Raytheon
BBN Technologies

This document primarily describes work sponsored by the United States Defense Advanced Research Projects Agency (DARPA) under contracts: F30602-99-C-0188 (APOD), F30602-00-C-0172 (ITUA), F30602-02-C-0134 (OASIS Dem/Val), N00178-07-C-2003 (CSISM), FA8750-10-C-0242 (A3) and HR0011-16-C-0058 (ARMED), and also mentions work sponsored by the United States Air Force Research Laboratory (AFRL) under contracts: FA8750-15-C-0079 (KAGE) and FA8750-15-C-0057 (CMT),

Adapt, Automate or Perish

February 2018

Dr. Partha Pal
Raytheon BBN Technologies

Agenda

- Introduction (3)
- A brief history (5)
- Tools of the trade and principles (6)
- Some recent examples (10)
- Challenges (1)
- Summary and discussion (1)

Font size proportional to section content

Distributed Systems Technology @ BBN
Brief Overview

Raytheon BBN Technologies

A History of Innovation

1950s

Acoustic Design for UN General Assembly Hall

AI Program for Pattern Recognition

1960s

Demonstration of Time Sharing

LOGO Programming Language

ARPANET- First Multi-node Packet Switched Network

1970s

First Person-to-Person Network Email & the @ Sign

Acoustic analysis of JFK Assassination Tapes

Analysis of Nixon Watergate Tapes

First Symmetric Multi-processor

First TCP for UNIX

1980s

First Electronic Mail

Defense Data Network

Natural Language Computer Interface

Intelligent Agents

SimNet

Collaboration Planning Technology

1990s

Secure email for DoD

DARPA Information Assurance

Broadband Wireless Technology

Genetic Algorithm Scheduling Tools

Collaborative Planning for Desert Storm

ATM Switch

40K Word Speech Recognition System

Safekeyper Certificate Management

Certificate Authority Workstation (CAW)

2000s

Call Director Natural Language Routing

DARPA Agent Markup Language

Microthunder Urban Environment Surveillance System

Ultra*Log Agent-Based Network Survivability

Boomerang Mobile Shooter Detection System

Quantum Cryptographic Network

2010s

Warrior-X soldier-wearable shooter detection

Quantum breakthrough in coupling of superconducting qubits

Nation's largest network science research center

This slide is produced (and distributed) by BBN's communication department, the images are BBN internal photos

BBN By the Numbers

Raytheon
BBN Technologies

800
Employees

75%
Staff with Security Clearance

120
TS or SCI clearances

57
SCIFs

64%
of technical staff have advanced degrees

383
Patents

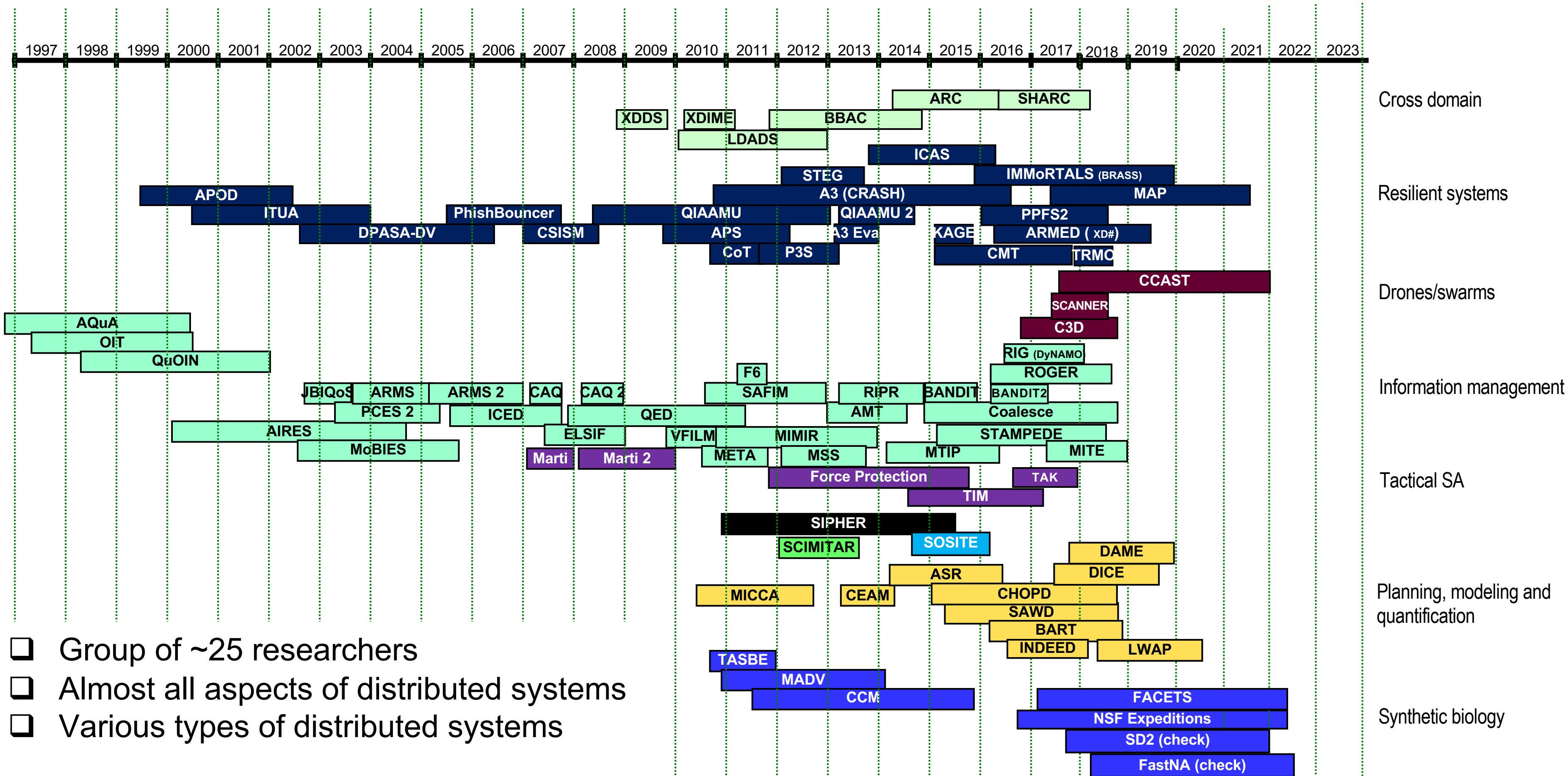
65
Years since BBN was founded

8
US locations

10,000
Boomerang systems deployed to Iraq & Afghanistan

Distributed Systems Tech at BBN

Raytheon BBN Technologies



- Group of ~25 researchers
- Almost all aspects of distributed systems
- Various types of distributed systems

- Smarter, Resilient, Trustworthy

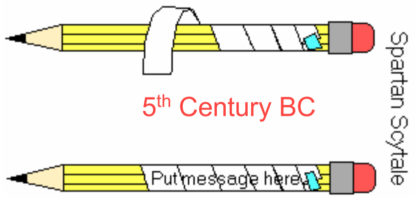
A Brief History

Security– A Brief History…

Raytheon BBN Technologies

There were "information" before the computers…

- ❑ Codes…Ciphers… Seals..
- ❑ Cryptology– cryptography and cryptanalysis
- ❑ From warfare to modern day economy!



Source: www.unmuseum.org

Enigma, WWII

Source http://math.arizona.edu/~dsl/enigma11.htm

Computers: Electronic machines that process and store information

- ❑ Access to computing resources and information
- ❑ Bell-La Padula, Orange Book…

Vulnerabilities

Attacks

Threats

Countermeasures

- ❑ Static (precaution)
- ❑ Dynamic (response)

Information Systems: Computers connected in a network. Processing, storing, deriving, transforming………… information

- ❑ Security of the network/communication over the network
- ❑ Intrusion detection, PKI…

Elements of Modern Information Security

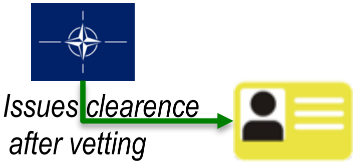
Raytheon BBN Technologies

- ❑ Physical security
- ❑ Procedural security
- ❑ Personnel/Personal/Inter-personal security
- ❑ Compromising emanation security
- ❑ Operating systems/Host security
- ❑ Network security
- ❑ Application security

Source: www.flickr.com

Source: icondoit.wordpress.com

Source: nato.int



Source: openclipart.org

Source: YouTube video of NHK Van Eck Phreaking

Source: www.wox.it

Information Assurance:

- ❑ Prevent, Deter, Detect, Respond, Recover….

Traditional Security Issues

- Prevent bad things from happening:
  - Prevent unauthorized disclosure of data
  - Prevent unauthorized modification of data
  - Prevent unauthorized consumption of computer or network resources
- Security Policy: policy to prevent bad things
- Mechanisms and elements supporting security policy:
  - Authentication: prevent masquerade, spoofing (of data origin, peer)
    - Identity based authorization
  - Encryption: prevent unauthorized visibility to data
  - Access Control: prevent unauthorized use and consumption
    - MAC, DAC, RBAC…
  - Non-repudiation: prevent deniability

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)

Trusted Computing Base

Access Control & Physical Security

Cryptography

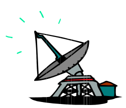
But intrusions will occur

1st Generation: Protection

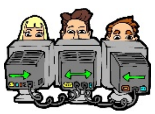
Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)

Firewalls

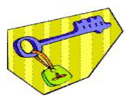
Boundary Controllers



Intrusion Detection Systems



VPNs



PKI

2nd Generation: Detection

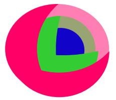
But some attacks will succeed

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

Intrusion Tolerance

Big Board View of Attacks
Real-Time Situation Awareness
& Response

Graceful Degradation



Hardened Operating System

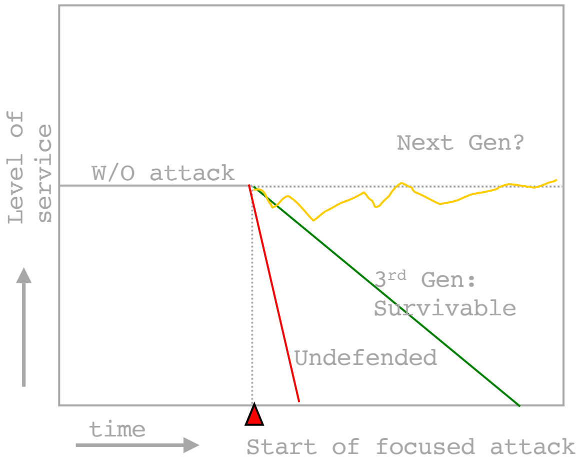
3rd Generation: Tolerance

3rd and 4th Generations

Raytheon BBN Technologies

3rd Generation: Tolerance and Survivability:

- Assumes that attacks/bad things cannot be totally prevented– some attacks will even succeed, and may not even be detected on time…
- Focuses on desired qualities or attributes that need to be preserved/ retained/continued even if in a degraded manner—
  - Availability: (of information and service)
  - Integrity: (of information and service)
  - Confidentiality: (of information)



Next Generation of Survivability (Resiliency):

- Regain, recoup, regroup and even improve…

Raytheon
BBN Technologies

Tools of the trade and principles

Fundamentals

- Adapt
  - Change is inevitable, some are natural but some are adversarial
  - Risks of not adapting
    - In the short term- sitting duck
    - In the long term- evolutionarily extinct

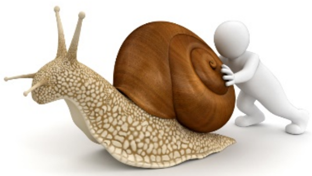
Source: oldsalshaker.blogspot.com

Source: openclipart.org

Source: www.dodo.blog.br

- Automate
  - Changes are rapid (sign of the time—*internet speed*), adversary is at machine speed
  - Risks of not automating
    - Human errors
    - Slow response → no response

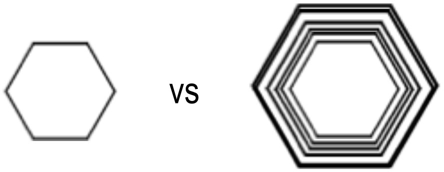
Source: www.empillsblog.com



Source: www.lowlevel.it

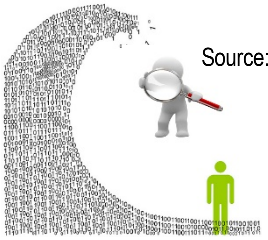
What to Adapt and Automate

- Adapt and Automate should cross cut basic security aspects
  - Protect:
    - responding to mission needs, threat level
    - balancing cost



  - Detect:
    - drowning in data

Source: asmemoriasdarute.blogspot.com



Source: acreelman.blogspot.com

  - And then some, for repair and recovery
  - Adapting for resilience
    - Configuration
    - Code
    - Policy

Some of the repair and recovery adaptations may actually adapt protection and detection mechanisms…

Proactive and Reactive

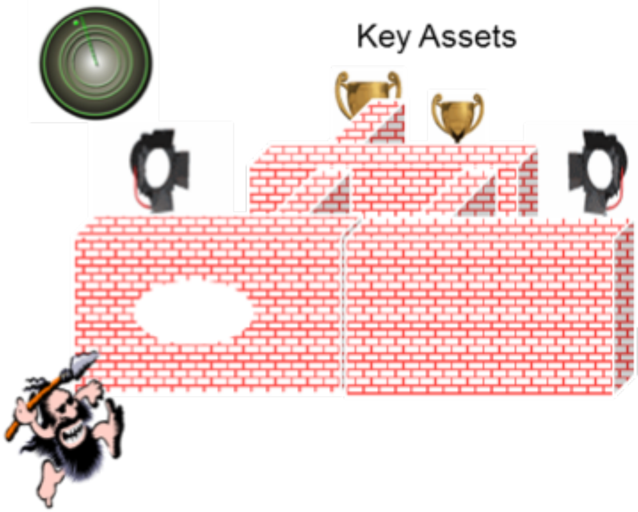
- Reactive: In response to an observed event (detection) or its derivative (suspicion)
- Proactive: Based on predetermined policy
- Combination: Modify the proactive policy based on detection or suspicion

- Proactive Adaptation
  - Rejuvenation (e.g., GMU SCIT)
  - Moving Target Defense (One of the recommendations from NCLY 2009):

- Food for thought
  - Is there anything that is truly proactive?
  - State reconstitution(Northeastern's DMTCP)

Context, Basis, Support

- Adaptation and Automation do not happen in a vacuum
  - Architecture: organization of components, both functional components from the undefended system and the added defense mechanisms, their interconnections, and protocols that govern them…
    - Entities, interconnections, protocols
  - Protect and detect supplements to adaptation
    - High barrier to entry (outside as well from one part to another)
    - Improve the chance to spot attacker activity
    - Adapt to changes caused by the attacker
    - Automate, when possible

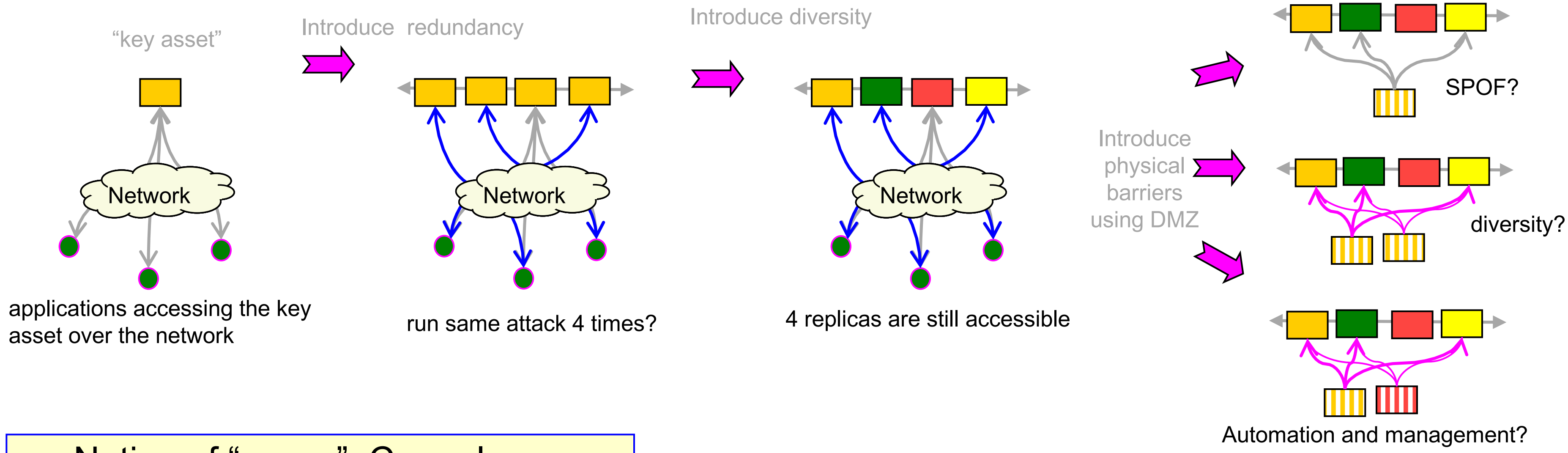


Principles/Rules of Thumb

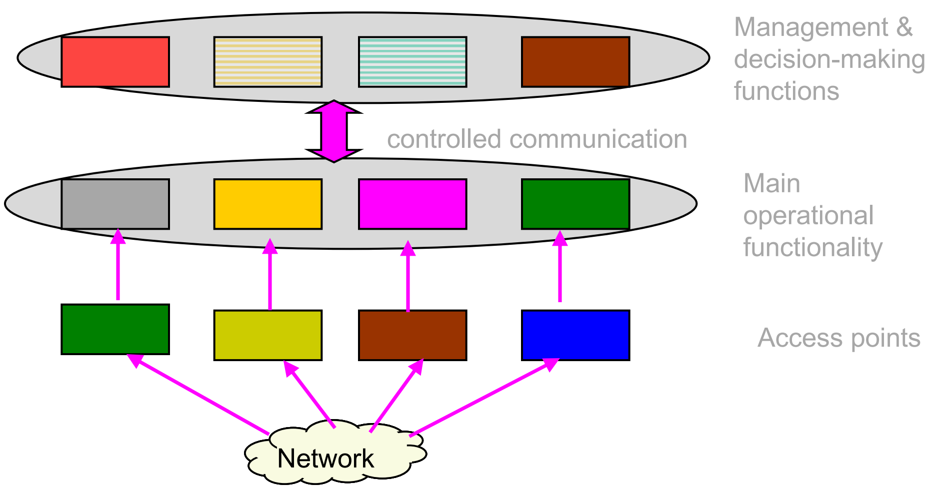
- SPOF protection
- Controlled use of diversity
- Physical barriers before key assets
- Robust basis of defense in depth
- Containment layers
- Modularity
- Range of adaptive responses
- Human override
- Minimalism
- Configuration generation from specs

- Many of these are surprisingly simplistic and intuitive– but it is also surprising how many of these are routinely ignored

A Quick Design Pass



- Notion of "zones": Crumple zone, Operations zone, Executive zone



- Executive zone enablers: AI, Planning, Learning
- Other advantages
  - Human interface and override
  - Out of band analysis and improvement

- Crumple zone enablers: proxies at various layers
- Other advantages
  - Rate limiting
  - Size limiting
  - Learning usage pattern
  - Tunnel termination
  - Insertion of protocol diversity
  - Control points

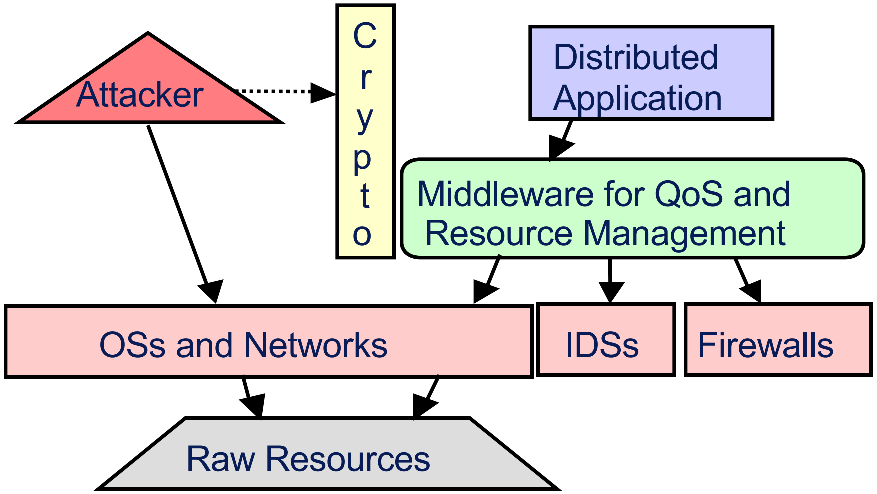
Some examples

Early Examples

- 1999-2000
  - APOD (sensor-actuator loops, pre-programmed MW-based defense-application integration for defensive response to unavailability attacks)
  - ITUA (redundancy, unpredictability, response to unavailability and integrity attacks)
- ODV (2005)
  - Architecture, integration
  - Highlighted the need for automation
- Intel/Automation (2007)
  - Cognitive cyber-defense reasoning

This arc is more personal/ BBN DST centric, other contemporary projects explored similar, alternative and complementary paths, e.g., EU MAFTIA

APOD (Aug 1999- Mar 2003)



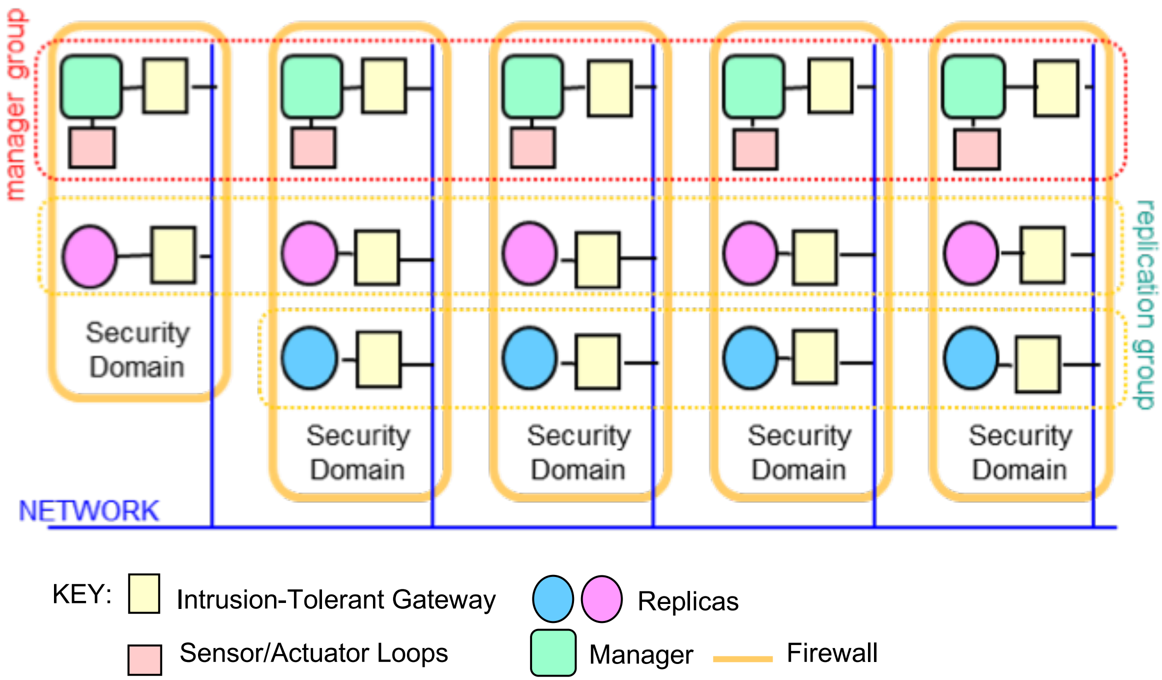
	Overcome	Avoid	Guard
Use QoS Management	Reserve bandwidth, CPU	Migrate replicas	Tighten access controls
Use Gateways	Block IP sources	Change protocols, ports	Strengthen encryption
Use application level adaptivity	Retry, use local calls	Choose alternate server, degrade service	Increase self-checking

- Red team evaluation
  - Goal: Deny the service offered by the defended application (imagebroker)
- Results
  - Most single attack runs failed
  - The red-team was forced to combine different attacks to cause a denial of service
  - Of the attack runs that succeeded, the average time-to-denial was ~45 minutes from start of attacks, with a minimum of roughly 10 minutes (without APOD defenses, service was denied immediately)
  - Defense added 5-20% overhead to the defended application's latency

This research was sponsored by DARPA under contract No. F30602-99-C-0188.

ITUA (Aug 2000-Jan 2004)

Raytheon
BBN Technologies

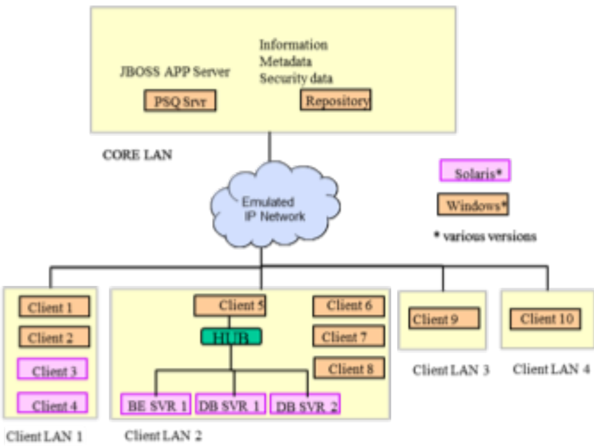


- An intrusion-tolerant middleware that uses
  - Redundancy and group communication protocols to tolerate arbitrary component failures
  - Sensor-actuator loops to mount quick and localized defensive response to intrusions
  - Decentralized managers to recover from intrusions and to manage redundant resources
  - Uncertainty in defense strategy to make adaptive response unpredictable to the attacker

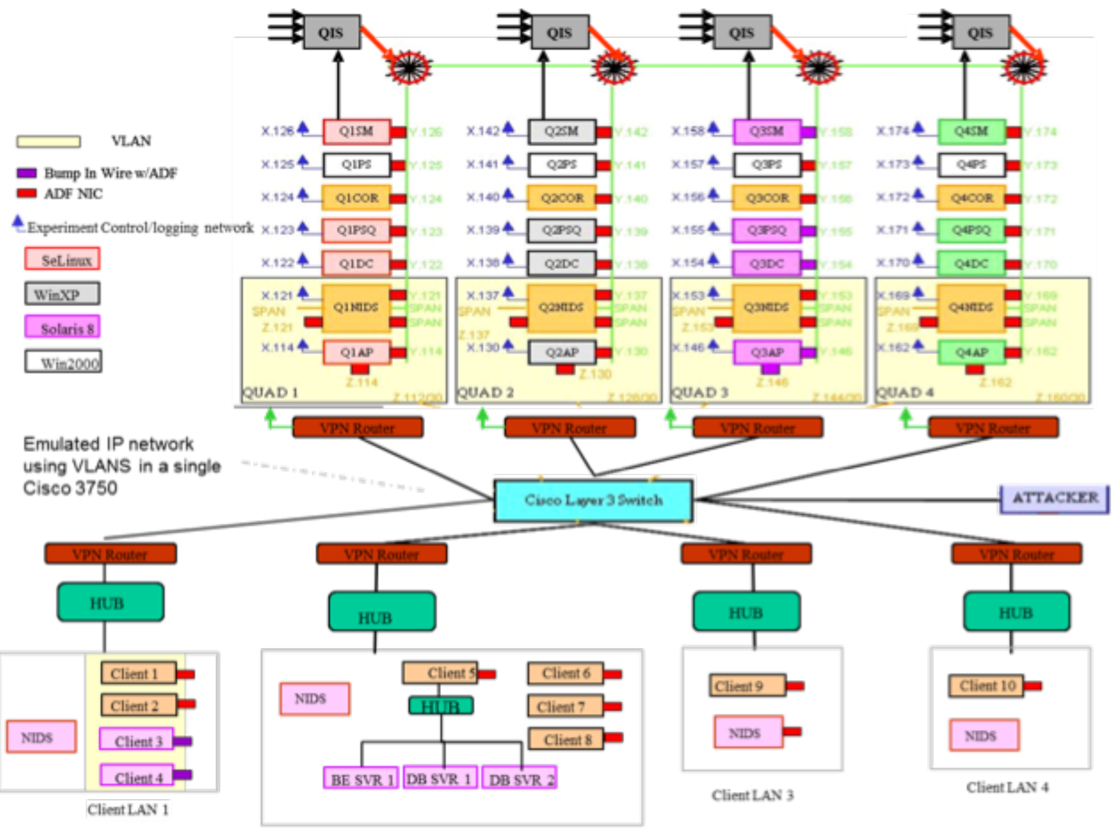
- Validated the middleware's intrusion tolerance by probabilistic and experimental methods
  - Transitioned developed technology to DoD application(s) (e.g., CECOM SMS, Boeing's IEIST) to improve their survivability, and to other DARPA programs (OASIS Dem/Val)

This research was sponsored by DARPA under contract F30602-00-C-0172 (ITUA).

DPASA (2002- 2005)



- High water-mark in survivable system design
- Protection-detection-adaptation baked in architectural resilience
- Need for intelligence and automation

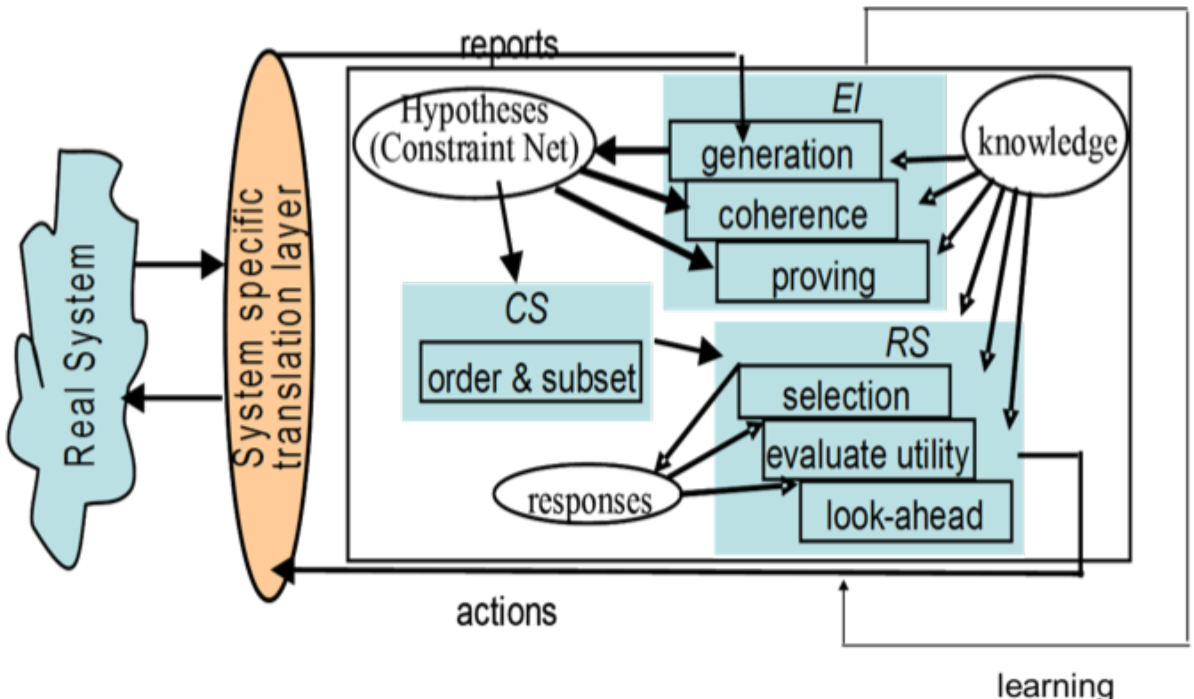


- Defense mechanisms: policy enforcement, encryption, authentication, detection and correlation, redundancy, recovery and response adaptation
- Design principles: No SPOF, layered defense, containment
- Architecture: Zones, quads, protection domains, middleware
- Protocols: Corruption tolerant PSQ, command and control

This research was sponsored by DARPA under contract No. F30602-02-C-0134.

CSISM (2005-2007)

Alerts → accusations, Observations→ evidences



Learn from past successes and failures

Proofs, coherences to select claims about the system state

Select the response from options available that provides the best remedy to the claimed state

Came close to "ground truth" decisions in controlled red team experiments, but building and working with a performant model where hypotheses can be proved turned out to be very very hard!

This research was sponsored by DARPA under contract No. N00178-07-C-2003.

Recent Examples

- Clean Slate Resilience (DARPA CRASH Program)
  - What would you do if you are to start fresh

Other works: Proven kernels, Tagged architecture covering hardware, OS and compiler support

  - What else remains unexplored
    - Among other things, *deception*

Advanced Adaptive Applications (A3) Environment

Raytheon BBN Technologies

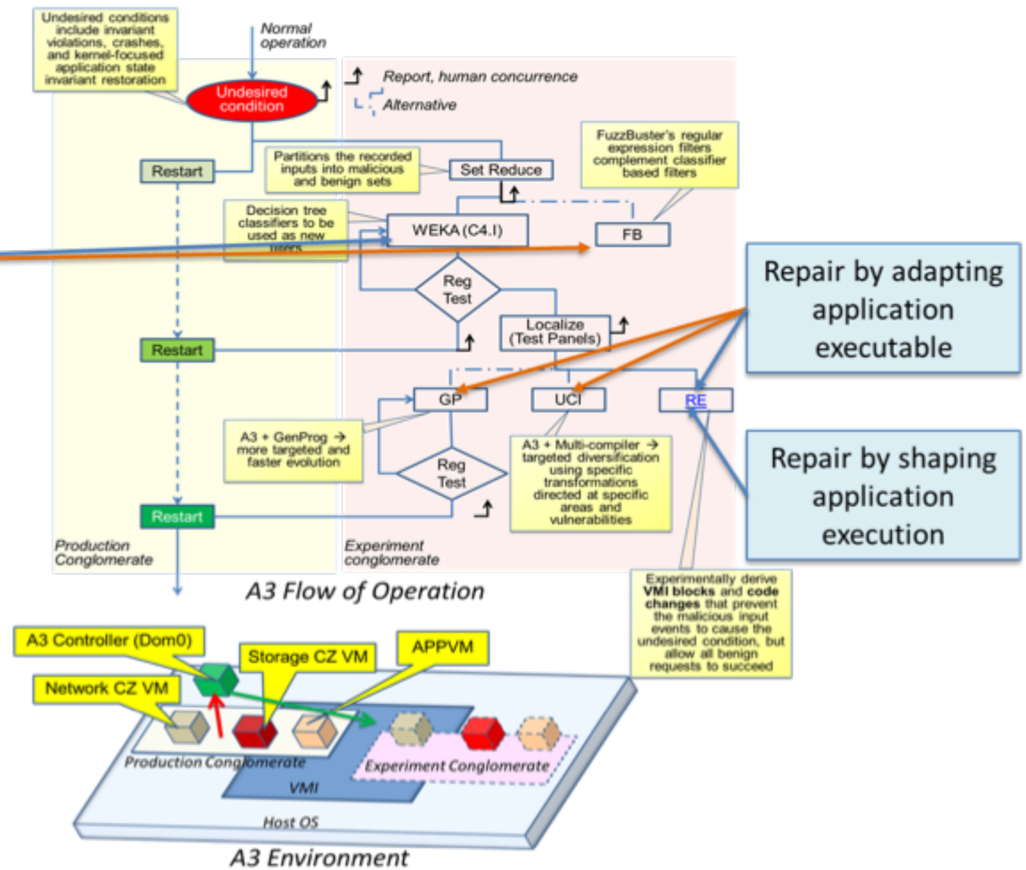
- Motivation
  - Defense of last resort
  - Time taken to address zero-days
- Opportunity
  - Host resources are becoming chip
  - Virtualization
- Approach
  - Near application/per application
  - Containerize
  - Mandatory mediation (I/O and execution)
  - Record and replay, experimentation

  - Advent of RASP

Repair by adapting mediation policy

A3 core

CRASH integration



Successfully demonstrated resilience against zero-days in red team experiments, and real CEs

This research was sponsored by DARPA under contract No. FA8750-10-C-0242

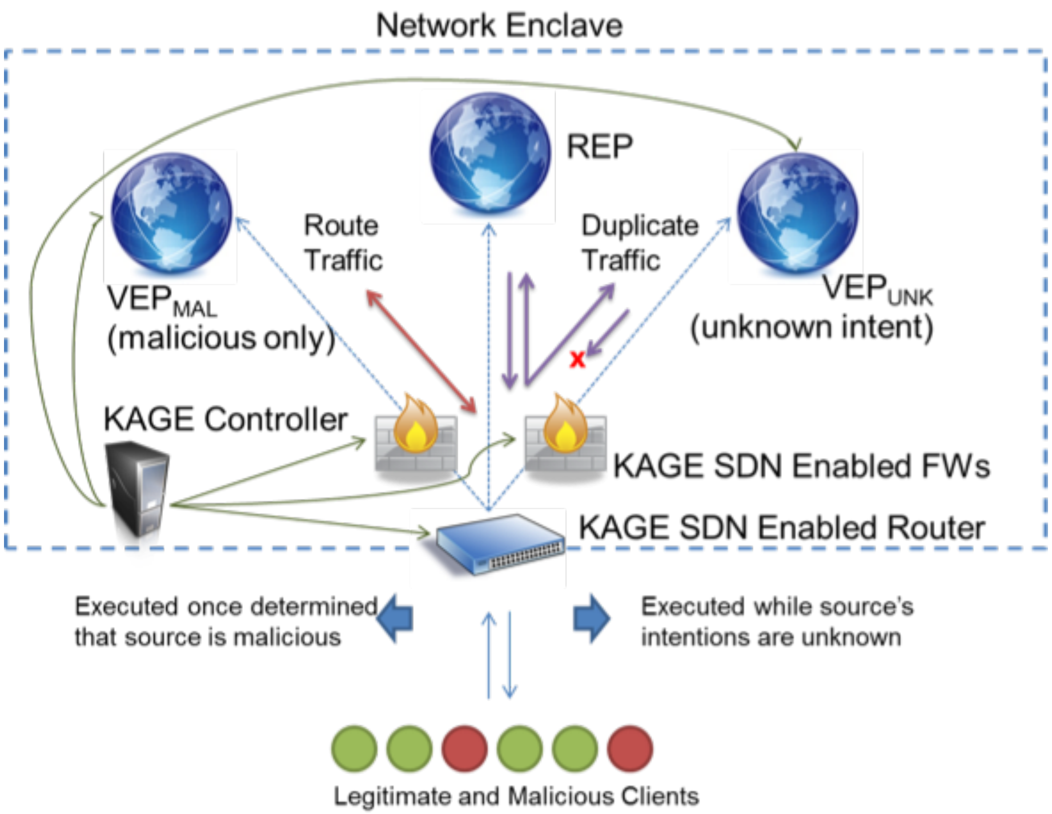
KAGE and ARMED

- Motivation
  - Adversary can cause a diversion, why cant we?
- Opportunity
  - SDN, Virtualization
- Approach
  - *Create* an alternate reality
    - KAGE
  - *Present* an alternate reality
    - ARMED

Keeping Adversaries Guessing and Engaged (KAGE)

Raytheon BBN Technologies

- Basic Construct:
- Employ Virtual End Points (VEPs)
  - Pseudo copies of a Real End Point (REP)
  - Without real (critical) data
  - Monitored at the hypervisor level to evade detection
- Employ SDN to
  - Hide the REP and only expose a VEP
  - Duplicate only application traffic to the REP, drop responses from the VEP
  - Upon detection of malice, isolate all adversary traffic to a VEP and begin targeted deceptions

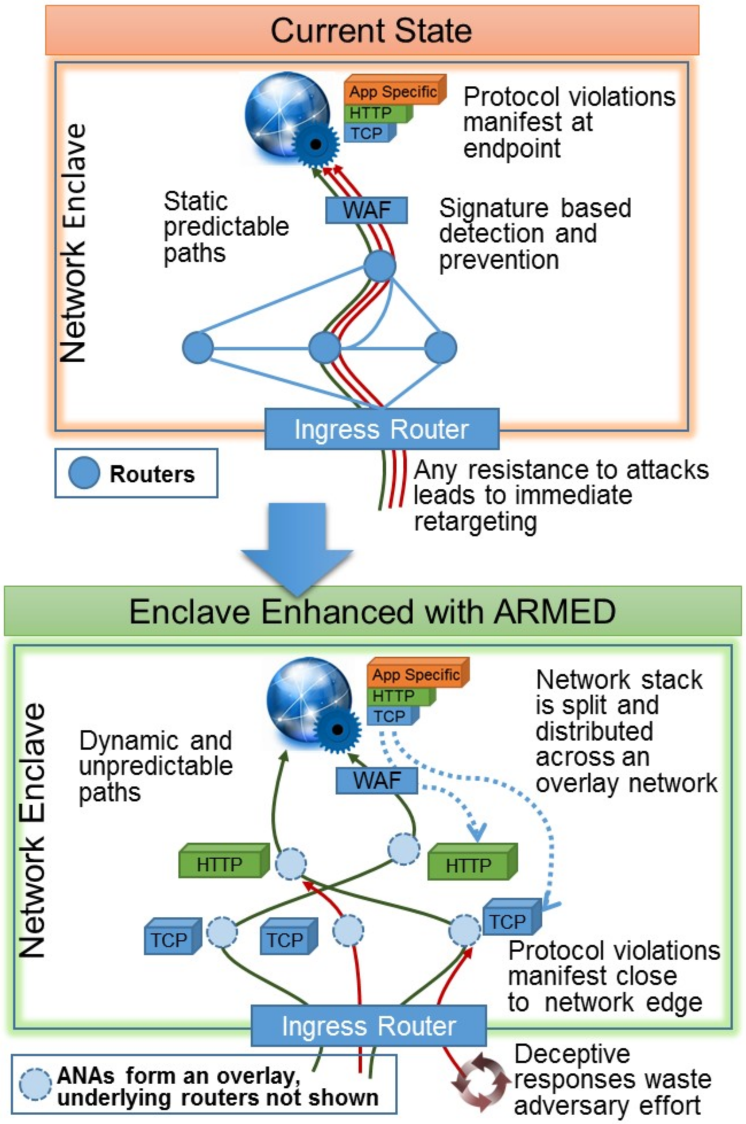


This construct enables complex interactions with the adversary, while protecting against cyber fratricide, as the vast majority of KAGE interactions occur separate from all benign traffic and computation.

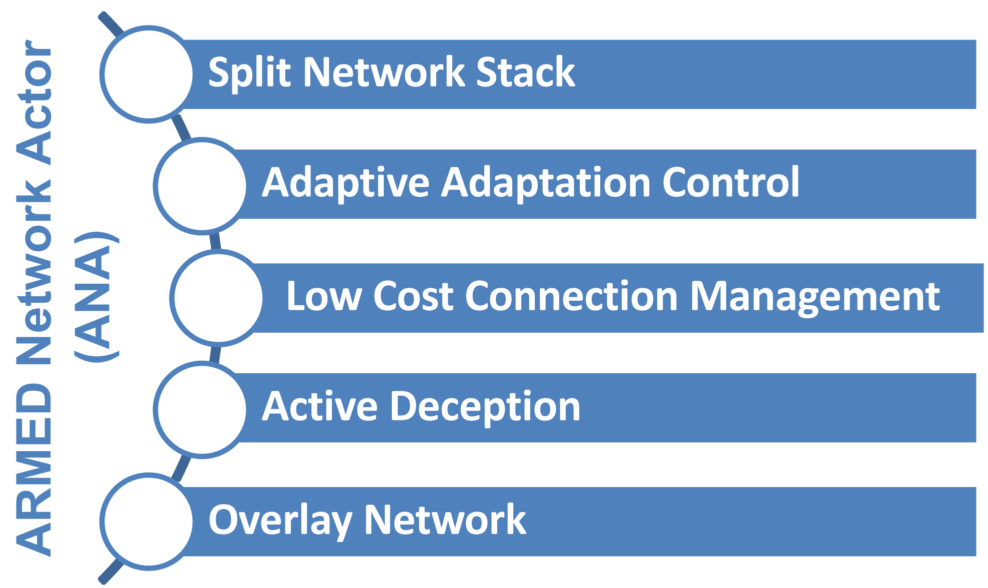
This research was sponsored by the US AFRL under contract No. FA8750-15-C-0079

Adaptive Resource Management Enabling Deception (ARMED)

Raytheon BBN Technologies



- Network maneuvers, including deceptive maneuvers, to defend aganst extreme DDoS attacks, including low and slow
- ARMED offers protocol specific network nodes that serve as anomaly detection points and deception injection platforms



This research was sponsored by DARPA under contract No. HR0011-16-C-0058

Challenges

We Progressed, but Are We Done?

- Technical Challenges
  - Stable and beneficial adaptation
  - Range and scope of adaptation
    - E.g., code modification
      - A3 only functionality reduction
      - Others (e.g., gen prog)- genetic programming/evolutionary search
  - Trust in automation
- Acceptance/Trust/Transition Challenges
  - Validation/Quantification (e.g., determine impact of deception?)
  - Certification

Composable Measurable Trust (CMT)

What does it take to earn the trust of mission stakeholders when a system under attack is recovered and repaired?

CMT is initially focused on embedded control systems (e.g., Pixhawk) and missions involving autonomous vehicles

Photo: a BBN-built rover

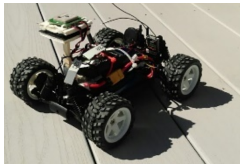
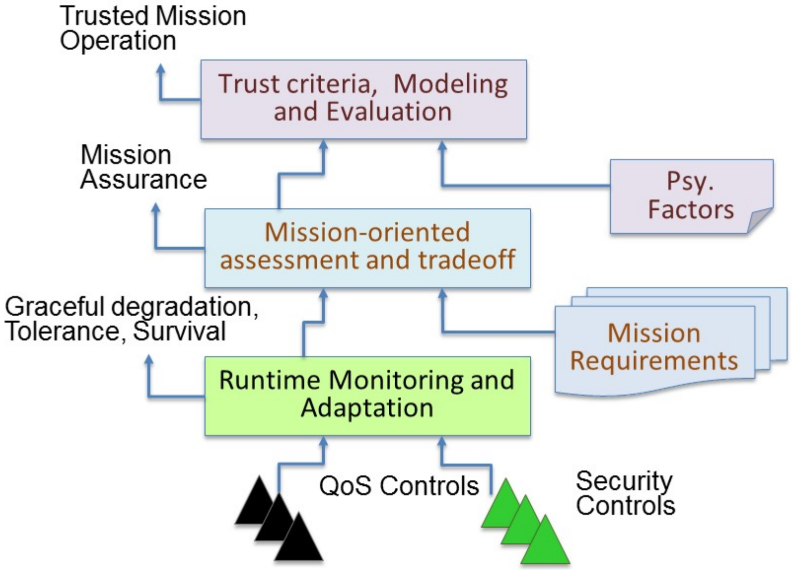
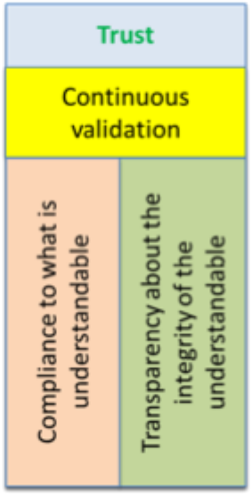


Photo: 3DR IRIS(stock)



- Trust: willingness to accept risk of the unknown
- How to increase trust passively (i.e., without adding new QoS and Security controls)
  - Reduce the scope (of the unknown)
    - More transparency
  - Reduce the risk (of the unknown)
    - Less uncertainty
- Usage of trust
  - tends to vary from mission to mission: periodic reassessment, trust but verify, complete mistrust



This research was sponsored by the US AFRL under contract No. FA8750-15-C-0057

Summary and discussion

Challenging, Scary, But Also Exciting

Raytheon BBN Technologies

- Arms race
  - Asymmetry
  - New payoffs, new vectors
- Challenge as well as an opportunity
  - Technical
  - Societal good
- Eat the humble pie: technology is not a silver bullet
  - Education
  - Ethics

Raytheon BBN Technologies

Backup

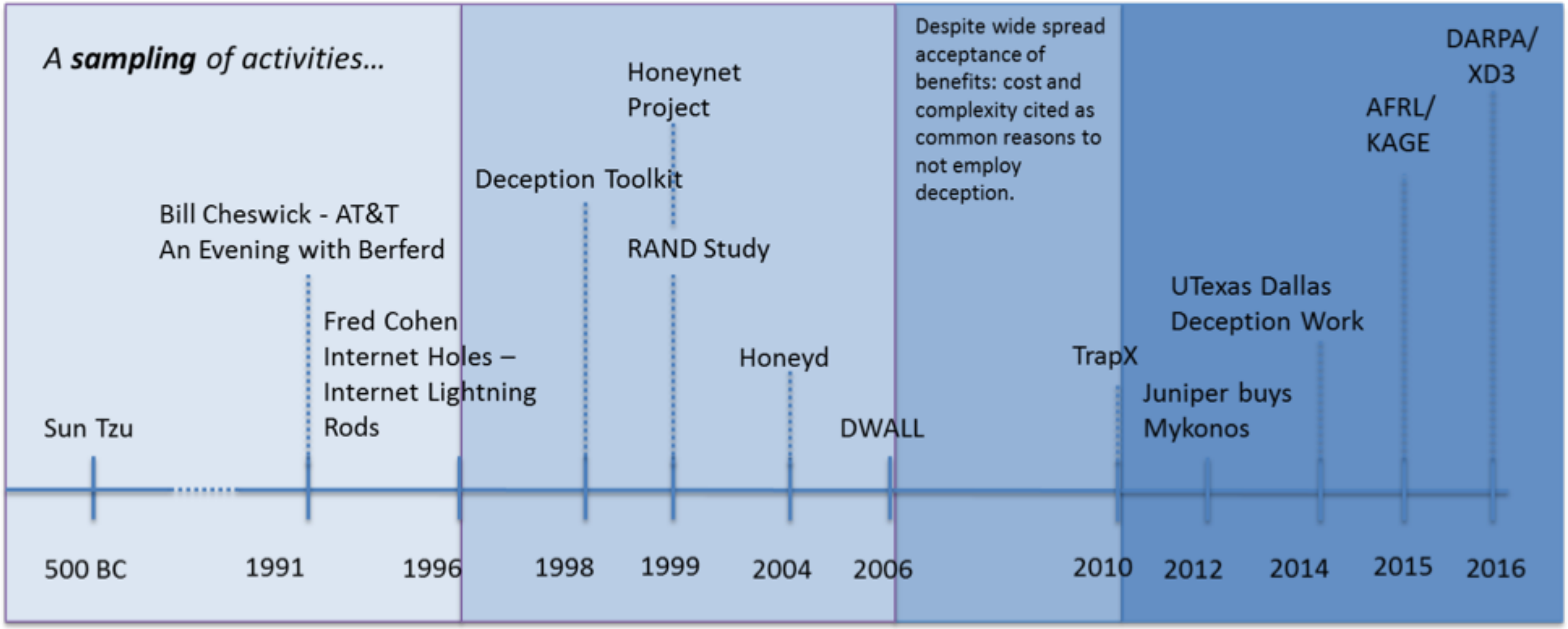
Proactive and Reactive

- Reactive: In response to an observed event (detection) or its derivative (suspicion)
- Proactive: Based on predetermined policy
- Combination: Modify the proactive policy based on detection or suspicion

- Both styles can be used to cause deception
  - Reactive: Divert ill-behaving (e.g., sending too many requests, sending out of order protocol messages)clients to a tar pit (instead of rate limiting, or sending error/terminating)
  - Proactive: Drop SYN packets with a certain probability, always respond to scans with a set of non-existent hosts

Deception-A Timeline Perspective

Raytheon BBN Technologies



- Deception beginnings
- Burst of defensive cyber deception activity : Cohen, Rowe, Provos, Bishop, etc. (even some in CPS – e.g., Cisco) Honeypots and honeynets really emerge. Systems to masquerade are developed.
- A downturn in activity in defensive cyber deception (though uptick in other deception-related areas such as MTDs)
- A notable resurgence in commercial, DoD, and academic settings. In the commercial space focused on the simpler space of deception for detection. Some potential drivers of this resurgence:
  - Availability and awareness of ***new domains and contexts*** such as CPS
  - Availability of ***enabling technologies*** such as malleable networks, virtualization
  - **Continued advantage** by the adversary in the cyber arms race

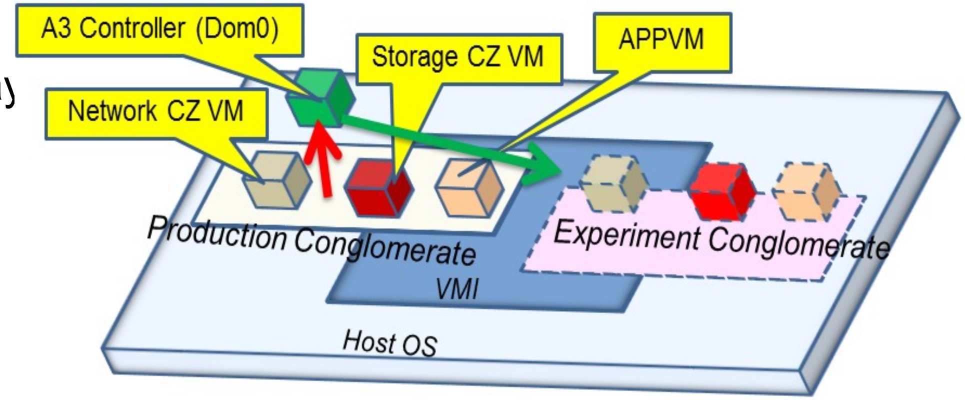
DDoS Background and Context

- Cloud based defenses have had reasonable success in protecting against traditional DDoS
- A particularly problematic variant of these attacks, however, has emerged: “low and slow” DDoS
  - Non-volumetric (attacks are not measured in Gbps)
  - Exploits vulnerabilities in protocols/systems
  - Goals and effects are the same: loss of service
  - Examples: “slowloris” family of attacks
    - Create connections to a web server, sending partial requests
    - Periodically write HTTP headers, keeping the connection alive, and operating within the HTTP protocol
    - Variants of this perform slow POST request, or perform a full request, but read the response very slowly (set TCP window size)
  - Requests in isolation often look legitimate, and unlike their noisy volumetric counterparts, the attacks tend to fly below the radar

Advanced Adaptive Applications (A3) Environment

Raytheon
BBN Technologies

- A3 is an execution management environment that makes network-facing server applications resilient against zero-day attacks
- Our most recent work in adaptive systems and resiliency
- Features isolation, interception, mediation, run forward proxying



Rapid Response Immunization Against Zero-Day Attacks

- Stop and absorb attacks using application-specific I/O and execution mediation policy, preventing attacks from spreading in the mission-critical network
- Monitor application and mission-specific undesired conditions that are indicative of successful attacks
- Automated localization and diagnosis of attack induced faults
- Mitigate exploited vulnerability by policy adaptation and application program repair

Without A3, deployed applications may become unavailable and/or stay vulnerable for days until a fix for the zero day is (manually) found and applied

This research was sponsored by DARPA under contract No. FA8750-10-C-0242

Raytheon
BBN Technologies

Questions?

Partha Pal
617-873-2056
partha.pal@raytheon.com