the work to be studied);
- Record (all relevant information about that work);
- Examine (the recorded information);
- Develop (an improved way of doing things);
- Install (the new method as standard practice);
- Maintain (the new standard proactive).

Many theories will be selected for review during this study.

- Network theory for the purpose of developing protocols to identify robots and determine if friend or foe.
- Robot development and usage.
- Forensic identification in relation to developing network DNA identification.
- Data mining techniques for detecting and predicting network intrusion.
- Intrusion detection techniques, specifically concentrating on botnets, honey pots, virus detection and removal and work detection and removal.
- Software engineering practices for information assurance

#### Deliverables

- Code for CadeBouBot for representative system.
- Software analog for bot identity based on DNA
- Framework for network bot defense development

#### Tentative Time Table

The study will be performed during the months of May through July, 2008, in three stages, culminating with a publishable results paper in September, 2008

Stage 1 - CadeBouBot development; May/June 2008

Stage 2 - Development of a network DNA identity, June/July 2008

Stage 3 - Software requirements engineering for network bot defense development July/August 2008

Stage 4 - Results paper September 2008

#### Selective Research Bibliography

Li, Zhi-tang, Jie Lei, Li Wang, Dong Li, A Data Mining Approach to Generating Network Attack Graph for intrusion Prediction, Fourth international conference in Fuzzy Systems and Knowledge Discovery, IEEE, 2007

Geer, David, Malicious Bots Threaten Network Security, IEEE Computer Society, 2005

Ishibash, Keisuke, et al, Detecting Mass-Mailing Worm Infected Hosts by Mining DNS Traffic, ACM SIGCOMM, 2005

Cheung-Leung Lui et al, Agent-based Network Intrusion Detection System Using Data Mining Approaches, Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05)

Bianconi, Ginestra, Albert-László Barabási, Bose-Einstein Condensation in Complex Networks, The American Physical Society, 2001

Bratus, Sergey, Hacker Curriculum: How Hackers Learn Networking, IEEE Computer Society, October 2007

Haifeng Yu et al, SybilGuard: Defending Against Sybil Attacks via Social Networks, ACM SIGCOMM'06, September 11–15, 2006