(ISC)²

SECURITY CONGRESS 2015

SECURE TOMORROW TODAY

congress.isc2.org • #ISC2Congress

Building an Immune System

Securing technological systems by modeling biological systems

Building a Computer Network Immune System

DC Grant – University of Washington – dcgrant@uw.edu
Center for Information Assurance and Cybersecurity
Master Infrastructure Management and Planning
Bachelor of Science Information Technology
Certified Information Systems Security Professional
Certified Information Security Manager

Securing technological systems by modeling biological systems

Cyber Immune System Secure Operational Response (CISSOR)

Modeling the biological immune system for advanced security of network attached computer infrastructure and control systems.

Agenda

- **Motivation**
- **Problem Statement**
- **Background as a Quick Overview**
  - Preventative and Detective Controls
  - Platform Assurance
  - Vulnerabilities

Agenda continued

- **Applying an Immune Systems**
  - Brief introduction to how an immune system works
  - Prior application in Anti-Virus and Intrusion Detection
- **Lightweight Mobile Digital Agents**
  - Moving Target Defense
  - Indirect Communications
  - Using an Artificial Grid
- **Introduction to Genetic Pattern Matching**
- **Put It All Together, then Take Questions.**

Motivation

Industrial Control Systems Joint Working Group Roadmap – Long-term goals for secure systems (2013)

- **"Development of fully automated security state monitors in most control systems networks"**
- **"Widespread implementation and use of automated self-healing control system architectures is a major long-term milestone.** ***Within ten years, ICSs detection and response tools should have the capability of performing real-time detection and response and should develop control system security certification programs for operators."***

Motivation

- **Network attached industrial controls and computer-based control systems are very prevalent in critical systems and infrastructures.**
- **Most of these systems are not very well secured.**
- **Long term security solutions do not currently exist.**
- **Recent technological advances change the game**
  - Allow for new approaches to be used
  - Allow old approaches to be modified

Motivation

- Current defenses are deficient, even on very advanced systems.
- **Malicious actors are well financed and share attack capabilities.**
- Long term information systems security solutions do not exist.
- **Trusted systems should self-monitor and respond automatically.**
- Intelligent systems can learn from their successes and failures.

Problem Statement

- **How can we assure any network attached technology against any type of malware and against unauthorized modification in real time?**

  - Zero-day threat discovery
  - Real-time monitoring required
  - Near immediate response mandatory
  - Integrity and security of system is critical

Problem Restatement

What autonomous systems can be developed to respond to all types of cyber security threats very rapidly and without direct cognitive guidance from humans?

Preventing and Detecting Intrusions

Image courtesy of http://isecurebusiness.com July 2014

Preventing and Detecting Intrusions

- A very important subset of control systems in general – which include prevention, detection, deterrence and compensation.
- Detection is only the first step in an immune system response, but it is unquestionably the most critical step.

Examples of Current P&D Controls

Preventative

- Firewall
- Intrusion Prevention
- Encryption
- Antivirus
- Security Guards
- Training

Detective

- System Logs
- Intrusion Detection
- Antivirus
- Reports and Reviews
- Frequent Audits
- Surveillance

Platform Assurance

- Maintaining known and tested standard hardware, operating systems and application software.
- Tactics to monitor and alert on all types of platform modifications (detective controls).
- Log all system activities and consolidate logs onto a separate system designed for capture and analysis: Security Information and Event Management (SIEM).
- Maintain updated standard images of all the operating systems and applications installed.

System Vulnerabilities

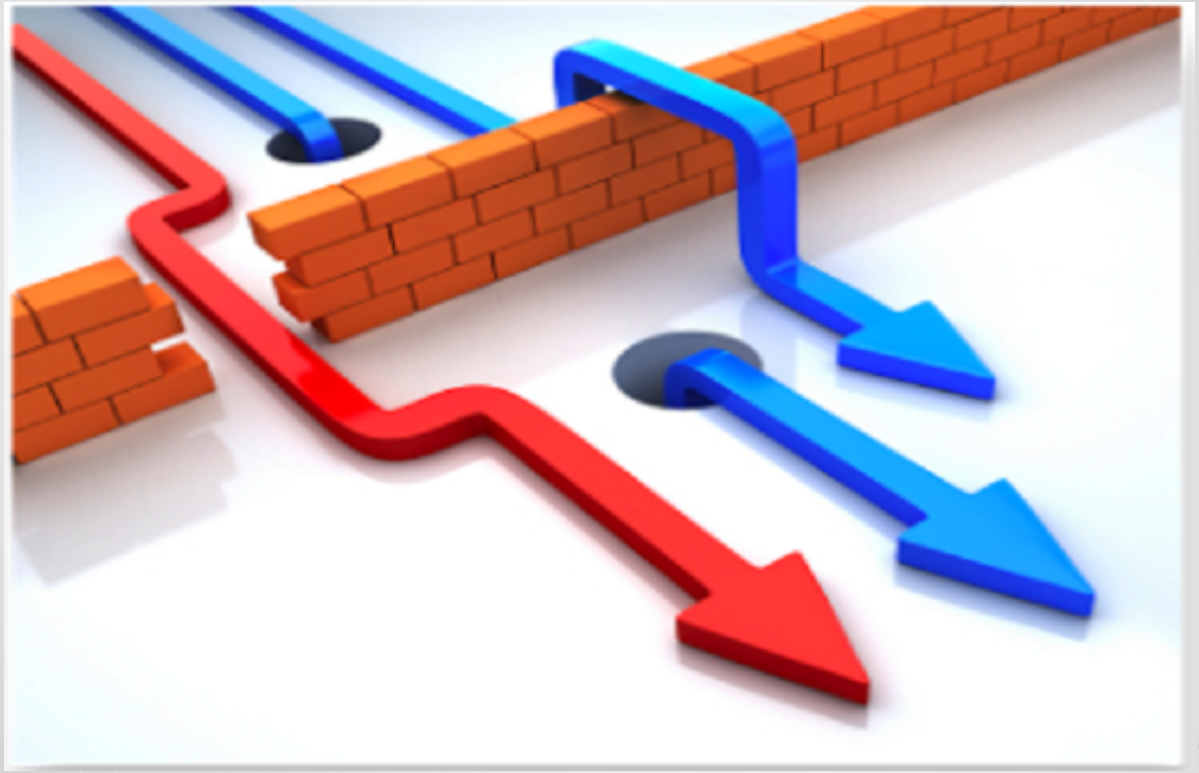


Image courtesy of http://isecurebusiness.com July 2014

System Vulnerability Examples

- Operating system and application defects.
- Available patches and fixes not yet installed.
- Buffer overflow, cross-site scripting and SQL injection.
- Operational gaps can allow attackers greater leverage.
- Inadequate security training.
- Insufficient input sanitation.
- New zero-day exploits are found on a frequent basis.
- Organizations are vulnerable to phishing, pharming and social engineering.
- Inadequate controls or policies contribute to the effectiveness of attacks.

Vulnerabilities exist everywhere

- It would be impossible *and impractical* to eliminate all types of vulnerabilities from any complex system.
- Nearly every networked system can eventually be compromised, given enough time and effort.
- Security professionals should assume some level of breach has already occurred.
- Don’t expect systems are secure before extensive testing has been performed to prove surety.

Understanding the Immune System

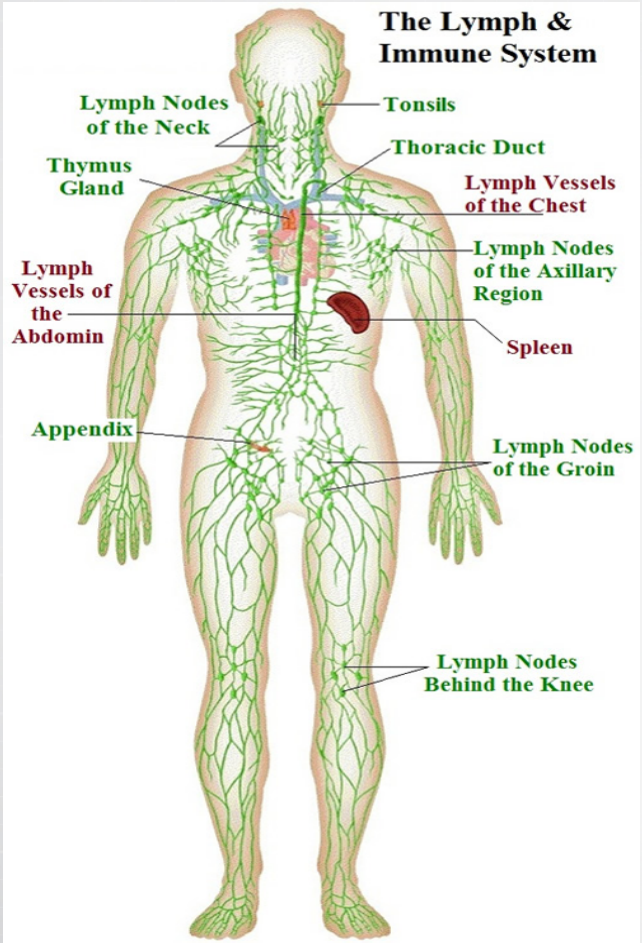
Background information on the biological immune system

Basic immunological theories

- The main theory is that the body distinguishes itself from non-native internal entities, which is aptly named the 'Self / Non Self' theory of immunology.
- In contrast with the 'Self / Non Self' theory, the Danger Model is based on the idea that the immune system is more concerned about factors that do damage than it is with whether something is foreign.

Immunological concepts

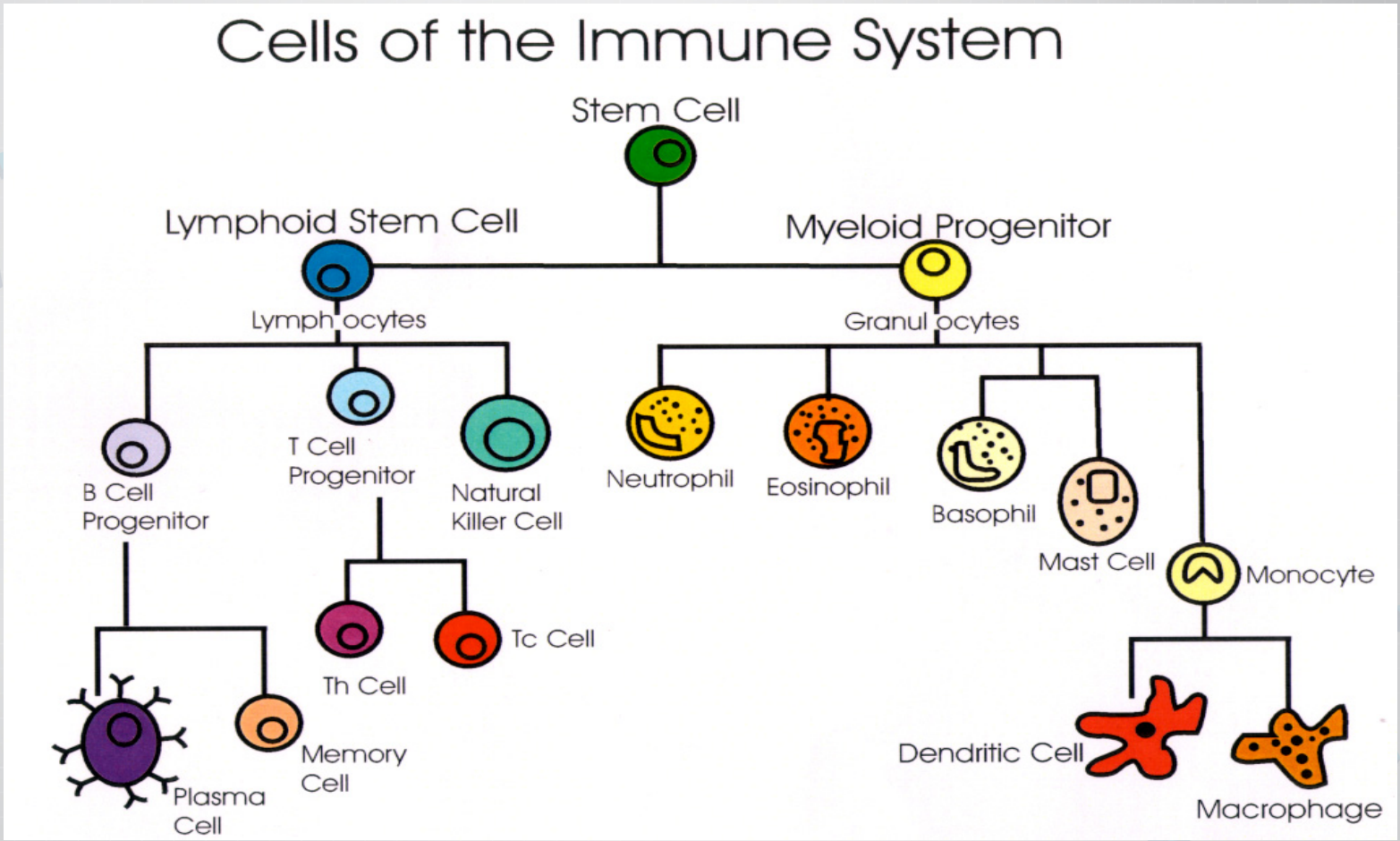
- *There are many different actors working in parallel as well as in series as part of the immune response*.
- The immune response is complex and actual tactics implemented vary dependent upon the threat.
- Lymph nodes are distributed throughout the body, to provide for local interpretation and response to immune sensing and regulating mechanisms.



Key immune system concepts:

- Control factors are distributed through the system for rapid detection and response.
- All attached components are integrated in the system.
- Many diverse agents roam the system to perform prevention, detection, deterrence and compensation.

Adapted from: http://www.getwellnatural.com/images/lymphatic-system-immune-system.jpg



Adapted from: http://www.omsusa.org/cellsis.jpg

Immune Cells

- Granulocytes include basophils, eosinophils, and neutrophils. Basophils and eosinophils are important for host defense against parasites. Granulocytes are also involved in allergic reactions.
- *Neutrophils are the most numerous innate immune cells. They patrol for problems by circulating in the blood. They can ingest bacteria, degrading them inside special compartments called vesicles.*
- Mast cells also are important for defense against parasites.
- *Mast cells are located in tissues and can mediate allergic reactions by releasing inflammatory chemicals like histamine.*

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Immune Cells

- *Monocytes*, which develop into *macrophages*, also patrol and respond to problems. They are found in the bloodstream and in tissues.
- *Macrophages are able to ingest and degrade bacteria. Upon activation, monocytes and macrophages coordinate an immune response by notifying other immune cells of the problem.*
- Macrophages also have important non-immune functions, such as recycling dead cells, like red blood cells, and clearing away cellular debris. These "housekeeping" functions occur without activation of an immune response.

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Immune Cells

- *Dendritic cells (DC) are an important antigen-presenting cell (APC), and they also can develop from monocytes.*[26]
- *Antigens are molecules from pathogens, host cells, and allergens that may be recognized by adaptive immune cells.*
- APCs like DCs are responsible for processing large molecules into "readable" fragments (antigens) recognized by adaptive B or T cells.
- *Antigens alone cannot activate T cells. They must be presented with the appropriate major histocompatibility complex (MHC) expressed on the APC.*
- MHC is a checkpoint to help immune cells distinguish between the biological host's cells and foreign cells.

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Immune Cells

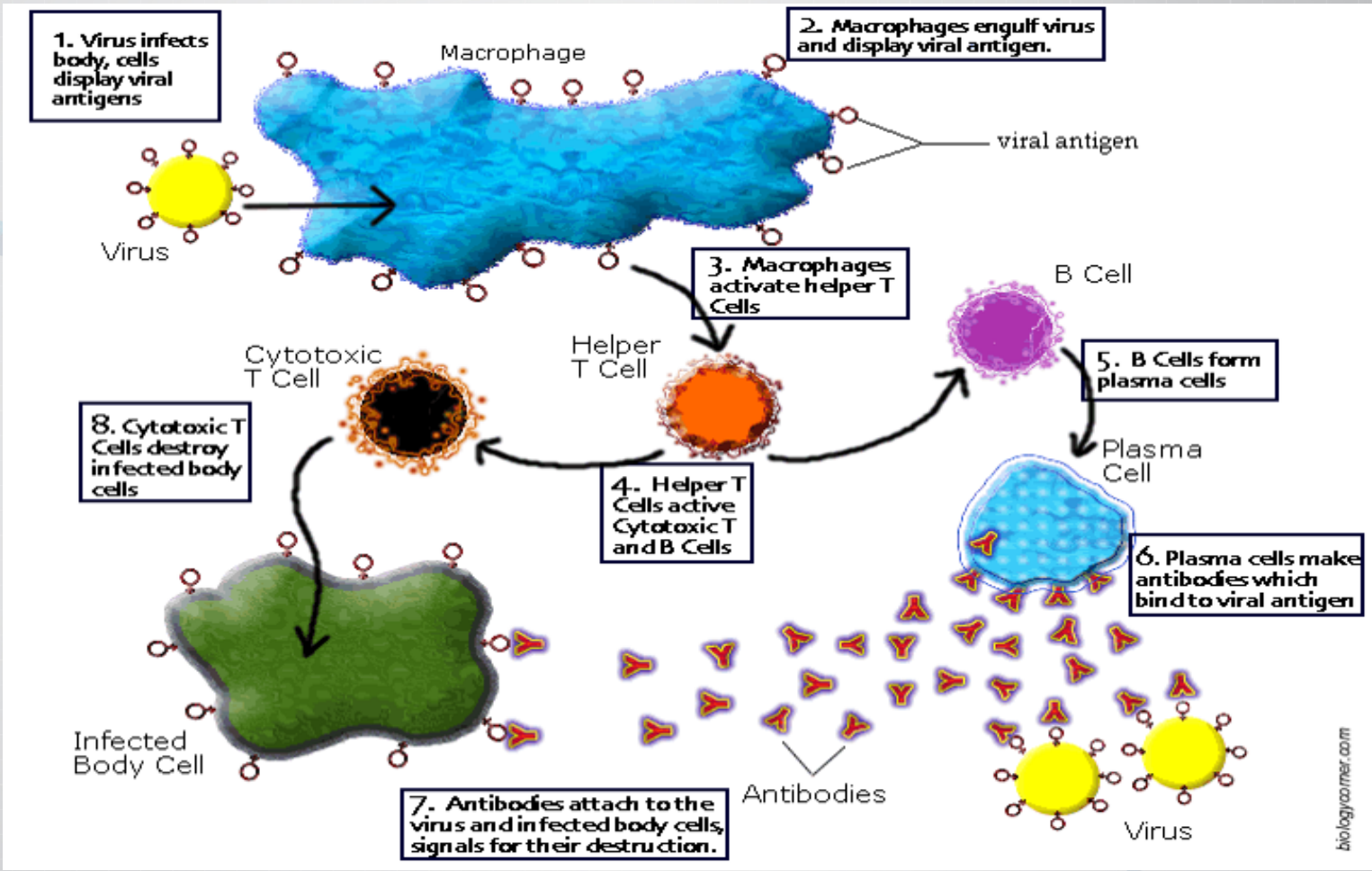
- ***Natural killer (NK) cells have features of both innate and adaptive immunity.***
- Natural killer cells are important for recognizing and killing any virus-infected cells or tumor-related cells.
- *Natural killer (NK) cells, like adaptive cells, can be retained as memory cells and respond to subsequent infections by the same pathogen.*

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Immune Cells

- Natural Killer cells use protein-filled granules to form holes in target cells and cause apoptosis, the process for programmed cell death.
- *It is important to distinguish between apoptosis and other forms of cell death like necrosis. Apoptosis, does not release danger signals that can lead to greater immune activation and inflammation – Necrosis does signal danger and causes increased immune response.*
- **Through apoptosis, immune cells discreetly remove infected cells and limit bystander damage.**

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx



Adapted from: http://www.biologycorner.com/resources/immune_response.gif

Adaptive Cells

- ***B cells have two major functions:*** *They present antigens to T cells, and produce antibodies to neutralize infectious microbes.*
- **Antibodies** coat the surface of pathogens to **serve 3 roles:** neutralization, opsonization, and complement activation.
- ***Neutralization*** *occurs when a pathogen is covered in antibodies and is unable to bind and infect host cells.*
- *In* ***opsonization****, other immune cells are alerted to engulf and digest the pathogen.*
- ***Complement*** *is a process for directly destroying bacteria.*

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Adaptive Cells

- Antibodies are expressed in two ways. B-cell receptors (BCR), on the surface of a B cell, are actually antibodies.
- B cells also secrete antibodies to diffuse in the bloodstream and bind to very specific pathogens.
- *This dual expression is important because the initial problem is recognized by a unique BCR and activates the B cell.*
- The activated B cell responds by secreting antibodies in soluble form. This ensures that response is very specific against the bacterium that started the process.

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Adaptive Cells

- Every antibody is unique, but they fall under five general categories: IgM, IgD, IgG, IgA, and IgE.
- (Ig is short for immunoglobulin, also known as antibodies.)
- While these have overlapping roles, IgM generally is important for complement activation; IgD is involved in activating basophils; IgG is important for neutralization, opsonization, and complement activation; IgA is specifically for neutralization in the gastrointestinal tract; and IgE is used to activate mast cells in parasitic and allergic responses.

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Adaptive Cells

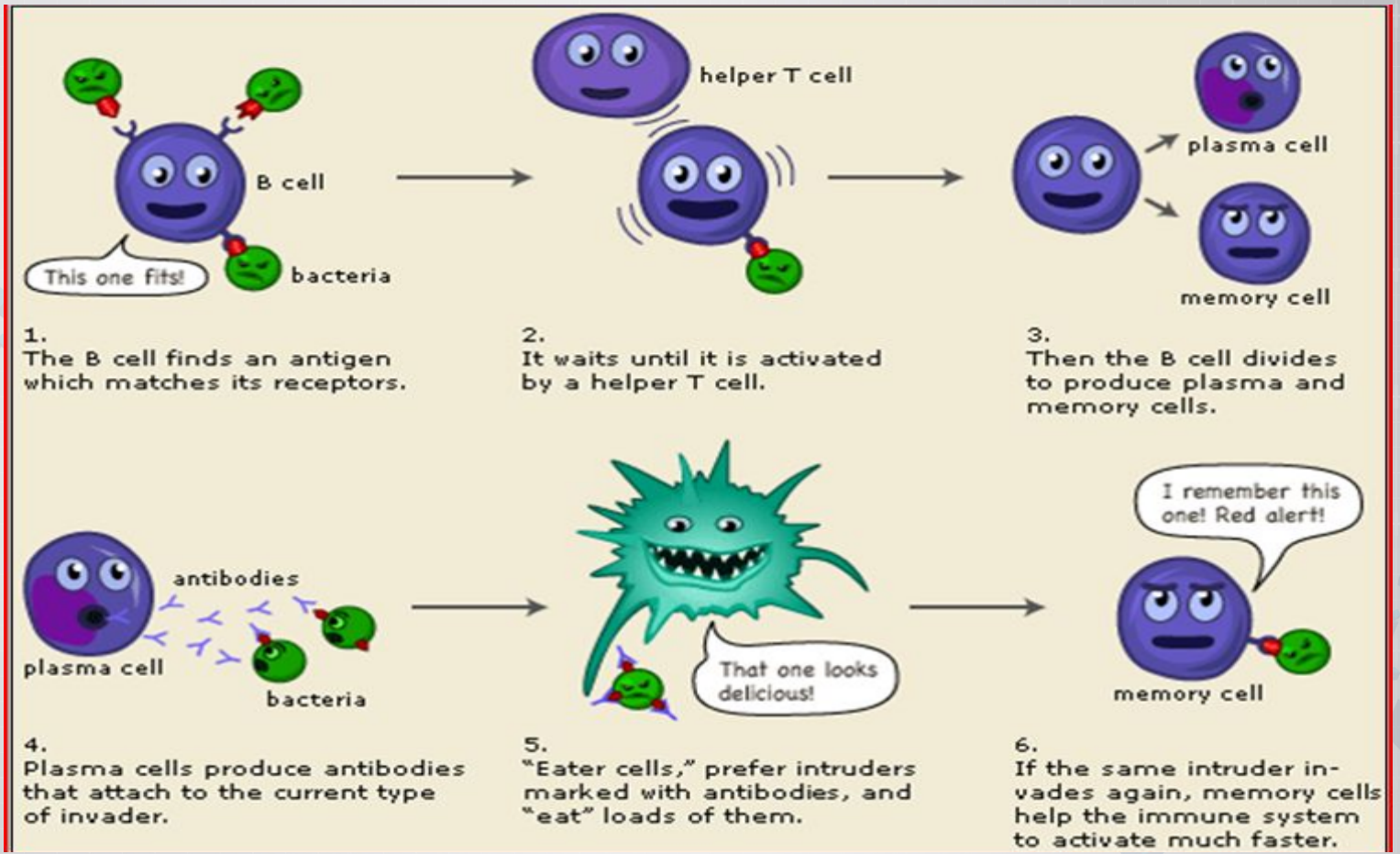
- **T cells** have a variety of roles divided into two broad categories: CD8+ T cells or CD4+ T cells, based on which protein is present on the cell's surface. T cells carry out multiple functions, including killing infected cells and activating or recruiting other immune cells.
- *CD8+ T cells also are called cytotoxic T cells or cytotoxic lymphocytes (CTLs). They are crucial for recognizing and removing virus-infected cells and cancer cells. CTLs have specialized compartments containing cytotoxins that cause apoptosis, i.e., programmed cell death.*

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx

Adaptive Cells

- **There are four major CD4+ T-cell subsets:** TH1, TH2, TH17, and Treg, with "TH" referring to "T helper cell." **TH cells all produce and secrete molecules to alert and activate other immune cells.** TH1 cells are coordinate responses against intracellular microbes, like bacteria. TH2 cells are important for coordinating immune responses against extracellular pathogens and parasites. TH17 produce interleukin 17 and are important for recruiting neutrophils.
- ***Regulatory T cells*** *(Tregs) monitor and inhibit activities of other T cells. They prevent adverse immune activation and responses against the body's own cells and antigens.*

National Institute of Allergy and Infectious Diseases National Institute of Health
http://www.niaid.nih.gov/topics/immunesystem/Pages/immuneCells.aspx



Adapted from: http://sjesci.wikispaces.com/file/view/immune_system_B_cells.jpg

Negative Selection

- The immune system has several processes typically referred to as "negative selection" which keep the body from attacking itself.
- One example is the biological functioning related to T-Cells:
- T-Cells are constantly produced by the body with 'biding receptors' varying according to a pseudo-random process. As T-Cells mature, the binding regions they use to adhere to potential threats are tested by the body. Any T-Cells which bind to self-generated proteins are eliminated and discarded. Other T-Cells are allowed to mature and become useful agents in the immune system. (Forest, 1997) (Hofmeyr, 2000)

Artificial Immune Systems (AIS)

- Modelling the success of biological systems
- **Learning from interactions with threats**
- Adapting to new unknown threats
- **Changing the defense paradigm**

Previous Attempts at AIS

Prior works related to the construction of **Artificial Immune Systems**

Previous Attempts at AIS

- *As early as the late 1990's, there were suggestions of the use of immunological response to computer virus threats.*
- **Specific works related to Artificial Immune Systems (AIS) performed at the University of New Mexico in Albuquerque can be considered exceptionally influential in this realm.**

Previous Attempts at AIS

- ***Anomaly-based detection models were applied to virus detection, host-based intrusion detection and network intrusion detection.***
- **Systems tested exhibited robust resilience due to a distributed design, were very tunable and scalable, were effective at both signature and anomaly based detection, and were highly accurate, adaptable and lightweight in relation to resources they required.**

(Forrest, 1997) (Somayaji, 1998) (Hofmeyr, 2000)

Previous Attempts at AIS

In 1999, Professor Dipankar Dasgupta at the University of Memphis, in Tennessee envisioned the use of mobile agent technology to adapt the immune systems paradigm to computer systems security based on three models: Self/Non Self, Infectious Non Self, and Danger Theory. (Dasguptaa, 2007).

Previous Attempts at AIS

An artificial immune system prototype based on Java development was also employed for computer security issues as a self-adaptive distributed agent-based defense in 2002, with limited success (Harmer, 2002).

Though the agent approach in that work provided great scalability, the prototype employed an approach to threat location which was less than fully effective.

Previous Attempts at AIS

Negative selection and dendritic cell algorithms were also applied to an anomaly based intrusion detection system (Boukerche, 2004 and 2007) with fairly good success.

Boukerche et al. employed mobile agent architecture for anomaly detection based on the analysis of system logs.

The methods employed yielded an improvement in detection, there were a significant number of false positives, based on the configuration.

Previous Attempts at AIS

- There were also a couple relatively successful attempts at misbehavior detection (Sarafijanovic and Le Boudec, 2005 and Dasgupta, 2005).
- Other theories including clonal selection and immune network algorithms gained applications in the fields of pattern recognition and data clustering (Watkins et al., 2004, Zhong et al., 2007 and Chen and Zang, 2009).

Previous Attempts at AIS

- Laurentys, Palhares and Caminhas first applied the danger model, then separately modelled Natural Killer (NK) cell mechanisms to enable Abnormal Event Management fault detection using a novel artificial immune system population-based algorithm.
- A key component in this second implementation was an education mechanism used in negative selection for maturation of the artificial killer cells to train them to become effective (Laurentys, 2010 and 2011). Both of these techniques were considered to be highly effective in testing that was performed.

Moving Target Defense

The importance of changing the defensive paradigm employed.

Moving Target Defense

- Attempting to regain an advantage
- Making defenses less predictable
- Improving the detection method
- Changing the attack surface

Mobile Agents

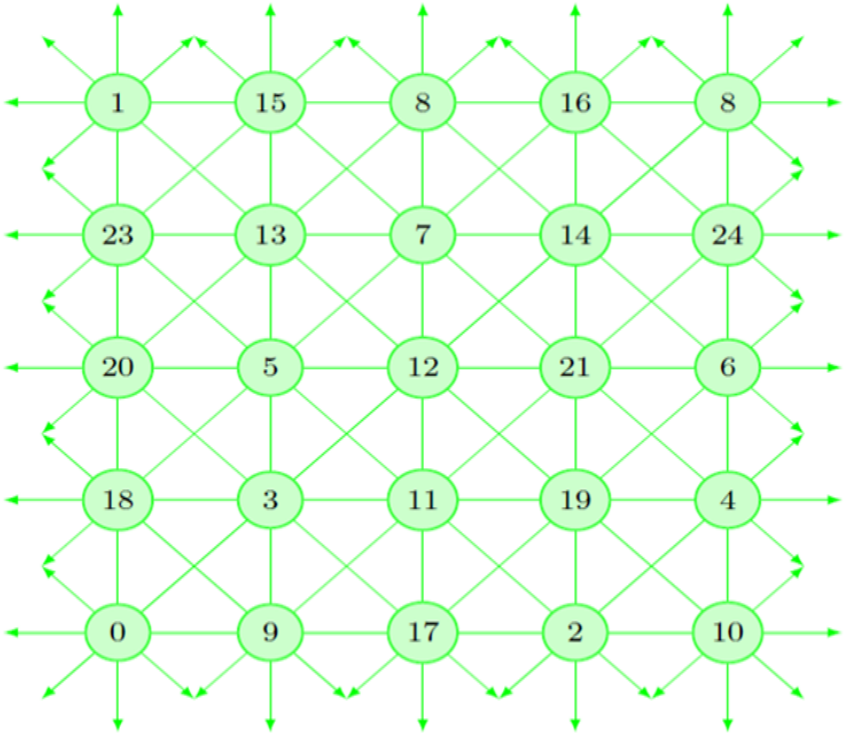
- Mobile software agents can be used to travel from host to host {influenced by an indirect communication (aka stigmergy) through digital signals} constantly looking for evidence of potential security concerns.
- These lightweight agents are designed to operate in a resource-constrained environment, as are commonly found in energy and transportation sectors, without disrupting normal operations. (Fink, 2014).

Organizing Amorphous Networks

- Response times do not often represent proximity
- Logical address doesn't often represent proximity
- Structure is required for a predictable trajectory
- Must delineate the extents of autonomous system
- Indirect communication (stigmergy) can require the ability to recreate the path taken through devices

Organizing Amorphous Networks

- To provide more uniform visitation probability, (a likelihood of the digital agents visiting every node in a network in a timely manner) digital agents wander around a grid which is overlaid on the network to form a simulated geographic distribution.
- A geographic representation provides all nodes with the same number of virtual neighbors, forming a regular graph, where the average visitation probability is similar for all nodes.
- Use of regular toroidal grids provides connectivity to eight neighbors for each node (Dawes, 2012).



Toroidal grid geography.

In the toroidal grid, nodes along the outer edges wrap across or back around to the opposite side.

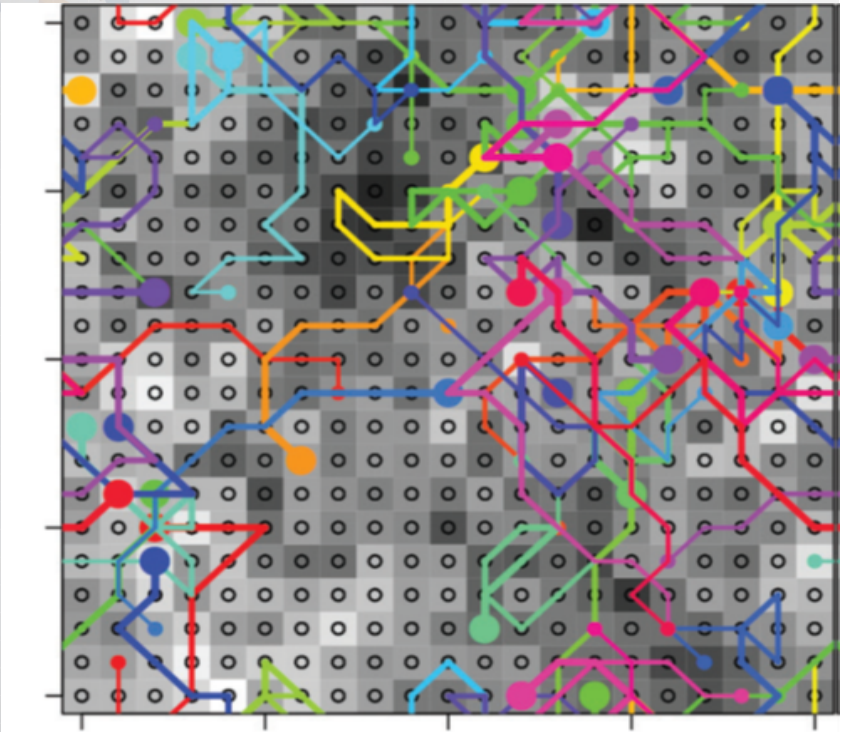
For example: node eight is connected to nodes nine, seventeen and two, as well as being connected to nodes fifteen, thirteen, seven, fourteen and sixteen.

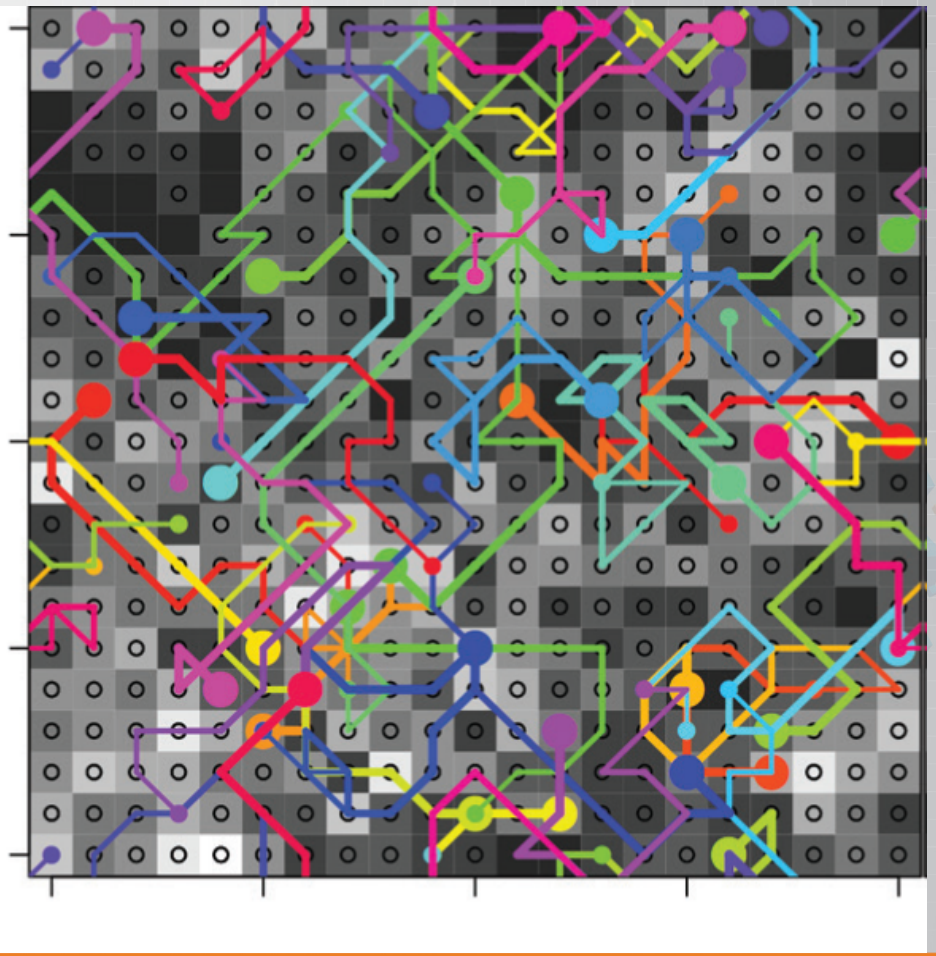
The Toroidal Grid, adapted from: *"Using Mobile Agents and Overlay Networks to Secure Electrical Networks"* (Dawes, 2012).

Prior work in Mobile Agent Defense

- Ant-Based Cyber Defense (ABCD) is a biologically inspired approach to monitoring and defense of computer networks using methods adapted from observation of foraging ants in nature.
- The digital ants in an ABCD system are autonomous and adaptive software agents.
- ABCD provides rapid, stable adaptation to ever changing attack tactics and a dynamic environment. (Fink, 2014).

Ants on the grid





Application of Bioinformatics

The use of genetic matching tools for enhanced anomaly detection.

Application of Bioinformatics

- Advances in rapid and lightweight matching
- Enable new standard in signature matching
- Allow locating new malware types rapidly
- Provide a new method of monitoring logs
- A major improvement in anomaly detection

Genetic Matching Tools

- There have been a lot of advancements in the speed and accuracy of genetic matching processes in recent years.
- FASTP → FASTA → BLAST
- BLAST → ScalaBLAST → ScalaBLAST 2.0
- These are major advancements in bioinformatics.
- *Bioinformatics: Sequence and Genome Analysis*
- These processes work very well for detecting new malware variants and the actions of malicious actors in system logs.

Application of Bioinformatics

Bioinformatic classification converts sequences of system behaviors or program instructions into text strings to use for similarity searches which are calculated using protein-sequencing tools. Similarity leads to family groupings, attribution and rapid identification (Oehmen, 2010). These can then be used to locate previously unseen malware (0-day), and suspect behaviors or attack patterns.

Bioinformatic Classification

- New matching technologies are key enabler not available to previous AIS researchers.
- Advances in rapid bioinformatic classification, as applied to cyber security issues by Dr. Christopher Oehmen, Dr. Elena Pederson and Dr. Glenn Fink of the Pacific Northwest National Laboratory, have yielded an unparalleled opportunity to increase effectivity of malware detection.

Pulling It All Together

Lightweight agents using genetic matching techniques to emulate the biological immune system.

Rapid Detection and Response

Rapid detection mechanisms incorporated with rapid response processes, translate to near machine speed recognition and reaction to emerging threats.

Modelling Biological Systems

- Previous pioneering works on artificial immune systems have proved the model to be effective in isolated sub-system implementations.
- Future work will construct a holistic immune-inspired implementation which interoperates interactively to interpret and respond to threats as they evolve.

Lightweight Digital Agents

Lightweight mobile agent approach and indirect digital communication methods are invaluable contributions to the effectiveness of this model. This is due to the ability of lightweight agents to operate in networked industrial control systems without adversely impacting their performance.

Integration of Successful Components

The separate systems analyzed have proven the capability of immune response mechanisms and the adaptability of an artificial immune system to tackle complex cyber security threats in many different networked system environments.

Complexity of the Problem

- The problem of securing many discrete components, each running their own operating system and applications, and many operating with proprietary protocols and architectures, is very complex and multifaceted.

Complexity of the Problem

- When one considers that each implementation in every organization is further quite unique and has its own vulnerabilities and inherent management issues, it is clear that the solution to the problem must be extremely adaptable and be able to operate independently of any type of architecture constraints.

Complexity of the Solution

Implementation of a holistic immune system approach presents considerable complexity and will require a determined effort to develop interoperability among many different types of mobile agents.

Complexity of the Solution

This complexity is considered to be invaluable however, to ensure an effective detection and response which is mandatory to solve rapidly evolving and complex cyber security problems.

Complexity of the Solution

Modelling many individual immune system components has previously been accomplished.

Modelling the entire immune system provides a much more resilient, adaptable and secure implementation, which can learn interactively.

Important Considerations

- Implementation will make use of network infrastructure equipment (routers, switches and wireless access points) to emulate lymph nodes.
- All stations on the network will be integrated into the immune system on a toroidal grid topology.
- All agents will employ a secure versioning technique to allow for aging out and replacement by new agents.

Important Considerations

- Encryption and versioning will be used to secure agents from emulation and impersonation by outside actors.
- Network components will provide reporting to event management devices for monitoring of the system.
- An experiential learning process will govern response.
- Considerable data on attack vectors and appropriate response will be input as a baseline intelligence.

Conclusions

- The use of diverse digital agents and moving target defense is an important improvement which greatly increases system effectiveness, resistance to attack and potential for misuse.

Conclusions

Digital agent indirect communication is an integral component that can allow distributed components to interoperate and request investigation from other constituents, in order to respond very rapidly to potential threats.

Opportunity to Collaborate

- This work is still in initial stages at this point.
- We are very interested in collaboration with other researchers as well as in any potential funding from various sources.
- These designs be can translated into all types of networked systems in any environment.

Building a Computer Network Immune System

DC Grant – University of Washington – dcgrant@uw.edu

Center for Information Assurance and Cybersecurity

Master Infrastructure Management and Planning

Bachelor of Science Information Technology

Certified Information Systems Security Professional

Certified Information Security Manager