Concept for a Future Architecture

Session: 3
Track: Army Cyber Command

LTC Terry McGraw
Army Cyber Command / 2nd Army
Defending traditional networks is complex

- Focused on service delivery
- Security historically under-emphasized
- Decentralized; not easily managed

Future model must support cyber maneuver

- Cyber as a man-made domain
- Build the terrain we defend
- Recognize cyber as contested terrain
- Holistic design; security as a consideration
Defend Cyberspace

★ Network must remain useable
★ Four tenets of defense
  • Identify and Secure What is Valuable
  • Build the Terrain to be Inherently Defensible, and Defend it Forward
  • Control the Key Terrain
  • Assure Accessibility
Protect What’s Important

★ Cannot defend everywhere, all the time
  • Data is the key asset to protect
  • Consolidate data, where it can be secured
  • Concentrate defenses around the data; establish as **key terrain**
  • Focus defense on key terrain

★ Accept risk at the end point
Defend Forward

- Build cyber terrain to enable defense
- Reduce avenues of approach, establish obstacles and engagement areas
- Focus defense on the key terrain
- Thin the client; less capable, less storage
- Push the client outside the “inner perimeter”
- Force threat to fight through prepared defenses
Control the Key Terrain

- Thin the client; serve the operating system / data remotely
- Non-persistent; reset to trusted baseline at every log-in
- Store the data in the cloud so user cannot lose it
- Greater analytics to identify malicious activities and anomalies
- Move all applications to the network; all future applications become standards-based and cloud-enabled
- Data from “outside world” logically separated from Army data resources
- Client endpoint becomes tactically irrelevant to the enemy
- Virtualized cloud environments can rapidly adapt its topology in response to threats
Assure Accessibility

- Two levels of access;
  - trusted (internal/LWN) and
  - untrusted (Internet/NIPR)
- Virtualized client; no ability to change VM image
- Data and app access tied to user’s ID
- “Mist” architecture – a cloud of federated small clouds at the tactical edge
Addressing Additional Concerns

- Centralizing resources
- Data-at-rest encryption within the cloud
- Data recovery
Way Ahead

★ Engage S&T, R&D fields
★ Begin transition to thinner clients
★ Develop secure virtual machine
★ Move applications and data to the cloud
  • Standards-based
  • Mandated for new acquisitions
Questions?

★ LTC Terry McGraw
   • terrence.j.mcgraw2.mil@mail.mil

★ MAJ Ian Tarasevitsch
   • lan.j.tarasevitsch.mil@mail.mil

★ CPT Ben Klimkowski
   • Benjamin.h.klimkowski.mil@mail.mil