

# Survivable Critical Network Services

Chuck Phipps

703-983-4044 • [cphipps@mitre.org](mailto:cphipps@mitre.org)

ARMY-Contract MOIE

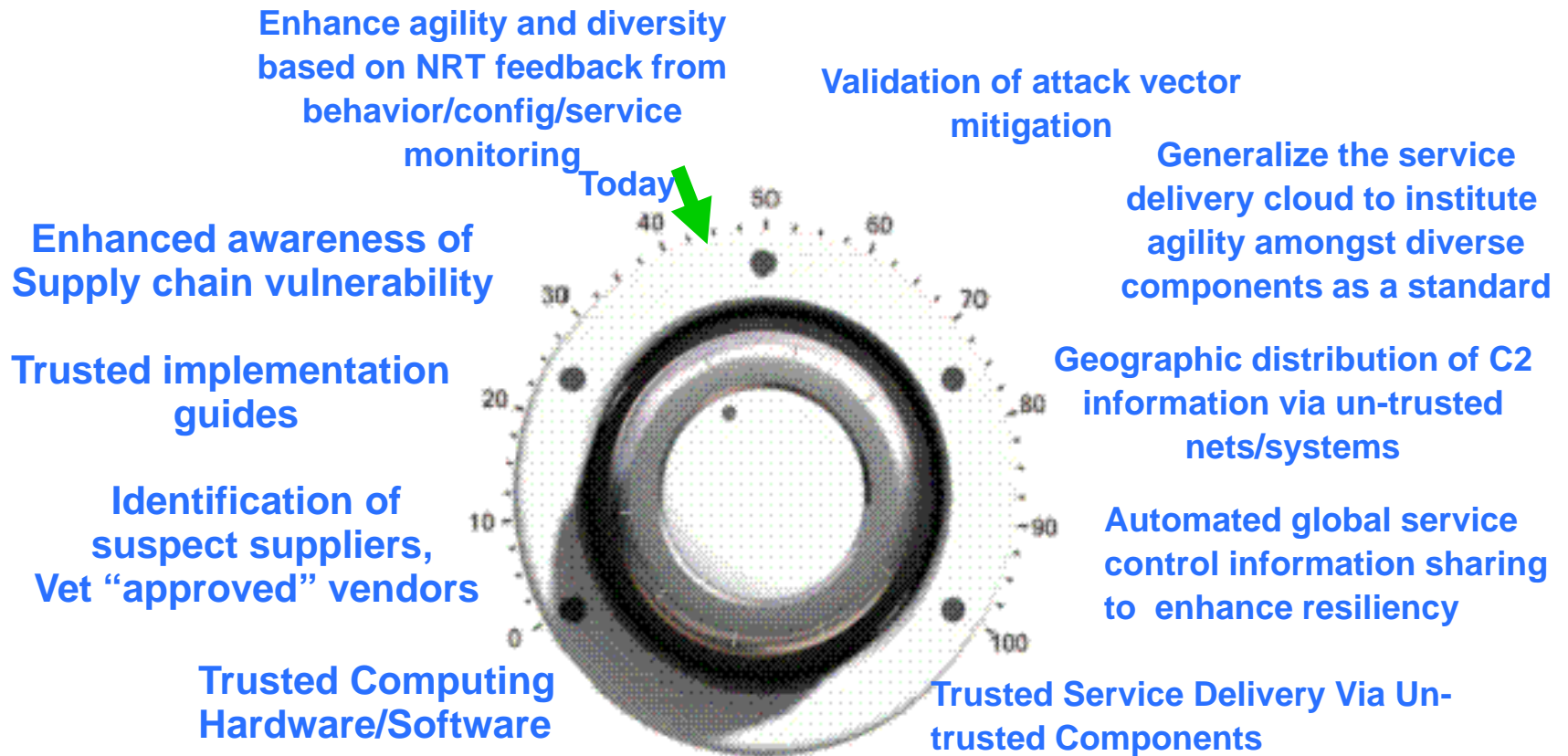


# Problem



- **Latent and “Zero-Day” vulnerabilities, including those introduced through supply chain infiltration, will continue to provide attack vectors that can bypass existing layered defenses.**
- **The ability to detect and prevent these attacks in a proactive manner is limited.**
- **The length of time that these vulnerabilities may remain in place, awaiting activation can be very long (months, years).**
- **The length of time that the attack vector can be utilized after activation is difficult to know, as the particular vulnerabilities are assumed to be undetectable with current processes.**

# Background



- Researching agility and diversity in service delivery to institute resiliency in the face of expected supply chain and "zero day" vulnerabilities.

# Objective



- **Demonstrate that service availability can be maintained while service delivery components are made to be agile across a diverse set of resources.**
- **Determine the constraints of service mobility and availability as related to the exposure of a particular service delivery configuration (i.e., can the service be rotated to a new set of components with a frequency that would preclude a typical attack vector from being fully exercised).**

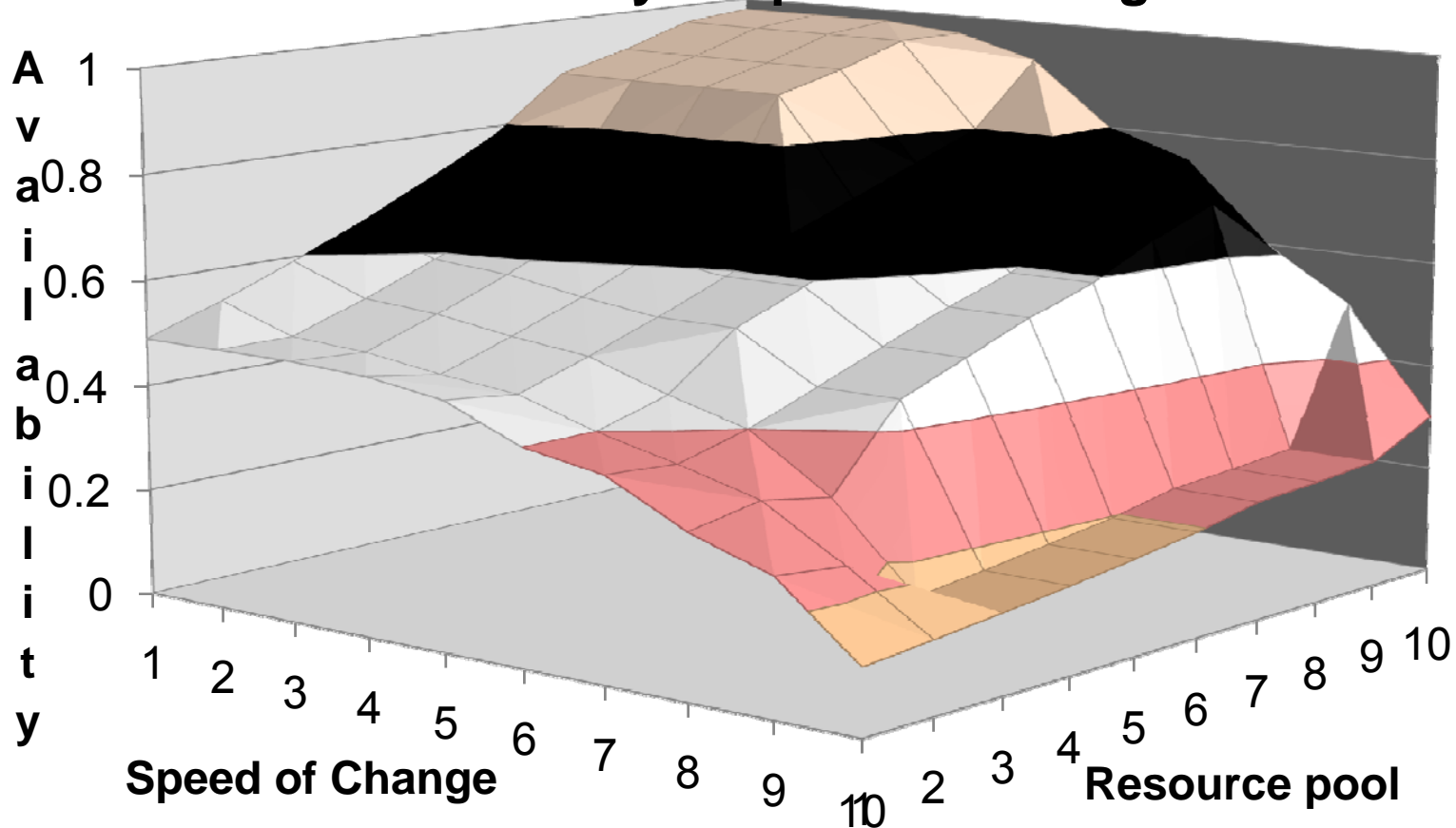
# Activities



- **Deploy virtualized infrastructure to support demonstration of objectives.**
- **Determine methods to allow rapid change of components while maintaining service delivery availability and quality.**
- **Demonstrate the techniques using the selected representative service (Domain Naming Service).**
- **Create scripts and API integration to implement movement of service amongst the pool of resources.**
- **Implement movement of retired service delivery components to a forensics sandbox for off-line analysis.**
- **Create feedback loop from forensics process to aid in control of resources used for production service delivery.**

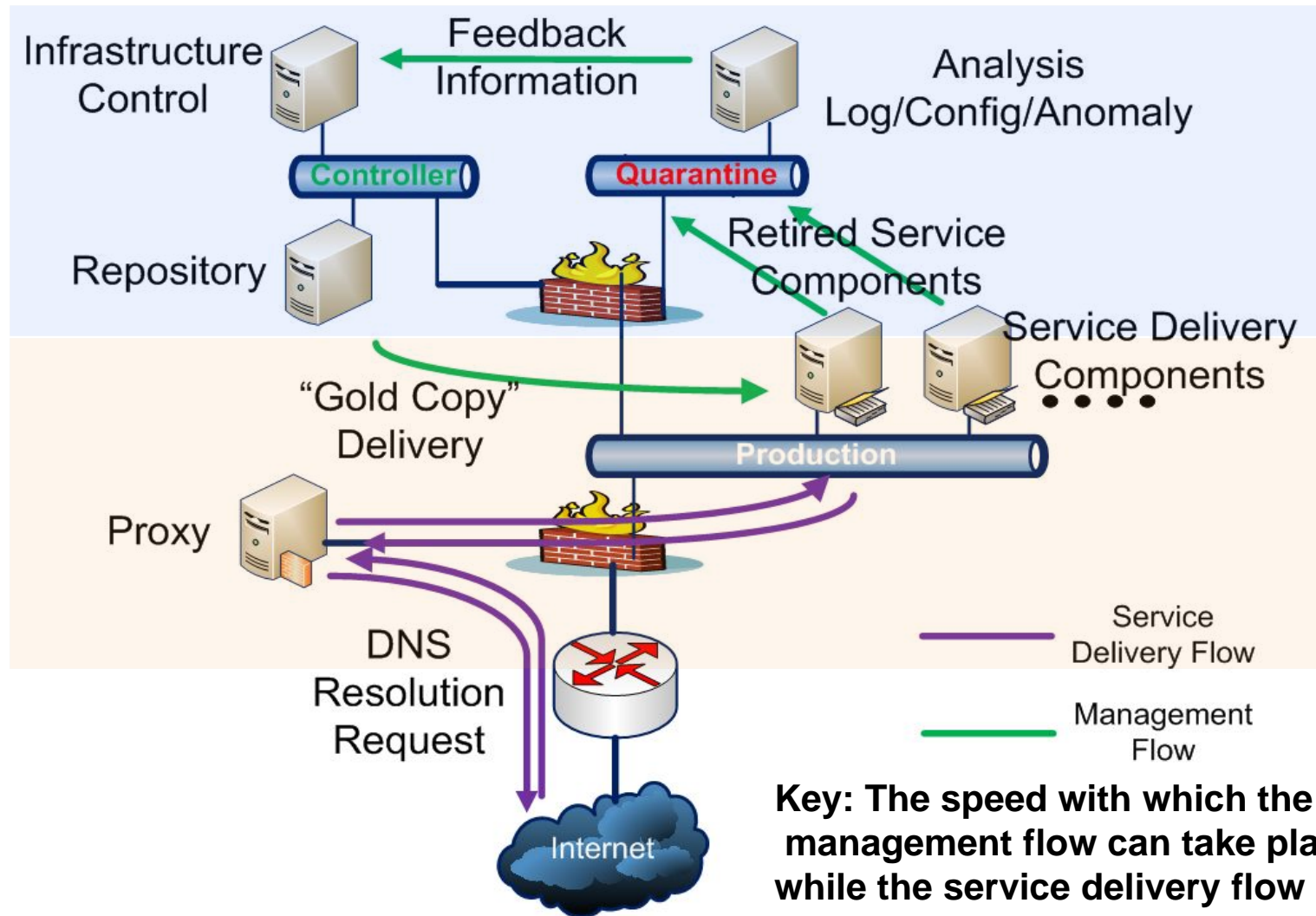
# Highlight

## "Availability v. Speed of Change"



Values depict the type of information we plan to develop, not actual experimentation results.

# Demonstration



# Impacts



- **The sponsor operational mission will be less vulnerable to supply chain, or other “zero day” (i.e., undiscovered) vulnerabilities.**
- **These techniques can be transferred and adopted by vendors for inclusion in their product offerings.**
- **The knowledge of how availability is impacted by the rapid migration of services amongst a pool of components will contribute to systems engineering practices incorporating these techniques.**
- **The applicable forensics tests to aid in determining how, and when, resources should be removed from the pool will be documented for use in applying these techniques to sponsor systems.**

# Future Plans

- **Expand the concept to include the use of all enterprise IT resources to be included in the pool of components utilized to deliver an IT service.**

