DARPA

Microsoft Research FacultySummit

Building Secure & Resilient Systems for the Future

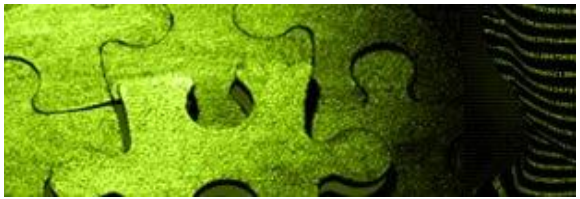
Dr. Howard Shrobe
Program Manager
DARPA/I2O
Principal Research Scientist , MIT CSAIL

FUTURE WORLD 2011 2031

I2O: Mission and Thrusts

Mission: Ensure U.S. technological superiority in all areas where information can be a force multiplier and provide a decisive military advantage.

Thrust Areas



Understand

Empower

Connect

- Intelligence, surveillance, and reconnaissance (ISR) exploitation
- Cyber
- Language, education and training
- Social networking and social sciences

DARPA

THE SITUATION

Increasing Malicious Cyber Activity

"If these trends continue through the end of 2009, there would be a 60 percent increase in malicious cyber activity compared to 2008. … in just the preceding six months, the U.S. military alone had spent more than $100 million … to remediate attacks on its networks"

2009 report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Eleventh Congress, November 2009

Figure 1: DoD Reported Incidents of Malicious Cyber Activity, 2000–2008, With Projection for 2009

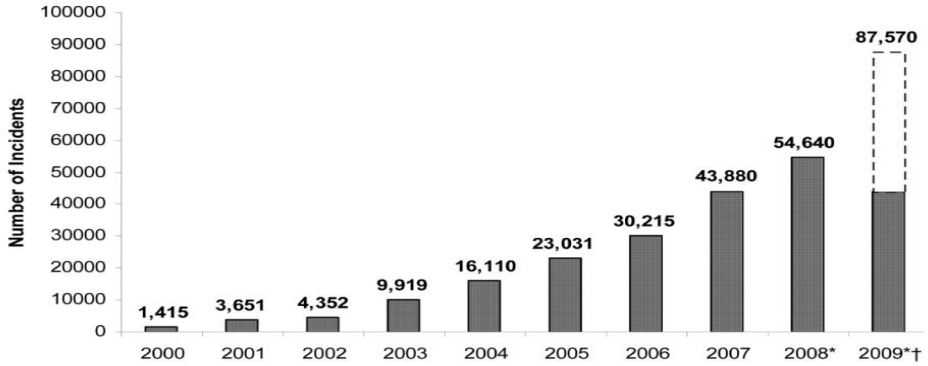
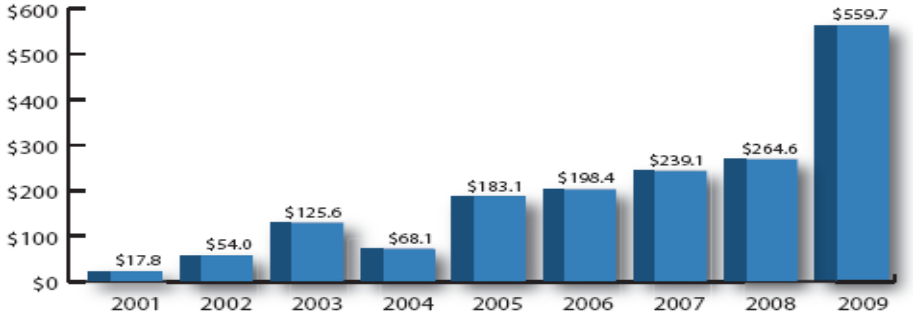
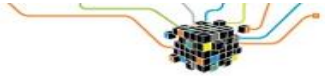


Figure 2: Yearly Dollar Loss (in millions) of Referred Complaints



Stuxnet: Cyber Physical Systems Under Attack

Bits (NY Times)



Business ▪ Innovation ▪ Technology ▪ Society

September 24, 2010, 8:41 PM

Malware Hits Computerized Industrial Equipment

By RIVA RICHMOND

… Security experts say Stuxnet attacked the software in specialized industrial control equipment made by Siemens … the first such attack on critical industrial infrastructure that sits at the foundation of modern economies.

Eric Chien, the technical director of Symantic … said it appeared that the malware was created to attack an Iranian industrial facility. … The specific facility that was in Stuxnet's crosshairs is not known, though speculation has centered on gas and nuclear installations.

… malware experts say it could have been designed to trigger such Hollywood-style bedlam as overloaded turbines, exploding pipelines and nuclear centrifuges spinning so fast that they break. "The true end goal of Stuxnet is cyber sabotage. **It's a cyber weapon basically**," said Roel Schouwenberg, a senior antivirus researcher at Kaspersky, a security software maker.

Power Grid At Risk

CNN.com /US

HOME | WORLD | U.S. | POLITICS | CRIME | ENTERTAINMENT | HEALTH | TECH | TRAVEL | LIVING | BUSINESS | SPORTS | TIME.COM | VIDEO | IREPORT

Hot Topics » Where The Jobs Are • CNN Heroes • Planet in Peril • First 100 Days • more topics » Weather Forecast International E

updated 9:17 a.m. EDT, Thu September 27, 2007

EMAIL SAVE PRINT

Mouse click could plunge city into darkness, experts say

STORY HIGHLIGHTS

- Sources: Similar attack could hurt generators that produce nation's electricity
- Experts fear attacks could cause damage that would take months to fix
- Department of Homeland Security said staged attack took place in March

INTERNET LAW - CIA Report: Cyber Extortionists Attacked Foreign Power Grid, Disrupting Delivery

Kelly O'Connell, IBLS Editor
Wednesday, January 23, 2008

Email Discuss Print

In an unusually bold statement detailing another incursion of the Net battle targeting government sites, the CIA admitted web hackers penetrated overseas power grids, compromising service while demanding payment in exchange for cessation. The U.S. Central Intelligence Agency made this announcement at a meeting hosted by the SANS Institute on January 16, in New Orleans, LA. The meeting was of 300 U.S., British, Swedish, and Dutch government officials, engineers and security managers from electric, water, oil & gas and other essential infrastructure industry asset owners from North America. The SANS Institute offers solutions for hacked companies.

Cyber War: The Georgian Campaign

The cyber attacks began on a large scale within a few hours of when the Russian military operations began, and they ended just after the Russian military operations ended. The targets for attack were nearly all ones that would produce benefits for the Russian military. The one target that was somewhat unusual from a military standpoint was a website for renting diesel-power electric generators, but even this target was presumably chosen to reinforce the effects of physical strikes on the Georgian power grid. More strikingly still, the news media and communications facilities, which would ordinarily have been attacked by missiles or bombs during the first phase of an invasion were spared physical destruction, presumably because they were being effectively shut down by cyber attacks.

Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008

DARPA

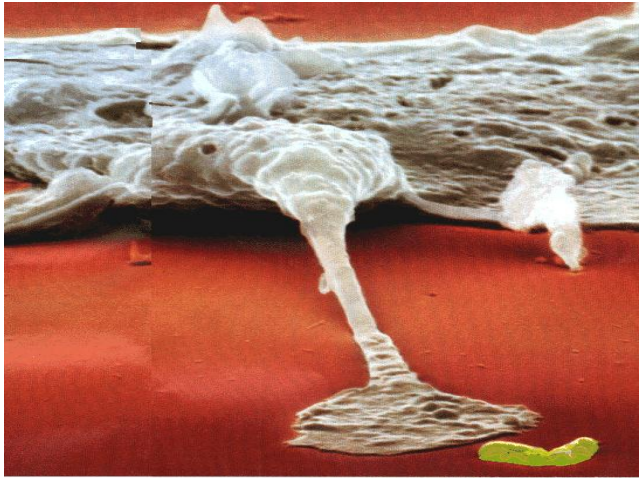
FRAMEWORK AND ANALYSIS

HOW DO YOU DEFEND AGAINST AN ORGANIZED CYBER THREAT?

Two Models of Survivability

Fortress (Traditional)

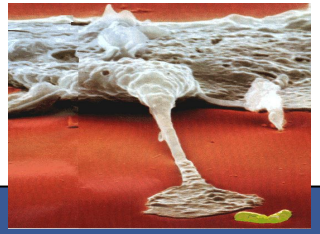
- Impenetrable (hopefully)
- Monolithic
- Single layer
- Rigid
- Immobile



Organism

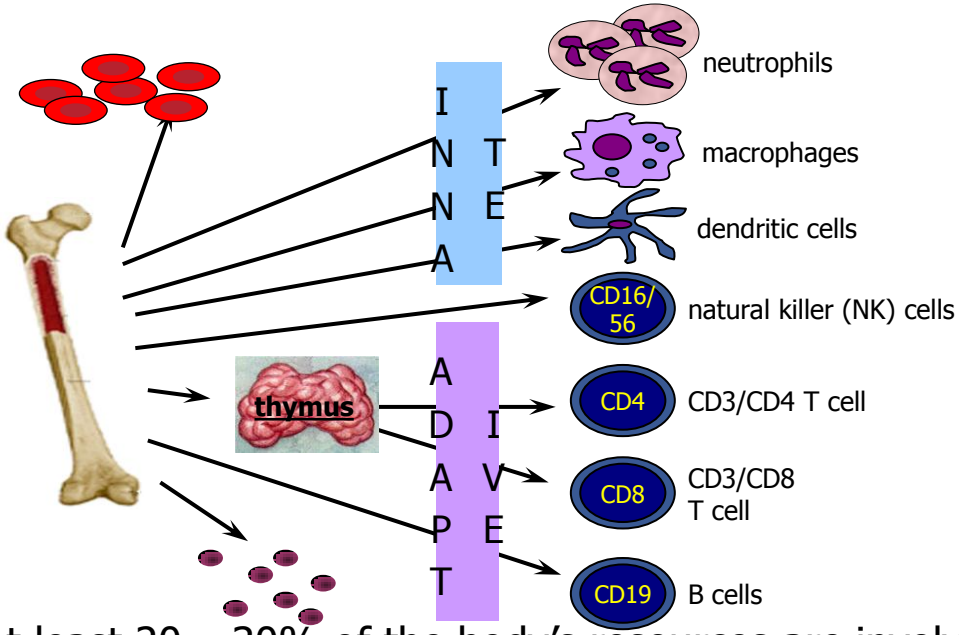
- Many partial barriers
- Heterogeneous
- Defense in depth and self healing
- Adapts, learns, evolves
- Mobile

Biology and Computation: Two Design Styles



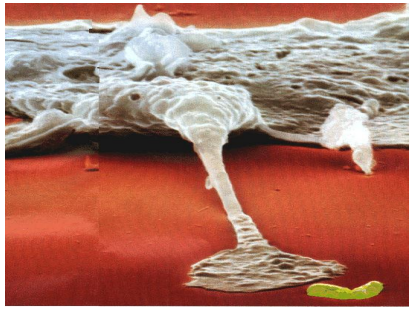
Computation	Biological
Near Perfect Components	Fallible components
Core design formed in era of scarcity	Abundance of resources
Core design formed in isolated environment	Evolution in ecosystem of predators and parasites
Evolutionary pressure from market: price, performance and features	Evolutionary pressure from ecosystem: survivability
Self-regulation and adaptation rarely considered. Runs open-loop.	Self-regulation and adaptation are core mechanisms. Closed loop control.
No enterprise-wide survivability mechanisms	Diversity for population survival Public-health systems in human society

Innate Immunity, Adaptive Immunity, Diversity



Fast, but inflexible, covers fixed sets of pathogen that are always present. Supports the adaptive immune system.

Slower, learns to recognize new sets of pathogens, distinguishes self from non-self, retains memory to guard against future attacks.

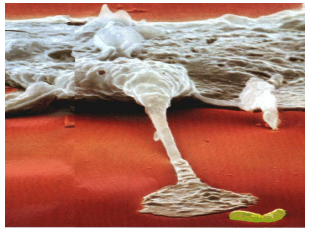


At least 20 – 30% of the body's resources are involved in constant surveillance and containment.

Diversity over time and across the population prevents mass extinction

CRASH: Clean-slate design of Resilient Adaptive Secure Hosts

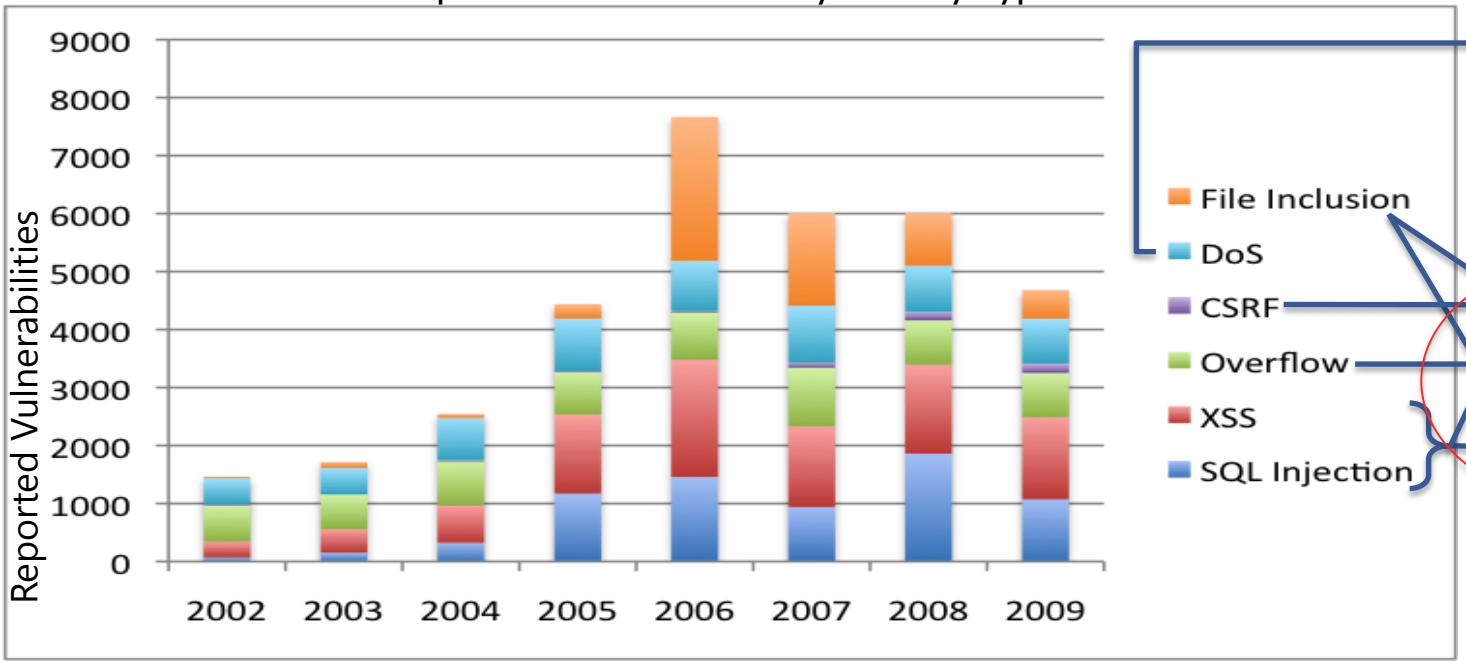
Innate Immunity 

 Adaptive Immunity

Dynamic Diversity

Few Root Causes of Technical Vulnerabilities

Number of Reported Vulnerabilities by Year by Type



The innate system only has to protect these very few key semantic properties

Meta-data Enforcement Is the Key

Objects:

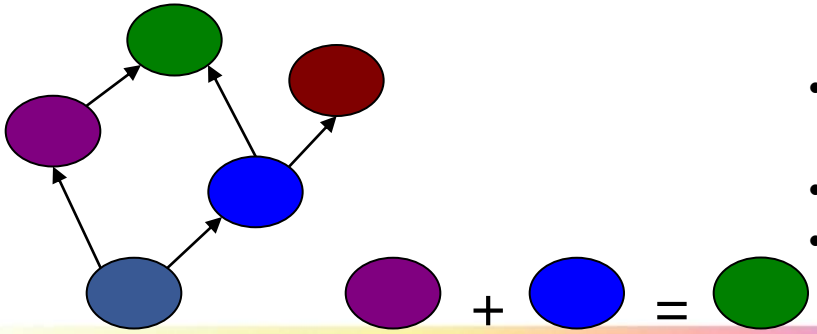
- Memory is a structured collection of objects
- Objects have: Type, Bounds, Identity

Compartments:

- Compartment = Collection of Data with common access rights
- Every thread has an associated compartment (where it can allocate data)
- Organized in a lattice

Principals:

- Principal = An active entity
- Each running process has an associated principal
- Principals are organized in a lattice

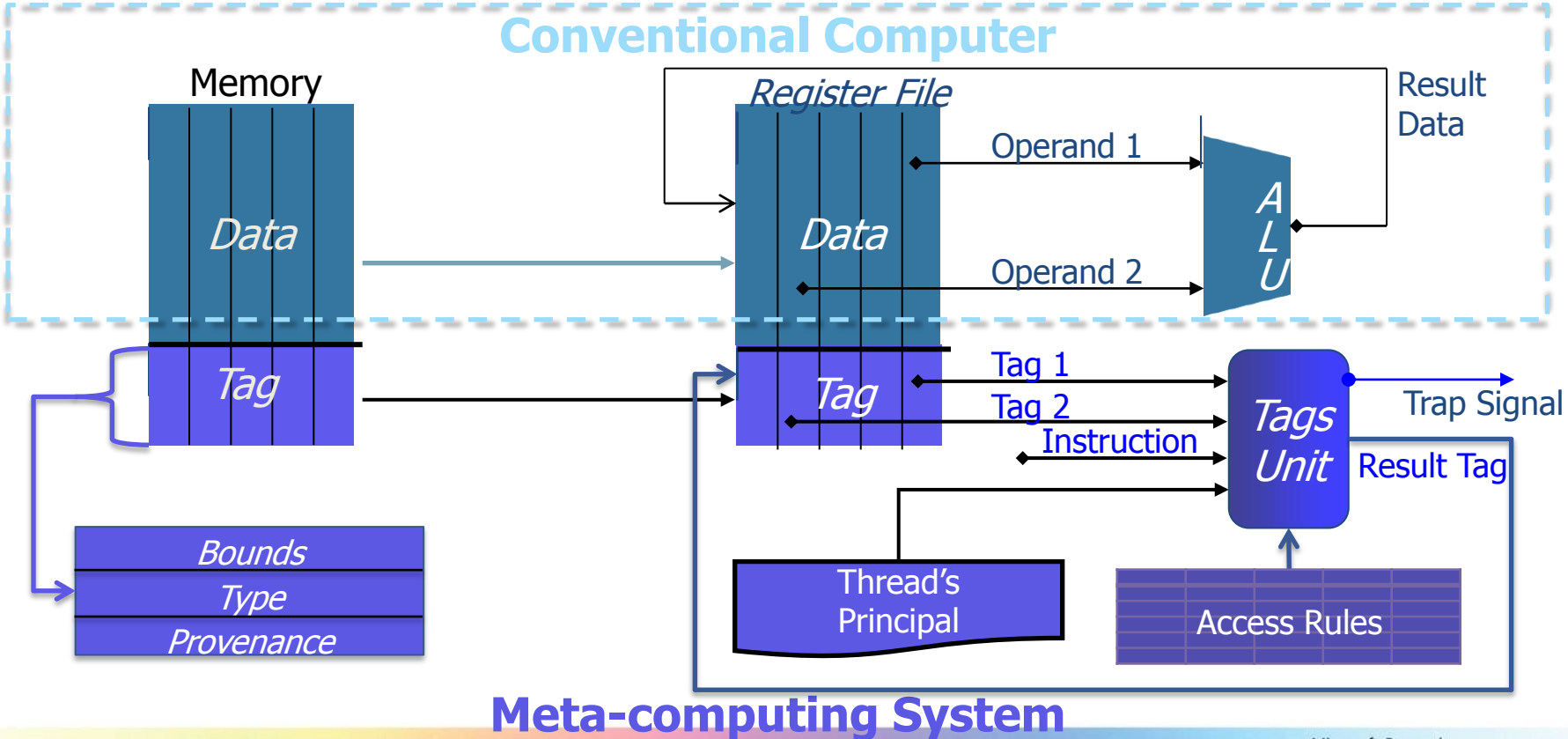


Access Rules:

- For each operation, a matrix of which principals can perform the operation on data in which compartments
- Specifies compartment of result
- Collectively enforces a policy restricting flows between compartments

INNATE IMMUNITY: COMPLETE MEDIATION THROUGH HARDWARE ENFORCEMENT

Hardware Mediation

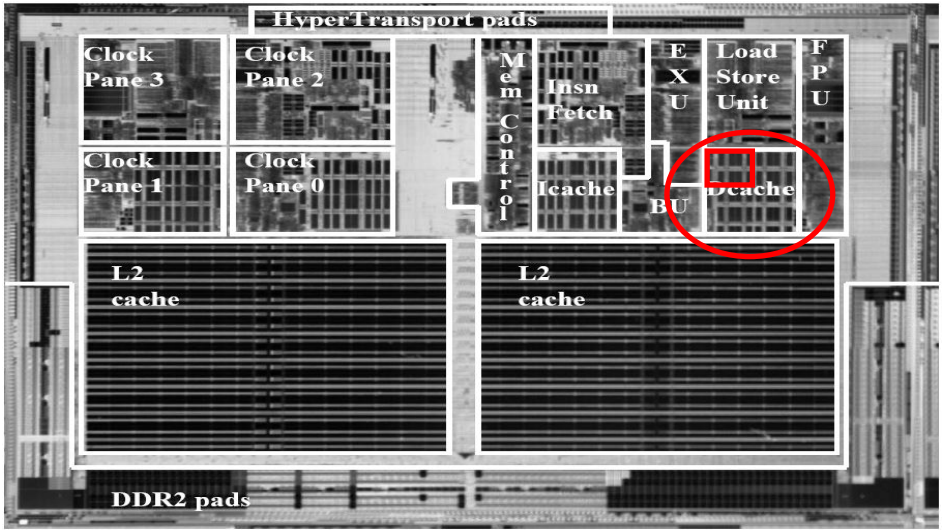


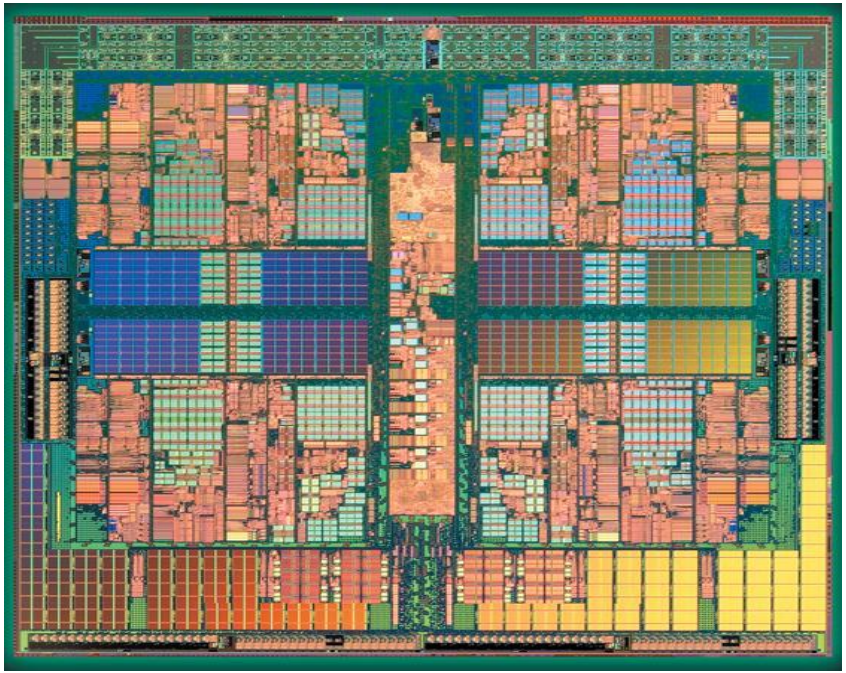
Hardware immunity comes cheaply

Tag Processing Unit is about 125K bits

125,000 SRAM bits < 16K Bytes

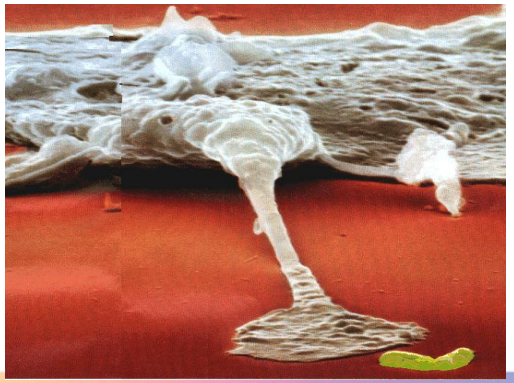
Note: L1 Dcache on Opteron is 64KB



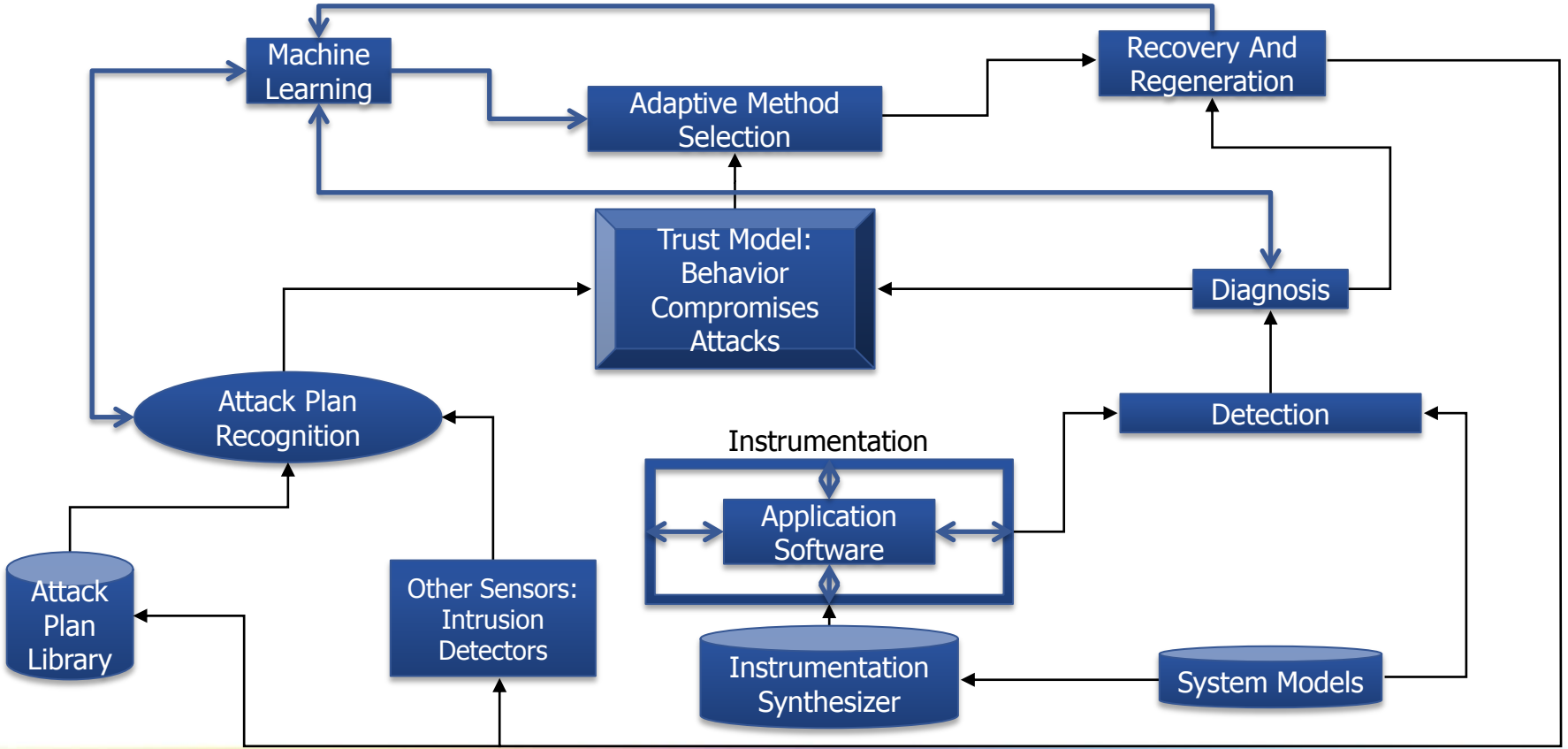


Dual and Quad Core Opterons

ADAPTIVE IMMUNITY: NEW SELF-ADAPTIVE SOFTWARE ARCHITECTURES

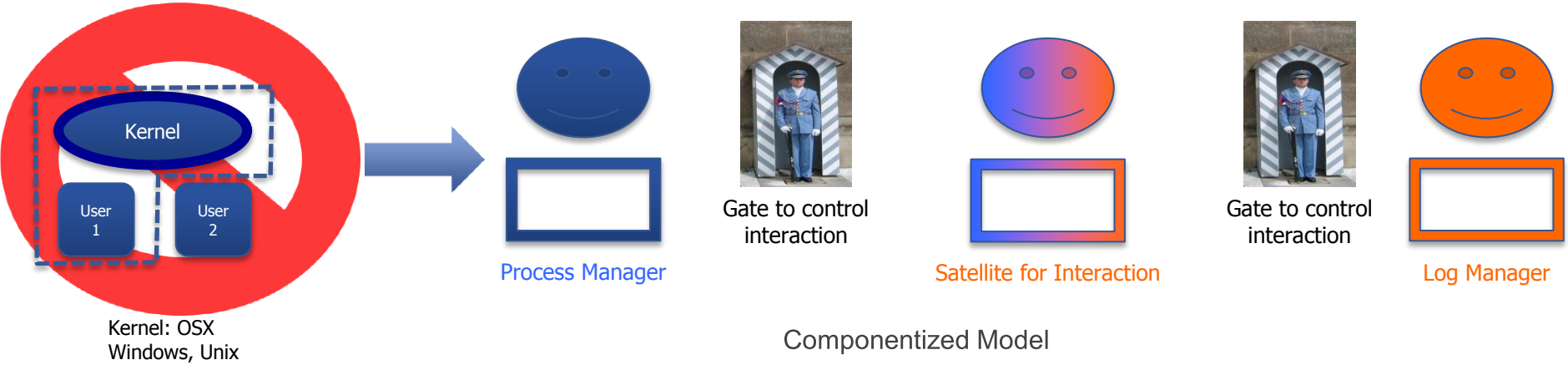


Self-Adaptive Defensive Architecture

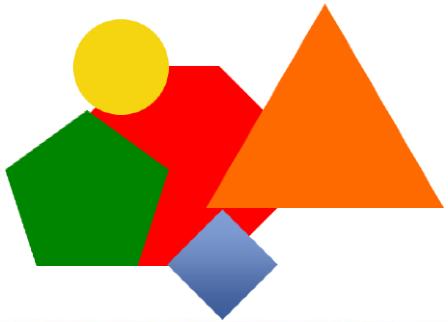


Information Flow and Componentization

- System software is a flat federation of components
- Components operate according to least privilege, no all powerful kernel
- Each system component has its own **compartment** for its private data
- Each system component has its own **principal** for indicating who it is representing
- System components may have "**satellite**" compartments and principals for controlled interactions with users and other system components
- Gates are used to manage privilege level, control and information flow between components

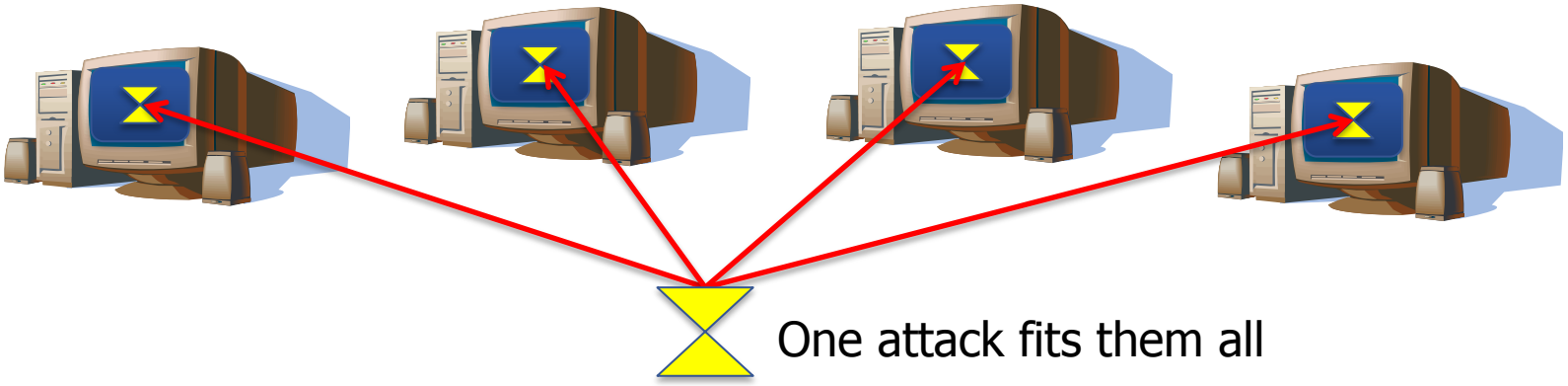


DYNAMIC DIVERSITY: BREAKING THE COMPUTATIONAL MONCULTURE



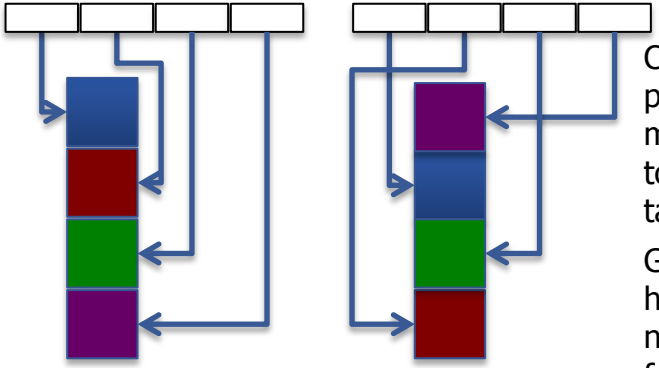
Monocultures are not survivable

- The attacker's work factor is proportional to entropy
  - When all systems are the same, a single attack disables them all
  - When a single system never changes, the same attack will work repeatedly
- We currently have a computational monoculture.



Dynamic Diversity

Address space randomization



Code and/or data blocks are periodically repositioned in memory so that attacker has to work harder to find a target.

Garbage-Collected memory has the property inherently, new methods may optimize for increased entropy.

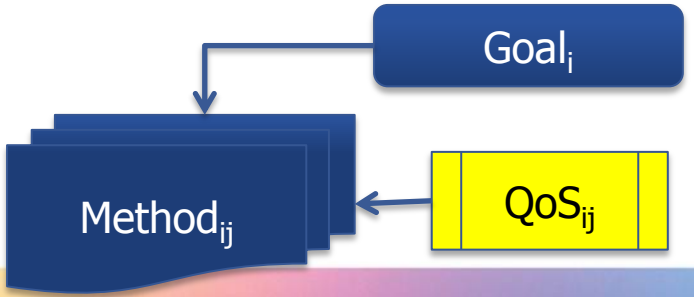
Instruction set randomization

Disk	Memory	ICache
Instruction-1	Encrypted-1	instruction-1
Instruction-2	Encrypted-2	instruction-2
Instruction-3	Encrypted-3	instruction-3
Instruction-4	Encrypted-4	instruction-4
Instruction-5	Injected-1	Encrypted-1
Instrution-6	Injected-2	Encrypted-1
	Encrypted-5	instruction-5
	Encrypted-6	instruction-6

Code is encrypted as it enters memory and Decrypted as it enters the instruction cache (or translation buffer). Injected code in native instruction set is then encrypted and not executable. Encryption key can be varied by process and time.

Functional Redundancy & Decision Theoretic Dispatch

There are multiple methods for achieving each goal ("n-version programming"). Each distinct method has different qualities of service. Method selection is driven both by preferences over QoS and by need for unpredictability.



Mission-oriented Resilient Clouds

Clean-slate mission-aware security for cloud computing and enterprise-scale networked systems

Clouds On The Horizon

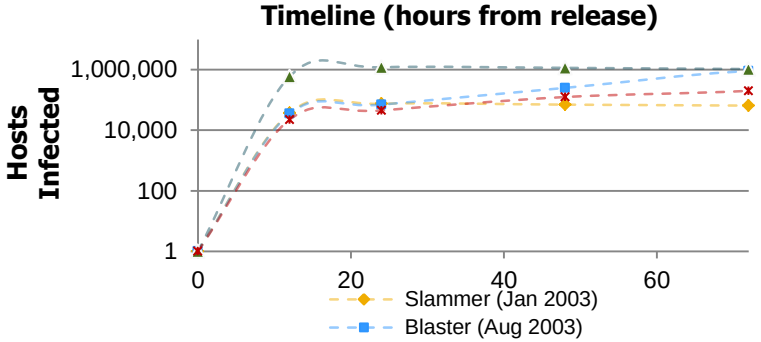
The drive to cloud computing:

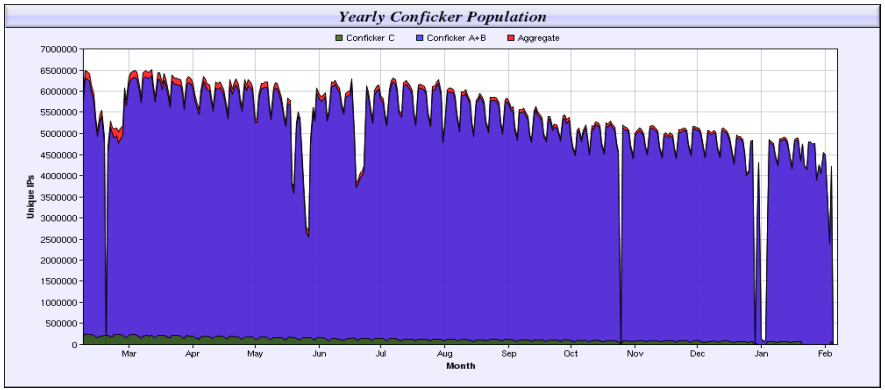
- The White House released a 25-point plan in December for reforming government IT, and it included a **requirement that agencies adopt a cloud-first policy** for new IT deployments
- "We believe that initiatives such as the federal CIO's plan … **are accelerating DOD toward cloud computing** and shared enterprise service," said Dave Mihelcic, the Defense Information Systems Agency's chief technology officer. (Defense Systems Jan 20, 2011)
- *"…Agencies will be expected to adopt cloud computing solutions where they represent the best value at an acceptable level of risk."* (8 June 2010 memo from Peter R. Orszag, OMB Director).

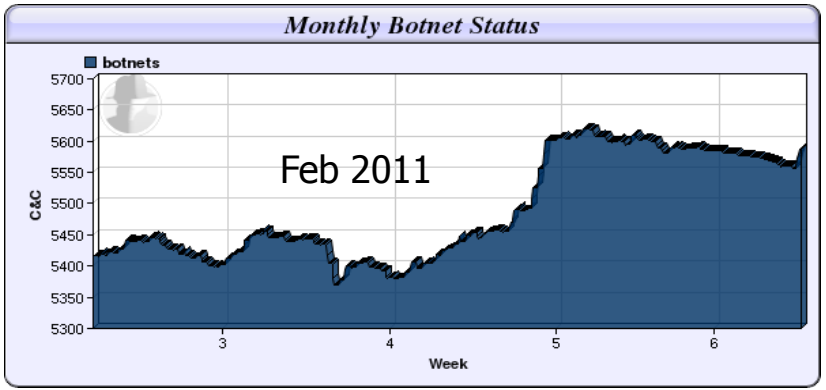
Motivations for moving to the cloud:

- (Undisputed) Economic efficiency of large scale data centers for both computation and storage
- (Putative) Manageability of large scale data centers
- Availability of "fungible computation" on demand
- Conceptual centralization of data for common analytics (ISAT "War Clouds" study)

The Network is a *Vulnerability Amplifier*

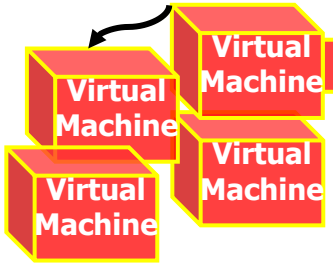




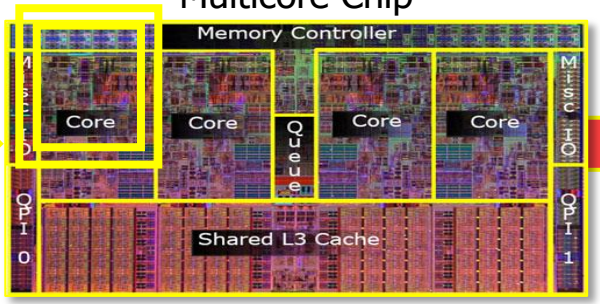


Cloud Computing Infrastructure

Your Software Lives Here



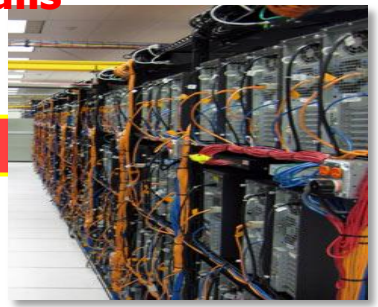
Multicore Chip



1U Blade in Blade Server

Your Software Lives On A Network with 100K Other Virtual Machines and Few Internal Firewalls

Modular Data Center Containers



Blade Server Racks

Blade Server Network

Resilient Clouds: A Community that uses the Network as a *Defensive Amplifier*

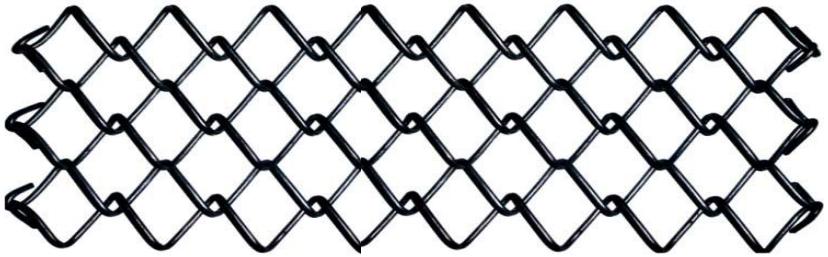
TODAY

Acting as individuals makes the enterprise weaker than the sum of its parts

- "Box" Oriented
- Vulnerable Components
- Static Sitting Duck
- Shared Vulnerabilities
- Implicit Trust is Amplifier

RESILIENT CLOUDS (CRASH++)

Acting as a community makes the enterprise stronger than the sum of its parts



- Mission Optimized
- CRASH-worthy components
- Moving Target
- Resilience through Diversity
- Collective Diagnosis is Damper

Resilient Clouds: a "Pubic Health System" for Cloud Computing

A diverse and changeable ensemble of "locked-down" hosts collects information from:

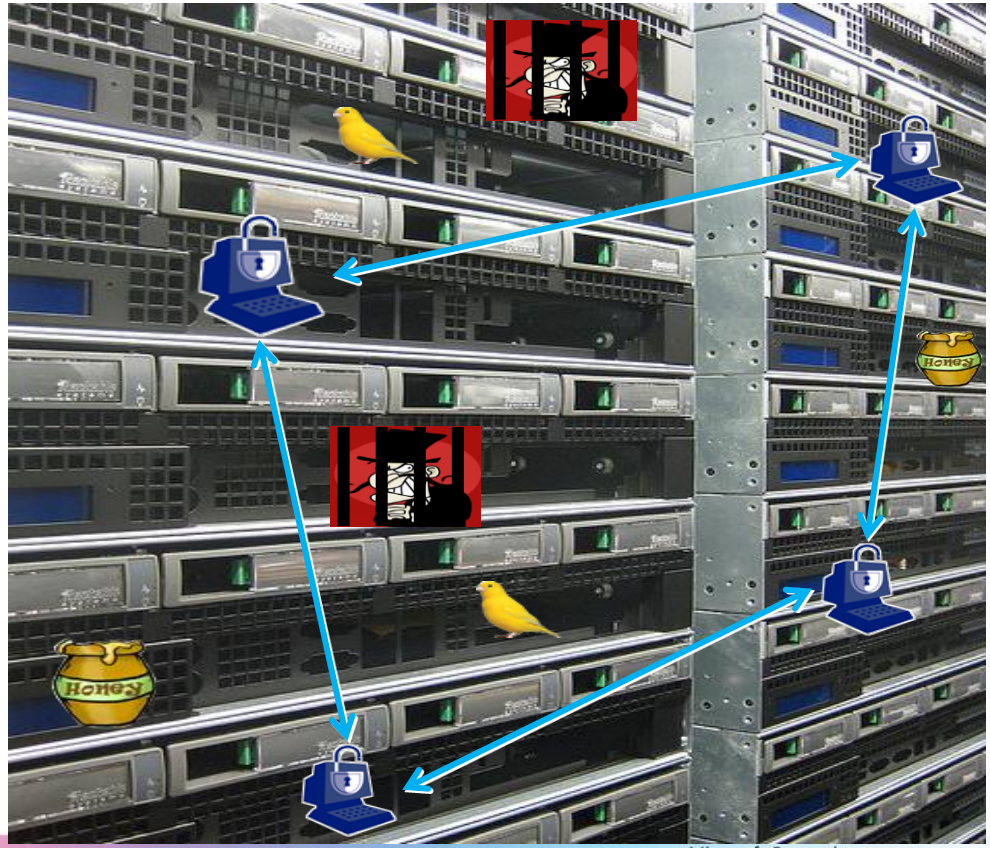
- Normal hosts
- Canaries
- Honeypots
- Encapsulated Malware

Functions:

- Diagnosis
- Attack plan prediction
- Patch distribution
- Quarantining
- Controlling diversification
- Allocation of resources

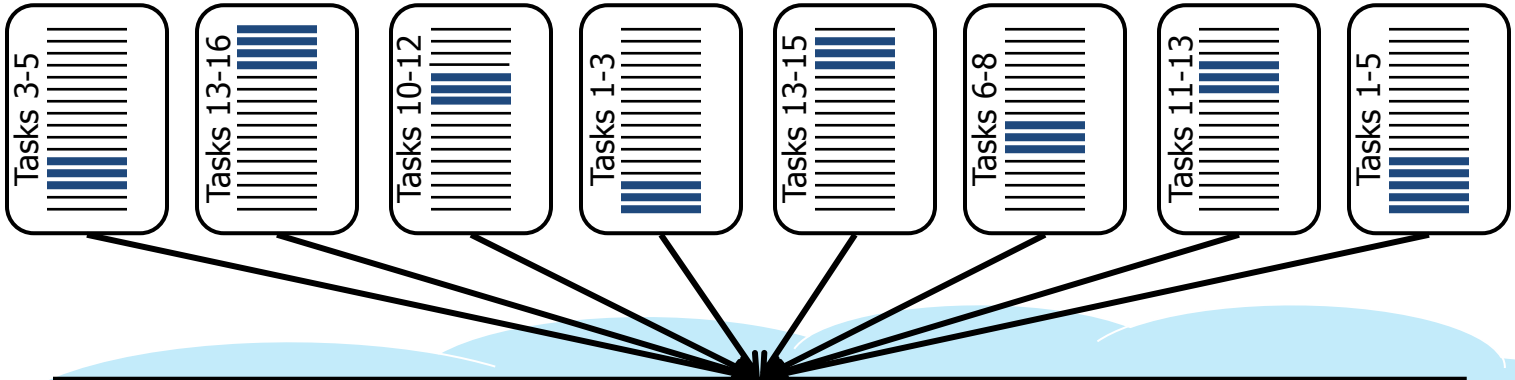
Self Protection through:

- Quorum Computation
- Threshold Storage
- Moving target defense
- CRASH components



Resilient Clouds In Action

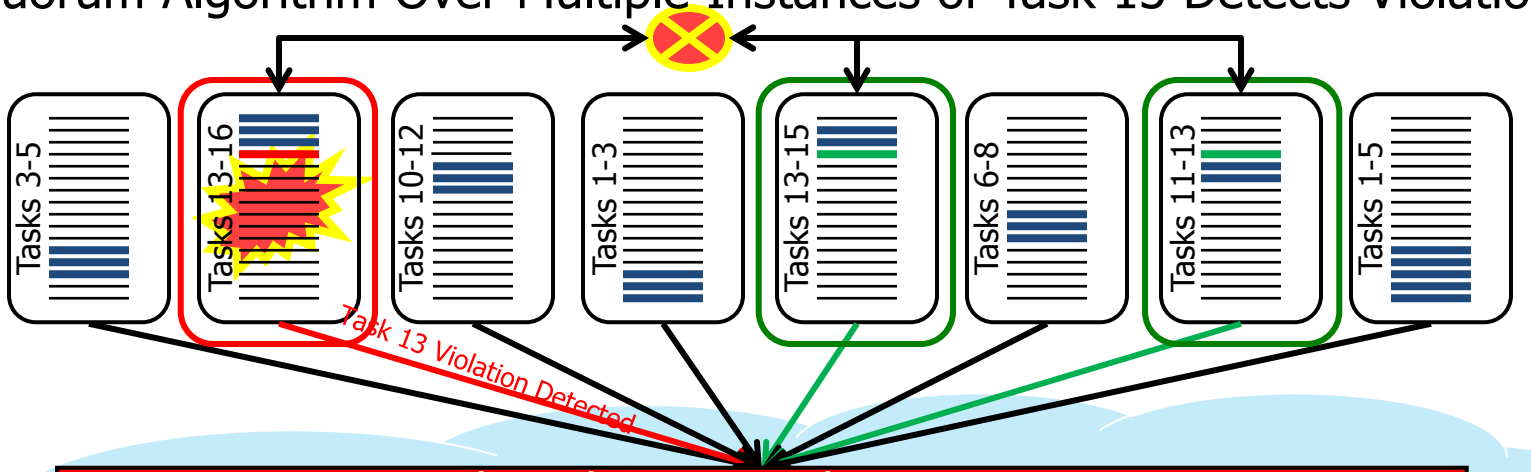
Initiating the Mission: Tasks are assigned to hosts and the network is configured to maximize mission effectiveness



Distributed, Highly Resilient Cloud Defense System

Resilient Clouds In Action

Quorum Algorithm Over Multiple Instances of Task 13 Detects Violation



Shared Situational Awareness

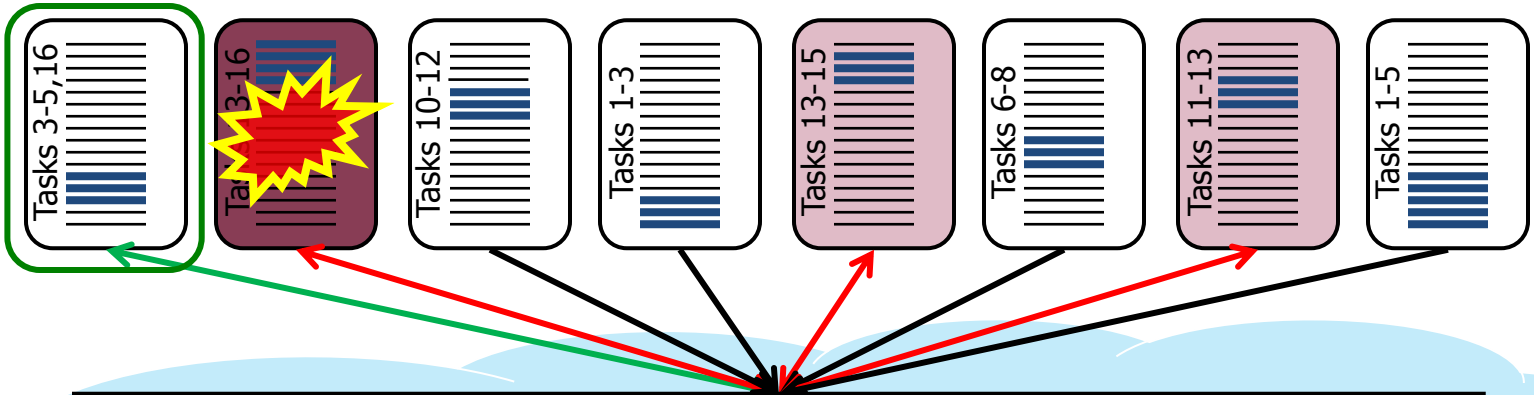
Mission-aware Resource Optimization

Taskable Diversity	Mission-Aware Networking

Distributed, Highly Resilient Cloud Defense System

Resilient Clouds In Action

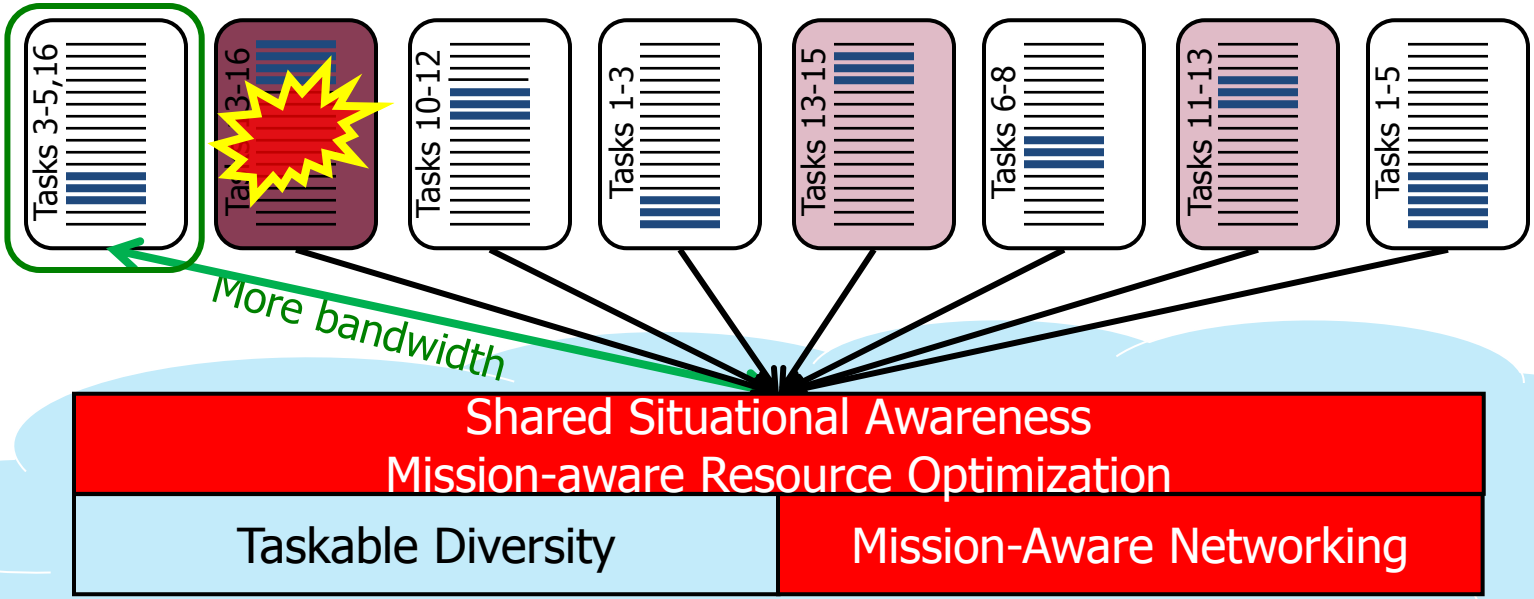
Migrate Task 16 to unaffected host



Distributed, Highly Resilient Cloud Defense System

Resilient Clouds In Action

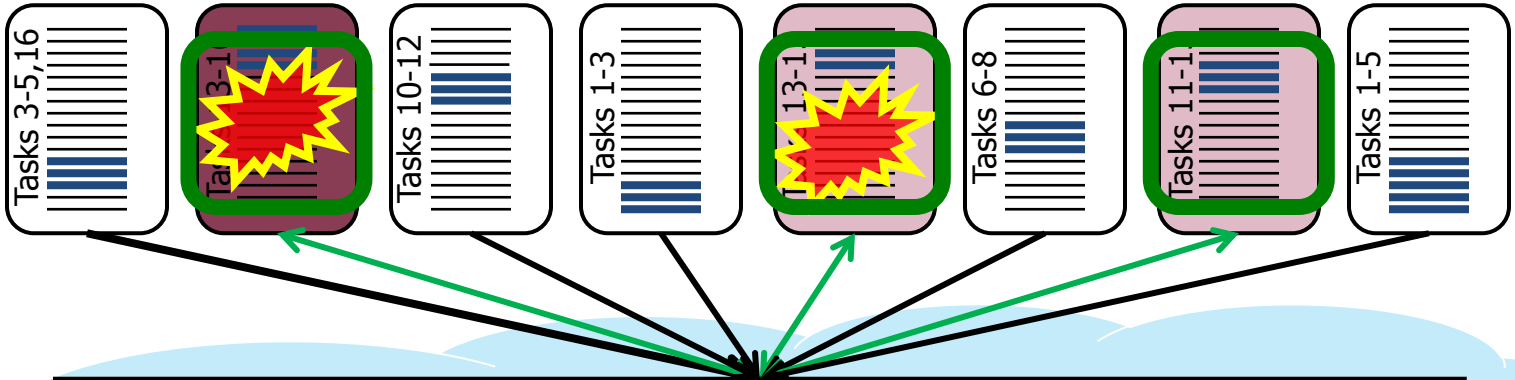
Increase communication network priority for host receiving task 16



Distributed, Highly Resilient Cloud Defense System

Resilient Clouds In Action

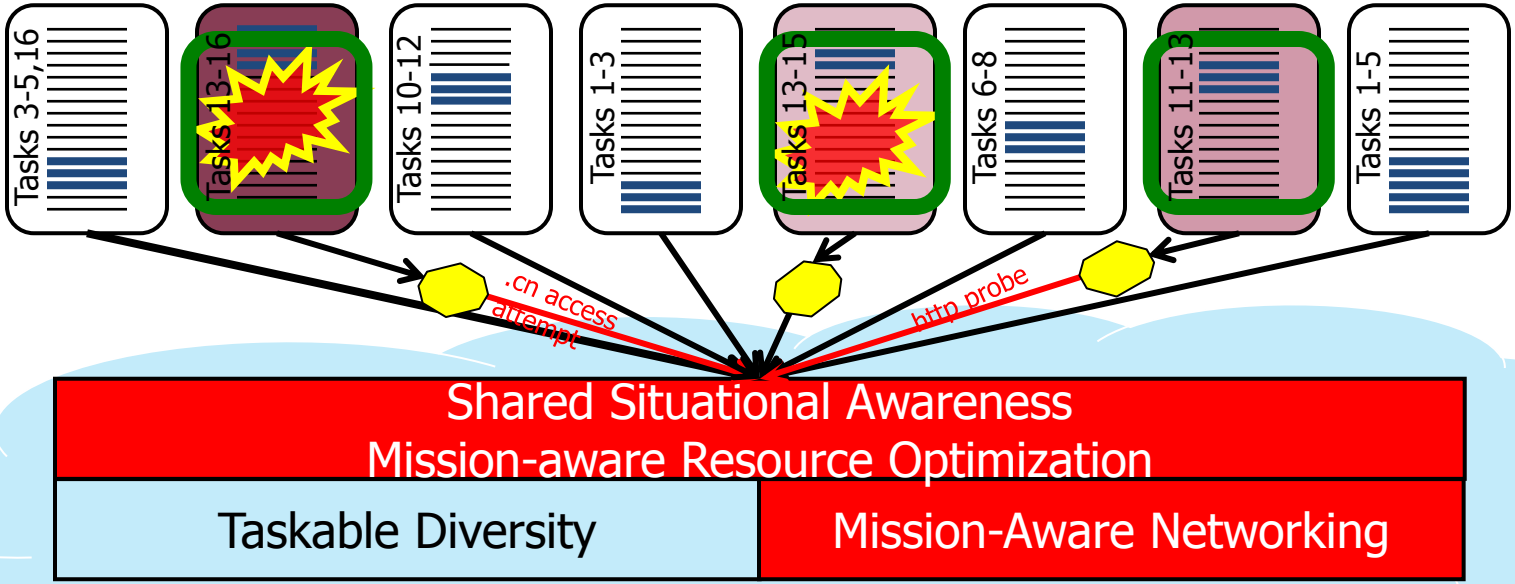
Detectors, Patches & Workarounds for Task 13 vulnerability are distributed to all affected hosts



Distributed, Highly Resilient Cloud Defense System

Resilient Clouds In Action

Attempt to communicate with hostile domain is detected.
Global plan for botnet attack is recognized.

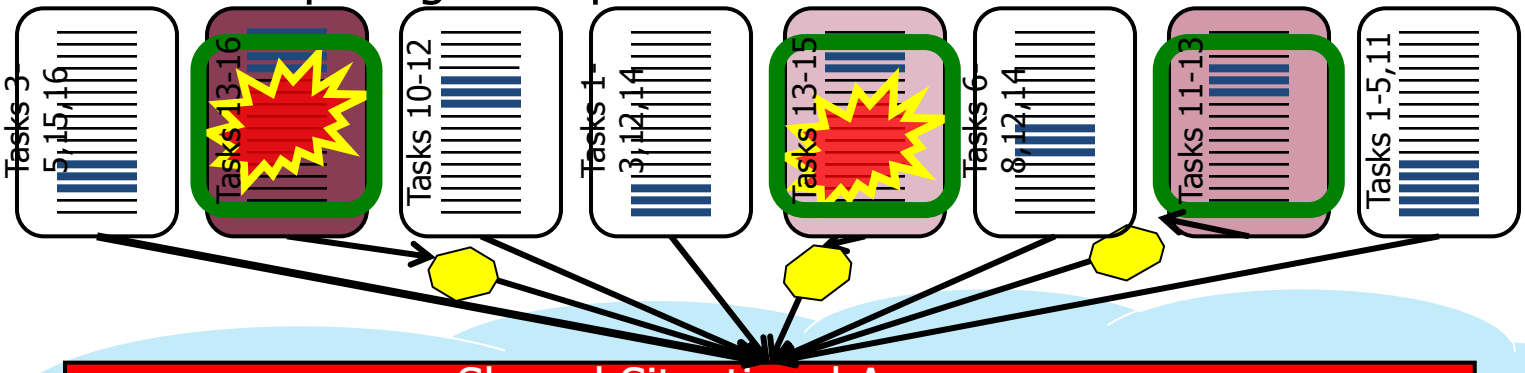


Distributed, Highly Resilient Cloud Defense System

Network Isolation and Monitoring

Resilient Clouds In Action

Quarantine hosts running Task 13.
Migrate Tasks 11, 12, 14, and 15 from those hosts.
Accept degraded performance on Tasks 11 and 15.



Shared Situational Awareness
Mission-aware Resource Optimization

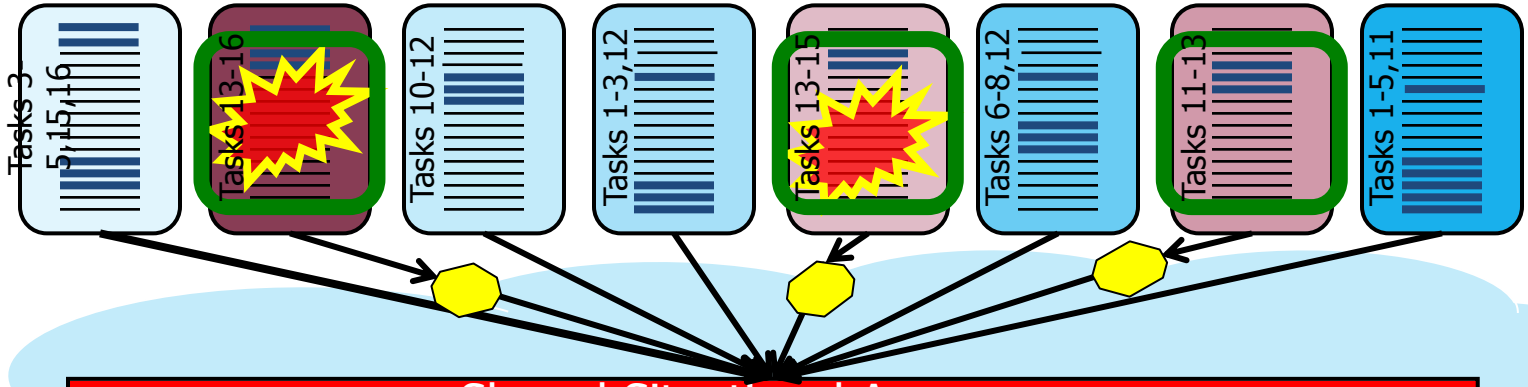
Taskable Diversity | Mission-Aware Networking

Distributed, Highly Resilient Cloud Defense System

Network Isolation and Monitoring

Resilient Clouds In Action

Uncompromised hosts directed to employ additional diversity.
Network directed to perform "IP hopping".
Task 14 sacrificed to compensate for diversity cost.



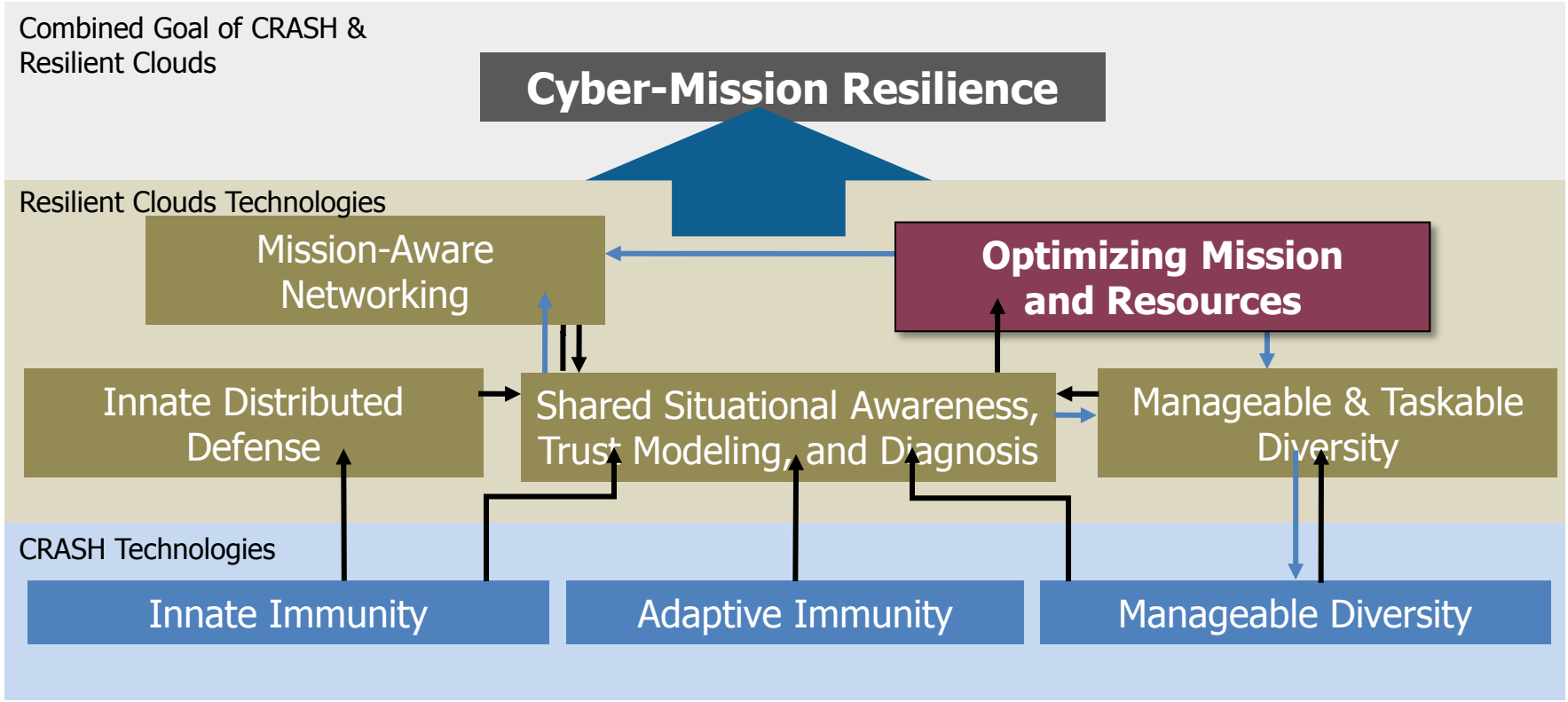
Shared Situational Awareness
Mission-aware Resource Optimization

Taskable Diversity | Mission-Aware Networking

Distributed, Highly Resilient Cloud Defense System

Network Isolation and Monitoring

Resilient Clouds Technology Areas



Biosocial Concepts Underpinning Resilient Clouds

RESILIENT CLOUDS	CRASH
Herd immunity	Individual immunity
Community-wide Public Health	Self-healing
Manageable diversity across the entire ensemble	Diversity of individual over time
Focused on achieving mission goals even if a host or network needs to be sacrificed	Focused on preserving the computations within a host

- **Herd immunity provides a measure of protection for individuals who have not developed immunity.** It occurs when a significant portion (the threshold) of a population (or herd) have been vaccinated or are innately immune.*
- **Cloud-wide community health makes the population more robust than any individual:** By sharing information about infections, their prevalence, transmission and their effective treatment, we can mount defenses (including quarantine, vaccination and relocation of important work) that make the population more immune than any individual.
- **Population diversity leads to population survivability:** Avoiding monoculture prevents any single infection from disabling the entire population.

* John TJ, Samuel R (2000). "Herd immunity and herd effect: new insights and definitions". *Eur. J. Epidemiol.* ***16 (7): 601–6***

www.darpa.mil