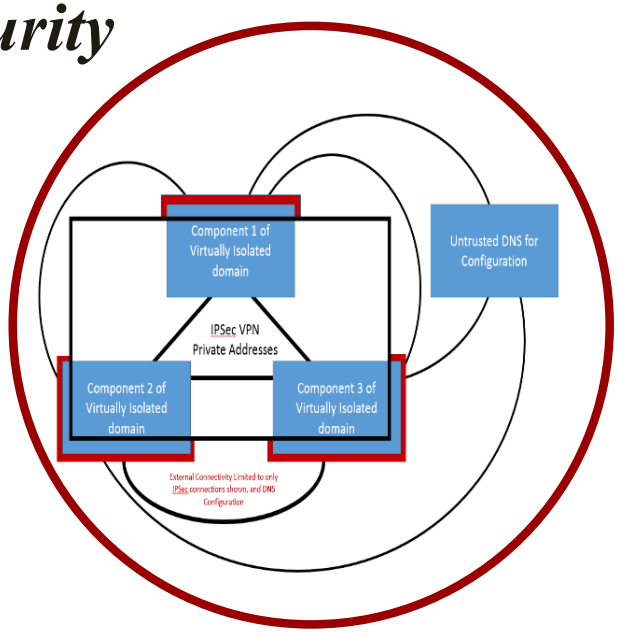
Distributed Virtually Isolated Domains

Clifford Neuman

Director, Center for Computer Systems Security

Information Sciences Institute

University of Southern California



Today's Systems Less Secure

- Functional requirements for today's distributed applications eliminate isolation.
  - Larger attack surface – applications and server interfaces reachable through the Internet.
  - Users demand instant access to their data from all devices, wherever they may be.
  - Users demand ability to move data between applications.
- But not all "applications" should allow this much sharing.
  - We need to restore isolation, but along functional boundaries.

© Can Stock Photo

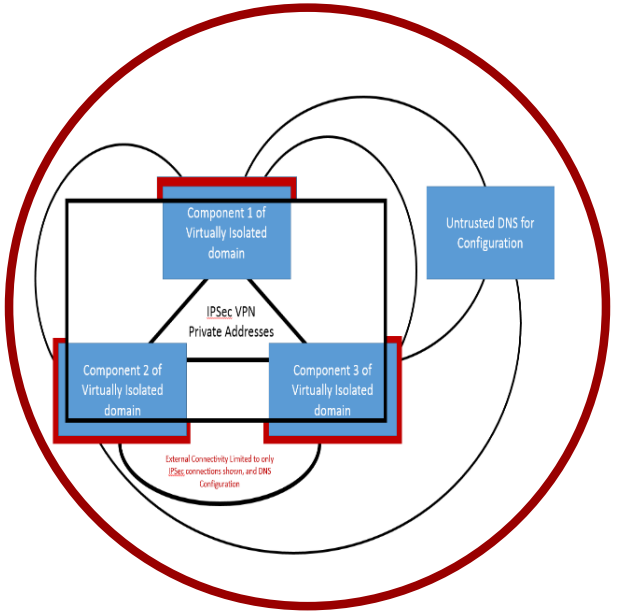
Many existing technologies *support* isolation

- Within computer systems
  - Virtual Memory
  - Virtualization
  - Trusted computing
  - Data Encryption
- Within Computer Networks
  - Firewalls
  - Virtual Private Networks
  - Communication encryption

- But our policies are too complex
  - Because they support isolation **and** sharing.

Changing our Concept of Isolation

- Changing the way we think of isolation
  - Not about artificial physical boundaries that are artifacts of how we build our systems
  - But rather around virtual boundaries that map onto the conceptual functions for which we use the systems.



Transition to Practice

- CentOS Extended to configure VM's or bare-metal systems in isolated domains.
  - FreeS/WAN IPSec tunnels to connected components
  - IP tables, internal configuration, and addressing prevent direct access to external internet)
  - Limits external subversion and internal exfiltration by reducing attack
  - Used for classes and CTF type exercises
  - Has been integrated with the DETER testbed for hybrid experiments.
- Further reduction of attack surface
  - Move network management into hypervisor (smaller code)
  - Consider appliance (e.g. firewall) - creates problem for attestation of systems inside the domain.
- Management of domains
  - Use of directory service to hold certificates for member components and dynamic address information.
  - This allows one to join a domain given its name, and a key or other authentication information.
  - Vulnerable to violations of availability policy, but information flow policies (subversion and exfiltration) not affected by directory service.
- Policy Management
  - Ability for a hardware/software component to join a domain based on domain's policy and accreditation of components.
- Performance
  - Use of trusted computing and accredited OS's to manage ability to join a domain.
- Contact us – bcn@isi.edu