



From Auto-Adaptive to Survivable and Self-Regenerative Systems Successes, Challenges, and Future

Michael Atighetchi, Partha Pal

matighet@bbn.com, ppal@bbn.com

July 9 2009

1st Workshop on
Biologically Inspired and Cognitive Approaches to Mission Survivability
(BioCoMS)

NCA 2009

1

www.bbn.com

Outline

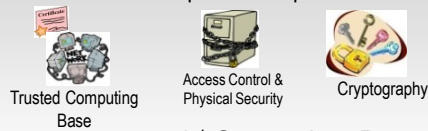
- Past work in Intrusion Tolerance
 - Successes So Far
 - Survivability Architecture
 - Cognitive Survivability Management
 - Bio-Inspired Defenses
- Challenges
 - Using Cognitive Approaches
 - Biologically inspired selection functions
 - Effective Evaluation
- New Trends and Opportunities
 - SOA, Cloud Computing

2

Generations of Security Research

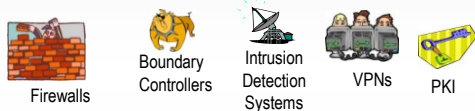
No system is perfectly secure— only adequately secured with respect to the perceived threat.

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)



But intrusions will occur

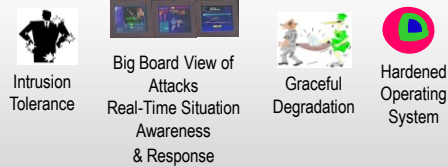
Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)



1st Generation: Protection

But some attacks will succeed

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)



2nd Generation: Detection

3rd Generation: Intrusion Tolerance and Survivability

Survivability and Intrusion Tolerance

Premise

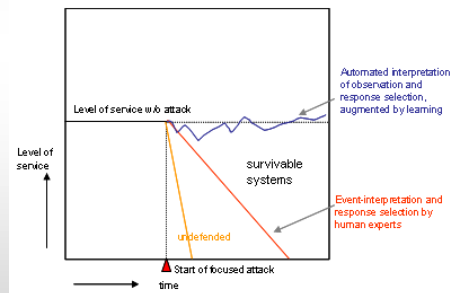
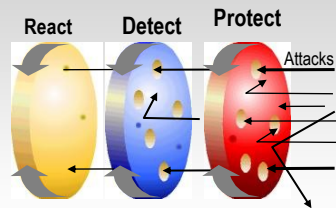
- The number & sophistication of cyber attacks is increasing – some of these attacks will succeed

Philosophy

- Operate through attacks by using a layered defense-in-depth concept
 - Accept some degradation
 - Protect (C, I, A) of most valuable assets (information, services, ...)
 - Move faster than the intruder

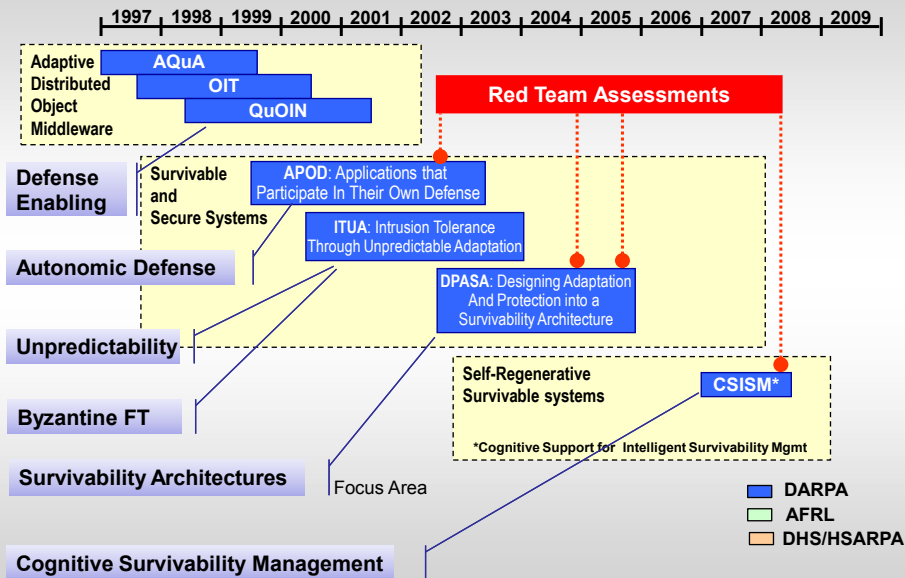
Approach

- “Defense Enabling” Distributed Applications
- Survivability architecture



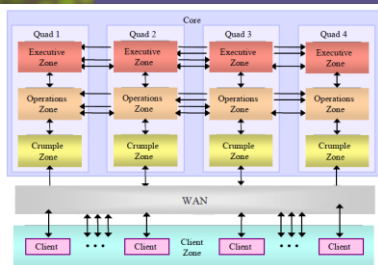
- Exploring beyond degradation— regain, recoup, regroup and even improve
- Semi-automated: Survivability architecture captures a lot of low level (and sometimes uncertain and incomplete) information – utilizes advanced reasoning and machine learning

A Decade of BBN Research in Intrusion Tolerant Systems



5

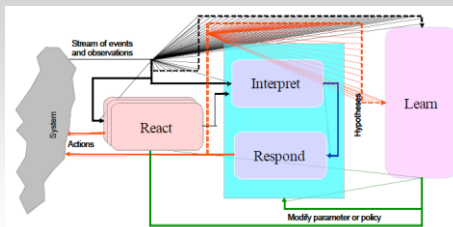
Achievements So Far



Military (USAF) Joint Battlespace Infosphere (JBI) information management system exemplar made survivable and subjected to sustained attacks over several weeks by multiple independent red teams

Results

- The system survived 75% of attacks
- Of those that succeeded,
 - Average time to failure was 45 minutes
 - Vs. immediately in the unprotected system
 - Minimum of 10 minutes to failure
 - Required combinations of attacks
- Adaptive defenses added 5-20% overhead to call latency



Challenge: Develop automated mechanism that would interpret the reports and decide the effective course of action

CSISM Approach: 3 level decision making- reactive, deliberate and learned; use theorem proving and coherence to reason about accusatory and evidentiary information contained in reported events

Results

- Possible to minimize expert involvement
- Reasoning about accusatory and evidentiary information wrt encoded knowledge
 - Made correct decision in ~75% cases in red team exercises
 - Compute intensive
- Integrating learned responses online needs additional research

6



Bio-inspired Defensive Ideas

- Common threads that runs through our intrusion tolerance and survivability work:
 - Adaptation for security
 - Like in nature, services migrate; change behavior, structure and configuration in order to survive
 - Unpredictability
 - Taking unexpected actions yield advantages
 - Intelligent behavior
 - Like high order life forms, cognitive capabilities are introduced to survivable systems for interpreting reported events and making decisions
 - Evolution
 - Learning to improve defenses over time

Our bio-inspired ideas go beyond “swarm” and “ant-colony” ideas

7



Challenges

- Evolving into a better defended system
 - Learning in Adversarial Environments
 - High degree of uncertainty and no clear quality signal
 - May learn the “wrong” thing
 - Simulation-based learning
 - Our simulator allows what-if analysis through injection of **attack effects**, snapshots, and quality signals.
 - Difficult to map online attack observations into injectable attack effects on the simulator
- Cognitive Decision Making
 - Encoding “self-preservative” invariants that guide selection functions
 - How to incorporate parameterized redundancy and diversity distributions
- Effective Evaluation of survivability
 - Difficult to begin with
 - Addition of automated, dynamic, and self-managing behavior makes it even harder

8



New Trends and Opportunities

- Service-Oriented Architectures and Cloud Computing
 - Biological-Inspired defenses can benefit from the flexibility and dynamics of new computing platforms
 - Dynamic composition and provisioning of compute resources
 - Potential to make tolerance more affordable, reusable, available
 - Opportunity: Increased redundancy and diversity promotes availability and integrity
 - Risks
 - Decryption of data and processing in the cloud poses risks to confidentiality
 - Opportunity: Parallel algorithms and split-key processing
 - Composition might break underlying assumptions
 - Opportunity: Safe composition approaches that preserve safety properties and flag inconsistencies in composed systems.

9



Conclusions

- Successes
 - Survivability architecture providing a robust foundation
 - Automated cognitive management defending a system in real-time
- Cognitive and Biological Approaches
 - Show promise
 - Adaptation, unpredictability, learning, cognition
 - But remain challenging
 - Learning in adversarial environments
 - Evaluation
- Future R&D
 - Survivable and Secure SOA-based architectures
 - Safe composition of systems of systems
 - Automatic policy deconfliction

10