Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Building the Theory of Resilience

NICHOLAS J. MULTARI, Ph.D.
PACIFIC NORTHWEST NATIONAL LABORATORY

nick.multari@pnnl.gov
509-375-2043

CHRISTOPHER S. OEHMEN, Ph.D.
PACIFIC NORTHWEST NATIONAL LABORATORY

christopher.oehmen@pnnl.gov
509-375-2038

PNNL-SA-97698

Ideally: A Strong Deterrence Posture

- Ultimate prevention depends upon your ability to deter the attacker

> **Deterrence** *noun* \di-ˈtər-ən(t)s, -The attempt to prevent or forestall undesired activity through influencing an attacker's or potential attacker's perception of the gain-loss balance

- Relies upon prevention, detection, response, and recovery
- Both policy and technology based
  - Willingness to respond in a meaningful, targeted way
  - Must have a range of responses built and ready to use
  - Must be able to deploy with pinpoint accuracy
- Goals
  - Reduce likelihood of success
  - Increase the attacker's "cost"

A man speaks on his mobile phone across from The New York Times headquarters building, April 21, 2011 in New York City. (Ramin Talaie/Getty Images)

abc NEWS

By LEE FERRAN (@leeferran)
Jan. 31, 2013

The New York Times and The Wall Street Journal have reported that their computer systems have been the infiltrated by hackers in China.

Recommend 192

Tweet 121 g+1

In a report published Wednesday, the Times said hackers managed to steal passwords and gain access to the personal computers of 52

CNNMoney
A Service of CNN, Fortune & Money

FORTUNE M

Home | Video | Business News | Markets | Investing | Economy | Tech

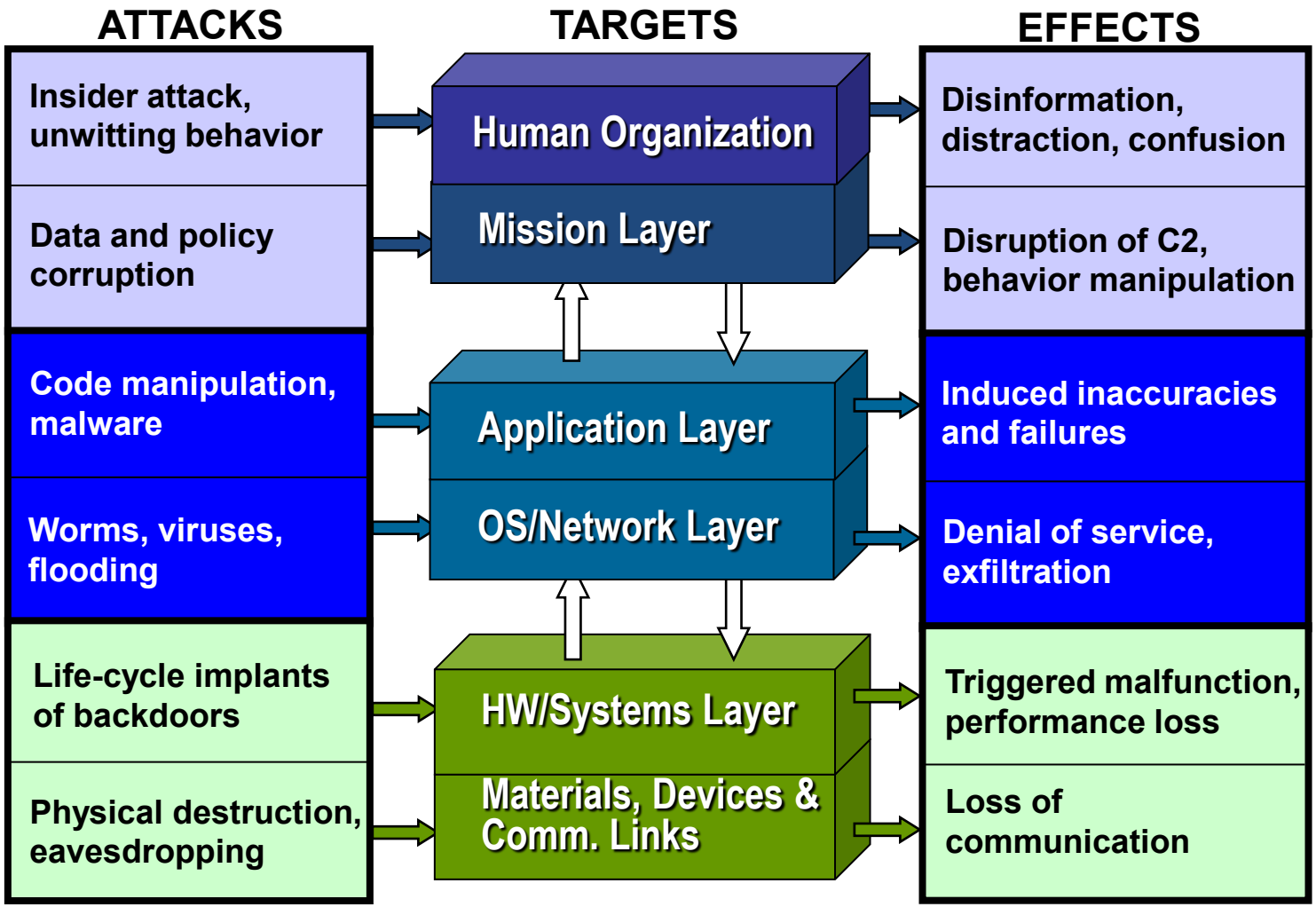
Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Video |

THE CYBERCRIME ECONOMY

Major banks hit with biggest cyberattacks in history

By David Goldman @CNNMoneyTech September 28, 2012: 9:27 AM ET

The Elements of a Contested Cyber Environment[1]

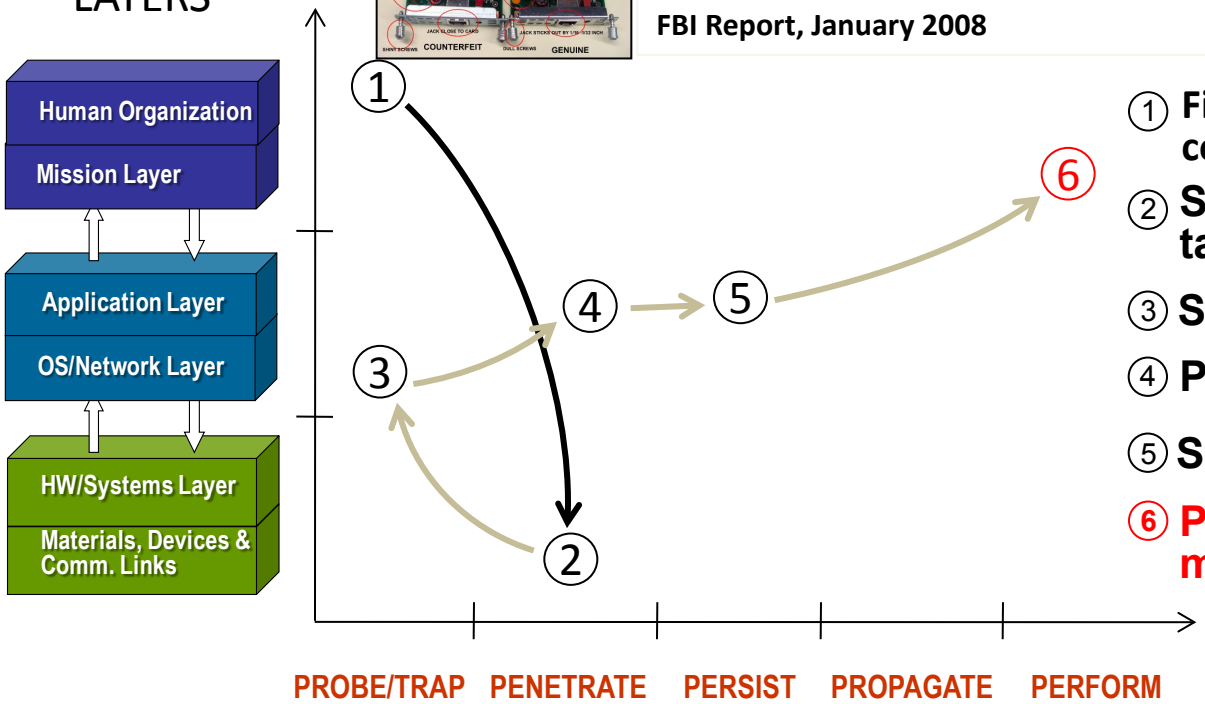


[1] 2008 AFSAB report "Defending and Operating in a Contested Cyber Domain"

Example for Attack Trajectories[2]

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Counterfeit CISCO 1721 Router
1/5 of cost of original
2002-2007
FBI Report, January 2008



1. **Find distributors for counterfeit equipment**
2. **Sell equipment to targeted place**
3. **Scan network**
4. **Plant malware**
5. **Stay hidden**
6. **Perform attack on mission**

Attack trajectories are dynamic:

- **Depend on target and choose the least resistance**
- **May leave out layers (such as network layer)**
- **May change dynamically by reacting to defensive actions**

[2] 2008 AFSAB report "Defending and Operating in a Contested Cyber Domain"

Given sufficient time and resources, any perimeter and system can be breached

Today's Reality

- Low cost of entry
- Software complexity guarantees vulnerabilities
- Unknown network and system configurations
- Advantages in luxury of time, location, and target
- Limited ability to identify the perpetrator

Attacker has the advantage

Where We Need to Go

- Ability to perform critical functions regardless of attacks launched and their success (Resilience)
  - Strong proactive and reactive defensive capabilities based upon scientific principles
- Good security metrics
  - Security and resilience based
- Real-time, all-source situational and configuration awareness
- Ability to detect attacks and provide attribution (a dual-edged sword)
  - Fusion of cyber and non-cyber data and information
  - Strong network real-time forensics/signature-creation capability
- Ability to produce near-error free products
  - Practical software generation from (semi-)formal specifications
  - Practical software and hardware verification
- Supportive international legal framework
  - Guaranteed prosecution
  - Framework for legal response

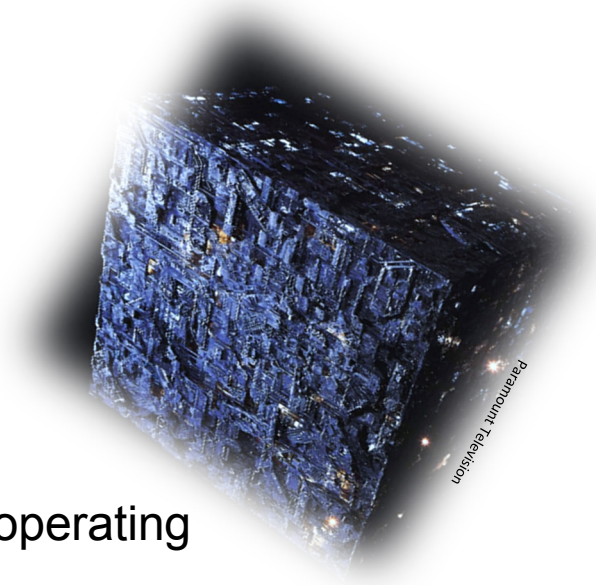
Why it is Difficult

- Resilience – What does this really mean?
  - Different groups use different terminology
    - Robustness, reconstitution, recovery, resourcefulness, adaptability, reliability, mission assurance, …
  - No scientific foundations, just engineered solutions
- Metrics
  - How do we measure security posture in real-time?
  - How do we select the “best” action to take?
- Situational Awareness
  - Fusing all sources in information in real-time
- Today, accurate and timely attribution is a pipe dream
  - Critical for successful active response or prosecution
- Error free software
  - Formal methods too expensive and time consuming
- Legal Framework
  - Not even going there!

Is Resistance Futile?

- No, but ….

- Need to know yourself
  - What is my mission?
  - What processes are critical to that mission?
  - What is the security posture of those processes?
  - How can I ensure those processes will continue operating even in face of a successful cyber attack?



- And, this information must be available in real-time

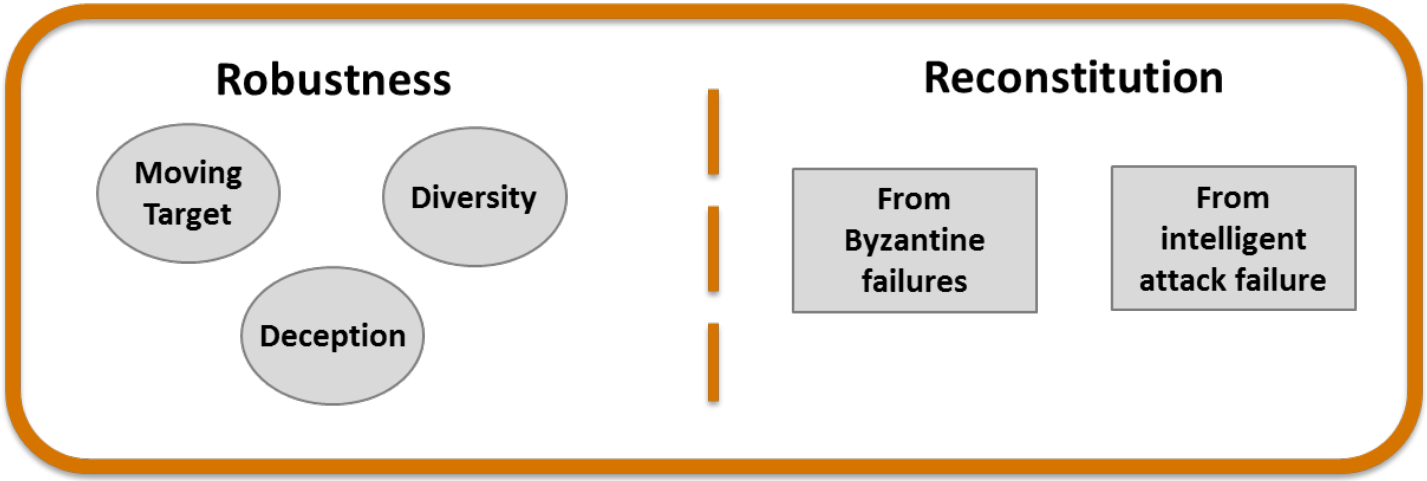
Know Yourself
Models

- What does it need to do?
  - Captures relationships, interactions, and attributes of the enterprise
- How is it done today?
  - Semi-automated data capture but at one layer
  - Manually at all layers
- What are the shortcomings?
  - Expensive, time consuming
  - Static
- What current and future work is needed?
  - Automated determination of component criticality
  - Capture of all intra/inter layer interactions/relationships/attributes
  - Immediate updates upon configuration change
  - Complexity reduction without loss of fidelity

Know Yourself
Metrics

- Key to driving proactive and reactive actions
- Security posture
  - Coarse or fine granularity
  - Updated upon each configuration change
  - Drives changes to the infrastructure
- Cost/benefit analysis
  - Calculated at cyber speeds
  - Quick evaluation of relevant responses
  - Drives specific response employed

Resilience



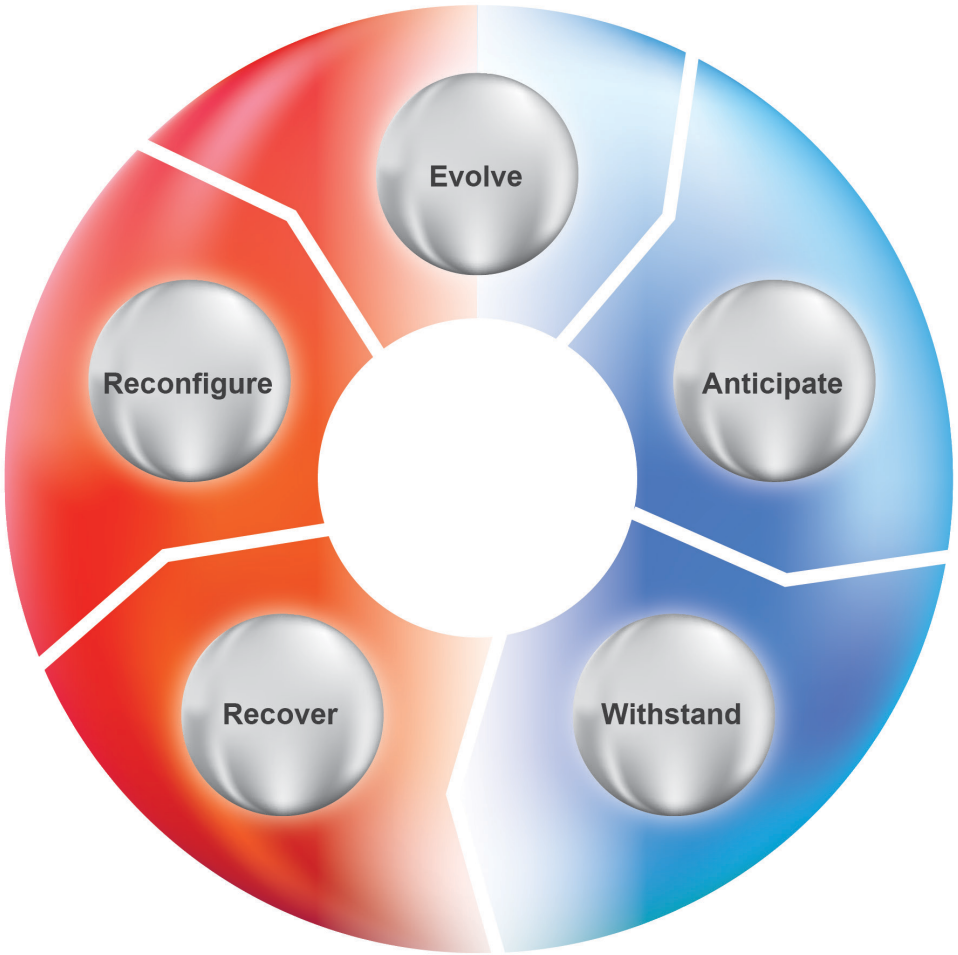
- Moving Target
  - Create motion or the illusion of motion
- Diversity
  - Get away from single system image notion
- Deception
  - Lots of information is broadcast
  - But not used
- Game Theory

- Fault Resilience
  - Detect/persist in the face of hardware failures
- Recovery
  - Re-grow or re-instantiate parts of a damaged enterprise?
- Self-stabilization
  - Regardless of starting state, ability to guarantee eventual convergence to safe state
- Self-organizing systems
  - May represent a delocalized way to coordinate regrowth

Relationship Between Robustness and Reconstitution

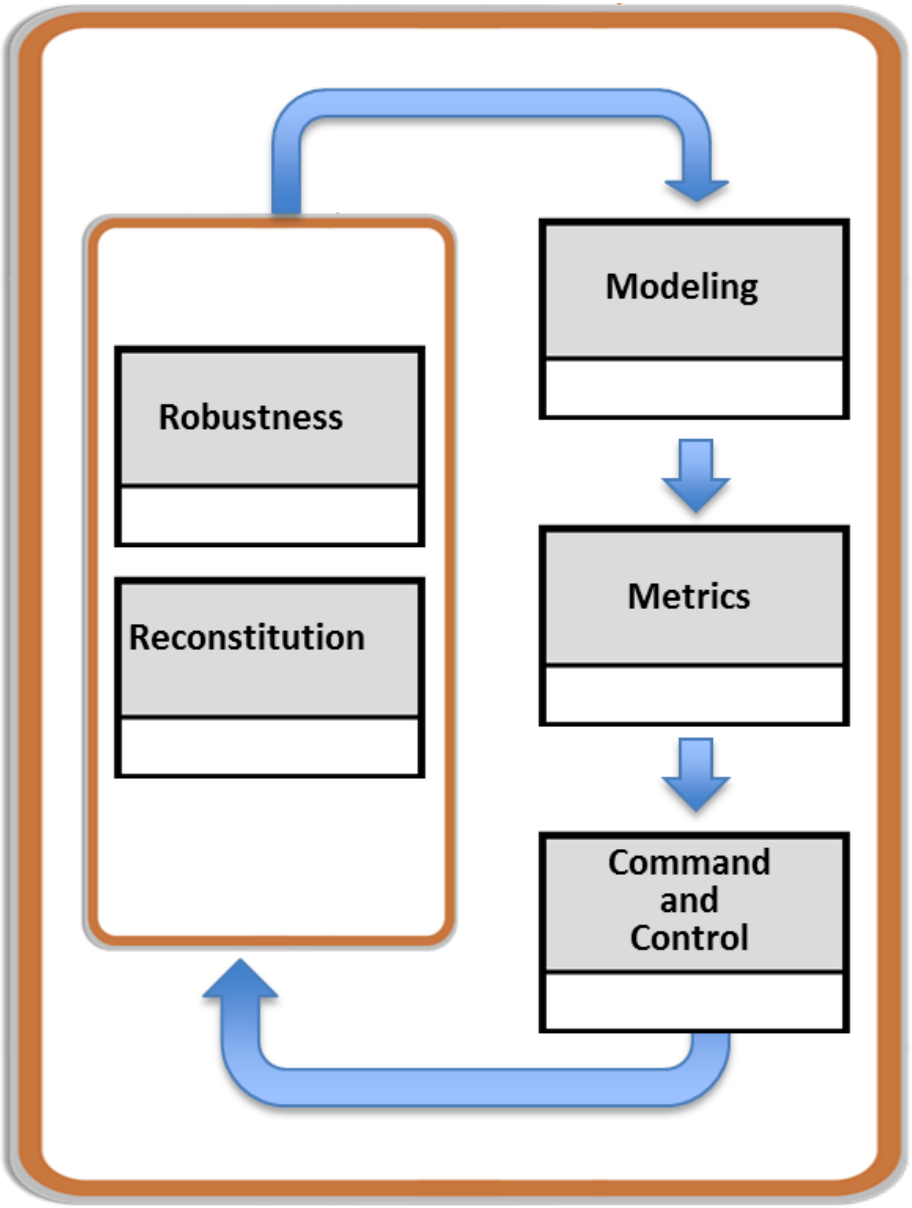
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Reconstitution



Robustness

Asymmetric Resilience



In Short …

- Deterrence is key in reducing attempts but …

  You will never successfully defend against, or stop all attacks

- Therefore, you need to **know yourself** via …

  Models and metrics

- To ensure critical functions to **continue to operate** by …

  Designing theory-guided resilient systems

- All with the goal of …

  *Improving deterrence by achieving an **asymmetric advantage** for the defender*

From Security to Resilience

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Physical Security	Cyber Resilience

Theory

Moving from conventional security to cyber resilience models

- Metrics/measures
  - Degree of trust in components
  - Health of a system
  - Degree of resilience
  - Experimental procedures for validating performance of a resilience concept
- System properties (state independent/passive)
  - What are the attributes of a resilient system?
  - How/why do each of these attributes contribute to resilience regardless of adversary actions?
- Context-dependent properties (state dependent/active)
  - What is our state now and where should we go next?
  - How do we get there from here in the most efficient way possible?
  - How do we control change in the face of partial compromise?

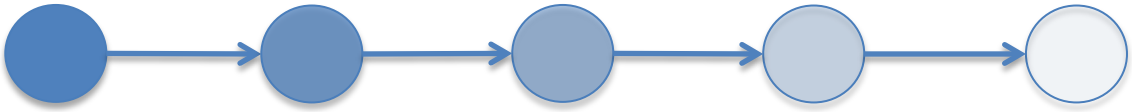
Trusted Elements
The Foundation of a Resilient System

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Metrics and Measures

- Supply chain
  - Securing data even when using global supply chain[3]
  - How does this change when you introduce adversarial actors?
    - Agency theory[4]

- Quantify degree of trust



Trust propagating through nodes

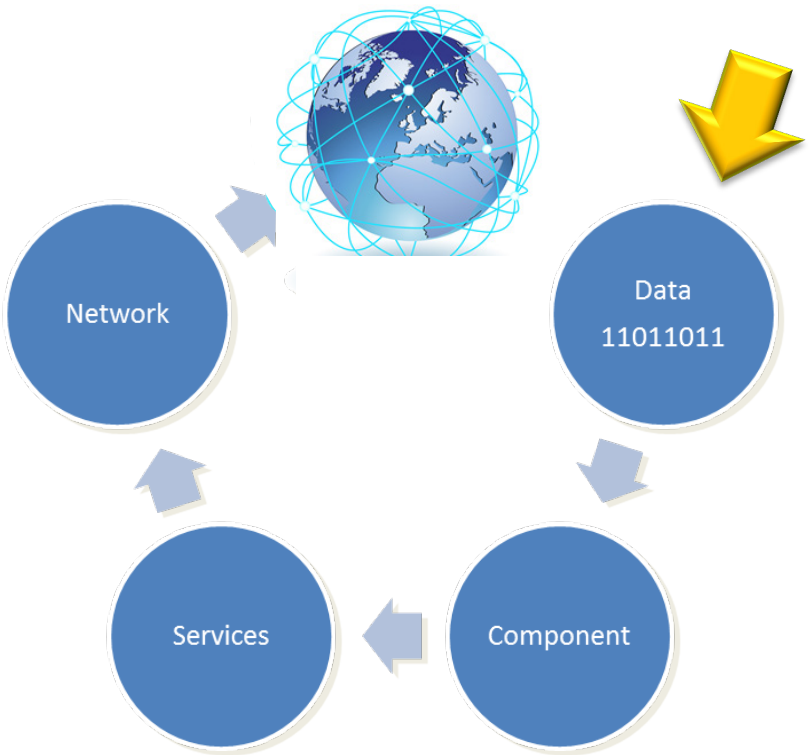
[3]Jin Y, Y Makris. (2012) "Proof carrying-based information flow tracking for data secrecy protection and hardware trust." IEEE 30th VLSI Test Symposium (VTS), 252-257.
[4]Plambeck L, P. Gibson. (2010) "Application of agency theory to supply chains." Oxford Business & Economics Conference Program ISBN : 978-0-9742114-1-9Cachon GP, S Netessine. (2006) "Game theory in supply chain analysis" - Tutorials in Operations Research: …, 2006 - books.google.com

Theoretical Foundation for Metrics from Model Systems

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Metrics and Measures

- Models may provide a source of quantitative measures that can be used to estimate properties of interest[5,6]
  - Cyber systems are multiscale in nature
    - Coupled small scale (component) and large scale (global) spatial events
    - Coupled rapid (software) and slow (mission) temporal events
  - Similar to multiscale modeling in high energy physics and climate modeling
    - But these apply to continuous systems Cyber is mostly discrete
    - AND absolute ordering of events is not always possible



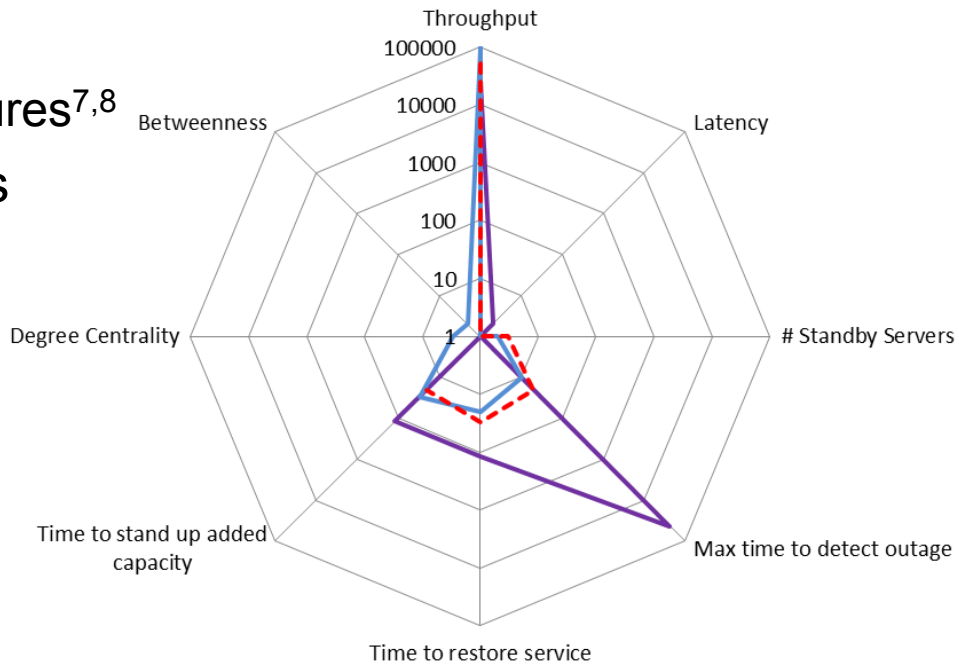
[5]Zeigler BP, H Praehofer, TG Kim. (2000) "Theory of modeling and simulation, 2nd ed. Integrating discrete event and continuous complex dynamic systems" Elsevier Science (USA).
[6]Majda AJ, RV Abramov, MJ Grote. (2005) "Information theory and stochastics for multiscale nonlinear systems." AMS

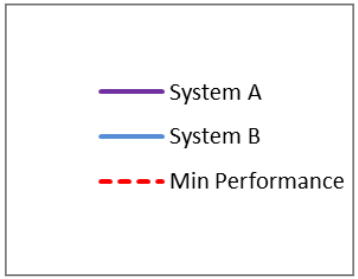
Quantifying System Health and Degree of Resilience

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Metrics and Measures

- Assessment of "health" is dependent on mission
  - Time dependent
  - Location dependent
  - May depend on multiple measures[7,8]
- Many different system attributes may contribute
  - "Acceptable" depends on current needs





[7]Challa S, RJ Evans, X Wang. 2003 "A Bayesian solution and its approximations to out-of-sequence measurement problems." *Information Fusion* **4**, 185–199.

[8] Beynon M, B Curry, P Morgan. 2000. "The Dempster-Shafer theory of evidence: an alternative approach to multicriteria decision modelling." *Omega* **28**, 37-50.

Measuring Cost and Benefit

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Metrics and Measures

- Benefit to defender[9, 10]
  - **How** much better?
  - **In what way** will I be better?
- Cost to defender
  - Cost of building, maintaining infrastructure
  - Organizational resources consumed by resilience infrastructure
    - Bandwidth
    - Disk space
    - Compute cycles
  - Availability of critical assets

- Cost to attacker
  - Cost for developing, using tools
  - Exposure is related to time spent in detectable state
  - Using tools makes our defenses stronger
  - Risk of prosecution, other pushback

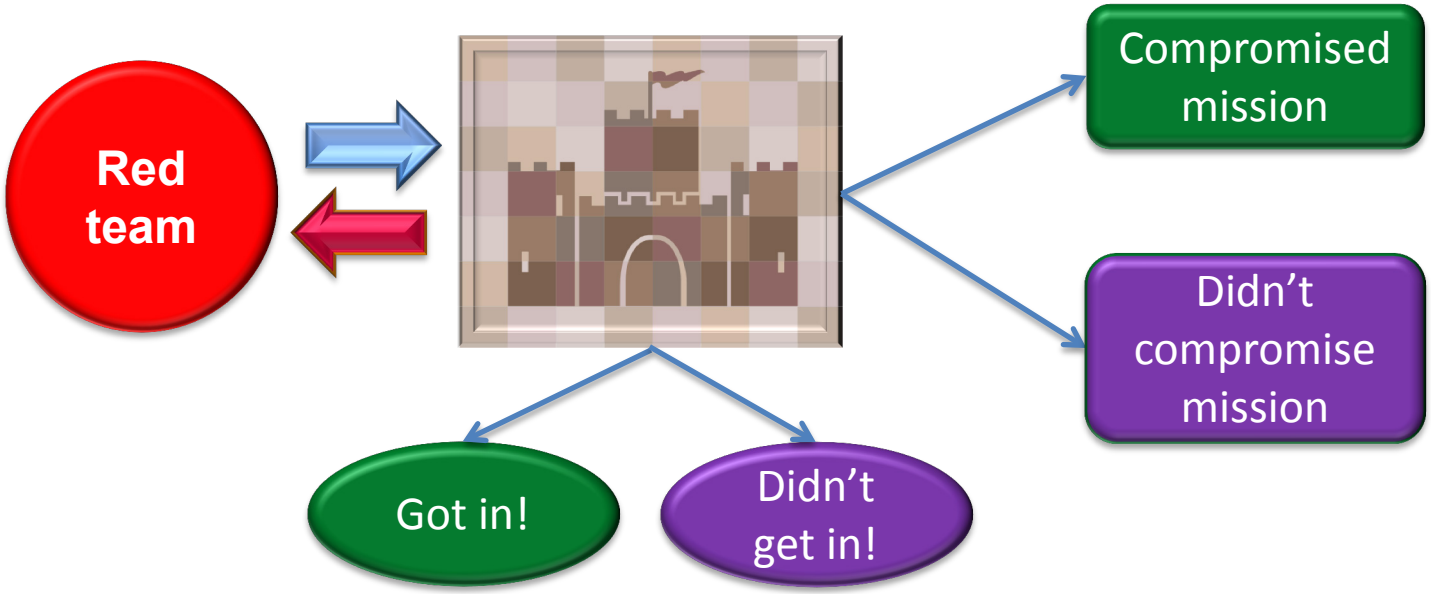
[9]Gordon LA, MP Loeb. (2006). "Managing cybersecurity resources: a cost-benefit analysis" McGraw Hill
[10]Bodin LD, LA Gordon, MP Loeb. (2008). "Information Security and Risk Management" *Comm. ACM*. **5** (4). 64-68.

Measuring Resilience
Rethinking the Red Team

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Metrics and Measures

- Traditional red team is focused on penetrating a network
- The concept of resilience is based on an assumption of compromise
  - We would need longer tests in which red-teamers (or software agents/some combination) engage a resilient infrastructure
  - Performance of the red team is not based on penetration, but on the ability to achieve goals that interfere with mission



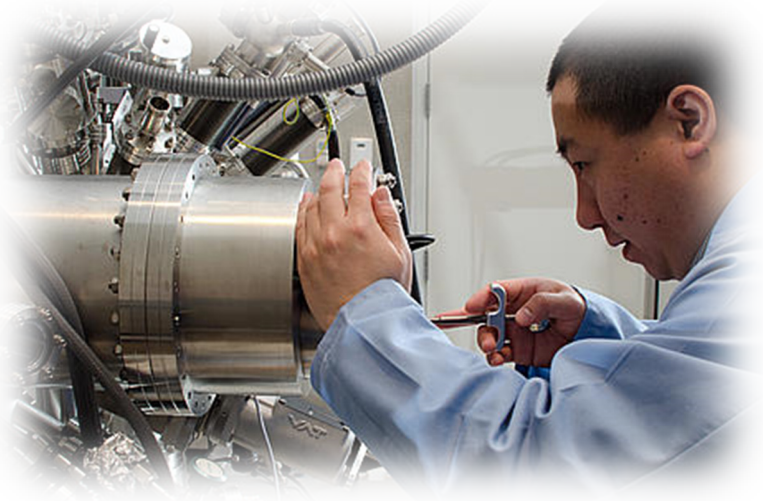
Beyond the Red Team

Theoretical Measures of Experimental Performance

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Metrics and Measures

- On what basis do we make quantitative assertions about the performance of a resilience technique?
  - Need to enumerate, validate assumptions
  - Need a theoretical foundation for proofs-of-concept
  - Resilience is a system property, **however,** measuring resilience requires treatment of the human element

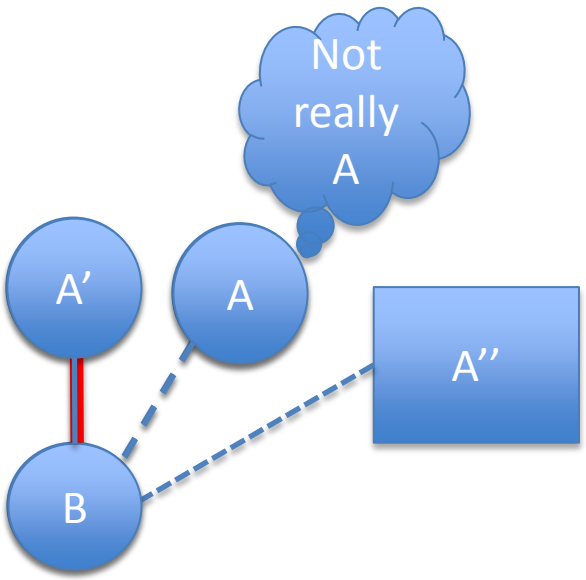


System Properties

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Attributes of Resilience

- Redundancy
- Diversity
- Self-stability
- Fault tolerance
- Velocity/fluidity
- Deceptiveness
- …



What are the properties of systems regardless of the adversaries' actions that increase the chances of achieving mission in the presence of faults, both natural and adversarial?

Which property combinations are necessary and sufficient?

Redundancy and Diversity

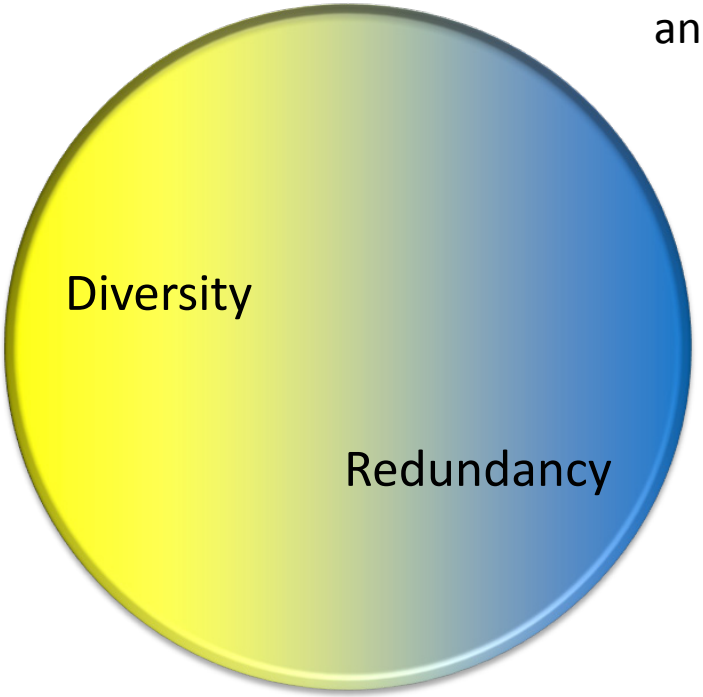
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Attributes of Resilience

Theory of diversity[11]
- Not additive
- Based on similarity
- Multi-attribute

Example attributes:
- Runs on which OS?
- Uses which protocol?
- Which network?

Gives us a way to quantify diversity AND the value of this diversity



Theory of combined diversity and redundancy[12]
- Focused on software
- Utilize undecidability
- Disproportionately raise attacker's cost

Extend to systems in general: Undecidability is even more prominent in complex systems. How do we harness this without raising our own cost?

[11]Nehring K, C Puppe (2000) "A Theory of Diversity" http://www.econ.ucdavis.edu/faculty/nehring/papers/divfinal.pdf
[12]Allan BA, RC Armstrong, et al (2010) "Theory of Diversity and Redundancy in Information Security" Sandia LDRD final report http://prod.sandia.gov/techlib/access-control.cgi/2010/107055.pdf

Self-stability

Attributes of Resilience

- Regardless of state, guarantee that a protocol will converge to a "safe state"[13]
  - Requires a time of correct computing
    - reasonable for natural faults
    - Possibly not for intelligent adversaries
  - How to extend this beyond just protocols?
- Combining this with distributed control, shown analytically to be possible[14]
- Passivity in design to mitigate imprecise timing in cyber systems[15]

How does this change in the presence of an intelligent adversary?
no assumptions about the distribution or frequency of faults

[13]Gouda MG, NJ Multari. (1991) "Stabilizing Communication Protocols." *IEEE Trans Comp*, **40** (4), 448-58.
[14]Dikjstra EW. (1974) "Self-stabilizing systems in spite of distributed control." *Comm ACM*, **17**(11), 643-4.
[15]Sztipanovits J, Koutsoukos X, Karsai G, Kottenstette N, Antsaklis P, Gupta V, Goodwine B, Baras J, and Wang S. (2012) "Toward a Science of Cyber–Physical System Integration" *Proc. IEEE*. **100**(1), 29-44.

Fault Tolerance

Attributes of Resilience

Given a collection of system elements participating in a collective operation, how can we guarantee correct operation in the presence of faults?

- High performance computing
  - Data[16]
  - Interprocess Communication[17]
  - Software[18]
- Network traffic routing[19]

How do we handle fault-tolerance across multiple layers simultaneously?

[16]Ali N, S Krishnamoorthy, et al. (2011) "Application-Specific Fault Tolerance via Data Access Characterization." *Euro-Par 2011.* **6853**, 340-352.
[17]Fagg GE, JJ Dongarra (2000) "FT-MPI: Fault tolerant MPI, supporting dynamic applications in a dynamic world" *Lec. Notes Comp. Sci* **1908**, 346-53.
[18]Bosilca G, R Delmas, et al. (2009) "Algorithm-based fault tolerance applied to high performance computing." *Trans. Parallel. Dist. Comp.* **69**(4), 410-6.
[19]Duato J (1997) "A theory of fault-tolerant routing in wormhole networks." *IEEE Trans Parallel Dist. Sys.* **8**(8), 790-802.

Velocity/Fluidity

Attributes of Resilience

- Moving target defense[20, 21]
  - Attack surface
  - Complexity and randomization
    - Instruction set
    - Base address
  - Game theory and modeling the adversary
- IP hopping (patents, product offerings)
- Virtualizing services, hosts

To be practically useful, we need to understand the cost and benefit of using these concepts

[20] Jajodia S, AK Ghosh, et al. (2011) "Moving Target Defense: creating asymmetric uncertainty for cyber threats". Springer
[21] Jajodia S, AK Ghosh, et al. (2012) "Moving Target Defense II: application of game theory and adversarial modeling". Springer

Deceptiveness

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

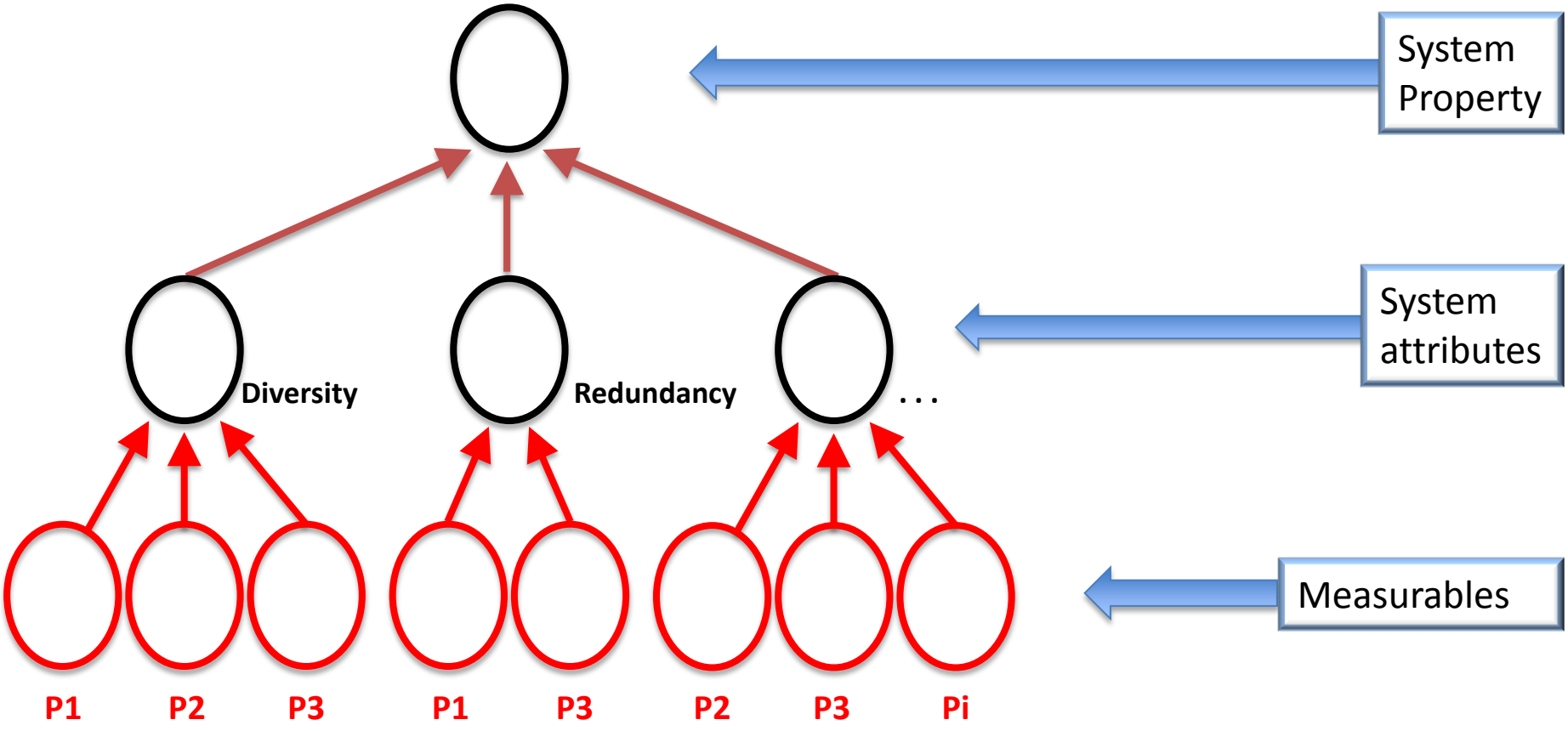
Attributes of Resilience

- To what extent can the adversaries' view of an infrastructure be manipulated?
  - User roles
  - Host roles/attributes/defenses
  - Network fabric
  - Data location
  - Policies
- What is the effect of deception on our own processes?
  - Service/process failures
  - Decrease in confidence in data
  - Decrease in utility for users

Relating Attributes to Resilience

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Attributes of Resilience



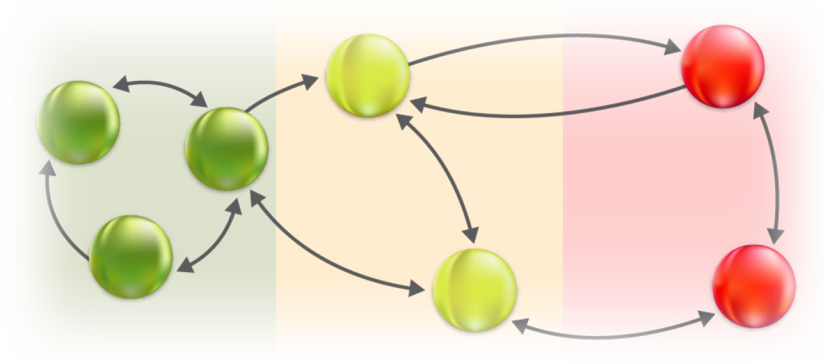
How do we relate measurables from a system or a model of a system to the desired property of the system?

Formulation as a State Problem

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- Express system and system transitions as a state problem
- Equivalence relation between states
  - Ideal = Sufficient and optimal
  - Partially degraded = sufficient
  - Degraded = insufficient



- Goal is to find state, transitions that tend toward ideal states
  - Not just turning back on all services
  - Which one is best in the current environment

Given that some elements will be compromised, how do we discover where we are, and decide where we want to be?

Constrained optimization problem

Formulation as an Adversarial Problem

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- Game theory[22]- using rules of games to understand and reason about adversarial relationships
  - Mathematical framework for capturing the effect of motivation, risk, on actions
  - Makes simplifying assumptions (bounding assumptions) about space of moves, rules, turn order, transparency of moves

- Serious gaming- developing gaming environments to "play out" complex adversarial scenarios
  - With right formulation, this could be foundation of new red-team protocols for resilience

[22]Roy S, C Ellis, S Shiva, D Dasgupta, V Shandilya, Q Wu. (2010) "A Survey of Game Theory as Applied to Network Security." *Proc of the 43rd Hawaii International Conference on System Sciences.*

Awareness in a Compromised State

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- Byzantine agreement- unknowable side effects of compromise
  - Many different potentially compromised elements are used to make decisions
  - Mathematical formulation of minimum conditions for making the right decision

- In decentralized control
  - No centralized authority
  - Need to share some information, but all-reduce is not scalable
- What about when adversary adapts[23]?
  - Statistical distribution of faults is not normal

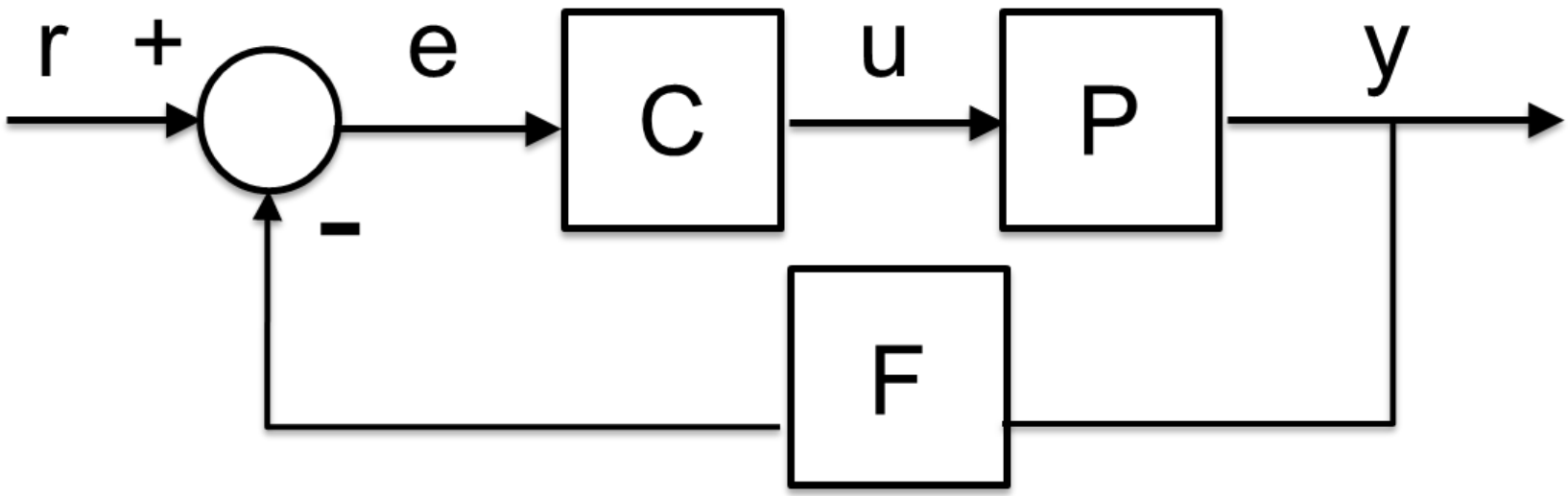
[23]King V, J Saia. (2010) "Breaking the O(n2) bit barrier: Scalable byzantine agreement with an adaptive adversary." *PODC'10.*

Changing State Through Linear Control Theory

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- Control theory to govern the dynamics of changing state[24]
  - Measuring deviation from intended state
  - Applying feedback term to correct



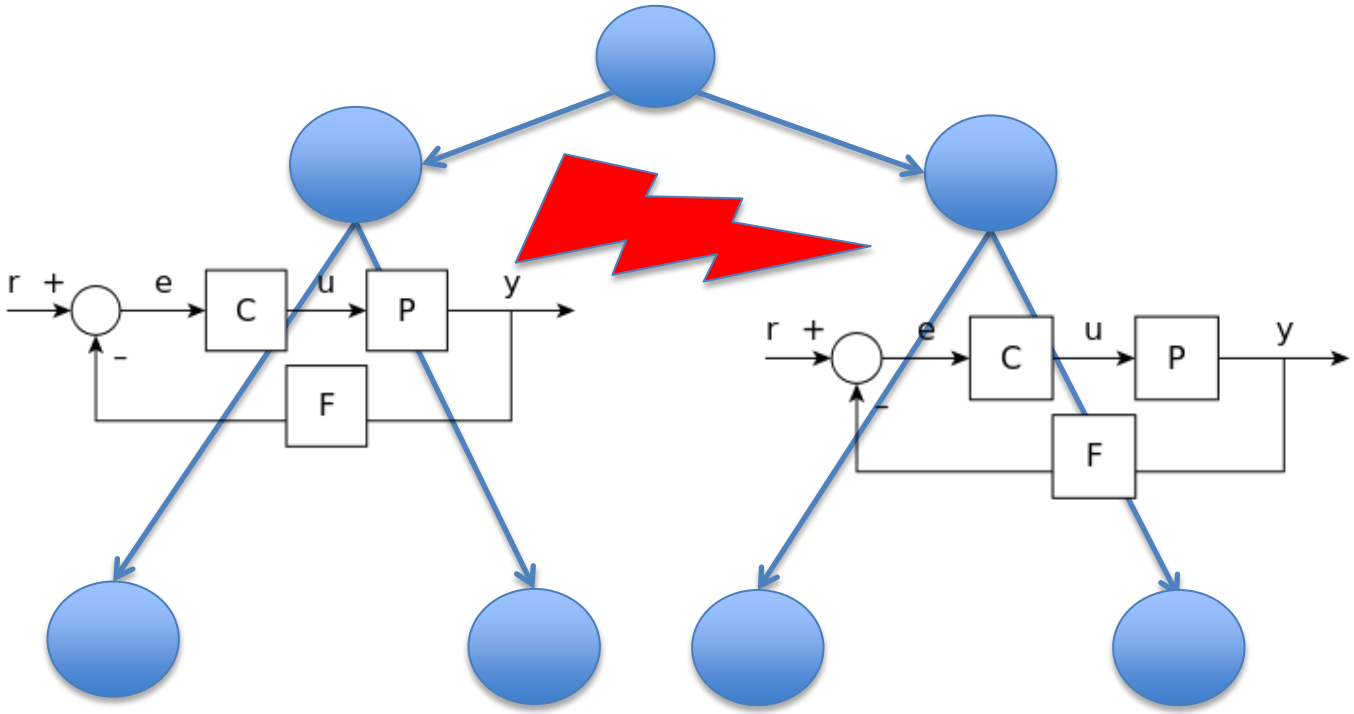
[24]Cardenas AA, S Amin, S Sastry. (2008) "Secure Control: Towards Survivable Cyber-Physical Systems" *The 28th International Conference on Distributed Computing Systems Workshops*, 495-500.

Command and Control in Fluid Environments

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- Solving an optimization problem to figure out how to move
  - distributed control theory[25]



[25]Sandell, NR Jr., R Varaiya, M Athans, MG Safonov. (1978). "Survey of Decentralized Control Methods for Large Scale Systems." *IEEE Trans Automat. Control*. **23**(2), 108-128.

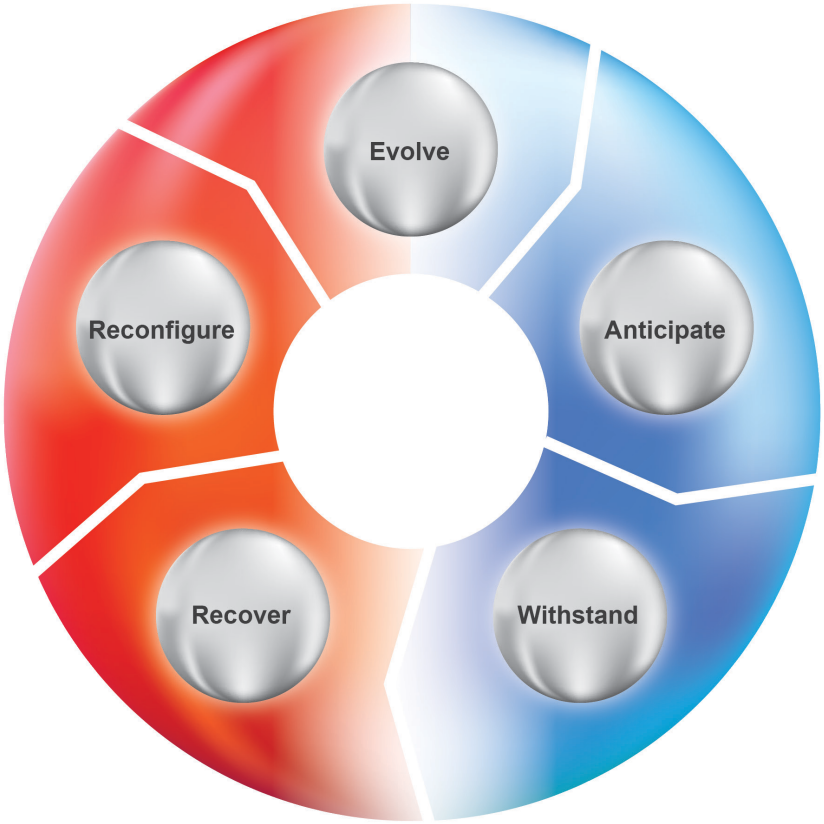
Co-evolution

Combining Context-dependent and Independent Views

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Context-dependent Properties

- How all three components fit together
  - Metrics
  - Passive
  - Active
- Resilience in combination with engaging an adversary = coevolution in real time!



Theory of Resilience Sessions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- **Supply Chain Integration for Integrity:** *Policy and Architecture for Built-in Supply Chain Integrity of Trusted Components*
  - Rick Sheldon (ORNL)
- **Metrics and Analysis Techniques for Cyber Defensibility, Resiliency, and Security:** *Looking Across Different Evaluation Environments*
  - Bill Heinbockel (MITRE)
- **Performance Assessment for Complex System Models using Probabilistic Formal Concept Analysis**
  - Jennifer Davidson (Iowa State University)
- **Towards a Unified Theoretical Framework for Reconstitution of Cyber Systems**
  - Mahantesh Halappanavar (PNNL)
- **Increasing Cyber System Resilience Through Predictability-based Defense**
  - Rich Colbaugh (SNL)

For more information regarding this session *Building the Theory of Resilience* contact us at:

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Nicholas J. Multari, Ph.D.
nick.multari@pnnl.gov
509-375-2043

Christopher S. Oehmen, Ph.D.
christopher.oehmen@pnnl.gov
509-375-2038