Critical Issues in C4I Symposium

Challenges in Cloud Computing Security

Dr. Krishna Kant

Center for Secure Information Systems

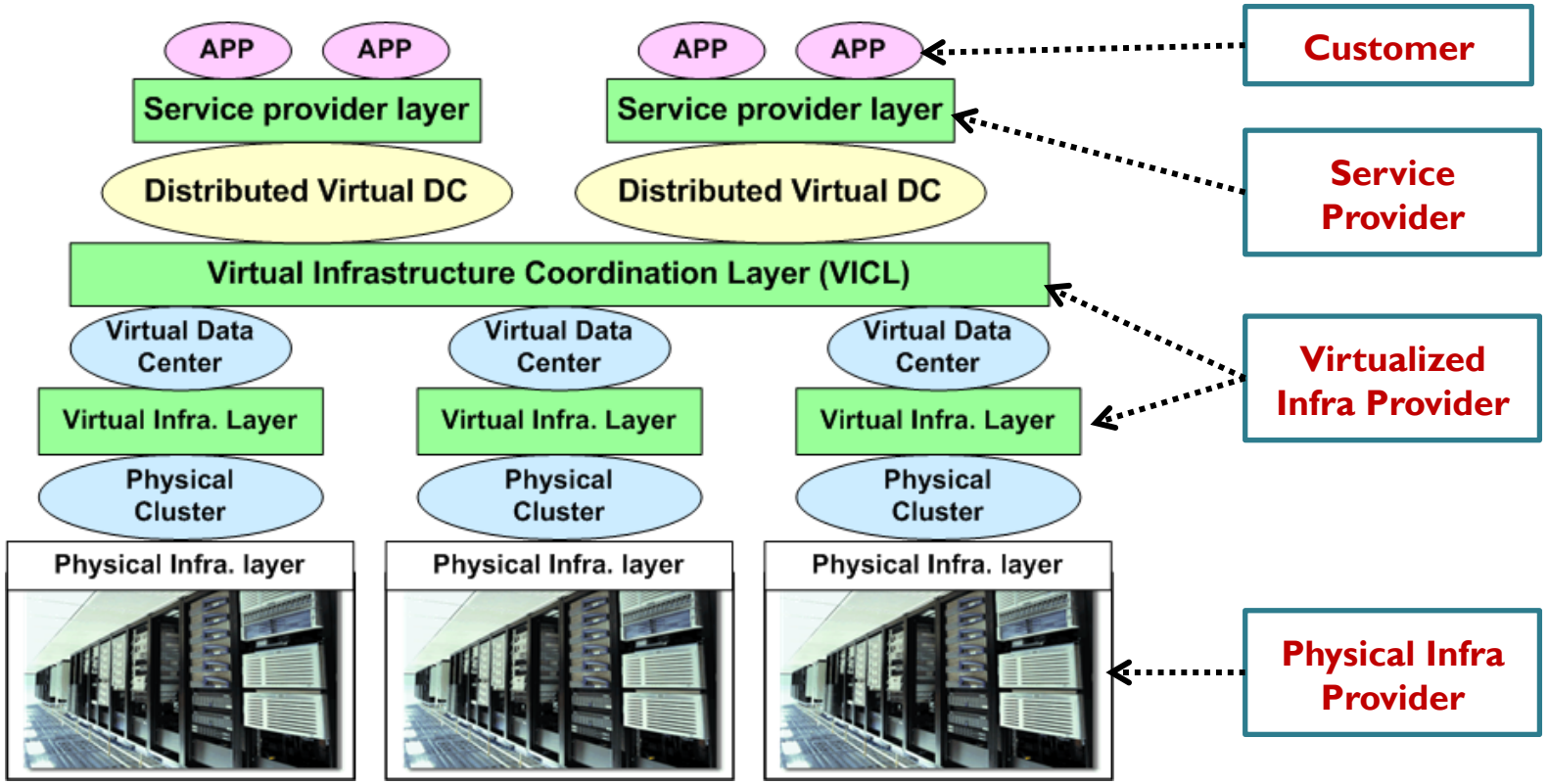
George Mason University

Cloud Computing Proliferation

- Strong momentum towards clouds
  - High infrastructure mgmt costs (up to 70%)
  - Low infra. utilization (10-15% typically)
  - Inflexibility – matching capacity & capabilities to demand
- Rapid proliferation
  - Federal cloud computing strategy
  - Expanding offerings by vendors
  - But many concerns …

What's Unique about Clouds?

- Old technologies mostly
  - Virtualization, consolidation, distributed computing, …
- New Twist: Un-owned infrastructure



Major Cloud Issues

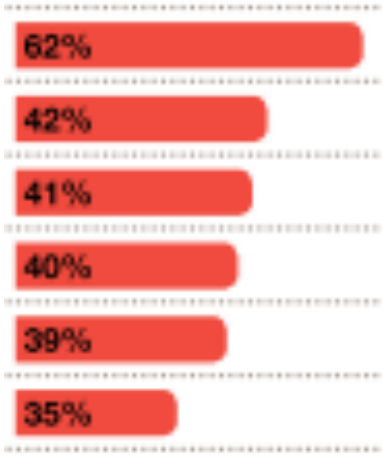
- Introduces at least one new party
  - Security, privacy & trust between parties
  - Lack of control – availability, performance, compatibility, involuntary sharing, etc.
- Customer concern
  - Security & privacy of data, attack resistance, …
  - Interference from other customers
- Operator concern
  - Ability to meet SLA requirements
  - Protection of customers from one another & hackers.

Survey of Issues

- Degree of business risk for movement to cloud:
  - 1: Minimal, 3: Moderate, 5: Very serious
- Security biggest issue, but not the only one

Percentage of respondents who indicated a 4 or 5

Data security
Data and systems integration
Data and system portability
Viability of third-party providers
IT governance
Service level agreements

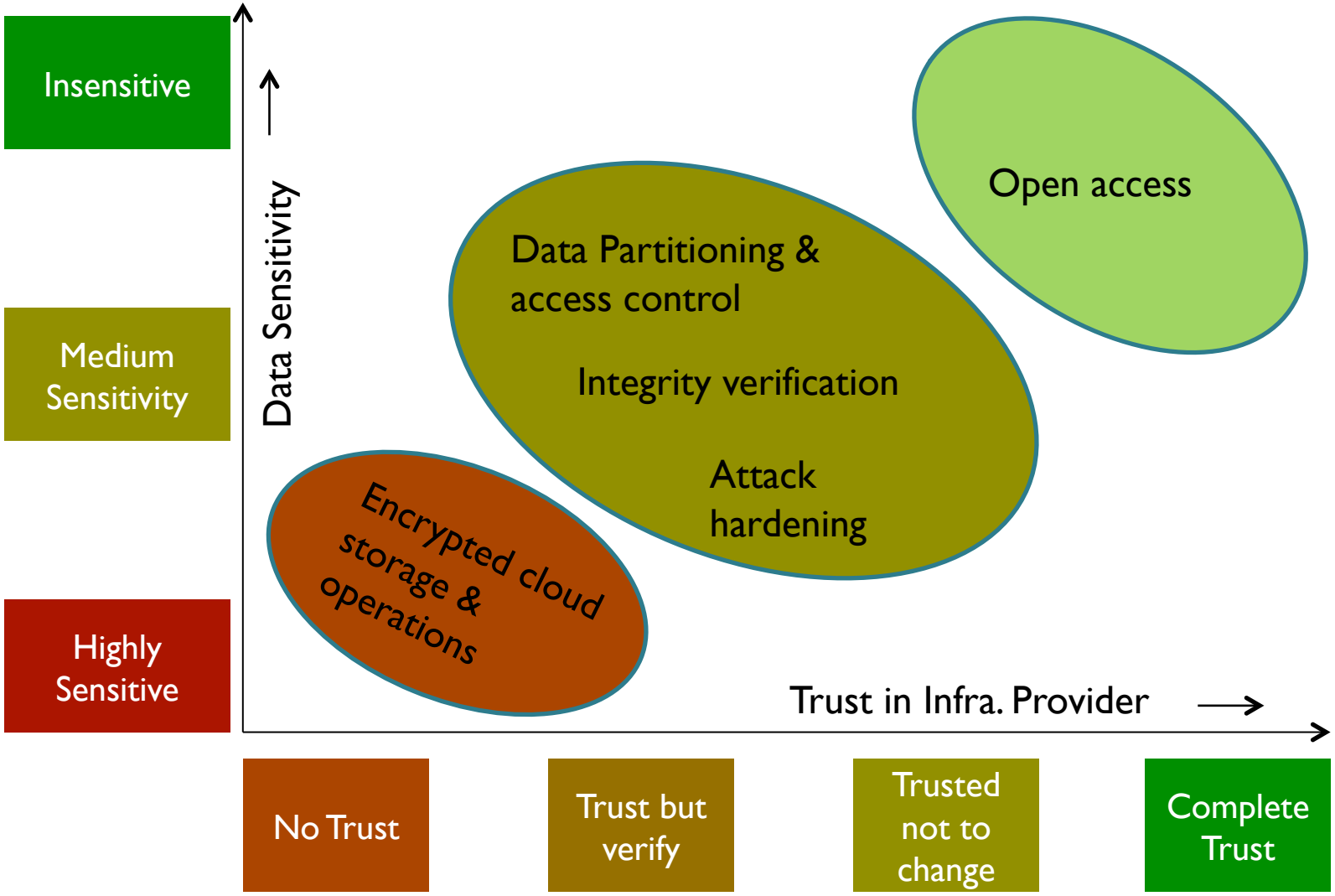


From PricewaterhouseCoopers LLP www.pwc.com

Trust in Cloud Computing

- Requires new trust relationships
  - Between customer & infra. provider (IP)
  - Vertically & horizontally between IPs.
- Security & Privacy Issues
  - Requirements, Enforcement & performance
  - Impact of multiple infra. provider layers (vertical)
  - Coordination among multiple providers (horizontal)

Levels of Trust on IP



Security vs. Visibility

- Multiple service models
  - SaaS: Very little visibility
    - SW deployment under control of IP, quite safe
  - PaaS :
    - Allows users to install malicious or disruptive SW.
    - SW may attempt to hog resources
  - IaaS: Complete visibility
    - Users can change drivers, VMs, even VMM, etc.
- Challenges
  - Detection of malicious SW and protection against such SW

Cloud Based Attacks

- Could deploy applications in cloud to
  - Silently monitor activity to grab sensitive information
  - Build private copy of databases via widespread active querying.
  - Disrupt normal operation via excessive computing/ comm. load, traffic misdirection, DNS poisoning, etc.
- Challenges
  - How do you identify such rogue deployments?
  - At the source (different from intrusion detection)
  - HW support?

Sharing Between Untrusted Parties

- Enterprise Computing on the Clouds
  - Infrastructure shared by businesses that may be competitors
  - Strong incentive to monitor competitor's workload
- Exploit shared environment
  - Obtain disproportionate use of resources at the expense of others
  - Resource consumption attacks
  - Possibly energy mgmt related attacks

Configuration Management

- Cloud config. mgmt very complex
  - Dynamic resource allocation over distributed infrastructure
  - Limited visibility across layers (vertically & horizontally).
  - But, intelligent config. mgmt requires fusion of information from multiple sources
- Attack on config mgmt databases can disable or disrupt the entire cloud
- How do you make config. mgmt robust to attacks?

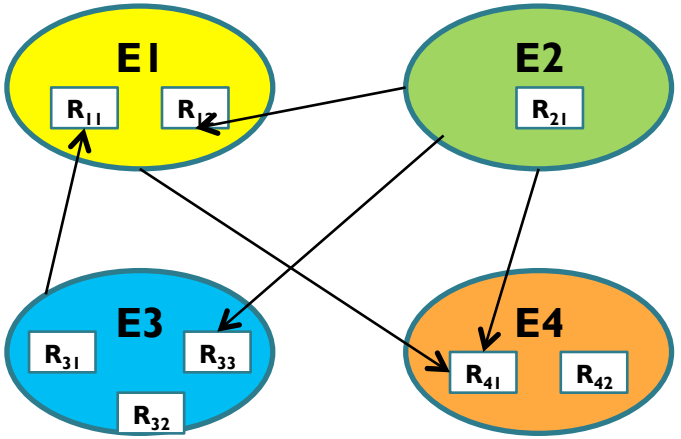
Using Clouds for Security

- Scattering data in the cloud
  - Make it difficult to obtain data & relationships in one place.
  - The scatter map needs to be secured.
  - Conflict between performance & security/privacy.
  - HW support?
- Migration to defeat reconnaissance
  - A form of moving target defense

Collaborative Computing

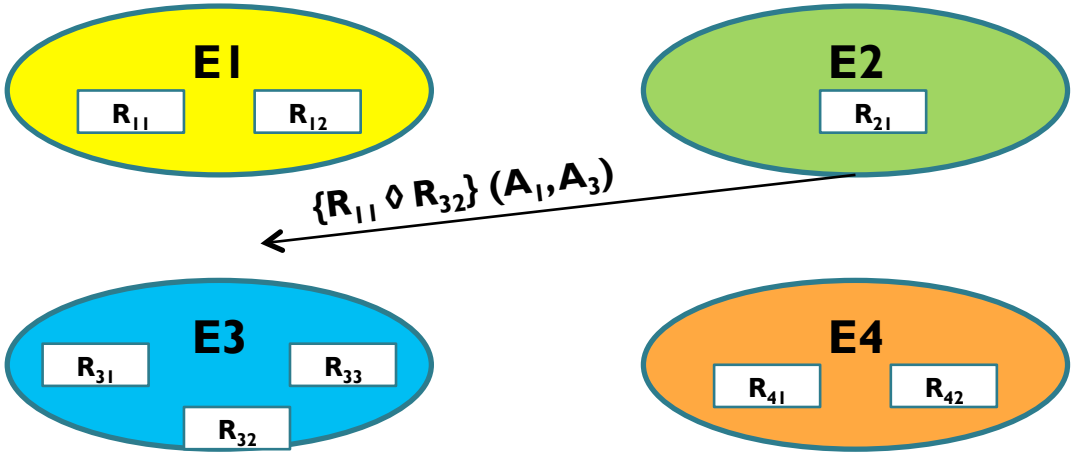
- Model
  - Multiple enterprises that need to collaborate to provide a service (e.g., e-commerce)
  - Mutually agreed data access rules
    - E.g., Relational data model w/ access over "join paths"
  - Enterprises may be hosted on cloud infrastructure
    - E.g., Using IaaS or PaaS model.

- Problem
  - Ensure consistency of rules
  - Efficiently authorize and implement queries



Why is this Hard?

- Problem complex because of complex rules
  - E2 can see ($R_{11} \Diamond R_{32}$) projected over attributes (A_1,A_3)
  - E2 can't see relations R_{11} & R_{32} individually
  - May be unclear who computes ($R_{11} \Diamond R_{32}$) and where.



Basic Research Questions

- Consistency
  - Mutual consistency between rules (relevant w/ deny rules)
  - Consistency against given policies (not considered)
- Implementability
  - E1 → $\{R_{11}, R_{11} \Diamond R_{21}(A,B)\}$, E2 → $\{R_{21}\}$:
    - E1 can't get $R_{11} \Diamond R_{21}$
  - Add the rule E3 → $\{R_{11}(A,C), R_{21}(B,C)\}$:
    - E1 can get $R_{11} \Diamond R_{21}$

Other Research Issues

- Query planning
  - Traditional methods do not consider access restrictions
  - If unimplementable, need to consider 3rd parties
    - 3P as a service w/ and w/o data retention
    - Multiple 3P's with different security/perf. properties
- Deny Rules
  - Consistency, conflict resolution, enforcement, …
- Enterprises hosted on clouds
  - Trust model and involvement of infra. provider
  - Optimization & implementation issues

Thank you!

Configuration Mgmt Security

- Security of CM is crucial
  - Misconfiguration or attacks can have global impact
  - Delayed impact – on restart, difficult to track
- Preliminary work
  - Exploits redundancy to check consistency.
- Numerous Challenges
  - Securing config data in clouds (restricted visibility)
  - Config security in sensor networks (limited resources)
  - Semantic info & context based protection.

Configuration Mgmt is Hard

- Growing Complexity
  - Heterogeneous HW/SW & network.
  - Multiple levels (devices to distributed data centers)
  - Virtualization -- #assets, increasing dynamicity.
  - A variety of config. repositories
    - Firmware in devices, config files, pkg DBs, CMDBs, …
    - Different interfaces, data formats, semantics, …
- Other Issues
  - Out of band vs. In-band access to config. data
  - Cradle to grave automated mgmt