National Cyber Leap Year Summit 2009:
Exploring Paths to New Cyber Security Paradigms
Draft Report of Participants' Ideas

August 24, 2009

New Game: Moving from forensics to real-time diagnosis.

This document explores Health-Inspired Network Defense (renamed as Nature-Inspired Cyber Health) as a path to this new game.

The following ideas were captured in unedited form at the National Cyber Leap Year Summit. The ideas are a summary of the discussion of the participants in the Nature-Inspired Cyber Health session. They do not necessarily represent the opinions of the co-editors or the organizations they represent. The Summit is managed by QinetiQ North America at the request of the NITRD Program, Office of the Assistant Secretary of Defense Networks and Information Integration, and the White House Office of Science and Technology Policy.

Please **provide your comments**, if any, **by September 3, 2009** for utilization by the Summit's program co-chairs at http://www.co-ment.net/text/1448/. To add a comment, select the "Add" tab in the left navigation menu, select (highlight) the portion of the document you are commenting on, and provide your comment. If commenting on an entire section, you may select the section heading to anchor your comment.

If you have any further questions or comments, please visit the National Cyber Leap Year Web site at the following address: http://www.nitrd.gov/NCLYSummit.aspx, or send email to leapyear@nitrd.gov.

What is the new game?

Today, weeks and months may elapse before successful network penetrations are detected through laborious forensic analysis. Despite their potential to function with intelligence, today's typical network components have very limited understanding of what passes through them, coupled with a correspondingly short memory. In medical terms, because we are not instrumenting for early detection of pathogens and their effects, our most common diagnoses are through autopsies of enterprises which have succumbed to attack. In the new game, network components have heightened ability to observe and record what is happening to and around them. With this new awareness of their health and safety they enjoy a range of options: they may take preventative measures, rejecting requests which do not fit the profile of what is good, a priori, for the network; they can build immunological responses to the malicious agents which they sense in real time; they may refine the evidence they capture for the pathologist, as a diagnosis of last resort, or to support the development of new prevention methods. The game

consists of considering very dynamic rather than static network architectures. Recent networking developments intend to allow more flexible network where mobility is one of the most important features as well as the connection of any sort of computing and communication devices. The new game should be able to monitor and control such dynamical cyber environments. In other words, the game is about real-time distributed monitoring, control and diagnosis of very dynamic and flexible cyber environments.

1 Nature Inspired Cyber Health

We propose to change the game for protecting Cyber-systems by looking to nature for inspiration. Examples in nature are the immune system, beneficial parasites, and social networks such as public health networks and social insects. The immune system protects the body remarkably well from panoply of threats that are continuously evolving in a dynamic and ever-changing environment. Natural systems are far more complex than our cyber-systems but they are extremely robust, resilient, and effective. Clearly, an investigation of these natural systems, such as the immune system, can be beneficial to changing the game for cyber-security. In this working group we explored and developed the following **four potential 'Game Changing' idea proposals**:

- Distributed Defense
- Centers for Cyber Disease Control (CCDC) and Prevention
- Using Attack Vectors
- Missing-Self Paradigm

These four potential game-changing ideas are described below.

1.1 Distributed Defense

1.2 Description

- Distributed defenses based on the resilience of natural systems
  - Multi-scale (computer, local network, globally)
  - Agility – new sensors, responses, etc., example: If there is an attack on the network, there should be instantaneous 99% immunity to the attack
- Sensing
  - Memory of health state – anomaly detection
  - Memory of characteristics of past attacks
  - Community reputation and trust measures for sensor data
  - Signaling

    - Collaborative signaling at multiple levels, federations of communities
    - Communications standards
    - Collaborative/federated communication
- Response
    - Automatic response – appropriate to false positive rates
    - Human-in-the-loop response for high-consequence or early deployment
    - Symbiotic relationships – responses that influence adversary or cause-desired side-effects
    - Responses that anticipate and mitigate likely next steps

1.3 Inertia

- Data rates are high
- Usually driven by knee-jerk reactions instead of designing a systemic defense
- Willingness to share raw data
- Specific targeting by the adversary can remove the benefit of communication
- Shared data may not represent invariants of attack
- Challenge to share more quickly than the adversary moves
- Sharing exposes what we know to the adversary
- Response systems can be gamed to deny service

1.4 Progress

- Critical systems more distributed now – drive distributed sensing
- Attackers more distributed now
- Sufficient additional CPUs required to do distributed processing
- Realization that peers have important real-time threat data to share
- Leverage new cloud computing architectures

1.5 Action Plan

- Develop CONOPS and requirements
- Gap analysis
- Use existing sensors opportunistically
- Identify new responses and sensors required to trigger them
- Develop new sensors and responses
- Verification and Validation (V&V)

- Test convergence (control theory)
- Quantify performance
- Measure performance under specific realistic attacks

- Distributed Robustness
  - Re-engineer functions must be robust to assess damage
  - Use diversity to limit assets affected by any given attack
  - Bound outages and to minimize impact on functions
  - Inertia:
    - Reliance on network availability
    - Rewriting applications or application protocols

1.6 Jump-Start Plan

- Pick high complexity, high savvy sites (e.g. research labs) to develop and deploy operationally
- Each of: Defense, Electrical Supervisory Control And Data Acquisition (SCADA), Health
- Fund multiple-threads of development and implementation simultaneously (~$50M/yr)
- Build a self-sustaining community, similar to Internet Engineering Task Force (IETF). to be stewards for standards communication mechanisms, and formats, etc.
- Use management mechanisms to drive adoption
- Encourage vendors to add support to COTS
- Get industry to provide private clouds

2 Centers for Cyber Disease Control (CCDC) and Prevention

Provide similar public health system services for our national computer infrastructure.

2.1 Description

- Public health infrastructure - cyber equivalent to CCDC
- Indication of “I’m Sick”
- Overcome barriers to sharing data
- High fidelity data required to gain full understanding of illness
- Conduct data collection similar to World Health Organization and public health departments
- Collect and distribute health information to support active response

- Provide cost/benefit of interventions
- Models should comprehend key factors
- Cyber geographical statistics concerning topology, applications communities, shared software, end users analogous to doctor office, city, state, or a CDC
- Profit motive that leverages commercial opportunities and business case, e.g., service providers, etc.
- Global scale reports that provide the state of the Internet assessments, e.g., e-crime, fraud, data breaches, Comprehensive National Cybersecurity Initiative (CNCI), 60-day report, and threat intelligence report, etc.

2.1.1 What is the Role of a Public Health System (PHS)?

- Assessment of a community's problems, needs and resources
- Health needs assessment
- Data and surveillance
- Leadership in organizing effective public and private sector strategies to address community health problems
- Assurance that direct services necessary for meeting local health goals are available to all community residents such as screening, education, prevention, outreach

2.1.2 What does a PHS do?

- Monitor health status to identify community health problems
- Diagnose and investigate health problems and health hazards in the community
- Inform, educate and empower people about health issues
- Mobilize community partnerships to identify and solve health problems
- Develop policies and plans that support individual and community health efforts
- Enforce laws and regulations that protect health and ensure safety
- Link people to needed personal health services and assure the provision of health care when otherwise unavailable
- Assure a competent public health and personal health care workforce
- Evaluate effectiveness, accessibility and quality of personal and population-based health services
- Research for new insights and innovative solutions to health problems

2.1.3 The Core Claim

- ”Surveillance” – The gathering and analysis of data on a national scale is a key enabler to providing public health services
- These functions can, and should be, automated for Cyberspace
- Multi-scale collection and reduction of cyber health data
- Represent the “ground truth” about cyber operations on the scale of the national infrastructure

2.2 Inertia

- Anti-virus companies are similar to drug companies
- Reactive “knee jerk” nature of business
- Absence of central driving force
- Data ownership and intellectual property issues
- Lack of Federal Government buy-in
- Fed has not created incentive system
- Data is disaggregated
- Lack of liability model
- Actuarial data needed for insurance
- Automated cyber-attack stress testing
- Public education

2.3 Progress

- Catalysts for sharing data
- Incentive and legal precedence for sharing data (potentially intellectual property)
- Consortiums that encourage sharing, e.g., best practices, threats and attack signatures
- Data characteristic specifications necessary to jump start
- Utilizing the power of human intelligence by increasing public awareness, e.g., epidemic warnings and best practices

2.3.1 Why is this the Right Time?

- Increased public awareness
- Magnitude of problem is heightened
- Represents a business opportunity
- Technology has matured to enable collection/filtration/dissemination of information
- Government can provide stamp of good practice
- Assurance for both big and small business
- Government has expressed willingness to address cyber security issues and stimulate action

2.4 Action Plan

- Define taxonomy and metrics categories
- Data collection
- Current state and sensitivity analytics
- Predictive mathematical models
- Prospective studies
- Temporal data on how a “healthy network” functions.
- Collect specific cohort groups of targeted populations

- Visualization of network behavior and structure
- Rapid response monitoring

2.4.1 Overall Recommendation Phase

- Criteria for being healthy
- Decision support, e.g., quarantine, barrier establishment, vaccination
- Synthetic cyber vaccine distribution
- Innovation center for catalyzing other health inspired innovations
- Promote continued cross-over among biological institutes and IT discipline
- Optimal sensor/actuator placement
- How much information do you need to make an optimal decision
- Control law algorithms versus machine learning on empirical data
- Given the right and/or enough data, can we machine learn the correct response

2.5 Jump-Start Plan

- Organize and survey
- Identify and address the required initial data
- Consider privacy issues
- Enumerate existing data sets
- Consider current taxonomies
- Detail frame and scope
- Identify other models (e.g., CDC, World Health Organization WHO)
- Identify potential partnerships
- Identify initial stakeholders and refine data
- Establish possible business models

Establish a community of interest to further develop the concept and evolving steps to produce an RFI and establish initial pilot with seed funding.

3 Using Attack Vectors

3.1 Description

3.1.1 Three Approaches:

A. Good Worms (aka gworms)
B. Piggybacking (aka ride the worm)
C. Drive-By Downloads

3.1.2 Motivation

- Hordes of vulnerable computers on the internet

- Not secure because of apathy, ignorance, just don't care, etc.
- Huge problem because of botnets, etc.
- Attackers have vectors into those computers
- Same vectors used to do good, e.g., patch
- Do it without the user's consent for the greater good, e.g, Oral Polio Vaccine (OPV)

3.1.2.1 Good Worms (aka gworms) an old idea

- Idea is to create gworms (good or benign worms) that spread love (patches, etc.)
- Been there - done that:
  - Suggested many, many times.
  - Real gworms, e.g, Welchia worm (2003): detects and terminates Blaster worm, patches system and reboots

3.1.2.1.1 Gworm Problems

- Spreading gworms considered harmful; results in network traffic overload
- Need to move faster than a gworm to catch it
- Unintended consequences from bugs
- Could harm systems that are not currently threatened and/or attacked
- Releases gworm code to the world
  - Exploit code available to blackhats
  - Transmission code available to blackhats
- Ethical and legal issues

3.1.2.2 Piggyback: Ride the Worm

- Use honey pots to catch worms
- Replace worm payload with a rider
- Rider prevents host damage
- Rider still allows network spread
- Rider goes where worm goes, possibly at the same rate the worm spreads

3.1.2.2.1 Piggyback Benefits over gworms:

- Dormant until activated, i.e. only do harm when harm is happening
- Easier to match spread rate to worm
- Rider contains no exploit or transmission code
- "More" ethical or legal than gworms
- Possibly could spread with worms even when vulnerabilities are not known a priori

3.1.2.2.2 Challenges for Piggyback

- Major technical challenges
  - –Replace worm payload with rider
  - –Constrain damage caused by worm

- –React fast against fast-moving worms
- –Control spread rate (if we want to)

- Legal and ethical issues need to be addressed

3.1.2.3 Drive-By Downloads

- Malicious webservers exploit client vulnerabilities to install malware
- "Good" webservers exploit same vulnerabilities to install whiteware
- Whiteware patches vulnerabilities on client, cleans off malware, etc.

3.1.2.3.1 The Pros and Cons of Drive-Bys

- The Pros
  - Patch vulnerabilities that can't be fixed by gworms/piggyback
  - Address common way of spreading botnets
  - Not viral (no harmful spreading)
- The Cons
  - Penetration and auto-patching could be harmful
  - Could be useless if system is already compromised
  - Ethical and legal issues need to be addressed, but are different in subtle ways from gworms?

3.2 Inertia

- Why haven't we done this before?
  - Gworms previously done, but ethical and other issues remain
  - Piggyback and drive-by downloads not previously done
- What will derail this?
  - Perception, liability, legality, side-effects, lack of efficacy
  - Technical challenges, e.g., payload replacement

3.3 Progress

- gworms have been technically feasible in the past
- Piggyback/drive-by may have been technically feasible in the past
- But now there are more technical tools available, e.g., virtual machines, more computing power
- Increased awareness of cyber-security issues may make this more palatable
- Increased problem with botnets and malware may change the cost-benefit analysis for society

3.4 Action Plan

- Requires research
- Technical feasibility
- Theoretical models and simulations
- Investigate non-technical aspects

- Legality, etc.

3.5 Jump-Start Plan

- Small workshop on using attack vectors, bringing together technologists, lawyers, government
- Early-stage research funding

UPDATE - WE WERE ABLE TO OBTAIN PRELIMINARY (AND PROMISING) SIMULATION DATA ON THE PIGGYBACK. WE HAVE FORMED A COLLABORATION GROUP BETWEEN LABS AT UCSD, LBL, AND LOS ALAMOS AND PLAN TO MEET WITHIN THE NEXT FEW WEEKS. WE ARE PLANNING TO WRITE A MANUSCRIPT ON THE *PIGGYBACK APPROACH.*

4 Missing-Self Paradigm

4.1 Idea – Missing Paradigm

4.1.1 Background

- Mammalian Immune System defines self in two major ways
  - *Primary* (Organic/Central) Self: Whatever is present at, or just before, birth, ***regardless of what it looks like.*** The **only** criterion is presence. This is tagged Major Histocompatibility Complex (MHC) which is an imperfect example)
  - *Secondary:* What comes later is interrogated for its behavior. If it causes damage or injury or stress, the Immune System is alerted to reject it. Damage is signaled to the immune system by alarm signals from the damaged cells. If it is harmless, it is not rejected. If it lasts long enough without causing harm or generating alarm signals, it becomes part of the definition of self**.**
- A Cyber or computer system can also define self in two similar ways
  - *Primary* (Organic/Central) Self: Whatever is present at, or just before boot time, ***regardless of what it looks like.*** The **only** criterion is presence.
  - *Secondary:* What comes later is interrogated for its behavior or its provenance. If it comes from a trusted source, and/or if it does not cause damage, it is not rejected, If it lasts long enough without causing harm, it becomes part of the definition of self. Comprehensive sets of alarm signals in Cyber systems have not yet been investigated.

4.2 Description

How can the Cyber system do this?

- **Primary (Organic/Central) Self**: whatever is present at, or just before, birth, ***regardless of what it looks like,*** is tagged. Anything that is not tagged can't run or be opened.

  Examples: The machine generates two random numbers

        - One is used to tag the "self' executable entities
        - The other points to the "space" that the tag is inserted.
    - All unlabeled executable entities that arrive later are not tagged, and cannot be "opened". This is similar to implementation of restrictive security posture, e.g. deny everything that is not explicitly permitted as in Trusted Platform Module (TPM) Management
    - At shut down, all unlabelled executable entities are deleted
        - This is repeated at every boot up
        - When a machine is cloned, all unlabelled executable entities are erased.
        - There is a mechanism to add to the Primary self (see behavioral self below)
    - Distinguishable difference from "code signing" scheme and trusted third provided tagging
- **Secondary/Behavioral Self:** what comes after completion of tagging is interrogated for its behavior or its provenance. If it comes from a trusted source, and/or if it does not cause damage or generate alarm signals, it is not rejected, and if it lasts long enough without causing harm, it can become part of the definition of self
    - This is a Multi-Scale, Collaborate behavioral pattern/model (e.g. process, host, network, user, community, enterprise, mobile device) That consists of three choices:
        - Add and Tag
        - Sandbox (Depending on Trust level)
        - Delete (generation of alarm signals)
    - "Fast response" aspect and "slow response" aspect
        - Fast = Primary → self allowed to change only when you tag it
        - Slow = Behavioral → more dynamic, puts human in the loop

4.3 Inertia - TBD

- The amount of arbitrary code execution increased significantly, for example, malwares are getting downloaded and executed covertly.
- Though there are many techniques (Vista Kernel-Module code integrity checks, Trusted Platform Module, Intel's Trusted Execution Technology, etc.) for code and process authentication and validation, there is room for further improvement.
- Different trust management systems (at process, platform and network level) are major initiators to explore tagging.

4.4 Progress

- Potential derailers - Primary self mechanism needs change to OS, creation of sandboxes
- Technically Feasible?
    - Primary: Yes
    - Behavior: Yes, scaling is feasible, given sufficient computer power
- Environmentally Feasible?
    - Primary: Yes
    - Behavior: Yes as an overlay to existing technologies
- Mitigation of Concerns

- Primary: none at this stage
- Behavior: Privacy concerns are mitigated because it is analysis of behavior with no knowledge of individual identity. Whatever length of time is set for a well-behaved program to be labeled as self, can be learned by the attackers and subverted.

4.5 Action Plan

Multi-dimensional, distributed characterization of "Primary and Secondary Self"

- Seed the research community (e.g. STTR, RFA, RFP, BAA, and SBIR) in three phases.
  - Fundamental research
  - Clinical trials (in various test environment e.g. DETER, NCR, HPC environment)
  - Deploy the system
- Standards for definition of common language & models used to signal threats & threat behaviors (e.g. threat ontology)
- Determine if self can be applied only at machine level or can it be applied to entire enterprise, cloud?

4.6 Jump-Start Plan

- Acquire Funding (5-10-10 million dollars for three phases)
- Create a collaboration between immunologist(s) and Cyber Security expert(s)
- Create a group of people who care about this proposal to further it, e.g., getting help on requirements, existing capabilities and estimating dollar amounts
- Notion of tagging should be part of research

APPENDIX A: Acronyms

Acronym	Description
BAA	
CCDC	Cyber Disease Control
CNCI	Comprehensive National Cybersecurity Initiative
DETER	
gworms	Good Worms
HPC	

MHC	Major Histocompatibility Complex
NCR	
OPV	Oral Polio Vaccine
PHS	Public Health System
RFA	
RFP	
SBIR	
(SCADA)	Supervisory Control And Data Acquisition
STTR,	
TPM	Trusted Platform Module
V&V	Verification and Validation
WHO	World Health Organization