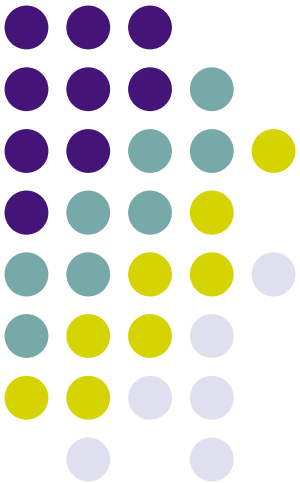
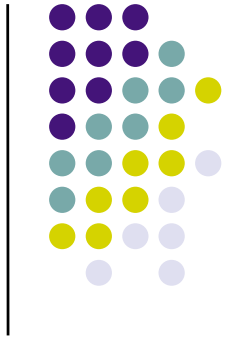
TIED: Trial Integration Environment built on DETER

The DETER folks:
Terry Benzel, Bob Braden, *Ted Faber,* John Hickey, Alefiya Hussain, Anthony Joseph, Calvin Ko, *Kevin Lahey,* Jelena Mirkovic, Steve Schwab, Keith Sklower, Arun Viswanathan, *John Wroclawski, …*



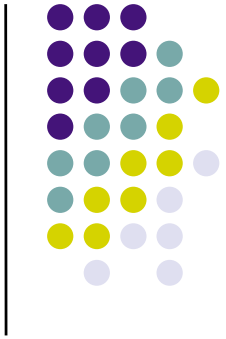
The DETER Facility

Cyber Security testbed at USC/ISI and UC Berkeley



- Funded by NSF and DHS, started in 2004
- Based on Emulab software, with focus on security experimentation
- 200 Nodes at ISI (128 Dell 1850, 8 Sun V65x, 64 IBM Netfinity 4500R)
- 96 Nodes at UC Berkeley (64 Dell 1850, 32 Sun V60x)
- Many tools for experimenters: GUIs, traffic generators, simulators, traffic analyzers, etc.

DETER Project Goals



- Scientific methods and infrastructure for advancing security in identified hard problems
- Enhanced availability of validated information about security protection technology
- Enduring realistic testbed for security research
- Advances in testing methods and methodology for network security devices
- Suite of reusable network security tests including traffic data sets

Today's DETER Testbed

Key New Capabilities:

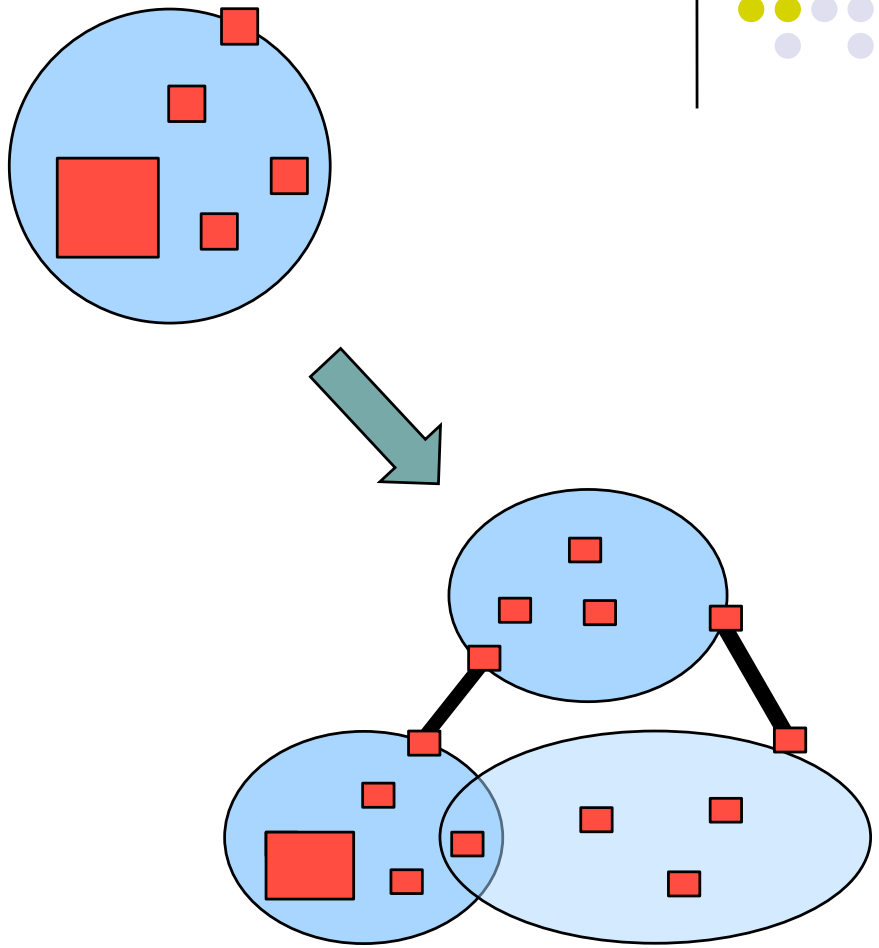
- Risky Experiment Management
- High Level User/Workflow Tools
- Experiment Health Management
- Dynamic Federation

Contributions to Next-Gen Facilities -

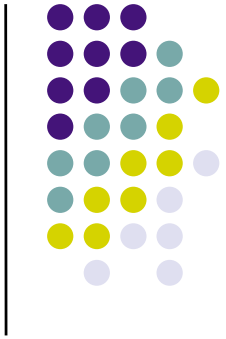
- National Malware Collaboratory (US)
- National Cyber Range (US DARPA)
- GENI/FIRE

Dynamic Federation

- *On-demand* creation of experiments spanning *multiple*, *independently controlled* facilities
- Why?
  - Scale
  - Unusual facilities
  - Data & knowledge sharing
  - Information hiding - multiparty scenarios
  - International cooperation
- Researcher
  - Controls experiment embedding
- Federants
  - Control Resource Access
  - Constrain Resource Use
- Related to (but not same as) *experiment composition*

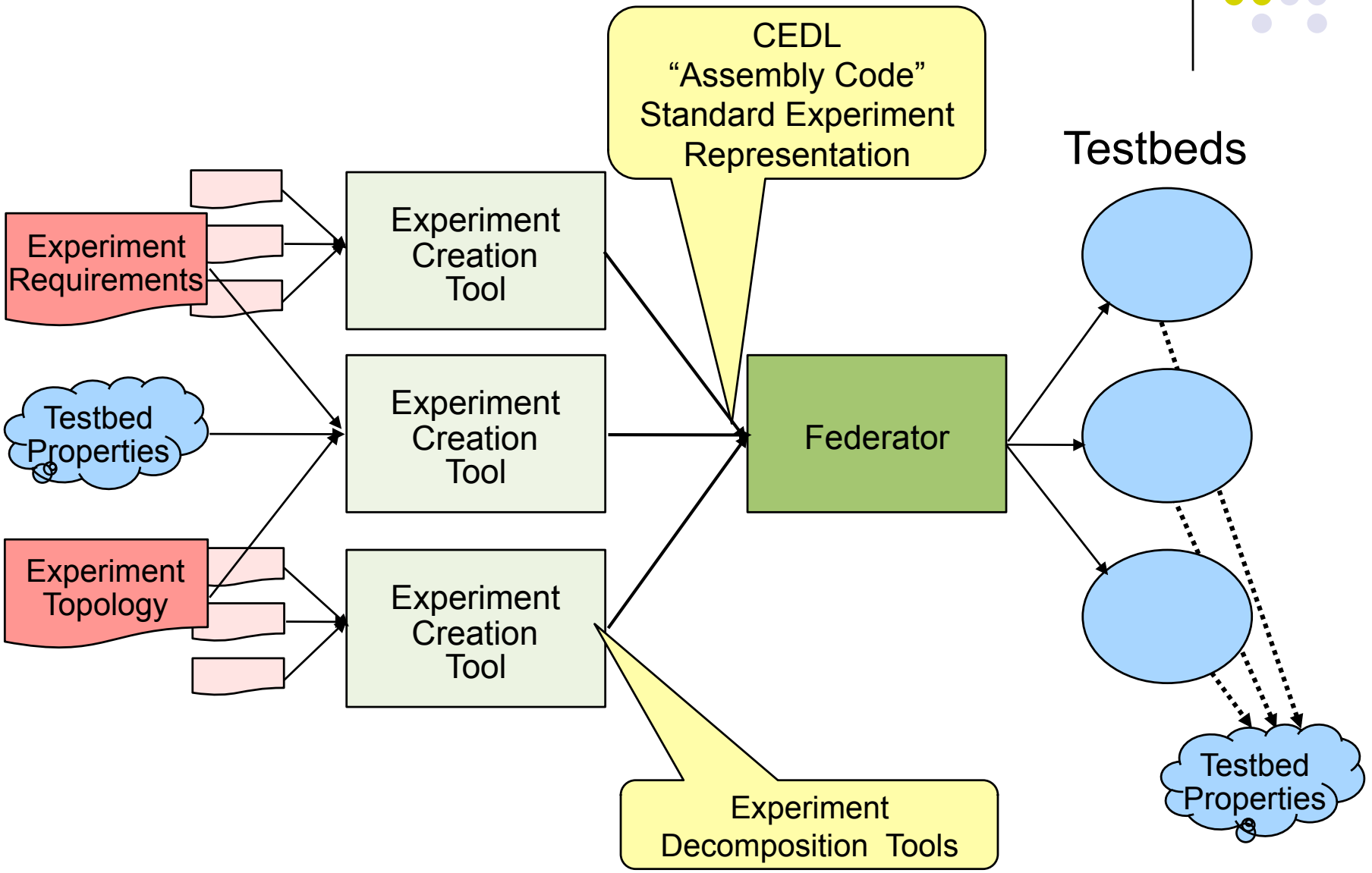


Three Key Elements

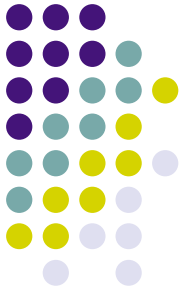


- Establish federated experiment
  - Create coherent distributed environment (embedding)
  - Guide experimenter about potential choices and effects
- Manage federated resources within local policies
  - Access / Authorization (who can use?)
  - Constrain use (how can they use?)
- Provide unified runtime environment to researcher and experiment
  - Shared file system, etc.
  - Events
  - Control hooks
  - *Failure management model*

DFA System Architecture



CEDL
Canonical Experiment Description Language

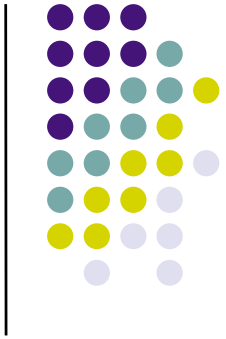


- Standard Experiment Representation - “Assembly Code”
- Output of all tools / input to Federator

- Expressiveness (today):
  - Core semantics: Logical {nodes, links, elements} topology (Emulab/ns2)
  - Annotations:
  - Logical attributes - eg, node type
    - Type information: router, switch, etc.
    - Physical selection: map to specific instance
  - Physical attributes
    - “Escapes” to allow physical configuration of hardware

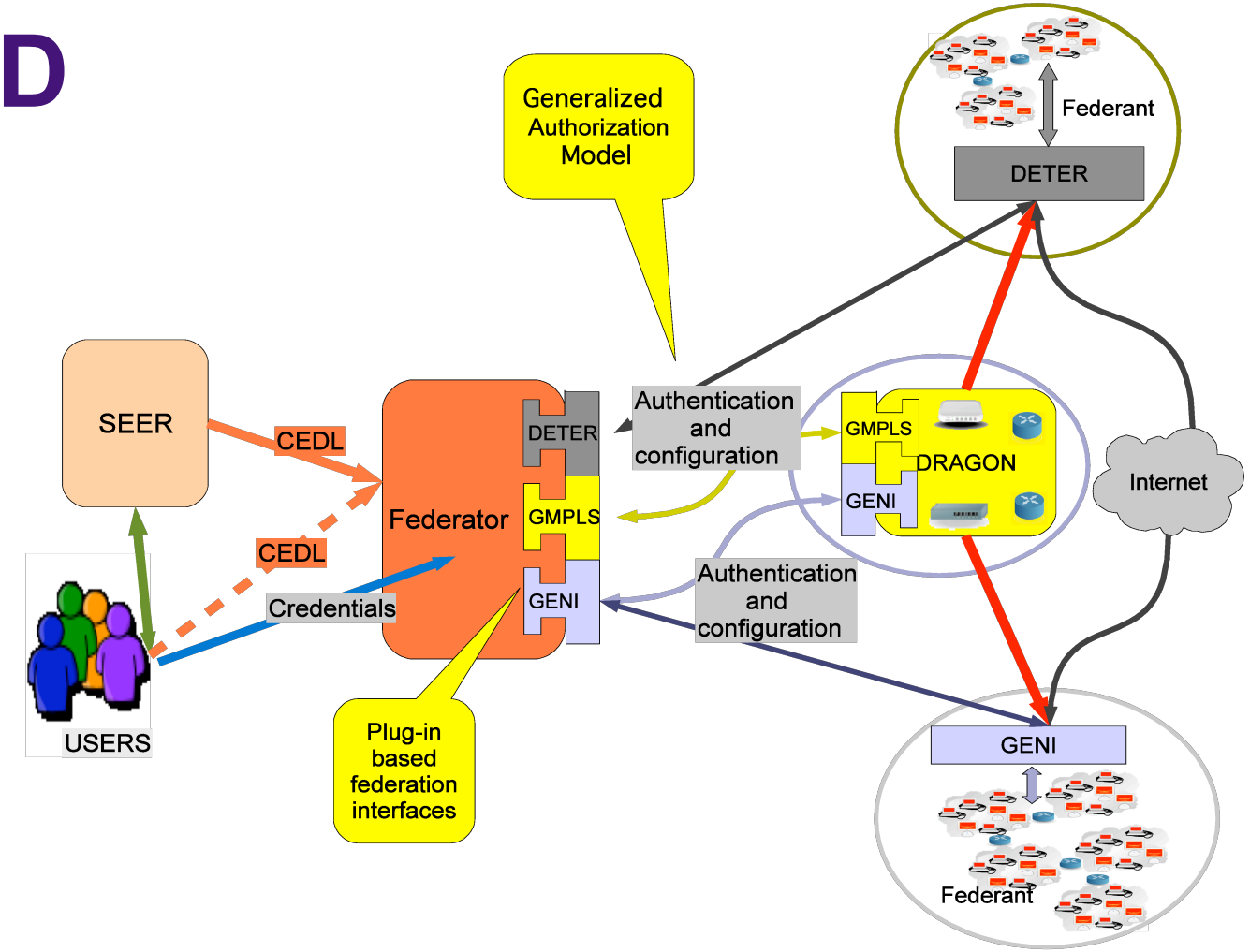
- CEDL is related to/one form of/one use of “GENI RSpecs”

DFA Access Control Architecture (Today)

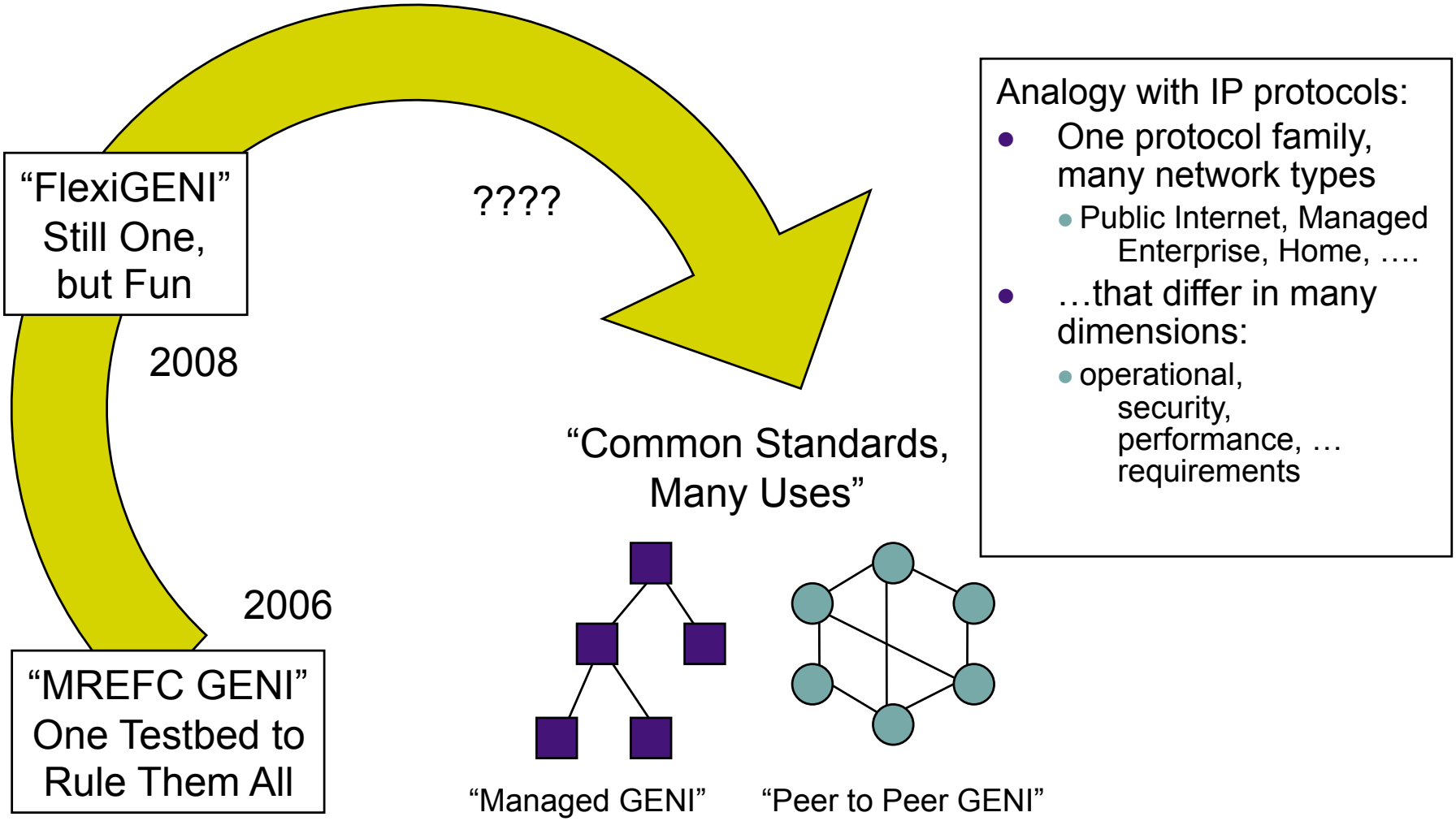


- Based on single-Emulab model:
  - *Projects* control resource access
  - User's project membership determines access
- DETER federation architecture - three level model:
  - Users, projects, testbeds have global names
  - Federants honor accesses based on:
    - Proof of name
    - Attested facts (evaluated wrt name)
    - Local information bound to name
  - Once accepted, federants assign accepted sub-experiments to local projects for resource control

TIED


Generalized Authorization Model
Federant
DETER
SEER
CEDL
CEDL
Credentials
USERS
Federator
DETER
GMPLS
GENI
Authentication and configuration
GMPLS
DRAGON
GENI
Internet
Authentication and configuration
Plug-in based federation interfaces
GENI
Federant

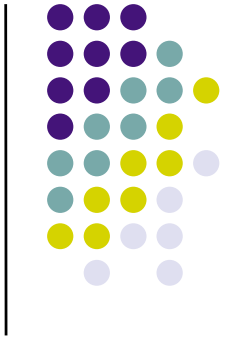
Philosophical Diversion



Analogy with IP protocols:

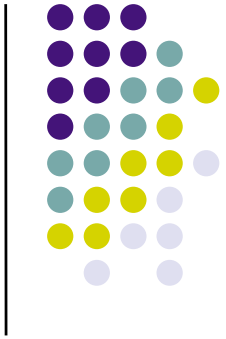
- One protocol family, many network types
  - Public Internet, Managed Enterprise, Home, ….
- …that differ in many dimensions:
  - operational, security, performance, … requirements

Authorization for Dynamic Federated Testbed Environments (with Steve Schwab, SPARTA)



- Decentralized, collaborative/competitive environment. Alliances form/ break frequently
  - Semantics appropriate for testbed federation
- Explicit, visible decision making
  - Corollary: clear auditing and understanding
- Multiple trust creation models, independent of mechanism
  - Examples: Hierarchical PKI, PGP web of trust, etc.
- Minimize unnecessary communication
  - For disconnected operation
- Control and limit revelation of info (credentials, etc.)
  - Corollary: potential multi-step negotiation

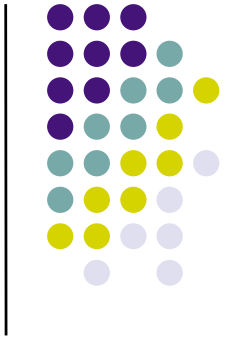
Attribute Based AC



- We build on *Attribute-Based Access Control*
  - Work by Winsborough, Li, Mitchell, others in turn

- Basic model:
  - *Principals*
    - In our work, user's identity established by local authority's local means - Kerberos, certs, passwords, …
  - Principals have *attributes*
    - Established by digitally signed credentials…
      … through which credential issuers assert judgments about the attributes of principals
    - Expressed in a formal language
  - Attributes and *Rules* drive a *reasoning engine*
    - Authorization decisions are based on applying rules to attributes of the requestor

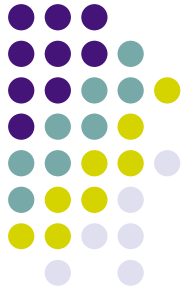
Expressivity of ABAC



- Decentralized attributes:
  - “University Registrar says Dan is a full time student”
- Delegation of attribute authority
  - “University delegates to its Registrar the determination of who is a full time student”
- Inference of attributes
  - “University considers a student to be full time if s/he is [has the attribute of] a PhD candidate”
- Attribute-based delegation of attribute authority
  - Delegate to strangers whose trustworthiness is determined based on their own attributes. Key to scalability.
  - “University delegates to the graduate officers of all departments the authority to determine who is PhD candidate”

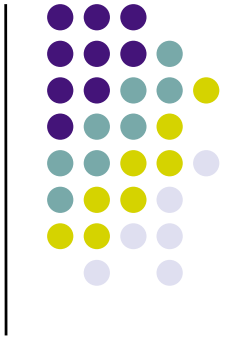
Words from “Toward Practical Automated Trust Negotiation”, W. Winsborough and N. Li, IEEE 3rd Int’l. Workshop on Policies for Distributed Systems and Networks

Timeline...



- Today
  - DETER accessible as an Emulab
  - Federation (DFA) in use across DETER, demo'd with Emulab and WAIL
  - SEER in use as a low-level user interface GUI
  - Basic DFA authorization is not ABAC-based
- 6 months
  - DFA available for Emulab/GENI slice based experiments
  - Internal ABAC prototype
- 1 Year
  - Control system based on DFA and ABAC available
  - Federation with DETER facility available through GENI interfaces
  - SEER available as experiment management tool
  - Interconnect with national DCNs

Collaboration

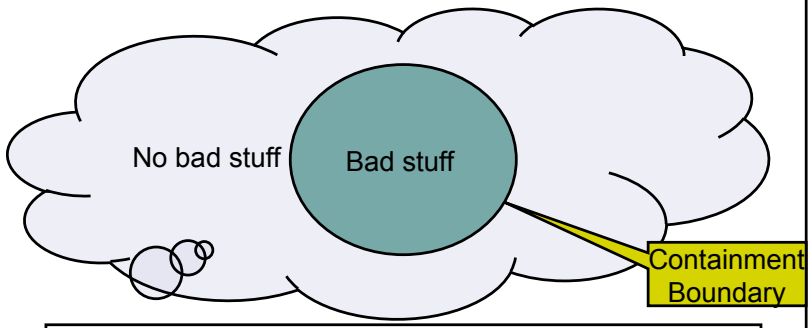


- Authorization and Allocation
  - Large Scale Trust Establishment methods
  - Attributes & Rules for Large Scale Federation
    - National attributes and delegation
    - Political Federations reflected in Testbed Federation
- GENI standards in broader world
- (DETER opportunities as well)

"Experiment Containment" ➔

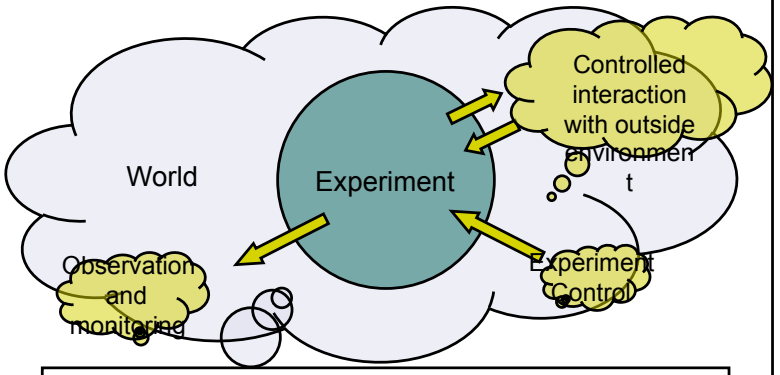
Risky Experiment Management

Classical Formulation



- Focus on isolation
- *De facto* emphasis of earlier testbed work

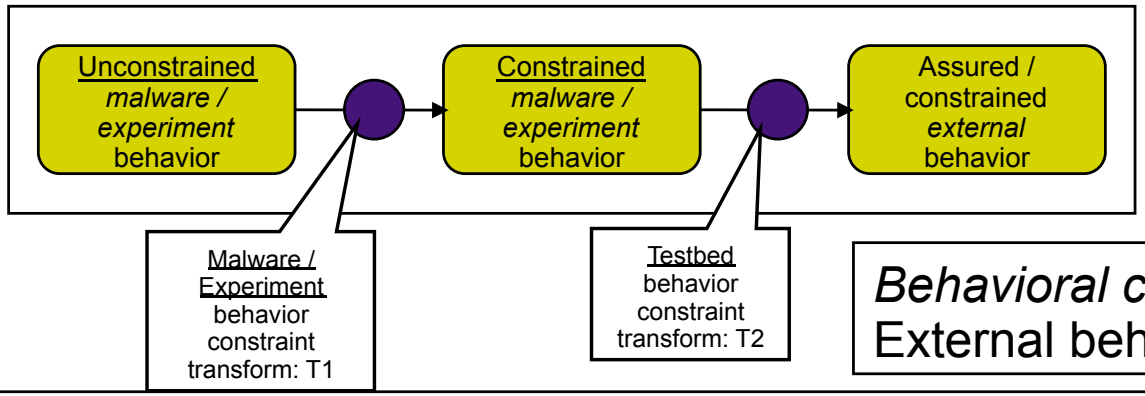
More accurate formulation



- Key issue:
  - Not "isolation and containment" but "understanding and assurance"

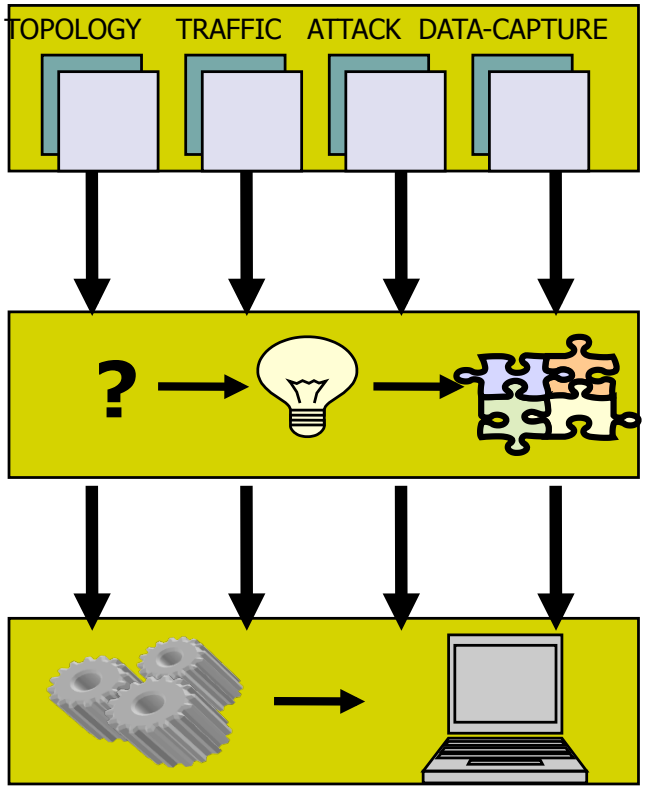
Model

- *Two-stage* approach:



Behavioral composition model:
External behavior == T2(T1(experiment))

Experiment Methodology and The SEER Facility



- Experimenters select from a *palette* of predefined elements: Topology, Background and Attack Traffic, and Packet Capture and Instrumentation
- *Methodology Engine* frames standard, systematic questions that guide an experimenter in selecting and combining the right elements
- *Experiment Automation* increases repeatability and efficiency by managing the experiment within the DETER testbed environment