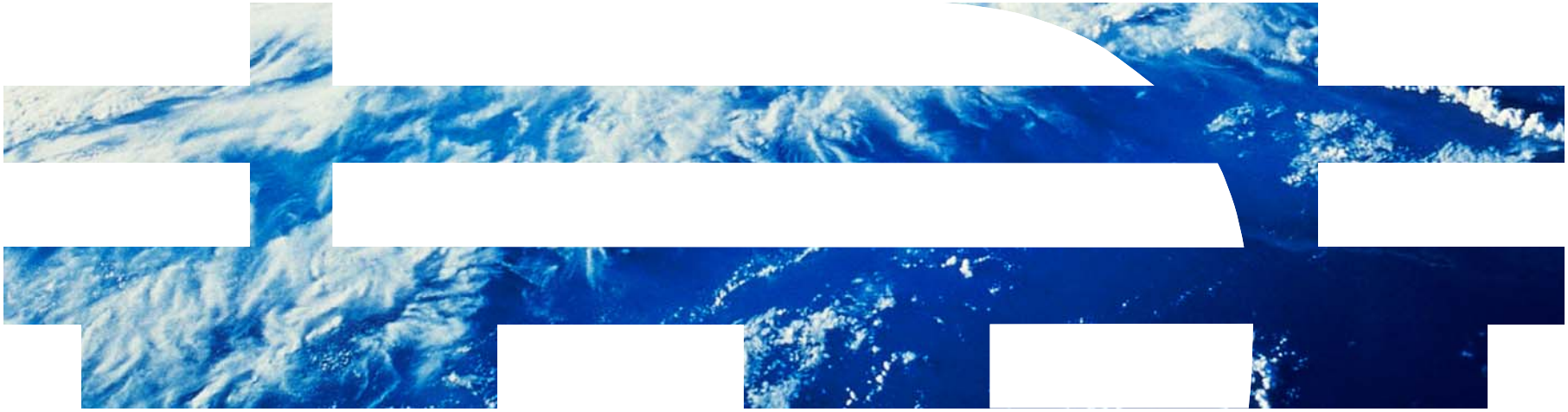
IBM

NITRD Cybersecurity R&D Kickoff Event

Industry/Academia Panel

Dimitrios Pendarakis, Manager, Secure Systems Group
IBM T.J. Watson Research Center



May 2010

What is Moving Target?

- **Moving Target enables controlled movement across multiple system dimensions to reduce the windows of opportunities for attackers to exploit vulnerabilities in our systems**
  - To an attacker, our systems look externally chaotic, however, they are internally manageable
  - Increase the marginal costs of the attacker (must do new recon for each attack), increase the range of defensive strategies available to the defender, and increase the resiliency and fault tolerance of a target
  - Maneuverability and Diversity: develop and deploy diverse and mutating systems
- **Examples Include**
  - Dynamic Networking, Just-in-time Compiling, Instruction Set Randomization
  - Non-persistent virtual machines
    - "Every time the enemy takes a hill, the hill goes away"
- **Objective: attacks only work once, if at all**

State of the Art – Sample Moving Target Games

- **Data Chunking and Decentralization**
- **Moving target servers & decoys**
- **Dynamic code & instruction set randomization**
- **Robust Cryptographic Authentication - Moving Target Credentials**
- **Moving target networks**
- **Smart Motion Adaptation/Management**

- **In part excerpted from co-chairs' and participants' report from the National Cyber Leap Year Summit, August 17-19, 2009, Arlington, VA**
- **Co-chairs**
  - **Professor Anup K. Ghosh**, Chief Scientist & Research Professor, Center for Secure Information Systems, George Mason University
  - **Mr. Ivan Krstić**, Core OS Security Samurai, Apple
  - **Dr. Dimitrios Pendarakis**, Research Staff Member & Manager, Secure Systems Group, IBM T.J. Watson Research Center
  - **Professor William H. Sanders**, Donald Biggar Willett Professor of Engineering, Director Coordinated Science Laboratory and Information Trust Institute, University of Illinois
- **Reports**
  - http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf
  - http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf

Moving Target Data Storage
Chunking and Decentralization (Distributed Data Shell Game)

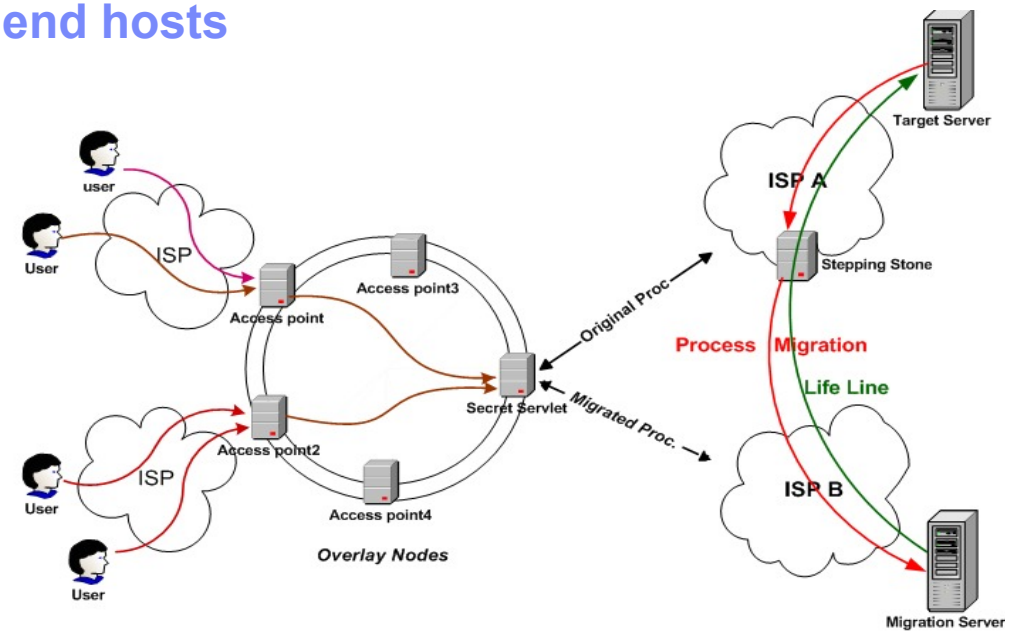
- **Stored files are broken into pieces that are encrypted and redundantly stored across multiple servers**
  - Redundancy is achieved through erasure coding and can be varied to provide desired level of availability guarantees
    - For instance, in a grid of ten storage servers, every file might be stored on five servers, of which any three need to be available to reconstruct the whole file
- **Data spread across a number of (potentially heterogeneous) machines; process coupled with strong encryption**
  - Data storage as a whole is transformed into a moving target
  - An attacker can no longer compromise a single storage server and obtain all the data; needs to compromise multiple servers as well as obtain the encryption keys
  - Example: Tahoe grid file system (http://allmydata.org/trac/tahoe-lafs), a cross-platform open-source software solution
- **Next steps: further research into development, experimentation and efficient application of these methods to more complex data organization systems, e.g., relational databases**

Robust Cryptographic Authentication - Moving Target Credentials

- **Current authentication methods largely employ static credentials – phishing attacks**
  - username/password Web authentication; TLS protects credentials *only while in transit*
- **Develop cryptographic methods for secure authentication without transmitting raw credentials**
  - Explore use of zero-knowledge, password-authenticated mechanisms
  - Example: the Secure Remote Password (SRP) (http://srp.stanford.edu) protocol
    - Constructs a special proof that the user knows the password, incorporates random numbers that are different each time and sends that proof to the server
- **Explore widespread deployment of diversity in authentication for both human users, devices and different software components**
  - Diversity in the type of credentials, the time requested, communication channel used
  - Protect against attackers that successfully compromise one component of a system
- **Objective: *transform Web authentication to a moving target* leaving attackers and phishers with useless information**

Moving Target Networks

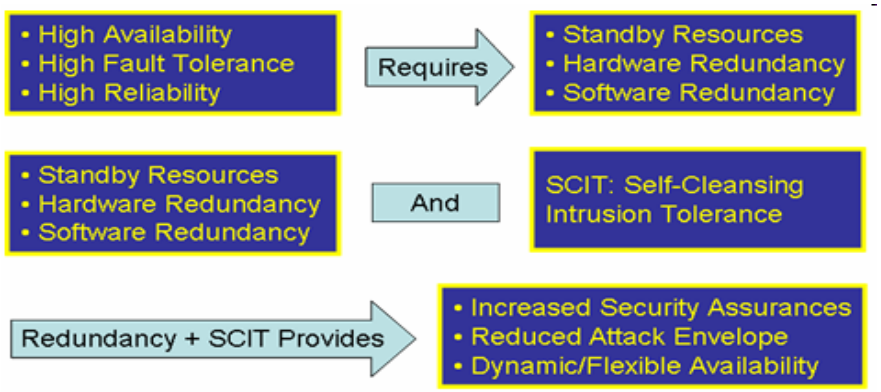
- **Vary addresses, names, access paths, topologies – both for physical networks & end hosts**



- **Example:** ***"MOVE: An End-to-End Solution To Network Denial of Service", A. Stavrou A. D. Keromytis J. Nieh V. Misra D. Rubenstein, Columbia University, NDSS 2005***
  - Use an overlay network, which treats authorized traffic preferentially
  - Lightweight process-migration allows moving services; functionality residing on a part of the system that is subjected to a DoS attack migrates to an unaffected location
  - Legitimate users, who are authenticated before they are allowed to access the service, are routed by the overlay network to the new location

Moving Target Servers & Decoys

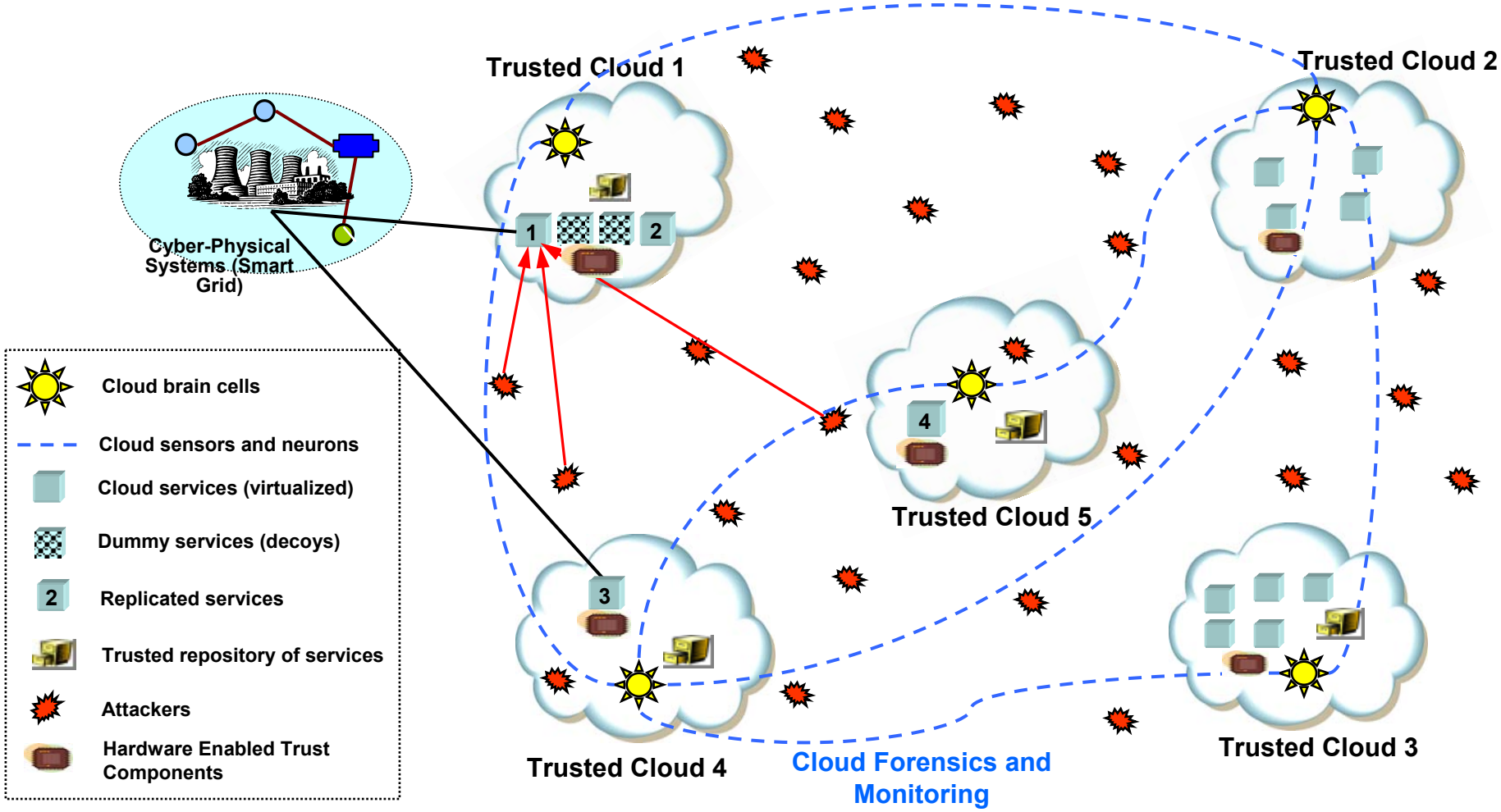
- **Moving Target Servers: create new (or use standby) servers when attacked**
  - Example: http://cs.gmu.edu/~asood/scit/



- **Decoys: dynamically deploy a large number of fake, mutating targets that appear to attackers indistinguishable from the real targets**
  - Serve as sensors that can detect and analyze new attack activity, pinpoint new vulnerabilities; used in honeypots and honeynets
  - Significantly increase the attacker's work factor; and require new recon for each attack
  - Enablement: virtualization allows fast cloning of VMs; resource optimization reduces cost
  - Cooperating service providers could use a combined “dark IP” space to deploy decoys as a moving target for malware detection and mitigation

IBM Research Vision on Moving Target Defense: Hydra

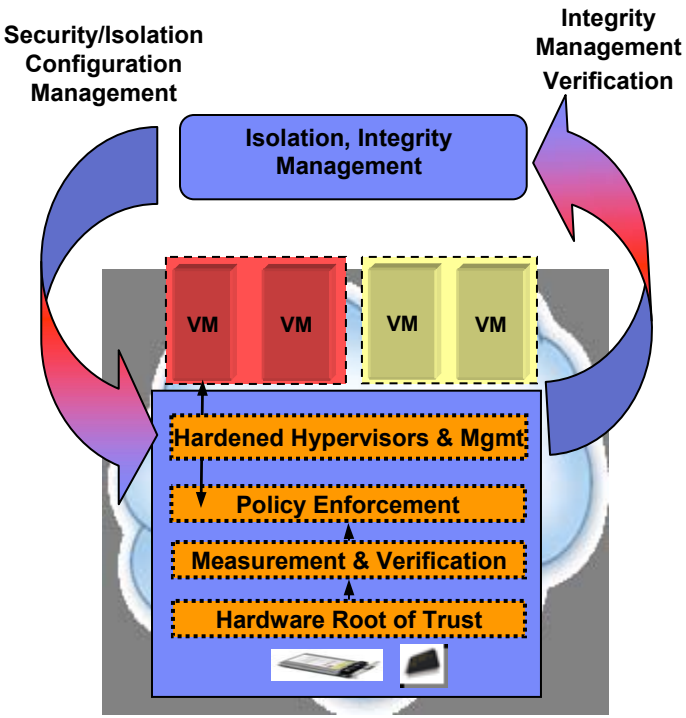
Use of virtualization, cloud computing & stream analytics technologies to construct resilient moving target defense systems



Hydra Vision: Elements of a Moving Target Defense

- **Current Status**: Attackers can inflict asymmetric damage by penetrating a small subset of targets; attackers enjoy relative anonymity while targets are typically well identified
- **Objective**: the attacked infrastructure can hide, evade detection and self-replicate (just like Hydra), while continuously performing analysis that pinpoints attackers and closes their window of opportunity by self-modification

- **Hardware enabled trust components** provide high integrity, tamper resistance
- **Large scale, low cost virtualization**: fast replication of services from preconfigured master images
  - **Services and data distributed** over one or more trusted clouds, in conjunction with information dispersal, physically diverse and reconfigurable communication channels
  - **Secure virtualization**: strong isolation between different VMs and ability to verify integrity of the software stack
    - Leveraging hardware trust components
  - In response to suspected/detected attacks, **target services replicated** in multiple physical servers, some as "decoys"

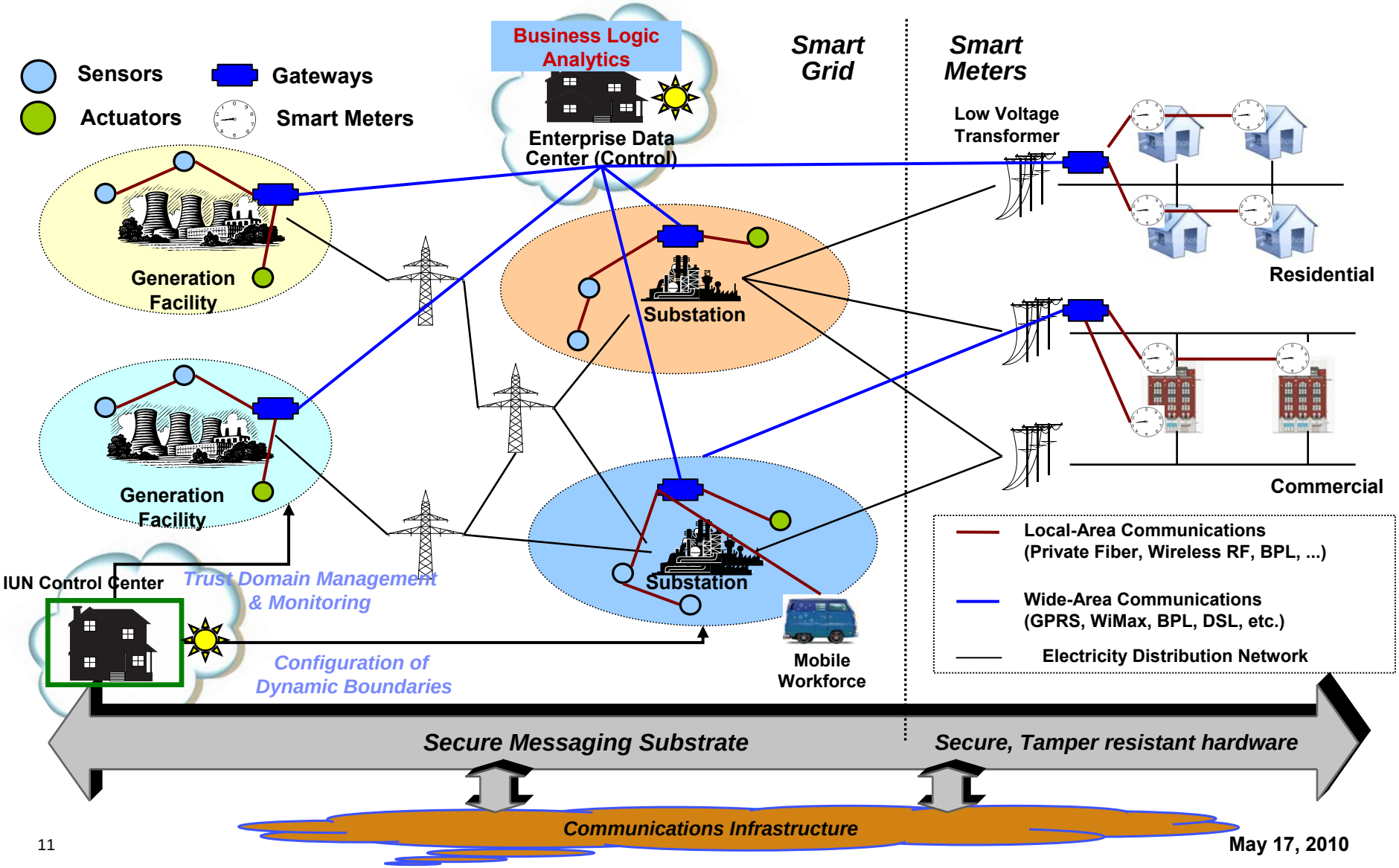


Foundation for Building
Tailored Trustworthy Spaces

Hydra: Elements of a Moving Target Defense (cont.)

- **Large, decentralized clouds** (private/hybrid) provide a flexible pool of virtualized resources that can be replicated and migrated dynamically, creating diverse and mutating systems
  - These capabilities can be harnessed to obfuscate the identity of targets and quickly identify and respond to attackers
- **Real-time high-volume stream analytics** – enable a set of cloud "brain cells"
  - Operate in a decentralized cooperative manner, processing massive amounts of data, to detect attackers and their behavior patterns
  - Cooperation between multiple cells and clouds to perform localization of attackers
- **Micro-virtualization**: new virtualization technologies with reduced overhead appropriate for cyber-physical systems
  - Loosen binding between physical location and computing services

Challenge: Building Tailored Trustworthy Spaces and Moving Target Defense Strategies in CyberPhysical Systems



Research Challenges

- **Performance & Scalability:** deployment limited to small testbeds currently?
- **Power efficiency:** impact of replication, decoys, etc.
- **Provable security properties** vs heuristics
- **Measures of improvement:** risk reward ratio?
- **New analytics**: low false positives and false negatives

Creating a Sustainable Process: Research, Policy & Commercial Deployment Considerations

- **Mechanisms to support a sustainable process to drive the envisioned game changing technologies**
  - Introspection: what technologies haven't worked so far and why?
  - **Overcoming inertia** caused by widespread deployment of legacy technologies
  - Anchor development and experimentation on **realistic settings and data**
  - Establish **metrics to track progress** towards successful development and adoption
  - Strong **partnerships** between government, industry and academia
- **What role should USG have in creating a sustainable process which could initiate and guide R&D**
  - Cybersecurity National Initiative to promote deployment of game changing technologies
  - Adopt an **urgent, but long-term view**; while essential, short term fixes insufficient
  - Promote and reward sound, consistent security engineering practices
    - Explore application of Cyber Economic Incentives to promote, verify and differentiate strong security implementations
  - Foster **partnerships of government, industry and academia** to facilitate coordinated research, development and adoption of game-changing solutions

Acknowledgements

- Cybersecurity R&D Kickoff Event organizers, USG
- Input from government representatives, organizers
  - Pat Muoio, Martin Ross, Tomas Vagoun, …
- NCLY Summit Co-chairs & Participants
- JR Rao, Reiner Sailer (IBM)
- Many others who have contributed to various discussions on these topics